LES DOSSIERS TECHNIQUES

QUE FAUT-IL SAVOIR SUR LE ZERO TRUST ?

Évolution de la sécurité ou révolution ?

Octobre 2023

CLUSIF

1 INTRODUCTION 5

2 LES CONCEPTS 6

2.1 Qu'est-ce que le Zero Trust ? 6

2.2 Quels sont les principes ? 7

2.3 Pourquoi l'identité est-elle le nouveau périmètre ? 9

2.4 Existe-t-il un modèle d'architecture Zero Trust ? 10

3 INTERET ET OPPORTUNITE 13

3.1 Pourquoi maintenant ? 13

3.2 Quels bénéfices devrais-je attendre de la mise en œuvre de Zero Trust ? 14

3.3 Le Zero Trust est-il adapté à tous les contextes métiers, IoT industriel et OT par exemple ? 16

4 LES IMPACTS 19

4.1 Quelles briques techniques pour implémenter le Zero Trust ? 19

4.2 Comment implémenter le Zero Trust dans mon organisation ? 22

4.3 Le Zero Trust signifie-t-il l'abandon du VPN ? 25

4.4 Quelle est la différence entre Zero Trust, Zero Trust Network Access (ZTNA) et Secure Access Service Edge (SASE) ? 26

4.5 Comment intégrer mon approche « Best-of-breed » dans ma stratégie Zero Trust ? 28

4.6 Le modèle Zero Trust est-il compatible avec un SI hybride ? 29

5 GOUVERNANCE ET CONFORMITE 31

5.1 Peut-on baser entièrement sa politique de sécurité technique sur le modèle Zero Trust ? 31

5.2 Le Zero Trust est-il uniquement un projet technique ? 32

5.3 Peut-on faire du Zero Trust sur des périmètres sensibles ? 34

5.4 Le modèle Zero Trust m'oblige-t-il à revoir ma politique de gestion des risques ? 36

6 MATURITE 37

6.1 Puis-je évaluer mon niveau de maturité Zero Trust par rapport à l'existant en sécurité ? 37

6.2 Finalement, faites-vous du Zero Trust sans le savoir ? 38

6.3 Migration progressive vers le Zero Trust : comment, quelles briques, quel périmètre ? 39

6.4 En conclusion, quels sont les points d'attention (à quelles difficultés peut-on s'attendre) ? 40

7 GLOSSAIRE 42

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Jean-Christophe	**TOUVET**	SIMPLOS

Les contributeurs :

Xavier	**AGHINA**	ORANGE
Sarah	**ATAKOU GAUTHIEROT**	CAPGEMINI
Romuald	**BLONDEL**	BPIFRANCE
Geoffroy	**CECILE**	SOPRA STERIA
Etienne	**COTASSON**	ACOSS
Renaud	**FELTEN**	KLEE GROUP
Jean-Yves	**GRASSET**	MICROSOFT
Fatiha	**HOUACINE**	EVABSSI
Mauro	**ISRAEL**	SECURITYSCORECARD
Arnaud	**JUMELET**	MICROSOFT
Rémi	**KOUBY**	CGI
Loïck	**PELET**	CNPP
Olivier	**PERRAULT**	ORANGE
Yasser	**SBAI**	ILEX
Anthony	**SBONG**	ITEC SECURITY
David	**SZNITEN**	KLEE GROUP
Nicolas	**TONDRE**	THEGREENBOW
Eric	**VEDEL**	CISCO

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Introduction

Le paradigme du Zero Trust est de plus en plus prégnant dans les réflexions des professionnels de la cybersécurité, une présence encore plus remarquable depuis le début de la pandémie. L'essor du télétravail, entre autres, les a en effet obligés à revoir leurs politiques de gestion des accès. Par ailleurs, le modèle de sécurité dominant depuis une trentaine d'années, celui de la défense périmétrique − même s'il reste valable pour certains accès et ressources sensibles dont l'hébergement demeure maîtrisé − est partiellement remis en cause par la recrudescence des cyberattaques utilisant les postes et comptes utilisateurs internes (où qu'ils se trouvent physiquement) pour rebondir vers les systèmes d'information (SI) d'entreprise.

Les fournisseurs de solutions se sont engouffrés dans la brèche et par la magie du marketing presque tous les produits de sécurité sont devenus « Zero Trust ». Cependant, le Zero Trust n'est pas qu'une affaire de solutions. Comment aujourd'hui protéger un capital informationnel quand les interconnexions entre les SI des organisations se banalisent ? Et alors que les utilisateurs eux-mêmes sont de plus en plus mobiles ? L'une des premières conséquences de l'évolution des usages au sein des organisations est que la localisation physique d'une ressource informatique (poste de travail, serveur, etc.) n'est désormais plus un critère suffisant pour déterminer une politique d'accès. Par ailleurs, une adoption généralisée du cloud entraînant, entre autres, de multiples interconnexions entre applications, et également une utilisation massive d'API, etc., sont autant de raisons qui poussent les directions des systèmes d'information (DSI) et responsables de la sécurité des systèmes d'information (RSSI) à revoir aujourd'hui leurs stratégies.

L'objectif de ce dossier technique est d'aider les professionnels de la cybersécurité à :

- répondre aux questions que suscite le principe du Zero Trust, en exposant ses concepts et l'intérêt qu'il représente, ainsi que les implications en termes de stratégie et de mise en œuvre ;
- déterminer quelle approche choisir, puis les guider afin d'identifier les briques nécessaires pour mettre en place une stratégie Zero Trust ;
- intégrer ce paradigme au sein de leur gouvernance, politique de sécurité et gestion du risque.

Cheminement dans le document en fonction des objectifs ou du profil du lecteur

Chapitre	Objectifs	Profil de lecteur
2	Appréhender les concepts du Zero Trust	Tous
3	Évaluer l'intérêt et l'opportunité d'adopter le modèle Zero Trust	RSSI DSI Risk Manager
4	Déterminer les impacts du Zero Trust sur l'organisation	RSSI DSI Chef de projet Zero Trust
5	Intégrer le Zero Trust dans son SMSI et sa gestion des risques et conformité	RSSI Risk Manager Responsable conformité
6	Évaluer son niveau de maturité (fait-on déjà du Zero Trust sans le savoir ?) et organiser la transition	RSSI Chef de projet Zero Trust

2 Les concepts

2.1 Qu'est-ce que le Zero Trust ?

Le Zero Trust est un modèle de sécurité pour le système d'information (SI) qui va bien au-delà de la simple protection périmétrique pratiquée depuis des décennies. Il tient compte des nouvelles menaces cyber dues notamment à l'adoption massive du cloud par les entreprises, aux nouveaux usages comme l'arrivée en masse du télétravail, à l'utilisation de nouveaux outils qui permettent la collaboration avec l'extérieur (clients et partenaires), etc. Il aide également à limiter un nombre de compromissions en perpétuelle croissance. L'accélération de la transformation numérique est en effet responsable de l'abolition des frontières physiques du SI, qui est désormais totalement ouvert à l'extérieur.

L'ANSSI, autorité nationale française en matière de sécurité et de défense des systèmes d'information, situe le modèle Zero Trust dans une même logique que la défense en profondeur promue par ses soins[1].

Les principes ne sont pas récents : la formulation « Zero Trust » a effectivement été lancée en 2010 par le cabinet d'analystes Forrester Research, mais c'est au Jericho Forum[2] que l'on doit les bases de la notion de « dépérimétrisation », soit ne plus reposer la sécurité du SI uniquement sur le contrôle de la frontière entre le réseau interne et Internet. Ce n'est qu'en 2019 qu'une définition officielle a vu le jour au travers du document « Zero Trust Architecture »[3] émis par le NIST (National Institute of Standards and Technology). Il y propose une formalisation complète du modèle et de ses composants. Pour reprendre la définition générale du NIST : « *Zero Trust est un paradigme de cybersécurité axé sur la protection des ressources et le principe selon lequel la confiance n'est jamais accordée implicitement mais doit être évaluée en permanence.* »

Cette définition met en exergue le fait qu'appliquer le Zero Trust implique une nouvelle manière de considérer la sécurité d'un SI. La conséquence immédiate est que la confiance en l'identité ou l'adresse IP du requêteur n'est plus un fait acquis, l'accès de l'utilisateur ou du service à une ressource nécessite dorénavant une vérification complète et systématique comme le contrôle du niveau de sécurité de l'appareil.

Cependant, sans périmètre physique, comment délimiter le nouveau contour virtuel du SI ? C'est encore le NIST qui apporte une réponse. Si l'on considère le document « Implementing a zero trust architecture »[4], c'est aujourd'hui la ressource qui devient la principale cible à protéger : « *Les organisations repensent le périmètre conventionnel de sécurité du réseau. Une architecture Zero Trust (ZTA) répond à cette tendance en se concentrant sur la protection des ressources, et non plus sur les périmètres du réseau, car l'emplacement du réseau n'est plus considéré comme le principal élément de la posture sécurité nécessaire pour une ressource* » (résumé page 3).

À partir d'un tel constat, considérer l'identité comme le nouveau périmètre virtuel du SI de l'entreprise n'a rien d'illogique. Une nouvelle réalité détaillée un peu plus loin en section 2.3 « Pourquoi l'identité est-elle le nouveau périmètre ? »

---

[1] Avis scientifique et technique sur le modèle Zero Trust ANSSI : « *Si le modèle Zero Trust s'inscrit dans la logique de "défense en profondeur" promue historiquement par l'ANSSI, il constitue une modification du paradigme de la stricte logique périmétrique qui a longtemps prévalu…* »

[2] Visioning White Paper, What is Jericho Forum? February 2005

[3] https://csrc.nist.gov/publications/detail/sp/800-207/final

[4] Implementing a Zero Trust Architecture NIST/National Cybersecurity Center of Excellence

Maintenant, la question que doit se poser tout responsable sécurité est : « Comment faire face à ces transformations et à l'élévation du niveau des menaces tout en renforçant le niveau de sécurité de mon organisation ? » La réponse qui suit la tendance actuelle est de faire évoluer le modèle de sécurité de l'entreprise en y intégrant les principes du Zero Trust (détaillés dans la prochaine section) que certains résument de la manière suivante :

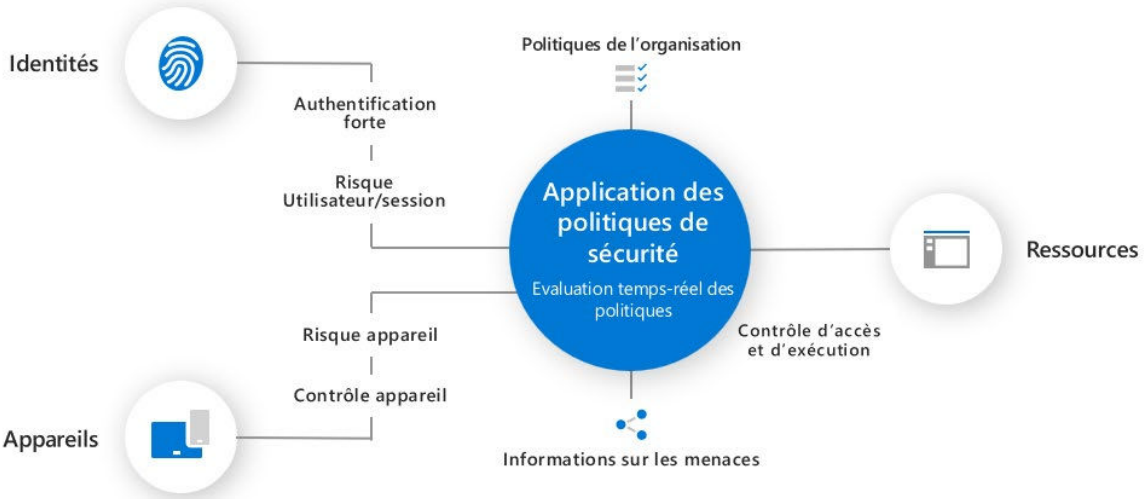
1. **Vérifier explicitement** : c'est le cœur du Zero Trust, la vérification dynamique de chaque demande de connexion. La décision d'accès doit se baser sur l'identité du demandeur, le statut de l'appareil, l'emplacement et l'application visée, plus tous les éléments de contexte permettant d'évaluer le risque. En fonction de cette analyse en temps réel, la connexion sera autorisée, rejetée ou acceptée sous certaines conditions comme une authentification renforcée (multifacteur). Ce mécanisme est appelé contrôle d'accès conditionnel.

2. **Appliquer le principe de moindre privilège** : ce principe est l'un des fondements de la sécurité et doit s'appliquer également en fonction du contexte d'accès. L'utilisateur ne doit se voir attribuer que les privilèges nécessaires pour accéder à l'application ou au service ciblé (JEA ou *Just Enough Access*), privilèges qui dépendent de son identité et qui peuvent évoluer dans le temps (par exemple, lorsque l'utilisateur change de fonction dans l'organisation). Dans la logique Zero Trust, les privilèges accordés peuvent aussi dépendre du contexte d'accès ou du risque évalué dynamiquement, et pour un intervalle de temps particulier (JIT ou *Just In Time*).

3. **Présupposer la compromission** : quelles que soient les protections mises en place, on doit admettre que l'on sera compromis un jour ou l'autre. La professionnalisation des attaquants, l'émergence de solutions de type RaaS (*Ransomware as a Service*), la sophistication des attaques par des officines soutenues par des États-nations augmentent la probabilité d'une compromission. Il faut mettre en œuvre des solutions de supervision qui seront en mesure de détecter les signaux faibles pour contrecarrer l'attaque et éviter sa propagation en isolant les éléments compromis. On utilisera les principes de segmentation pour isoler les actifs les plus critiques et compartimenter le réseau interne.

2.2 Quels sont les principes ?

Selon la définition du NIST : « *Zero Trust est devenu [alors] le terme utilisé pour décrire diverses solutions de cybersécurité qui ne basent plus la sécurité sur une confiance implicite en lien avec l'emplacement réseau, mais se concentrent plutôt sur l'évaluation de la confiance sur la base de la transaction* » (NIST SP 800-207 page 2).



Le schéma ci-dessus montre un scénario d'accès générique conforme aux principes du modèle Zero Trust.

Une identité (que ce soit celle d'un utilisateur ou d'un service) fait une requête d'accès à une ressource depuis un appareil. La demande arrive sur le composant central chargé d'appliquer les politiques de sécurité paramétrées par l'organisation. Ce moteur, ayant pour fonction le contrôle d'accès dynamique, prend en entrée des informations sur l'identité (groupes/rôles, localisation, privilèges), l'appareil (système d'exploitation, géré par l'entreprise ou non, l'état de santé, mise à jour de correctifs de sécurité, etc.) et plus globalement sur le contexte d'accès. L'utilisateur a-t-il l'habitude de se connecter depuis cet emplacement ou ce pays ? Le même utilisateur s'est-il authentifié récemment depuis un autre endroit éloigné, ce qui impliquerait un don d'ubiquité ou un voyage impossible ? L'appareil depuis lequel l'utilisateur se connecte est-il son poste habituel ? En y ajoutant des informations sur les menaces, le composant d'accès conditionnel évalue un niveau de risque pour l'identité et l'appareil. En considérant la ressource ciblée, il applique les politiques de sécurité qui lui permettent de prendre la décision d'autoriser l'accès ou de le refuser. L'accès peut être autorisé sous condition, par exemple sous réserve d'une authentification multifacteur, et un accès réduit à l'application peut être également imposé, en lecture seule par exemple.

Pour illustrer le cas de figure précédent, prenons l'exemple d'un utilisateur travaillant dans le département des ressources humaines (RH) et souhaitant accéder à une application RH de l'entreprise. L'utilisateur s'authentifie et le moteur prend en compte les informations sur l'identité (c'est bien un utilisateur du groupe RH avec des autorisations pour accéder à l'application visée), sur l'appareil (c'est un appareil référencé et géré par l'organisation et conforme) ainsi que des éléments complémentaires sur le contexte (l'utilisateur en télétravail accède depuis son réseau privé, il s'est authentifié en multifacteur, etc.), auxquels s'ajoutent des informations sur les menaces (l'identité de l'utilisateur n'a pas été compromise). En intégrant ces éléments et en appliquant les politiques de sécurité, le composant de contrôle d'accès conditionnel génère un jeton d'accès qui permet de se connecter à l'application avec les autorisations adéquates pour le temps de la session. À noter que dans le cas où l'utilisateur accéderait depuis une tablette personnelle non gérée par l'organisation, l'accès pourrait être refusé ou conditionné à une authentification forte et l'autorisation pourrait être également restreinte à certaines données ou à un simple accès en lecture seule.

L'évaluation en temps réel des politiques de sécurité nécessite de mettre en place une supervision de manière transversale pour capter les événements en provenance des diverses sources et être capable de les traiter de manière efficace pour détecter les signaux faibles

indicateurs d'un début d'attaque en cours. Les événements récoltés proviennent de sources de données liées à l'identité (annuaires *on-premises* et cloud), aux appareils (log de sécurité, client EDR[5]), au réseau (pare-feu, trafic réseau, etc.), aux applications, etc. Ils sont analysés en continu en vue de détecter le plus rapidement possible les prémices d'une attaque. L'objectif est de pouvoir réagir au plus vite pour éviter la propagation de la compromission, en isolant les éléments compromis puis en effectuant les actions de remédiation nécessaires.

On trouve cette notion de surveillance et alerte en mode continu dans les fonctions principales de certaines solutions *Cloud Security Posture Management* (CSPM). Un outil dont l'utilisation est préconisée dans le cadre d'une implémentation Zero Trust dans le cloud. Une utilisation parfaitement décrite dans le document « Cloud Security Technical Reference Architecture »[6] édité par le CISA (*Cybersecurity and Infrastructure Security Agency*) en août 2021. L'utilisation de solutions à base d'intelligence artificielle (IA) est un quasi-prérequis pour être en mesure d'analyser des volumes substantiels de signaux, de minimiser les faux positifs (qui submergent les analystes du SOC[7]), de corréler efficacement les alertes (pour les intégrer dans des scénarios facilitant les investigations) et de s'appuyer sur l'automatisation pour la réponse aux incidents.

2.3 Pourquoi l'identité est-elle le nouveau périmètre ?

Le modèle de sécurité périmétrique, mis en œuvre depuis que les entreprises se sont ouvertes sur Internet, partait du postulat qu'en construisant une frontière entre le réseau d'entreprise et l'extérieur, on pouvait garantir que tout ce qui était situé à l'intérieur était sécurisé : les postes de travail, les serveurs, les services, ceux d'Active Directory par exemple, etc. Les pares-feux situés en périphérie et les systèmes de proxy et d'analyse des flux étaient souvent considérés comme suffisants pour assurer cette isolation.

Les postes de travail, qui pour la plupart restaient dans les locaux de l'entreprise, étaient aussi protégés des menaces extérieures : on les construisait selon les modèles de sécurité *ad hoc*, on les équipait d'une solution anti-malware et on s'assurait qu'ils recevaient régulièrement les correctifs de sécurité.

Quant aux utilisateurs mobiles qui représentaient une population limitée, ils se connectaient aux applications et ressources de l'entreprise à travers un canal VPN assurant que tous les flux sont encapsulés et redirigés vers l'interne.

Mais les temps ont changé avec les grandes mutations que sont le cloud, la mobilité – avec l'apparition de nouveaux appareils, smartphones et tablettes – et le travail à distance qui s'est généralisé lors de la crise sanitaire. De plus en plus d'applications sont hébergées dans le cloud en mode SaaS, c'est-à-dire accessibles depuis Internet, et les postes des utilisateurs ont largement déserté les locaux de l'entreprise.

De plus, les menaces ont progressé en termes de dangerosité, tandis que les attaques se sont nettement complexifiées, rendant encore plus difficile la protection des SI d'entreprises désormais ouverts sur l'extérieur. Les attaques suivent un scénario malheureusement classique où un poste compromis (souvent par un mail de phishing) sert de point d'entrée dans le réseau, et l'attaquant – par déplacement latéral et élévation de privilège –, va pouvoir compromettre l'annuaire, puis l'ensemble du SI. Le réseau interne étant souvent insuffisamment surveillé, les attaquants peuvent plus facilement s'y déplacer et propager une compromission.

---

[5] *Endpoint Detection & Response*, cf. glossaire

[6] https://www.cisa.gov/publication/cloud-security-technical-reference-architecture

[7] *Security Operation Center*, cf. glossaire

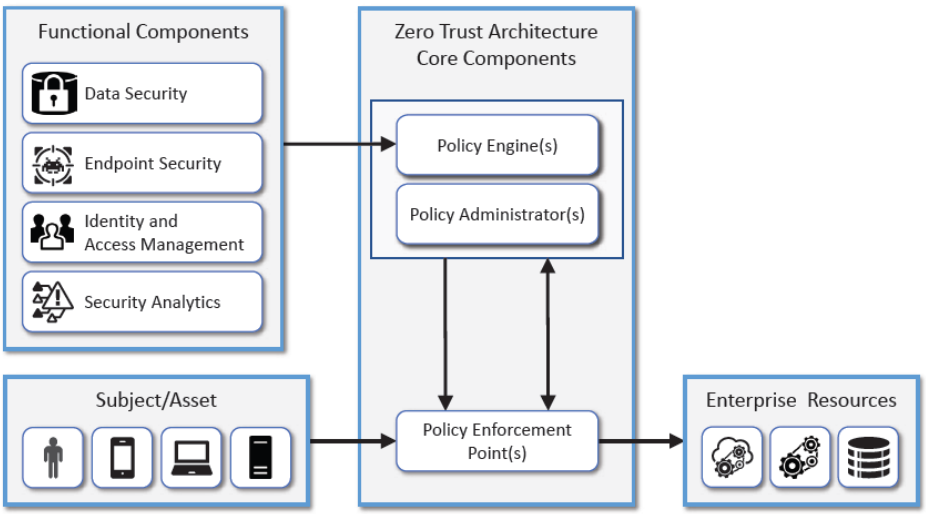
Le modèle périmétrique est clairement devenu insuffisant. Aujourd'hui, la sécurité ne peut plus reposer essentiellement sur le réseau, l'identité doit être au centre du dispositif qui permet de contrôler l'accès à toute application ou service.

Prenons l'exemple d'un utilisateur en télétravail qui se connecte depuis un poste quelconque à une application SaaS mise à disposition et contrôlée par son entreprise. L'utilisateur peut potentiellement accéder à l'application avec une connexion Internet privée : il devra alors au préalable s'authentifier (si possible fortement), disposer selon son profil des autorisations qui lui sont nécessaires et par ce biais, respecter les politiques d'accès définies par l'entreprise. La connexion entre son poste et l'application est naturellement chiffrée de bout en bout pour assurer la confidentialité du trafic.

Le réseau s'abstrait donc de l'équation et redevient un simple médium pour le transport, laissant la place à l'identité pour définir le nouveau périmètre virtuel.

2.4 Existe-t-il un modèle d'architecture Zero Trust ?

L'architecture Zero Trust de haut niveau la plus largement acceptée par les acteurs du secteur est celle que propose le NIST[8], représentée fonctionnellement dans le schéma suivant :

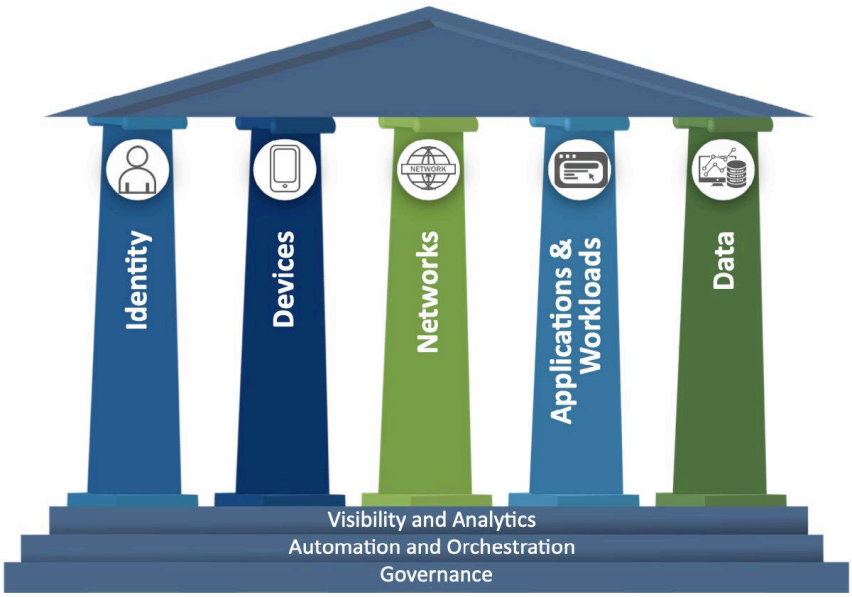


On retrouve dans la colonne centrale le moteur du contrôle d'accès dynamique. Il régit les accès entre les sujets ou actifs (utilisateurs, appareils, objets connectés, etc.) et les ressources de l'entreprise. Les autres blocs fonctionnels concernent la sécurité des données, la sécurité des appareils (à partir desquels les identités demandent l'accès), la gestion des identités et l'analyse des données de sécurité.

Au-delà de ce schéma, il est intéressant d'observer le principe selon un autre angle, notamment celui proposé par l'agence fédérale américaine CISA (*Cybersecurity and Infrastructure Security Agency*). Dans son document « Zero Trust Maturity Model »[9], elle propose l'approche « par pilier » décrite ci-dessous :

[8] Implementing a Zero Trust Architecture NIST/National Cybersecurity Center of Excellence

[9] Zero Trust Maturity Model, Cybersecurity and Infrastructure Security Agency (CISA)



- **Identité** : « l'identité est le nouveau périmètre », puisque le réseau ne constitue plus la frontière du SI. Qu'il s'agisse d'un utilisateur (humain) ou d'un service, l'identité est à l'initiative de la demande d'accès à la ressource qui passe par le point d'entrée géré par le composant de contrôle d'accès dynamique. L'identité doit être administrée correctement (socle Gouvernance) tant au niveau des droits d'accès, y compris lors de changement de rôles (respect du principe de moindre privilège), que des sorties – lorsque l'employé quitte l'organisation. Le risque sur l'identité est calculé en se basant sur le contexte à travers l'analyse de signaux qui pourra déclencher, par exemple, une demande d'authentification multifacteur.
- **Appareil** : la sécurité et la conformité de l'appareil doivent être assurées par une gestion des politiques de sécurité – dont on s'assurera qu'elles sont bien respectées – , par l'application sans délai des correctifs de sécurité, des mises à jour du système, des signatures antimalware, etc., et par la mise en œuvre d'un outil de type EDR pour la détection et réponse aux menaces. L'état sanitaire de l'appareil est pris en compte dans l'évaluation du risque par le composant de contrôle d'accès.
- **Réseaux** : la taille du réseau interne se réduit à mesure de la diminution des ressources internes qui migrent vers le cloud, mais certaines ressources critiques resteront tout de même hébergées sur site et elles devront être protégées. Les bonnes pratiques d'isolation réseau sont à respecter en explorant les solutions de microsegmentation. Les applications et ressources qui migreront dans le cloud devront, de la même façon, être protégées avec les composants réseaux disponibles sur la plateforme. La détection passera par des solutions d'analyse de flux réseau et par la consolidation des logs en provenance des équipements – à destination des outils de supervision.
- **Applications et charges de travail** : les nouvelles applications cloud sont plus exposées car accessibles depuis Internet et doivent être développées en tenant compte de la sécurité dès la conception (*Secure by Design*) tout en s'appuyant sur des outils de modélisation de menaces et de test de détection de vulnérabilités. Les architectures de référence servent de guide pour implémenter les bonnes pratiques. Les outils de gestion et de contrôle de la posture de sécurité des applications sont utilisés pour s'assurer de bien détecter toute erreur de configuration. Les outils de type CASB (*Cloud Access Security Broker)* permettent de découvrir et contrôler les applications SaaS tout en bloquant les applications non autorisées et en protégeant les données sensibles.

- **Données** : les données constituent les actifs informationnels les plus importants de l'organisation et doivent être traitées comme telles. La mise en place d'une classification efficace est le moyen d'identifier les données sensibles de manière à les protéger par chiffrement et à s'assurer qu'elles ne fuitent pas de manière intentionnelle ou non. Si elles doivent être partagées en interne ou externe, les outils de collaboration assurent qu'elles sont accessibles uniquement aux personnes désignées dotées des droits nécessaires. Pour aller plus loin, la mise en place d'une classification peut être complétée par l'identification d'un propriétaire en mesure d'évaluer la légitimité des demandes d'accès. Un suivi du partage des données et des délais de fin d'accès limite les risques de fuite. De plus, une gestion correcte des données personnelles permet de renforcer la mise en conformité en les identifiant et les protégeant en accord avec les réglementations (RGPD, etc.).

Les trois socles « Gouvernance », « Automatisation et Orchestration », et « Visibilité et Analyse » sont transverses et s'appliquent donc à l'ensemble des piliers. Par exemple, la gouvernance des identités est assurée par un ensemble de processus de gestion des identités qui doit s'appuyer sur les différents référentiels d'identité, y compris les annuaires cloud. La gouvernance des applications permet de contrôler qu'elles sont bien déployées dans le respect des politiques de sécurité et qu'elles y restent conformes dans le temps. La gouvernance des données associe des processus (demandes d'accès, demande d'ouverture d'un site collaboratif, demande de partage externe, etc.) à des outils techniques qui en assurent l'automatisation.

Le socle « Visibilité et Analyse » doit, quant à lui, assurer la détection d'attaques ou simplement de ses prémices sur l'ensemble des piliers. Il doit être capable de corréler de multiples alertes pour les inclure dans un scénario d'attaque présenté à l'analyste du SOC : par exemple, une alerte sur un utilisateur accédant depuis un nouvel appareil, la détection de l'installation de composants particuliers sur un poste, une alerte sur des accès non habituels à de multiples sites collaboratifs, des événements qui, une fois corrélés, feront suspecter une attaque avec usurpation d'identité, etc.

L'automatisation de nombreuses tâches sert à obtenir plus rapidement des réponses pour contrer le plus rapidement possible une compromission et ainsi en éviter la propagation.

Cette illustration du modèle par le CISA sous forme d'un édifice met en exergue le fait qu'appliquer le Zero Trust au SI ne peut se faire qu'avec une approche globale portant sur tous les socles et piliers, sans quoi l'ensemble ne reposerait plus sur des bases solides.

3 Intérêt et opportunité

3.1 Pourquoi maintenant ?

L'intérêt grandissant pour le modèle Zero Trust est lié à plusieurs facteurs :

1. **Transition technologique vers le cloud :** durant la dernière décennie, de nombreuses avancées technologiques ont vu le jour. La plus impactante étant sans conteste le cloud dans lequel les organisations ont vu de nombreuses opportunités de business. Elles l'ont donc massivement adopté. Selon « The 2021 State of SaasOps Report »[10] de BetterCloud, édité fin septembre 2021, une entreprise de taille moyenne utilise 110 applications SaaS, soit sept fois plus qu'en 2017. Cependant l'adoption du cloud apporte également son lot de défis : la gestion des identités dans une architecture en mode hybride, l'identification des données sensibles et leur protection, la gestion des applications SaaS et PaaS, l'administration des ressources cloud, la supervision, etc.
2. **Évolution des organisations :** avec la révolution du numérique, les entreprises ont dû s'adapter pour offrir de nouveaux services, de nouveaux scénarios de mobilité pour leurs employés (télétravail) et s'assurer une ouverture vers l'extérieur pour une meilleure collaboration avec les partenaires. Les défis posés par ces transformations ont mis en évidence les limites du modèle de protection périmétrique imposant dès lors une nouvelle approche de la sécurité du système d'information (SSI).
3. **Recrudescence des attaques et des compromissions :** les attaques par rançongiciels sont devenues un véritable fléau et un vrai business pour les organisations criminelles, avec pour cibles privilégiées le grand public, la finance et l'industrie. Durant la pandémie, les hôpitaux et entreprises du secteur de la santé ont fait partie des cinq secteurs les plus touchés. Concernant la France, selon le secrétaire d'État chargé du Numérique de cette période, « *il y a eu 27 attaques majeures d'hôpitaux en 2020, il y en a une par semaine depuis 2021*[11] ». Plus récemment, c'est l'hôpital de Corbeil-Essonnes qui a été la cible d'une attaque par rançongiciel par le groupe de pirates russophones LockBit 3.0, qui n'a pas hésité à divulguer 11,7 gigaoctets de données de santé après que l'hôpital a refusé de payer la rançon exigée[12]. Début décembre 2022, c'est l'hôpital Mignot du Chesnay (Versailles) qui a été victime d'une cyberattaque impliquant l'arrêt complet du SI, la fermeture des urgences, le transfert de patients vers d'autres hôpitaux et le retour au papier-crayon[13]. Plus généralement, selon l'ANSSI plus de 1 000 intrusions ont été perpétrées contre des infrastructures informatiques françaises sensibles en 2021, en augmentation de 37 % par rapport à l'année précédente, les attaques par rançongiciel s'étant stabilisées en 2021 avec 203 attaques recensées[14]. Bien que ces chiffres aient baissé en 2022, la menace reste omniprésente[15].
4. **Mise à disposition de briques technologiques issues du cloud :** certaines briques comme le moteur de contrôle d'accès conditionnel – qui doit traiter les demandes d'accès en temps réel et la surveillance en continu des sessions dans le cadre du Zero Trust – n'existaient tout simplement pas. Il aura fallu attendre que le cloud apporte la puissance nécessaire en s'appuyant sur de nouvelles architectures basées sur des

[10] The 2021 State of SaaSOps Report, BetterCloud

[11] Cybersécurité des hôpitaux : « 27 attaques majeures en 2020 et une par semaine en 2021 »

[12] Les pirates informatiques qui ont attaqué en août l'hôpital de Corbeil-Essonnes ont divulgué 11,7 giga-octets de données de santé.

[13] Nouvelle cyber attaque d'un centre hospitalier au Chesnay dans les Yvelines

[14] ANSSI : un millier de cyberattaques contre des infrastructures critiques françaises en 2021

[15] https://www.ssi.gouv.fr/actualite/un-niveau-eleve-de-cybermenaces-en-2022/

microservices pour disposer de ces fonctionnalités clés. C'est également le cas pour des solutions de supervision SIEM ou des XDR[16] que les principaux éditeurs proposent désormais en tant que service cloud ; cela leur permet de bénéficier des possibilités de montée en charge et de services d'IA assurant l'ingestion, le traitement et la corrélation d'alertes quasiment sans limites.

5. **Une maturation de l'approche Zero Trust et des retours d'expérience :** une vision Zero Trust doit se concrétiser avec des briques technologiques, encore faut-il être en mesure d'assembler correctement les composants nécessaires. Si les premières implémentations étaient concentrées uniquement sur le réseau dans une approche *Zero Trust Network Architecture* (ZTNA), le modèle Zero Trust va bien au-delà du réseau en plaçant ce qu'il considère comme les principaux composants d'un SI au centre de toutes les attentions : identité, appareils, données, applications et infrastructure[17] (voir section « 2.4 Existe-t-il un modèle d'architecture Zero Trust ? »).

   Les premiers retours d'expérience ont permis de forger de bonnes pratiques sur lesquelles il est aujourd'hui possible de s'appuyer pour réussir son projet de mise en œuvre du Zero Trust.

3.2 Quels bénéfices devrais-je attendre de la mise en œuvre de Zero Trust ?

Avant de se lancer dans un programme de transformation Zero Trust, on doit se poser la question des bénéfices qu'on en attend. Pourquoi investir temps et budget sans, au préalable, définir précisément les bénéfices attendus et les mesurer au fil de l'avancement du projet Zero Trust ?

On peut classer les bénéfices attendus en trois grandes catégories :

1. **Meilleure maîtrise du SI et renforcement de la cybersécurité :** une remise à plat du modèle existant permet de s'interroger sur les points forts et points faibles des solutions actuellement déployées ou des processus en place. Par exemple, les identités sont-elles bien gérées et protégées ? L'authentification forte est-elle généralisée ? La sécurité des appareils de l'entreprise qui sont désormais à l'extérieur, est-elle au meilleur niveau avec une gestion des mises à jour et une détection effective des menaces ? L'approche Zero Trust apporte une structuration sur laquelle on peut s'appuyer pour acquérir une vision globale et cohérente du SI (prérequis nécessaire pour mettre en œuvre correctement le modèle) et des solutions qui sont déjà en place ou que l'on devra déployer pour augmenter le niveau de sécurité global. Par exemple, le déploiement d'une solution de supervision de sécurité plus récente, capable de gérer des signaux en provenance du cloud et/ou de l'interne, assurera une meilleure détection et un délai de réponse aux incidents plus court tout en couvrant un périmètre plus étendu.
2. **Ouverture vers de nouveaux scénarios :** Les métiers ont de plus en plus besoin d'ouvrir leur SI aux clients et partenaires, le télétravail se développe massivement, l'utilisation de dispositifs personnels (BYOD) pour accéder à des données professionnelles se généralise : le modèle Zero Trust prend en compte les nouveaux scénarios d'usage en s'appuyant sur la fonctionnalité centrale de contrôle d'accès conditionnel pour limiter les risques de compromission du système d'information. Par exemple, si l'entreprise développe une application cloud, celle-ci disposera, grâce aux composants du Zero Trust, d'un annuaire d'identités déjà provisionné et accessible

[16] *Security Information & Event Management* / *Extended Detection and Response* : cf. Glossaire

[17] Le pilier « Infrastructure » n'est pas systématiquement présent, par exemple dans le modèle de maturité du CISA (Zero Trust Maturity Model, Cybersecurity and Infrastructure Security Agency, version 1.0, June 2021)

depuis Internet et pourra automatiquement profiter de l'identification unique ou *Single Sign-On* (SSO)[18] et du contrôle d'accès conditionnel en définissant ses propres politiques d'accès. L'application bénéficiera immédiatement des solutions protégeant les identités (authentification multifacteur ou sans mot de passe, détection des attaques sur les identités, etc.), de celles contrôlant le niveau de sécurité des appareils, de la protection contre la fuite d'information basée sur la classification, etc. L'administrateur de l'application pourra définir ses propres politiques pour restreindre les accès en fonction de critères sur l'identité de l'utilisateur, du niveau de confiance dans l'appareil utilisé, de la localisation, du niveau de criticité de l'application, etc.

3. **Conformité réglementaire :** Implémenter le Zero Trust aide les organisations à adopter les meilleures pratiques en matière de sécurité du SI, et donc à remplir certaines obligations réglementaires dans ce domaine, mais à ce jour et au moment de la rédaction de ce document, seuls les États-Unis imposent aux organisations fédérales une transition vers le Zero Trust. Des recommandations sur une approche similaire seront peut-être imposées dans le futur au niveau européen (cf. section « 5 GOUVERNANCE ET CONFORMITE »). Si on prend l'exemple du RGPD, ce règlement impose aux organisations de référencer l'ensemble des applications traitant des données personnelles et de justifier des contrôles de sécurité mis en place pour sécuriser ces données. On voit l'avantage d'un point de vue conformité de disposer d'un référentiel d'applications et d'une homogénéisation des contrôles de sécurité dédiés à leur protection tels que requis dans une approche Zero Trust.

La section « 4.1 Quelles briques techniques pour implémenter le Zero Trust ? » traite des composants nécessaires pour une implémentation réussie du Zero Trust dans son organisation. Dans la suite de cette section, nous traitons des mesures de sécurité et des bénéfices auxquels il faut s'attendre après leur mise en place.

Les bénéfices d'un point de vue technique

1. **Supervision, analyse dynamique et automatisation : une meilleure administration**

   Le Zero Trust permet de traiter chaque entité comme un attaquant potentiel et accorde l'accès aux ressources en appliquant une politique du « moindre privilège » et sur la base d'une session limitée dans le temps. Une journalisation des actions permettra d'analyser le comportement du SI en temps réel afin d'améliorer automatiquement sa posture contre les risques en cours.

2. **Gestion des autorisations : une granularité plus fine**

   Les utilisateurs n'ont accès qu'aux ressources nécessaires à l'exécution de leurs fonctions et jamais à l'ensemble du réseau et des ressources. Pour réduire la surface d'attaque, la stratégie Zero Trust octroie les accès en fonction : de l'identité de l'utilisateur, de sa position géographique, du type de ressource auquel il requiert l'accès et du contexte général du système d'information dans lequel il évolue (tenant compte des attaques en cours, des vulnérabilités identifiées…).

3. **Ressources du système d'information : un renforcement de la cyber-résilience**

   Le Zero Trust permet de limiter au maximum les facteurs d'indisponibilité, augmenter la résilience et protéger l'intégrité du système grâce à des contrôles en amont. Particulièrement sur les téléphones mobiles, les ordinateurs portables, les serveurs, et tous les autres équipements qui souhaitent accéder aux ressources.

4. **Applications et données : un contrôle dynamique**

[18] Sous condition d'utiliser les protocoles « modernes » interopérables tels que SAML, OpenID Connect, OAuth, etc.

L'implémentation des différentes briques du Zero Trust va permettre de superviser les comportements des applications présentes dans le système d'information, veiller à ce que les mises à jour soient régulièrement effectuées et remonter tout comportement suspect ou vulnérabilité identifiée ce qui provoquera une révocation immédiate des autorisations précédemment octroyées. Les données seront classifiées en fonction de leur degré de sensibilité et des règles dynamiques peuvent être appliquées sur toute transaction les concernant.

Les bénéfices d'un point de vue business

L'implémentation du Zero Trust va permettre de :

1. Renforcer le sentiment d'assurance de l'organisation dans la maîtrise des risques auxquels elle peut être exposée.
2. S'inscrire dans une attitude d'amélioration continue de sa posture en matière de sécurité.
3. Se démarquer de la concurrence et apporter la confiance attendue par les parties prenantes pour encourager des partenariats de longue durée en respectant les normes et les standards.
4. Se conformer et garantir sa conformité par rapport aux obligations légales et réglementaires sur les sujets de la sécurité.
5. Avoir une démarche structurée et sécurisée au sein de l'organisation tous les jours, notamment lors des incidents.
6. Mobiliser et définir les responsabilités de chaque membre de l'organisation à tous les niveaux.

3.3 Le Zero Trust est-il adapté à tous les contextes métiers, IoT industriel et OT par exemple ?

Bien que le Zero Trust puisse être considéré à tort comme un simple élément d'infrastructure au même titre que le réseau, les postes de travail, Active Directory, etc., la réalité est beaucoup plus complexe. Comme détaillé plus loin (section « 4.2 Comment implémenter le Zero Trust dans mon organisation ? »), il ne s'agit pas d'un simple service qui peut être fourni par une direction des systèmes d'information (DSI) indépendamment des métiers – et quels que soient les besoins de ceux-ci –, mais d'un changement de paradigme qui nécessite d'impliquer tous les acteurs du SI.

Par exemple, on ne peut pas faire de « véritable » Zero Trust (au sens où on ne se limite pas au ZTNA – cf. section « 4.4 Quelle est la différence entre Zero Trust, Zero Trust Network Access (ZTNA) et Secure Access Service Edge (SASE) ? ») sur une application métier sans intégrer la logique applicative et la gestion des privilèges liés aux identités et aux données dans le mécanisme d'accès conditionnel. Mais les besoins métiers ne se limitent pas à des applications homme-machine dans lesquelles il est souvent aisé de définir des profils utilisateurs, ils comprennent également :

- Des échanges de données entre applications internes et/ou externes – sur lesquelles le concept s'applique plus difficilement ;
- Et surtout, le plus grand défi concerne certaines activités qui reposent sur des communications entre machines complexes à intégrer dans un modèle Zero Trust : Smart City, véhicules autonomes, contrôle industriel, protocoles non-IP…

Concernant l'IoT[19] industriel et l'OT[20], plusieurs facteurs rendent en effet la tâche particulièrement ardue :

- ces appareils exécutent des tâches automatisées (donc sans « utilisateur » au sens IT[21]) et potentiellement critiques ;
- ils reposent souvent sur des plateformes, protocoles et infrastructures « exotiques » ou vieillissantes – leur durée d'exploitation et d'amortissement étant bien supérieure à celle des appareils IT, parfois des dizaines d'années, en raison de la durée des programmes industriels ;
- leurs capacités de calcul ou de communication sont souvent limitées, rendant par exemple le chiffrement asymétrique ou les mises à jour en continu impossibles ;
- ils sont parfois exposés aux attaques physiques (appareils déployés dans des espaces publics), contrairement à des serveurs situés dans un datacenter, par exemple.

Cependant, la convergence économiquement inévitable avec l'IT plaide en faveur de l'adoption d'une stratégie Zero Trust pour renforcer la sécurité de l'IoT/OT, comme le montre par exemple le modèle de maturité de sécurité (IoT SSM[22]) mis en avant par le Consortium IIoT (Industry IoT Consortium).

De même, pour faire face aux enjeux de cybersécurité posés par les véhicules connectés et *a fortiori* autonomes, un certain consensus semble également se dégager dans l'industrie automobile autour d'architectures de sécurité reprenant les concepts du Zero Trust[23].

En septembre 2022, l'ETSI a publié un livre blanc[24] sur la sécurité du « *Multi-Access Edge Computing* » (traitement des données multiaccès à la périphérie du réseau). La technologie *Edge Computing* est souvent opposée à celle du *Cloud Computing* comme meilleure solution de traitement et de stockage des données dans les environnements IoT autonomes et dans l'industrie 4.0, alors que les partisans du *Cloud Computing* pointent la vulnérabilité des appareils en périphérie de réseau.

Selon certains analystes, le taux de données traitées par *Edge Computing* devrait atteindre 75 % en 2025 contre 9 % en 2020. Les environnements *Multi-Access Edge Computing*, qui jouent un rôle essentiel dans les infrastructures 5G, sont par nature complexes, car ils intègrent à la fois des composants matériels et logiciels dans un écosystème multipartite (multivendeurs, multifournisseurs et nombreuses parties prenantes) et des services supportant la mobilité et les communications radio. Compte tenu de ce niveau global d'hétérogénéité, les domaines de la sécurité, de la confiance et de la confidentialité sont ici des sujets clés, mais l'ETSI relève « *qu'on ne peut pas supposer qu'une entité centrale puisse assurer la sécurité à l'échelle du système ou accepter l'entière responsabilité en cas de problème* » tout en mettant en avant le Zero Trust comme une stratégie fondamentale à adopter.

En réalité, dans les documents cités précédemment, il est recommandé, voire imposé, d'adopter les concepts du Zero Trust, mais sans se conformer aux architectures NIST/CISA ou du schéma de la section « 4.1 Quelles briques techniques pour implémenter le Zero Trust ? », qui sont difficilement applicables dans ces environnements.

---

[19] *Internet of Things* : Internet des objets

[20] *Operational Technology* : technologies matérielles et logicielles destinées à la gestion et au contrôle des équipements physiques et industriels

[21] *Information Technology* : technologies de l'information, dont le domaine d'application est plus axé sur les données et processus métiers, par opposition à l'OT axé sur la gestion et le contrôle des systèmes matériels (mais la convergence entre les deux domaines est en marche !)

[22] https://www.iiconsortium.org/smm/

[23] Voir par exemple WITH CONNECTED CARS, ZERO TRUST IS BEST SECURITY ADVICE ou ZERO-TRUST BLUEPRINT TO CLOSE THE SECURITY AND SAFETY GAPS IN THE AUTOMOTIVE INDUSTRY

[24] ETSI - MEC SECURITY; STATUS OF STANDARDS SUPPORT AND FUTURE EVOLUTIONS

Les principes de Zero Trust qui sont mis en avant concernent :

- l'élimination du contrôle d'accès basé uniquement sur l'adresse réseau ou la confiance implicite dans une ressource, sauf si son intégrité peut être prouvée au moyen d'un composant sécurisé (TPM/HSM[25]) ;
- la sécurisation de toutes les communications ;
- l'authentification renforcée ;
- le principe de moindre privilège ;
- la segmentation et l'isolation des ressources critiques ;
- la politique de sécurité dynamique.

En revanche, l'identité, qui est au cœur de l'accès conditionnel, passe au second plan : s'agissant de communications entre machines, pour respecter les standards de sécurité de ces environnements, les flux doivent être authentifiés et chiffrés de bout en bout en s'appuyant sur des certificats embarqués en TPM ou HSM.

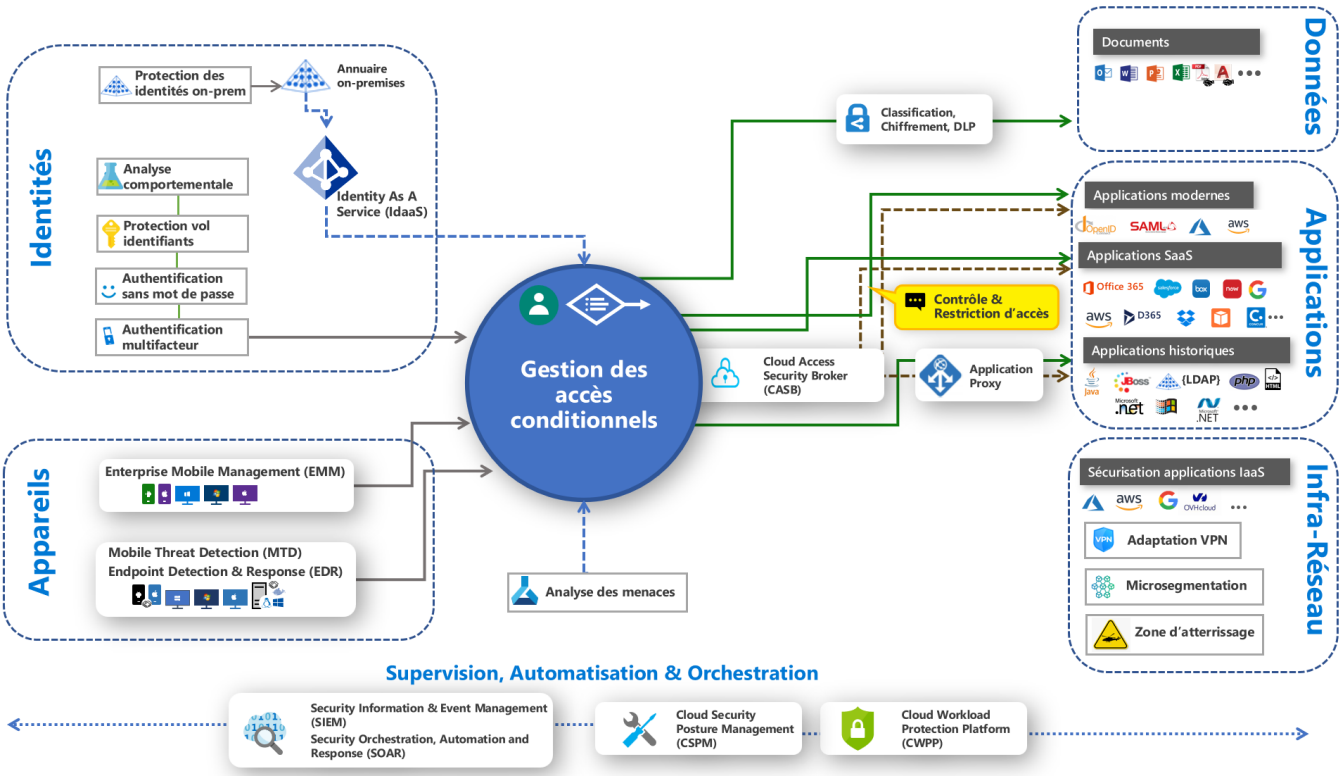
Pour conclure, bien que les concepts restent valables dans tous les cas de figure (de nombreux reprennent des bonnes pratiques de sécurité), les architectures Zero Trust décrites dans ce dossier technique seront principalement adaptées aux environnements IT.

En tout état de cause, la mise en œuvre du Zero Trust doit tenir compte du contexte métier de l'organisation et s'adapter à ce dernier et non le contraire. Outre une meilleure sécurité, elle peut apporter des bénéfices sur le plan business (cf. section « 3.2 Quels bénéfices devrais-je attendre de la mise en œuvre de Zero Trust ? »), et dans un tel contexte il faut bien évidemment consulter les parties prenantes internes et externes pour définir les besoins réels en termes de fonctionnalités attendues et de sécurité.

[25] *Trusted Platform Module* / *Hardware Security Module* : composants de sécurité matériels, cf. Glossaire

4 Les impacts

4.1 Quelles briques techniques pour implémenter le Zero Trust ?



Le schéma ci-dessus montre des exemples de briques techniques pouvant être mises en œuvre dans le cadre d'une implémentation Zero Trust. Le lecteur doit garder à l'esprit qu'il n'existe pas de solutions universelles pour les domaines évoqués dans la suite de cette section et que chacun devra identifier – au moyen d'une étude de transformation Zero Trust –, celles qui sont réellement adaptées à son contexte métier et à son environnement technique.

Il est nécessaire de garder une cohérence dans l'architecture pour rester aligné avec la vision Zero Trust. Pour décider quelles briques technologiques permettront de déployer une architecture de sécurité conforme, il est recommandé de s'appuyer sur la structuration en piliers proposée par le CISA telle que décrite en section « 2.4 Existe-t-il un modèle d'architecture Zero Trust ? ». Pour les fonctions nécessaires à chaque pilier, un ensemble de technologies sont mises en place − abordées succinctement ci-dessous −, qu'il faudra déployer non pas de manière isolée mais, au contraire, en s'appliquant à les intégrer avec celles des autres piliers.

- **Identité** : il est préconisé de commencer la démarche par ce pilier. Le composant central d'une implémentation Zero Trust intègre à la fois la fonction d'annuaire des identités incluant les mécanismes d'authentification et celle de contrôle d'accès conditionnel.

  Selon le contexte technique de l'organisation, une solution IDaaS[26] pourrait être la réponse la plus logique, car elle est accessible depuis l'extérieur et l'intérieur d'un SI et est donc la mieux adaptée pour prendre en compte l'ensemble des scénarios d'accès aux applications et services externes comme internes. Elle s'appuie sur des protocoles

[26] Publique ou privée, selon les besoins de sécurité de l'organisation

standards qualifiés souvent de « modernes » comme OpenID Connect, SAML pour l'authentification et SCIM pour le provisioning. Le SSO est disponible nativement pour plusieurs milliers d'applications SaaS et il est aisé de l'intégrer à ses propres applications – excepté celles continuant à utiliser des protocoles obsolètes.

L'intégration du moteur de contrôle d'accès avec le système de gestion des identités existant est un prérequis, sachant que l'objectif à terme pourrait être idéalement de basculer totalement sur une solution IDaaS en tant qu'annuaire primaire du fait de sa compatibilité avec le principe Zero Trust. Le fait de basculer sur un annuaire primaire de ce type permettrait, par exemple, de supprimer les redondances entre les annuaires internes et l'annuaire cloud afin de gagner en simplification.

Une des premières recommandations pour se prémunir des menaces sur l'identité est de généraliser l'authentification multifacteur qui, selon plusieurs sources, peut aider à bloquer plus de 90 % des attaques sur l'identité[27].

Il faudra ensuite enrichir la base de connaissance avec les informations sur le contexte d'accès et intégrer de manière progressive les politiques d'accès conditionnel pour implémenter les scénarios et cas d'usage qui auront été définis.

- **Appareils** : la gestion maîtrisée des appareils d'un point de vue sécurité est également un objectif prioritaire. Certains appareils – postes de travail portables, smartphones ou tablettes –, se retrouvent à l'extérieur de l'entreprise dans un environnement non contrôlé : il est donc nécessaire de renforcer leur configuration de sécurité et de les administrer et surveiller avec circonspection. Le type d'outil généralement chargé de cette gestion est l'*Enterprise Mobility Management* (EMM). Il permet d'administrer les appareils mobiles, y compris les PC depuis le cloud, dès qu'ils se connectent à Internet. Au-delà d'une simple protection antimalware, l'outil *Endpoint Detection & Response* (EDR) sera quant à lui chargé de surveiller le comportement des appareils – indépendamment de leur système d'exploitation –, pour détecter tout signe de compromission et y répondre au plus vite. La fonctionnalité de *Mobile Threat Defense* (MTD) est tout particulièrement adaptée à la sécurisation des appareils mobiles (iOS, Android) et peut idéalement fusionner avec l'EDR. Le niveau de maîtrise et de contrôle de ces outils sur les appareils peut être plus ou moins fort en fonction des enjeux de sécurité de l'entité.

  Ces différentes briques de sécurité, qui assurent le renforcement du niveau de sécurité des appareils en alliant détection et protection, vont devoir s'intégrer d'une part avec le composant d'accès conditionnel – pour lui fournir les éléments de contexte sur l'appareil –, et d'autre part avec les outils de supervision, vers lesquels les événements ou alertes de sécurité seront remontés pour offrir une visibilité plus large sur les attaques potentielles.

- **Réseaux** : le réseau interne de l'entreprise subit une transformation radicale. Avec la migration progressive des applications dans le cloud, il perd de son importance sur la partie *on-premises*. De plus, l'accès aux ressources situées dans le cloud se faisant de plus en plus directement en HTTPS depuis des appareils situés à l'extérieur, une simple connexion Internet suffit, plus besoin dans ce cas de maintenir un réseau privé. Ne pas oublier de s'assurer que les bonnes pratiques de sécurité réseau sont maintenues, voire améliorées avec le cloud. Des « zones d'atterrissage[28] » seront créées pour les applications en s'assurant de la segmentation et du contrôle des flux entre composants. De la microsegmentation sera mise en place si besoin pour assurer un contrôle plus fin des flux réseau.

---

[27] *Infosecurity Magazine*: "Multi-Factor Authentication Can Prevent 90% of Attacks"

[28] Une zone d'atterrissage est un environnement pré-provisionné par du code pour héberger les charges de travail d'une application en respectant des modèles d'architecture structurés pour respecter notamment des bonnes pratiques de sécurité.

La plupart des accès aux applications ne nécessitant plus de reboucler par le réseau interne, l'utilisation du VPN traditionnel va fortement décroître pour se limiter à l'accès à des ressources critiques ou historiques. Les stations d'administration sécurisées avec des configurations renforcées devront continuer, quant à elles, de s'appuyer sur les connexions VPN pour la gestion des ressources critiques, qu'elles soient *on-premises* ou externes (dans un cloud privé, par exemple).

Pour sécuriser les infrastructures IaaS, des modèles de déploiement (*blueprint*) sont utilisés. Ils limitent les erreurs humaines et assurent le respect des bonnes pratiques promues par l'entreprise. L'utilisation de certaines solutions de type *Cloud Security Posture Management* (CSPM) permettra une évaluation en mode continu du niveau de sécurité des composants d'infrastructure (charges de travail, VM, ressources, etc.). Il émet des recommandations pour renforcer cette posture. Une solution de type *Cloud Workload Protection Platform* (CWPP) sera utilisée pour la détection des menaces sur les ressources et charges de travail, en environnement multicloud comme *on-premises*.

- **Applications et charges de travail** : en premier lieu, les applications doivent être en mesure de s'intégrer avec le contrôle d'accès conditionnel grâce à l'utilisation de protocoles d'authentification/autorisation « modernes [29]». Moteur de contrôle d'accès qui offre également le SSO. Une solution du type *Cloud Access Security Broker* (CASB) assure l'identification et le contrôle des applications SaaS utilisées par l'entreprise afin de limiter le « Shadow IT ». Elle assure également la protection contre les menaces et la fuite d'information. Dans l'idéal, le CASB devrait être intégré à une solution de classification afin qu'il puisse également tenir compte des labels associés aux données.

  Dans une approche DevSecOps, la sécurité sera prise en compte pendant le développement des applications et ce, dès la phase architecture, grâce à une « équipe Zero Trust ». Cette dernière devra maîtriser les concepts et les bonnes pratiques d'implémentation. Le CSPM jouera également un rôle dans le cycle DevSecOps.

  L'administration des applications et services sera opérée par un nombre réduit de personnes dont les privilèges seront accordés pour des tâches précises et pour des temps limités dans le respect du principe de moindre privilège.

  La gestion des règles de contrôles d'accès est cruciale pour assurer la sécurité. Consultez le paragraphe « Mise en œuvre du Zero Trust » de la section suivante pour en savoir plus sur la nécessité d'une approche méthodique.

- **Données** : le préalable à toute protection des données est l'établissement d'une classification qui sera liée au secteur d'activité de l'organisation. Il s'agit d'identifier les données sensibles en termes de confidentialité (secret de fabrication, brevet, plans industriels, formule pharmaceutique, etc.) et également celles soumises aux réglementations (données personnelles dans le cadre du RGPD, par exemple). Il faut ensuite être en mesure de repérer ces données sensibles parmi la masse d'informations et de leur apposer une étiquette, label qui servira à appliquer des protections particulières (autorisations, chiffrement, etc.) ou tout simplement à éviter qu'elles ne fuitent. Des solutions de gouvernance pour automatiser la découverte des données dans les environnements *on-premises* et également cloud existent. Elles attribuent des labels en fonction de gabarits et/ou s'appuient sur des algorithmes de reconnaissance. Des solutions de collaboration peuvent aussi proposer une fonction de classification. Ainsi les utilisateurs peuvent par eux-mêmes apposer un label sur les documents qu'ils produisent. En cas de non-respect des politiques de sécurité établies par l'organisation, l'utilisateur concerné peut, par exemple, recevoir une simple mise en garde, ou se voir opposer un refus de transfert, ou encore se faire imposer un chiffrement du document.

[29] On désigne sous le terme de protocoles « modernes » les protocoles d'authentification-autorisation ouverts tels que SAML, OpenID Connect ou Oauth 2.0 qui offrent une interopérabilité et permettent de se connecter à des fournisseurs d'identité pour entre autres profiter du SSO

Des passerelles de type CASB s'appuient sur ces labels pour lutter contre la fuite d'information : elles bloquent le transfert, voire imposent un chiffrement des données concernées. Il est important que les labels puissent être pris en compte par l'ensemble des solutions de protection et de DLP[30] pour une meilleure efficacité de la stratégie de protection.

Enfin, la protection des données au niveau des applications est une nécessité. Pour chaque application, une démarche d'analyse de risques doit être menée – en cohérence avec toutes les réglementations auxquelles l'entreprise est soumise, notamment le RGPD. L'objectif est d'identifier si des données sensibles sont traitées et s'appuyer sur les contrôles de sécurité disponibles sur les plateformes cloud pour appliquer les protections nécessaires (chiffrement, anonymisation, etc.).

Au-delà des solutions technologiques qui adressent chacun des piliers décrits par le modèle du CISA, une seconde série de solutions intègrent les fonctions transversales s'appliquant au socle commun à tous les piliers. Fonctions réparties dans trois catégories : « Visibilité et Analyse », « Automatisation et Orchestration » et « Gouvernance » (cf. section « 2.4 Existe-t-il un modèle d'architecture Zero Trust ? »). La détection des événements de sécurité doit s'appliquer transversalement sur l'ensemble des piliers, dans les environnements *on-premises* et cloud. Les outils appropriés s'appuient sur les technologies SIEM les plus récentes. Elles profitent des avantages du cloud pour offrir des volumes d'ingestion d'informations quasi illimités et des fonctions de *Machine Learning* pour corréler les incidents et détecter les signaux faibles des attaques. Elles offrent de plus l'automatisation de la réponse à incidents en implémentant la fonction de SOAR (*Security Orchestration, Automation and Response*).

4.2 Comment implémenter le Zero Trust dans mon organisation ?

Zero Trust : à la fois modèle et programme

Au-delà de la dimension purement technique qui a été décrite dans la section précédente, il faut comprendre que le Zero Trust ne se limite pas au déploiement de quelques briques de sécurité : il représente une véritable évolution dans l'approche de la sécurité et correspond à un changement de modèle.

Si on doit faire une comparaison, l'introduction de la sécurité dans le processus de développement a débuté il y a une vingtaine d'années, pour faire face aux premières attaques virales sur les applications internes ou exposées sur Internet. Il était nécessaire de professionnaliser le développement en s'appuyant sur des méthodologies de développement sécurisé telle que *Security Development Lifecycle* (SDL). C'est ce qui a été ensuite formalisé dans la norme ISO 27034 / INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – APPLICATION SECURITY[31], avec pour objectif de « *s'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information* ».

C'est ce même principe d'adaptation qui doit s'appliquer désormais plus largement au modèle de sécurité basé sur une approche Zero Trust.

Par son périmètre et les nombreux sujets à aborder, prendre en compte les idées du Zero Trust s'apparente plus à mettre sur pied un programme, c'est-à-dire un ensemble de projets qui se développent dans le temps. Ce programme devra être transversal et va devoir impliquer l'organisation au-delà des seules équipes sécurité et réseau, par exemple l'équipe en charge de la gestion des identités, celle des postes de travail, ou encore celle de la supervision, les

[30] *Data Loss Prevention* : cf. Glossaire

[31] https://www.iso.org/standard/44378.html

responsables applicatifs également, etc. On se rapproche ici de la vision du Cigref, qui dans son livre blanc *Vers une philosophie Zero Trust*[32] précise que : « *Le Zero Trust est une évolution des modèles d'architecture avec un cœur de décision qui fait le lien entre les identités, les données et les applications. L'approche doit être globale, cohérente et intégrée dans une architecture complexe avec une coordination des équipes autour de cet objectif commun.* »

En fonction de son niveau de maturité de sécurité par rapport aux principes du Zero Trust et de son parc d'administration existant, une organisation doit définir des objectifs prioritaires et d'autres plus lointains. Objectifs qui composeront sa feuille de route Zero Trust.

Mise en œuvre du Zero Trust

La mise en œuvre doit se faire à pas mesurés, en débutant avec des « gains rapides » (*quick wins*) qui apporteront en peu de temps des résultats visibles. Par exemple, débuter en mettant la priorité sur le pilier Identité en commençant par la mise en place du centre névralgique du Zero Trust : le contrôle d'accès conditionnel. Quelques applications viendront rapidement se greffer dessus ; ensuite, passer à l'authentification multifacteur pour compenser la faiblesse des mots de passe, etc.

Pour maintenir en condition opérationnelle un système de sécurité Zero Trust, il est important de gérer les règles de manière efficace. Cela implique d'établir des critères, tout en évitant de bloquer de manière inutile des utilisateurs légitimes. Les critères doivent prendre en compte non seulement les identités et l'authentification, mais aussi l'analyse comportementale et d'autres facteurs basés sur des données empiriques.

La mise en place de ces critères de blocage nécessite une approche méthodique similaire à celle utilisée pour les composantes initiales du Zero Trust. Il est crucial de les définir avec soin en se basant sur des données empiriques fiables. De plus, il est essentiel de mettre en place une boucle de réaction rapide pour débloquer rapidement une session ou une connexion une fois qu'elle a été vérifiée.

Auparavant, la gestion des postes de travail et des appareils mobiles (incluant le référencement, le contrôle, l'application des politiques de sécurité, le déploiement des correctifs de sécurité, et le déploiement des mises à jour) était effectuée exclusivement à partir de services internes. Toutefois, une action à moyen terme consisterait à adopter un mode de gestion « moderne » des postes de travail et mobiles en utilisant un service cloud. Cette approche permet à n'importe quel appareil, peu importe sa position géographique, d'être géré sans nécessiter un tunnel VPN.

À plus long terme, la classification exhaustive des données de l'organisation pourra également être adoptée – un sujet encore trop souvent mis de côté, même si son importance est cruciale notamment pour se conformer aux réglementations comme le RGPD.

Adoption et gouvernance

Les principes de Zero Trust doivent « infuser » dans l'organisation pour que chaque nouveau projet puisse s'intégrer rapidement dans l'architecture : par exemple, une nouvelle application développée en interne devra respecter un certain nombre d'exigences comme la prise en compte de la sécurité dès la conception (*Secure by Design*), l'intégration avec l'annuaire et les mécanismes d'authentification (protocoles SAML, OpenID Connect, etc.), l'intégration avec les systèmes de supervision, etc. De même, lors du choix d'une application SaaS, on s'assurera qu'elle s'intègre facilement au niveau des identités et de l'authentification avec le moteur d'accès conditionnel etc.

[32] Vers une philosophie Zero Trust – Une rupture dans la continuité pour la sécurité des applications, Cigref, février 2022

Ceci implique la mise en place d'une gouvernance qui permettra de définir les exigences propres au respect des règles d'intégration dans les briques Zero Trust, de s'assurer de leur application et de former les personnes concernées en s'appuyant sur des référents Zero Trust. Des référents qui constitueront une équipe qui devra être transversale pour intégrer toutes les parties prenantes de la DSI.

Le voyage vers le Zero Trust se fera donc de manière progressive : par exemple, la bascule des identités du référentiel sur site (*Active Directory*) vers le référentiel cloud pourrait passer par une étape intermédiaire hybride où une partie des identités serait dupliquée dans les deux annuaires ; les applications existantes pourraient être adaptées progressivement ou peut-être abandonnées à terme si leur intégration s'avérait trop coûteuse ou complexe ; les nouvelles fonctionnalités seraient déployées d'abord sur un périmètre réduit avant d'être progressivement généralisées.

Et pourquoi pas définir un label Zero Trust comme le préconise le Cigref ? « *Pour permettre de voir sur le moyen terme les évolutions de l'organisation vers le Zero Trust, le groupe de travail propose de* ***mettre en place un label « Projet Zero Trust »*** *ou « Conforme Zero Trust » au sein des DSI pour identifier les projets qui intègrent la feuille de route Zero Trust ou qui pourraient l'intégrer aujourd'hui ou plus tard, au cours d'évolutions progressives.* »

Les utilisateurs ne seront pas oubliés et devront être formés aux nouvelles fonctionnalités. Certaines d'entre elles pourront être plus contraignantes, comme l'activation de l'authentification multifacteur uniquement dans des cas suspects ou lors de l'accès à des ressources sensibles. D'autres, en revanche, apporteront plus de confort à leurs utilisateurs, comme l'authentification sans mot de passe (*passwordless*) et/ou le SSO.

L'adoption par tout le monde est primordiale. Et tout particulièrement pour des fonctions comme la classification des données, où tous les utilisateurs devront devenir acteurs en déterminant le niveau de sensibilité de l'information qu'ils produisent.

Conformité réglementaire et coût

Concernant les aspects réglementaires, le *Data Protection Officer* (DPO) sera, par exemple, intégré dans l'équipe chargée de la gouvernance. Il s'assurera que les exigences liées à la sécurité des données sont bien prises en compte dans le cadre du projet Zero Trust. Sur le chemin emprunté pour implémenter une stratégie de type Zero Trust dans un SI, l'on s'assure également que toutes les applications de l'organisation – et les traitements associés –, s'appuient bien sur les nouveaux contrôles de sécurité mis en place. Par exemple, la mise en œuvre d'une classification des données avec la possibilité de recherche et d'étiquetage de celles qualifiées de sensibles doit être traitée dans le pilier Données. Ceci permettra également de lutter contre la fuite d'information (DLP) en s'appuyant sur ces étiquettes et de protéger automatiquement par chiffrement ces données sensibles.

Le coût d'un programme Zero Trust dépendra de nombreux facteurs : la taille d'une organisation, l'historique et la complexité de son SI, le niveau de maturité de son approche Zero Trust, l'utilisation du cloud ou *a contrario* son aversion à l'utiliser, son agilité, etc. Quel que soit le choix qui sera fait, notre recommandation est de commencer « petit » en mettant en place en premier lieu les composants de base du Zero Trust (brique de gestion des identités et de contrôle d'accès conditionnel, etc.) ; s'appuyer également sur des « *quick wins* » pour assurer des résultats tangibles et surtout rapidement visibles (permettant de continuer à obtenir du budget). Et d'avancer progressivement dans le temps avec des chantiers que l'on aura définis comme prioritaires parmi les différents piliers.

Enfin, rappelons qu'un programme Zero Trust présente toujours deux facettes : un renforcement de la sécurité devenu indispensable – car encore trop souvent considéré comme un centre de coût –, mais aussi l'ouverture à de nouveaux scénarios sans oublier une certaine agilité, de nouveaux éléments qui peuvent également apporter de véritables bénéfices business.

4.3 Le Zero Trust signifie-t-il l'abandon du VPN ?

Non, pas nécessairement. Il est important de souligner que la connexion traditionnelle d'un administrateur à un poste distant via VPN IPsec reste une solution adaptée et sûre dans certains cas, tels que ceux des OIV et des OSE[33]. Par exemple, pour accéder au poste de commande d'une centrale nucléaire, une connexion VPN depuis un poste dédié garantit un niveau de sécurité rigoureux et simple à mettre en place. Par conséquent, il n'est pas nécessairement recommandé de se passer de cette méthode dans ces situations.

Dans le cas général, au moment de se poser la question du passage à Zero Trust, il faut déterminer si les données et les applications accessibles se trouvent déjà dans le cloud, *on-premises*, ou si on se trouve dans un mode hybride. En fonction de ces éléments, il peut être judicieux de conserver un VPN et dans ce cas on verra comment le configurer au mieux pour répondre aux exigences Zero Trust.

Tout est déjà dans le cloud

Lorsque les données ou les applications sont en SaaS, on ne passe déjà pas, pour y accéder, explicitement par un VPN, mais par un logiciel client (la plupart du temps un navigateur Internet) ; c'est celui-ci qui va créer une connexion privée et chiffrée à travers un tunnel TLS entre l'utilisateur et les données. D'autres cas de figure (IaaS, PaaS) peuvent nécessiter de conserver une forme de VPN pour garantir la sécurité des communications. Passer au Zero Trust va alors consister à appliquer les mécanismes recommandés (MFA, SSO, IAM, VPN si nécessaire, moindre privilège, segmentation réseau, SIEM, etc.) pour assurer la sécurité des données et des accès aux applications dans le cloud.

Tout est *on-premises*

Certaines organisations, étant donné la nature de leurs activités, peuvent être frileuses à mettre leurs données dans le cloud (perte de contrôle, de souveraineté, etc.). D'autres organismes (OIV, OSE) ont même l'obligation de garder la main sur leurs données et ne peuvent pas faire le choix du « tout dans le cloud public ». Dans ce cas, une connexion VPN reste une solution simple et sécurisée pour se connecter au SI.

À l'intérieur du SI, l'administrateur réseau veillera à cloisonner les différents sous-réseaux pour assurer à chaque collaborateur la possibilité d'accéder, à distance aussi bien que sur place, aux seules informations auxquelles il a droit.

La conservation de la défense périmétrique n'empêche pas ici de renforcer le niveau de sécurité avec des règles Zero Trust. À cet égard quelques bonnes pratiques d'utilisation d'un VPN sont précisées dans la dernière section de cet article.

Mode hybride

Dans le cas d'un système d'information hybride, dans l'idéal, les connexions doivent se faire de façon transparente pour l'utilisateur, que ce soit au SI interne ou au cloud externe.

Pour se connecter au SI, un VPN reste une solution compatible Zero Trust à partir du moment où il est bien configuré (voir plus loin). Les connexions au cloud peuvent alors se faire soit à travers le SI – on parle de « tout dans le tunnel » –, ce qui garantit une protection des échanges, soit directement depuis le poste vers l'application cloud, sans passer par le SI – on parle de « *split tunneling* ».

Le mode « tout dans le tunnel » apporte une sécurité optimale, car aucun flux ne peut rentrer dans le poste ou sortir du poste sans passer par le tunnel. C'est un mode qui semble pertinent lorsqu'on a les outils nécessaires dans le SI pour garantir la sécurité des données et vérifier les accès.

[33] Opérateurs d'Importance Vitale / de Services Essentiels (cf. Glossaire)

Néanmoins, la philosophie Zero Trust consiste à considérer que le réseau interne est également vulnérable. Avec ce point de vue, il ne paraît plus nécessaire de passer systématiquement par le SI pour accéder au cloud. Au contraire, il paraît plus sûr et moins consommateur de bande passante de se connecter directement aux services cloud.

De plus, pour apporter une expérience d'utilisation optimale, des mécanismes de type SSO permettront d'utiliser la même authentification pour la connexion au cloud que pour l'accès aux données à l'intérieur du SI.

Comment configurer le VPN pour être conforme & Zero Trust ?

Un VPN bien utilisé et bien configuré est indispensable pour garantir la sécurité des connexions. L'authentification forte, à base de certificats, idéalement localisés dans un *token* (ou une carte à puce) – première authentification –, pour éviter qu'ils ne soient recopiés et transmis, un code pin – deuxième authentification –, étant requis pour y donner l'accès[34].

Dans le cas de machines dédiées et gérées par l'administrateur, un renforcement de la sécurité est possible avec l'association d'une authentification de la machine (par TPM, par exemple) avec authentification utilisateur avant d'accepter l'ouverture de la connexion VPN.

De façon symétrique, le poste devra également authentifier la passerelle à laquelle il se connecte en utilisant des certificats.

Une fois connecté au réseau distant, pour éviter tout parcours latéral dans les données, le réseau devra être correctement cloisonné. L'accès d'un utilisateur doit être limité strictement aux données auxquelles il a les droits.

Conclusion

En conclusion, comme précisé par le NCSC (*National Cyber Security Centre* du Royaume Uni)[35] :

- si vous avez des ressources *on-premises* déjà accessibles via VPN, il est tout à fait possible de conserver le VPN tout en veillant à se conformer à la philosophie et aux recommandations de sécurité proposées par Zero Trust sans remettre en cause votre architecture réseau ;
- si vous n'avez pas de *on-premises*, vous pouvez démarrer directement avec une architecture Zero Trust tout dans le cloud – pour autant, les communications devront être sécurisées, que ce soit par VPN IPsec ou au moyen d'autres protocoles chiffrés ;
- enfin, ces deux options n'étant pas mutuellement exclusives, une approche hybride peut être pertinente en particulier si vous avez à la fois des ressources *on-premises* et dans le cloud.

4.4 Quelle est la différence entre Zero Trust, Zero Trust Network Access (ZTNA) et Secure Access Service Edge (SASE) ?

Souvent dans le discours Zero Trust, la différence n'est pas faite avec *Zero Trust Network Access* (ZTNA) même si dans ce dernier sigle le réseau est bien présent. D'où vient cette ambiguïté ? Du fait que l'approche ZTNA proposée par le Gartner s'appuie sur les principes de Zero Trust (tels que présentés précédemment par le Forrester, puis formalisés ensuite par le NIST[36]), mais en se concentrant sur une vision complètement orientée sur le réseau.

---

[34] Voir par exemple le guide de l'ANSSI https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/

[35] https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures

[36] Se référer à la section « 2.1 Qu'est-ce que le Zero Trust ? » de ce document.

De part et d'autre, le constat est le même et doit mener à revoir la manière dont on implémente la sécurité : l'adoption du cloud, l'inefficacité du modèle réseau centralisé, la généralisation du travail à distance, les performances pour l'accès aux applications SaaS, etc. Mais l'approche pour implémenter les principes de Zero Trust est éminemment différente.

Sans nier l'importance de l'identité, le postulat du ZTNA est que toute la sécurité peut être contrôlée par le réseau. Par exemple, le composant qui contrôle dynamiquement l'accès aux ressources est une passerelle réseau qui va autoriser les flux entre le client et l'application en fonction du résultat de l'authentification.

Ce qui peut s'avérer exact pour des applications historiques l'est moins sur les applications Web plus modernes : l'accès aux applications se fait de plus en plus avec une connexion chiffrée de bout en bout entre le client et l'application protégée dans un canal HTTPS. Selon l'avis même de l'ANSSI dans une note blanche sur Zero Trust Network[37] : « *La détection doit également prendre en compte la tendance visant à généraliser l'usage de protocoles chiffrés, potentiellement de "bout en bout", ce qui amoindrit grandement l'efficacité des sondes réseau et conduit à un déplacement des sources d'événements exploitables, du réseau vers les systèmes.* »

Dans une approche Zero Trust basée sur le réseau (ZTNA), le contrôle s'effectue au niveau des couches réseau, alors que dans l'approche Zero Trust basée sur l'identité, le contrôle se fait au niveau de l'accès applicatif : une fois l'accès autorisé par le moteur d'accès conditionnel, un jeton est émis, le client est redirigé vers l'application qui autorisera l'accès après vérification du jeton. La sécurité est traitée au niveau de l'application elle-même et non plus sur les couches réseau.

A contrario, l'implémentation ZTNA s'appuie sur une passerelle qui se positionne en rupture de flux. En outre, les protocoles applicatifs sont de plus en plus complexes, ce qui rend leur analyse lourde et inefficace et introduit des délais de traitement pouvant s'avérer critiques lorsque l'on doit traiter des flux en temps réel comme la vidéo.

L'approche *Secure Access Service Edge* (SASE) franchit un nouveau cap puisque le Gartner la définit comme la convergence entre le *Network as a Service* et le *Network Security as a Service*[38]. L'approche SASE est plus « large » que l'approche ZTNA : elle y ajoute la technologie *Software-Defined WAN* (SD-WAN[39]). Selon le fournisseur Netskope : « *SASE combine plusieurs concepts, ceux du Zero Trust, du SD-WAN et du* Security Service Edge *(SSE) pour proposer une posture de sécurité et de mise en réseau qui protège et régit le cloud et le nouvel environnement de travail à distance.*[40] »

Dans la vision SASE, le cloud est mis en avant comme étant incontournable dans l'implémentation, le réseau de l'organisation se fondant dès lors dans le réseau du fournisseur cloud pour relier l'ensemble de ses sites distants dans le but avoué de supprimer tous les liens MPLS coûteux et de les remplacer pour un SD-WAN configurable à volonté (*Software Defined Network*). En forçant à peine le trait, on peut considérer que SASE est une approche périmétrique dans le cloud : la frontière réseau s'est simplement étendue dans le cloud et le contrôle d'accès se base sur les briques réseau classiques, mais proposées cette fois sous forme de services cloud – *Secure Web Gateway* (SWG), *Cloud Access Security Broker* (CASB), DNS, *Firewall as a Service* (FWaaS), etc.

---

[37] SYSTEME D'INFORMATION HYBRIDE ET SECURITE : UN RETOUR A LA REALITE, ANSSI, août 2021

[38] The Future of Network Security Is in the Cloud, Gartner, August 2019

[39] « *Un réseau étendu défini par logiciel ou Software-Defined WAN (SD-WAN) est une architecture WAN virtuelle, dans laquelle n'importe quel mélange de types de transport de réseau – non seulement la commutation multi protocole par étiquette (MPLS), mais aussi l'Internet à large bande, la téléphonie cellulaire et le satellite – peuvent être virtualisés et liés, puis gérés de manière centralisée par logiciel, afin de connecter en toute sécurité les utilisateurs aux applications et aux postes de travail conformément à la politique.* » Source : https://www.citrix.com/fr-fr/solutions/sd-wan/what-is-sd-wan.html

[40] Security Service Edge for dummies, Netskope 2022 (traduction)

Ce schéma est relativement contradictoire avec le fait qu'avec Zero Trust, l'identité devient le nouveau périmètre et surtout qu'Internet devient le réseau d'entreprise en réduisant *a minima* le réseau interne. De plus, dans une vision SASE/ZTNA, les autres piliers de Zero Trust ne sont pas abordés, ou tout au mieux à peine cités.

On comprend que le SASE soit poussé par des acteurs réseau (souvent reconnus) en s'appuyant sur les concepts de Zero Trust : l'approche préconisée est de commencer par revoir le réseau de l'entreprise pour adopter le SD-WAN, d'où l'intérêt suscité par cette technologie pour les équipes réseau. Ensuite, seront ajoutées les solutions de sécurité basées sur le cloud (SWG, FWaaS, CASB, etc.).

En résumé, Zero Trust définit des principes et prône une approche plus globale en termes de piliers (modèle CISA) avec comme point de départ l'identité. ZTNA est une implémentation du contrôle d'accès par coupure des flux réseau dans une vision sécurité grâce à des analyses réalisées au niveau réseau, ce qui semble moins adapté aux applications et services cloud. SASE pousse encore plus loin l'approche en intégrant ZTNA et les technologies SD-WAN, dans une volonté d'inclure le réseau d'entreprise dans le cloud en conservant une vision de sécurité périmétrique.

4.5 Comment intégrer mon approche « Best-of-breed » dans ma stratégie Zero Trust ?

L'approche *Best-of-breed* (meilleur de la catégorie) visant à sélectionner la meilleure solution technique pour chaque domaine d'application ou groupe de fonctionnalités, permet généralement de réduire la dépendance à l'égard d'un éditeur de logiciels et de ses solutions. Cela permet d'apporter une certaine modularité du SI et ainsi une agilité : si un système ne répond plus aux exigences de l'entreprise, il peut être remplacé plus facilement.

La multiplication des solutions induite par le *best-of-breed* présente néanmoins de nombreux inconvénients, voire certains risques ; l'interopérabilité des solutions devient un réel défi et l'information est disséminée dans plusieurs interfaces de contrôle. En revanche, certaines solutions techniques sont plus adaptées et facilitent la transformation vers un modèle Zero Trust. Il faut donc pouvoir identifier les solutions les plus adaptées au contexte.

Comment s'assurer d'une cohérence Zero Trust sur un ensemble de composants hétérogènes ?

Dans un tel environnement, la complexité induite par cette multiplication des systèmes et leur hétérogénéité nécessite un effort supplémentaire pour la mise en place d'une approche Zero Trust ou pour le maintien de celle-ci.

D'abord, à l'introduction ou à l'évolution de chaque composant l'approche Zero Trust doit être réévaluée et appliquée : la gestion des identités et contrôle d'accès au nouveau composant, les applications introduites, les données traitées, les infrastructures utilisées (*on-premises*, cloud privé, SaaS, cloud public) ainsi que le réseau (connectivité vers la solution, réseau externe, etc.) doivent faire l'objet de cette évaluation.

« Best-of-breed » et impact sur des ressources

Impliquant de multiples technologies, l'approche *best-of-breed* nécessite diverses compétences souvent difficiles à réunir. Les exploitants font face à des profils plutôt généralistes pouvant avoir un niveau de maîtrise standard sur le panel de solutions déployées, mais l'entreprise peut faire face à une réelle difficulté à réunir des experts maitrisant l'ensemble des solutions.

Le niveau de complexité lié au « Best-of-breed » ainsi que les pénuries d'expertise évoquées peuvent directement impacter les coûts liés à l'exploitation et au management de la sécurité du SI de l'entreprise et introduire une multiplication d'entités d'exploitation externes.

Quelle que soit la stratégie de l'entreprise, privilégier le « tout-en-un » ou le *best-of-breed*, la déclinaison du paradigme Zero Trust doit traiter avec un existant souvent en transformation et doit prendre en compte la gouvernance associée.

Les organisations doivent définir des politiques en fonction de la sensibilité des services, des actifs et des données qu'elles hébergent pour chaque brique.

Actuellement la multiplication des solutions en tant que service (SaaS), mais également une approche de sécurisation orientée produits et les limitations des budgets renforcent cette tendance *best-of-breed*. Il revient ainsi aux équipes IT de maintenir une cohérence de la sécurité Zero Trust de bout en bout.

Cette cohérence d'ensemble doit être garantie en considérant la conformité des solutions *best-of-breed*, et en particulier SaaS, comme une partie intégrante de la sécurité d'entreprise et supervisant chaque achat de logiciel effectué par l'entreprise et examinant ces fournisseurs d'entreprise aussi minutieusement que les technologies.

4.6 Le modèle Zero Trust est-il compatible avec un SI hybride ?

Un SI hybride (nous utiliserons dans ce document le terme Hybridation de l'IT également) se définit comme une approche de l'informatique d'entreprise dans laquelle une organisation fournit et gère ses ressources de technologie de l'information en interne, mais aussi utilise en parallèle des services cloud (IaaS, PaaS, SaaS).

Les principaux avantages et fondements de cette démarche résident dans la quête d'une agilité accrue, d'une prédictibilité des coûts et d'une optimisation des ressources. En termes d'adoption, le cabinet Gartner prévoit que les dépenses mondiales en services de cloud public s'élèveront à 494,6 milliards de dollars en 2022, en raison à la fois de la croissance des services d'infrastructure natifs du cloud et de la tendance aux scénarios d'hybridation de l'IT. Il s'agit d'une augmentation de 20,4 % par rapport aux 410,9 milliards de dollars de ventes en 2021, juste en dessous de la croissance de 21,2 % à 599,8 milliards de dollars que Gartner prévoit pour 2023.

Dans un contexte de mobilité, de télétravail, et de prolifération d'objets connectés (Internet des Objets – IoT), les défis posés par l'hybridation de l'IT pour le RSSI sont de plusieurs ordres.

Comment pallier la perte de visibilité et assurer une homogénéisation et orchestration des politiques de sécurité ?

En effet, nos utilisateurs sont-ils vraiment ceux que nous pensons qu'ils sont ? Qui se connecte, avec quels équipements (ordinateurs personnels, tablettes, smartphone, IoT) ? Quel est leur niveau de protection ? Via quel type de réseau wifi ? Quelle est leur activité, à quel cloud/service/application se connectent-ils **?** Quelles sont les matrices de flux inter and intra applicatives ?

Nous comprenons aussi aisément que cette « explosion » du périmètre de sécurité a multiplié les portes d'entrée et introduit d'éventuelles failles, que les acteurs mal intentionnés peuvent exploiter en mettant en péril des ressources vitales de l'entreprise.

C'est pourquoi l'hybridation de l'IT impose une évolution des architectures de sécurité et la mise en place de nouveaux gestes de cyberbarrière, en passant d'un mode centré sur les sites vers un mode centré sur la protection des identités/des utilisateurs/des données où que ces derniers se trouvent. Cela, en cohérence avec les principes de Zero Trust exposés au préalable dans ce document.

De manière très concrète, il est clair que si le SI devient hybride, les identités deviennent elles aussi hybrides. En particulier les référentiels peuvent être *on-premises* ou dans des services SaaS. Le corollaire est que l'hybridation de l'IT impose à la SSI, dans une logique de cybersécurité optimale, des outils de configuration et supervision transverses qui vont être

capables d'assurer une cohérence globale des règles de sécurité propres aux identités, services et applications tout en captant et corrélant les signaux faibles afin de détecter des comportements malicieux et y répondre.

Nous assistons à une dynamique très forte dans le marché relatif à la simplification et la rationalisation des plateformes existantes listées ci-après, dont la promesse est de résoudre la problématique énoncée ci-dessus dans cette transition d'hybridation de l'IT.

- CSPM (*Cloud Security Posture Management*) qui se focalise essentiellement sur la gestion de la conformité en environnement cloud.
- CWPP (*Cloud Workload Protection Platform*) facilitant la protection au niveau des charges applicatives (*workload*) en environnements distribués.
- CIEM (*Cloud Infrastructure Entitlement Management*) qui surveille les identités cloud et leurs droits.
- CNAPP (*Cloud Native Application Protection Platforms*) qui permet aux équipes de sécurité et développeurs d'identifier, de hiérarchiser et de corriger les risques de sécurité, juridiques et de conformité en mode cloud natif.

Nous allons assister sans aucun doute à une consolidation du marché et invitons les organisations à bien évaluer leurs besoins au regard des fonctionnalités de chacune de ces plateformes.

La perte de visibilité est aussi un sujet qui concerne les applications plus précisément au niveau des codes, scripts, librairies constituant les applications cloud.

Dans le monde numérique dans lequel nous vivons, nous assistons à une recrudescence des attaques sur les chaînes d'approvisionnement (*Supply Chain Attack*). C'est pourquoi il est primordial d'accompagner les équipes du développement Agile, DevOps et DevSecOps en appliquant les principes fondamentaux du Zero Trust pour garantir la sécurité des applications qui aujourd'hui sont construites à partir de plusieurs sources de code. En effet, certaines parties sont développées en interne, d'autres composants utilisent des codes tiers (loués ou achetés) venant de l'open source. C'est pourquoi la compréhension fine de l'inventaire de la chaîne d'approvisionnement logistique entourant l'activité principale de l'entreprise (développement interne et consommation de solutions tierces) est critique pour minimiser le risque global dans un contexte d'hybridation de l'informatique.

Conformité et régulation

La mise en conformité dans une informatique hybride nécessite des considérations supplémentaires relatives à la distribution du SI à prendre en compte dans un environnement réglementaire strict. Les organisations doivent s'assurer de mettre en œuvre des systèmes de journalisation qui enregistrent les événements relatifs à l'authentification des utilisateurs, à une consommation « hors norme », à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité du SI ainsi qu'au fonctionnement du SI. Ce besoin fait partie intrinsèque des offres constituant une architecture Zero Trust (MFA, NAC, ZTNA).

Fort de ces constats, nous voyons que la question fondamentale n'est pas en relation avec une notion de compatibilité du Zero Trust avec l'hybridation du SI, puisque les principes du Zero Trust s'appliquent et doivent impérativement être pris en considération. Les organisations devront se doter des outils et solutions assurant une visibilité transverse, une cohérence dans les politiques de sécurité dans des environnements extrêmement distribués, dynamique soumise à des régulations de plus en plus strictes et qui nécessite un travail d'urbanisation et de cartographie du SI.

5 Gouvernance et conformité

5.1 Peut-on baser entièrement sa politique de sécurité technique sur le modèle Zero Trust ?

Lorsque l'Opération Aurora, une série de cyberattaques de type APT[41] très sophistiquées, a touché Google et de nombreuses autres grandes entreprises en 2009, le géant d'Internet a lancé une initiative interne pour réinventer son architecture de sécurité et la façon dont ses employés et leurs appareils accèdent aux applications internes. Les principes directeurs de ce projet, dénommé BeyondCorp[42], ont été publiés par Google dans une série d'articles[43] à partir de 2014. De son côté, en 2014 également, Microsoft préconise le concept *« assume breach »*[44] (présumer la compromission) pour lutter plus efficacement contre les attaques visant les réseaux d'ordinateurs Windows. Ces prises de position, entre autres, ont contribué à populariser les principes du Zero Trust en matière de politique de sécurité technique.

En mai 2021, c'est le gouvernement américain qui adopte officiellement ce modèle, au travers d'une directive[45] qui donnait 2 mois à l'ensemble de son administration pour planifier la migration de ses SI vers des architectures « as-a-Service » appliquant le principe Zero Trust[46]. En faisant référence aux vagues de ransomware ayant frappé plusieurs institutions, aux vulnérabilités ayant conduit le FBI à intervenir sur des serveurs américains et à l'attaque SolarWinds, il annonce : « *Le gouvernement fédéral doit montrer la voie et accroître son adoption des meilleures pratiques de sécurité, notamment en déployant un modèle de sécurité Zero Trust et en accélérant le mouvement vers des services cloud sécurisés.* » Bien entendu, ce ne sont pas les seules mesures énoncées par la directive, qui définit une politique de sécurité informatique fédérale globale allant bien au-delà des modèles d'architectures techniques, mais elle place les principes fondamentaux du Zero Trust au centre de cette politique.

Faisant suite à cette directive, l'OMB (*Office of Management and Budget*) américain a publié en septembre 2021 un document intitulé « Moving the U.S. Government Towards Zero Trust Cybersecurity Principles »[47] qui définit une stratégie d'adoption de l'architecture Zero Trust d'un point de vue technique. Les lignes directrices de cette stratégie pourraient parfaitement être adaptées aux besoins de la plupart des organisations.

On pourrait donc imaginer baser la protection technique d'un SI (pour au moins atteindre des objectifs de disponibilité, de confidentialité, d'intégrité et d'authenticité) entièrement sur un modèle Zero Trust, au plus près des ressources à protéger, mais cela obligerait à mettre la gestion des identités au centre du fonctionnement de l'entreprise et de ses valeurs alors que c'est souvent le parent pauvre de la SSI.

Depuis début 2022, la norme ISO 27002 a évolué en profondeur en prenant le titre de « Sécurité de l'information, cybersécurité et protection de la vie privée – Mesures de sécurité

---

[41] *Advanced Persistent Threat,* cf. Glossaire

[42] https://www.beyondcorp.com/

[43] Voir « *BeyondCorp, A New Approach to Enterprise Security* » https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf

[44] Cf. « *Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft* » https://www.microsoft.com/en-us/download/details.aspx?id=36036

[45] Executive Order on Improving the Nation's Cybersecurity https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[46] Cette directive a été complétée en janvier 2022 par une feuille de route fixant la date limite mise en œuvre de ces objectifs à fin 2024 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[47] https://zerotrust.cyber.gov/downloads/Office of Management and Budget - Federal Zero Trust Strategy - DRAFT For Public Comment - 2021-09-07.pdf

de l'information ». Cette nouvelle version comprend 34 mesures technologiques, les autres catégories de mesures portant sur l'organisation, les personnes ou la sécurité physique. Il est intéressant de noter que l'application stricte des principes du Zero Trust décrits dans ce dossier technique permet de couvrir directement environ la moitié seulement de ces mesures technologiques. On pourrait donc penser que baser sa politique de sécurité technique entièrement sur le Zero Trust est très insuffisant, par exemple dans le cadre d'une certification ISO 27001[48]. Mais en observant quelles mesures de sécurité technologiques de la norme ne sont pas directement couvertes par le Zero Trust, on s'aperçoit que ce sont plus des mesures liées à l'organisation ou à des bonnes pratiques informatiques au sens large (ITIL) que de la pure « sécurité technique (ou technologique) » : sécurisation, test et audit des développements, *capacity planning*, redondance, sauvegardes, planification et gestion des changements, etc. En tout état de cause, aucune des mesures de sécurité détaillées dans la norme ISO 27002 n'entre en contradiction avec les principes du Zero Trust.

Cependant, même si l'approche Zero Trust couvre et valide intrinsèquement un grand nombre de règles d'hygiène informatique promulguées par l'ANSSI, notamment la défense en profondeur[49], la réglementation actuelle impose le cloisonnement réseau renforcé sur les périmètres dits « sensibles ». En effet, la PSSI[50] est bâtie à partir d'objectifs d'entreprise, tout en s'appuyant sur des aspects réglementaires (RGPD, NIS 2, RGS, etc.) et normatifs (famille ISO 27000, NIST, etc.). D'un point de vue stratégique, il est possible d'exiger de renforcer la SSI autour des identités, du contrôle d'accès, des données, des postes de travail, etc. Cela se traduirait certainement dans certains cas par l'adoption d'une démarche Zero Trust dans le plan d'action opérationnel. De plus, la PSSI est souvent initiée à partir d'analyses de risques métiers (avec une vision stratégique et opérationnelle des chemins d'attaques), et dans le plan d'action de traitement des risques – qui est adossé parfois à la PSSI – la défense périmétrique n'est plus toujours suffisante.

La question est de savoir s'il est possible (ou nécessaire) de continuer pour certains SI à adopter une défense périmétrique et pour d'autres SI à aller vers le modèle Zero Trust. Baser entièrement sa PSSI sur ce modèle est donc une question de risques, de coût et de maturité (des solutions et des organisations). Ces points seront développés dans les sections suivantes.

5.2 Le Zero Trust est-il uniquement un projet technique ?

Au-delà des évolutions techniques nécessaires pour mettre en œuvre les principes du Zero Trust, quatre évolutions de nature organisationnelle sont essentielles à engager pour la réussite de cette adoption :

- une évolution de la culture sécurité auprès des acteurs principaux de la sécurité ;
- le soutien du projet par les parties prenantes de l'organisation jusqu'au plus haut niveau ;
- la classification des informations en vue de déterminer leur besoin de protection ;
- l'implication des équipes métiers et la gestion du changement auprès des utilisateurs finaux.

[48] Rappelons que l'annexe A de la norme ISO 27001, qui reprend les mesures de sécurité de la norme ISO 27002, est normative, donc d'application obligatoire pour assurer la conformité dans le cadre d'une certification ; les utilisateurs peuvent mettre en œuvre des mesures de sécurité différentes, mais doivent les comparer à celles de la 27002 (cf. ISO 27001 § 6.1.3 c) et apporter une justification de leur exclusion (cf. ISO 27001 § 6.1.3 d).

[49] L'ANSSI définit en effet le Zero Trust comme « ***de la défense en profondeur, dynamique et automatisée*** » https://2022.cesar-conference.org/program-media/CESAR-2022_keynote-ZT_slide-deck.pdf

[50] Politique de sécurité du système d'information

En premier lieu, il est nécessaire de **faire évoluer la culture sécurité** auprès des acteurs principaux de la sécurité dont les architectes SI. En effet, la combinaison des différents principes nécessite une information plus poussée pour éviter d'avoir une vision trop partielle sur le sujet. Il est essentiel de les sensibiliser et de les former au bon niveau afin d'éviter de mauvaises interprétations et de faire des raccourcis.

Un raccourci souvent entendu parmi des acteurs sécurité : *« Une application qui est exposée sur Internet et met en œuvre une authentification multifacteur est Zero Trust. »* Cette formulation est trop limitative. Les chapitres précédents du document démontrent en quoi cela est forcément insuffisant et ne permet pas de répondre à l'ensemble des risques et prédicats d'une architecture Zero Trust, notamment la présupposition de l'attaque réussie.

Un autre raccourci souvent entendu : *« Cette application est trop sensible, il est donc impossible de l'exposer sur Internet selon le modèle Zero Trust. »* Là encore, il est désormais démontré que des périmètres sensibles (encore reste-t-il à définir et s'accorder sur ce terme, cf. section suivante) sont exposés sur Internet et la mise en œuvre d'une architecture Zero Trust peut aider à réduire les risques associés, en délaissant les mécanismes de sécurité basés sur le cloisonnement périmétrique réseau et en renforçant la sécurité sur les extrémités de la connexion, avec d'une part un renforcement de la vérification de l'identité et de l'appareil de l'accédant et d'autre part, une analyse temps réel des comportements du côté de la ressource accédée.

Pour éviter ces raccourcis et les erreurs tactiques qui pourraient en être la conséquence, l'accompagnement des acteurs de la sécurité et de l'architecture ainsi que la mise à niveau des connaissances sur l'intégralité des principes est essentielle. Attention à bien inclure les acteurs qui ne sont pas en lien direct avec la technique comme les acteurs en charge des analyses de risques et, bien sûr, les RSSI. Et surtout, n'oubliez pas les prestataires !

Par ailleurs, la mise en œuvre des principes de Zero Trust nécessite un accompagnement et une adaptation des équipes. En effet, la mise en place des composants techniques, de manière similaire à ceux de la sécurité périmétrique, nécessite des compétences spécifiques. Ces compétences sont différentes de celles recherchées plus traditionnellement : un ingénieur sécurité réseau n'aura pas forcément les compétences pour déployer un XDR ou paramétrer les différentes briques. La formation aux nouvelles compétences techniques SSI est nécessaire en parallèle d'une réorganisation des équipes et du recrutement des nouveaux talents qui sont à anticiper.

D'après les experts et analystes de Gartner, « *60 % des organisations adopteront une stratégie Zero Trust comme point de départ pour leur cybersécurité en 2025, mais plus de la moitié d'entre elles n'en tireront aucun bénéfice* »[51], car elles ne sauront pas convaincre leur top management de l'intérêt de cette démarche. Pourtant le Zero Trust permet de réconcilier la résilience et l'agilité, ce qui représente une réelle opportunité de développement du business et pas seulement un énième projet technique de cybersécurité. Les RSSI doivent mettre ce point en avant **au plus haut niveau de leur hiérarchie et impliquer celle-ci** dans le programme, afin de s'assurer de son soutien, indispensable à la réussite du projet.

La mise en œuvre des principes Zero Trust va également de pair avec une **classification** des informations et fonctionnalités accédées. Il faudra déployer un programme de classification, notamment des documents. Dans ce cadre, les utilisateurs finaux doivent tous être formés pour être en mesure de la déterminer. Une compétence pas simple à acquérir. Elle demande la mise en œuvre d'une réelle gestion du changement, au sein des organisations, peu habituées à cet exercice. Attention, un simple e-mail de présentation et un e-learning ne suffiront pas ! Enfin, les maîtrises d'ouvrage métier seront également sollicitées dans le cadre de la classification des données manipulées par les applications métiers.

[51] https://www.gartner.com/en/newsroom/press-releases/2022-09-12-gartner-security-and-risk-management-summit-emea-2022-day-1-highlights

L'implication des équipes métiers est essentielle dans cette démarche Zero Trust. Celles-ci jouent un rôle déterminant dans la classification des données, mais devront également prendre en compte les nouveaux modes de fonctionnement, y compris techniques, par exemple sur la gestion des identités et du contrôle d'accès aux applications, notamment dans le cadre de l'expression des besoins fonctionnels d'évolutions d'applications ou de création de nouvelles.

La gestion du changement que cela implique, notamment auprès des équipes métiers, doit intégrer les utilisateurs finaux. Dans ce cadre, le concours des équipes de communication interne doit être envisagé.

En synthèse, l'approche Zero Trust n'est pas uniquement un projet technique mais bel et bien un **projet d'entreprise** auquel bon nombre d'entités et de ressources participent, notamment les métiers. Le Zero Trust impose une vision transverse et globale de la sécurité, pour garantir le succès de son implémentation.

5.3 Peut-on faire du Zero Trust sur des périmètres sensibles ?

Tout d'abord, chaque organisation doit définir le terme sensible selon son propre contexte. La sensibilité doit être déterminée en fonction des activités métiers, des cadres réglementaires à appliquer, etc. Une analyse de risque transverse permet de déterminer des niveaux de sensibilité.

Trois types de périmètres sensibles se distinguent :

- le premier, de nature informatique, relatif à l'administration des systèmes ;
- le deuxième, sensible en raison des impacts critiques qu'un sinistre ferait peser sur l'entité ou sur les personnes dont les données sont traitées, mais non soumis à une réglementation spécifique de sécurité ;
- le troisième, sensible car soumis à une obligation réglementaire spécifique, qu'il s'agisse d'un SIIV (LPM), d'un SIE/EE (Directive européenne NISv1 et NISv2 et leur transposition) ou bien d'un SI classifié au sens de la protection du secret de la défense nationale.

Sur chacun des périmètres, l'opportunité et le bénéfice attendu de Zero Trust doivent être évalués.

Pour ce qui relève de l'administration des systèmes, un consensus semble émerger :

Si l'on prend en considération l'approche historique des systèmes *on-premises* en termes de périmètre, les risques associés à de mauvaises pratiques d'administration avaient des impacts limités. Cependant, avec l'évolution vers les technologies cloud, la surface d'attaque augmente mécaniquement, en particulier par l'utilisation d'Internet pour faire transiter les flux internes de l'entreprise. Les ressources, les comptes et les secrets d'administration deviennent particulièrement attractifs pour les attaquants, car ils leur permettent de compromettre un système de manière généralisée et discrète. Il est donc impératif de réfléchir attentivement à la protection des accès aux interfaces d'administration afin de garantir un niveau de sécurité optimal pour le système. Les recommandations relatives à l'administration sécurisée des SI de l'ANSSI[52] proposent des principes techniques et d'architecture qu'il convient d'adapter d'une part au principe du Zero Trust et d'autre part au choix d'architecture technique de l'entreprise pour sa transformation.

[52] https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/

L'approche Zero Trust peut représenter une opportunité pour renforcer la sécurité des ressources d'administration et, par conséquent, la sécurité de son système d'information.

Il est toutefois admis qu'exposer sur un réseau public tel qu'Internet les systèmes donnant un accès direct aux machines présente des risques difficiles à accepter. La bonne pratique est alors la suivante :

- interdire les accès « directs »[53] sur les services d'administration depuis Internet ;
- utiliser des protocoles et mécanismes cryptographiques qui assurent la confidentialité et l'authentification mutuelle des communications, conformément aux guides de l'ANSSI[54] ;
- mettre en œuvre des interfaces d'administration, web par exemple, permettant d'appliquer un contrôle d'accès et des privilèges en fonction des périmètres techniques de chaque équipe d'administration.

L'accès à ces interfaces d'administration serait alors protégé par des mécanismes de sécurité en suivant les principes de Zero Trust. C'est, par exemple, ce que sont en mesure de proposer les principaux fournisseurs de services cloud. Cependant, attention, toutes les options de sécurité utiles ou nécessaires ne sont pas forcément incluses avec les premiers niveaux de souscription.

Pour les systèmes sensibles en raison du risque qu'ils font peser sur l'entité ou sur les personnes dont sont traitées les données, le sujet est un peu plus ouvert. Si l'exposition sur Internet est nécessaire ou demandée par le métier, alors la mise en œuvre de mécanismes Zero Trust sera ici impérative. Pour ce type de système, une défense en profondeur basée sur des règles statiques ne suffira pas à combattre l'exposition forte du système et les apports de la vérification dynamique apportés par le Zero Trust, ainsi qu'une supervision sécurité amplifiée, renforceront le niveau de sécurité.

Enfin, en ce qui concerne **les périmètres soumis à une** réglementation **spécifique,** le sujet est finalement assez simple à traiter. En première lecture, il n'est pas possible de respecter les exigences de cloisonnement des différentes réglementations (II 901, IGI 1300, LPM, NIS) en mettant en œuvre une architecture cloud exposée sur un réseau public, y compris en appliquant les mécanismes Zero Trust. Cependant, les réglementations NIS et LPM n'interdisent pas l'usage de services cloud publics, mais les exigences sur la protection des systèmes et des données ne sont aujourd'hui pas atteignables sur la base des seules offres cloud commerciales « généralistes » disponibles sur le marché. Les offres qualifiées SecNumCloud offrent un certain nombre de garanties (notamment protection des données contre les lois extra-européennes et confiance dans l'administration de l'environnement cloud) qui ne sont pas incompatibles avec la réglementation, sans toutefois être suffisantes en matière de mesures à mettre en œuvre.

À noter que dans tous les cas, les composants permettant le Zero Trust peuvent venir en complément de la sécurité périmétrique existante, en allant dans le sens de la « défense en profondeur » promue entre autres par l'ANSSI. Le rapport entre le bénéfice et le coût doit alors être évalué.

Toutefois, gardons en tête que l'instruction interministérielle n° 901, dans son article 19, ouvre la porte au non-respect strict d'une exigence avec une prise de risque ou la démonstration de la couverture du risque par la mise en œuvre d'autres moyens, par l'autorité d'homologation. Encore faudra-t-il trouver l'autorité qui prendra ce risque !

---

[53] On entend par administration directe tout type d'accès aux interfaces à privilèges permettant de gérer et modifier les configurations des matériels, des logiciels, des applications, etc., par exemple un accès *shell* sur les serveurs.

[54] « Règles et recommandations concernant les choix et le dimensionnement de mécanismes cryptographiques » et « Guide de sélection d'algorithmes cryptographiques » https://www.ssi.gouv.fr/guide/mecanismes-cryptographiques/

En conclusion, les périmètres sensibles, et notamment ceux soumis à la réglementation française, ne sont pas les meilleurs candidats pour démarrer un projet de migration en adoptant l'approche Zero Trust. Mis à part les cas de création d'un nouveau système d'information, il est plutôt recommandé de les traiter en dernier. Cela permettra de s'assurer que l'ensemble des mesures techniques et organisationnelles sont performantes, mais également que les différents acteurs disposent d'une maturité en matière de gestion des risques que cela représente, par expérience des sujets moins sensibles abordés auparavant.

5.4 Le modèle Zero Trust m'oblige-t-il à revoir ma politique de gestion des risques ?

Face à l'augmentation de la complexité et de la fréquence des attaques, les entreprises et les organisations ont majoritairement intégré une gestion des risques IT au même titre que ceux de nature financière, juridique, industrielle, etc.

Le modèle Zero Trust ne se cantonne pas à implémenter des mesures de sécurité pour traiter les risques.

En effet, le Zero Trust doit être appréhendé comme une transformation transverse et structurelle qui nécessite d'adapter la posture et la culture sécurité globalement au niveau de l'entreprise. Les politiques de sécurité et de gestion des risques devront alors détailler et décliner les objectifs et les apports du Zero Trust au sein de l'entreprise.

En plus d'imposer une transformation sur le plan de la gouvernance et de l'organisation, le Zero Trust impose de nouveaux principes qui vont exiger non seulement une compréhension globale des sujets, des ressources, des données, de l'automatisation et de l'orchestration, mais aussi une organisation performante qu'il conviendra de transformer progressivement selon une trajectoire.

Par exemple et comme indiqué plus haut, la classification des données et des applications est une des premières briques à mettre en place. Chaque application doit faire l'objet d'une classification en fonction de son usage et de sa criticité face aux risques évolutifs que connaît l'organisation. L'entreprise fixe alors les règles d'accès conditionnel aux applications par rapport à cette classification.

En outre, le Zero Trust permet d'appréhender la gestion des risques différemment, car le modèle de sécurité part du postulat que le réseau (interne) n'est pas de confiance et qu'il faut considérer les applications comme si elles étaient exposées sur Internet. Ce postulat qui « élimine » la notion de périmètre traditionnelle va permettre de renforcer les mesures de sécurité et de réduire l'exposition aux risques.

Les opportunités offertes par le Zero Trust peuvent cependant avoir pour conséquence une augmentation de la surface d'attaque sur les données et les traitements. Il convient donc d'apprécier les risques dans les plans de transformation Zero Trust au même titre que dans tout autre projet, sans excès de confiance.

Par ailleurs, et s'agissant des méthodes et normes en matière de gestion du risque, le Zero Trust ne vient pas modifier la mise en œuvre de méthodes telles qu'EBIOS Risk Manager ou encore la norme ISO 27005 décrivant les préconisations et les exigences pour la gestion des risques liés à la sécurité de l'information.

Pour conclure, le modèle Zero Trust n'oblige pas à revoir la politique de gestion des risques. Mais, selon les périmètres et les types d'applications, il va apporter de nouvelles mesures de remédiation dans les plans d'action consacrés au traitement des risques, et dans tous les cas le projet de transformation Zero Trust doit s'inscrire dans la démarche de gestion des risques de l'entreprise.

6 Maturité

6.1 Puis-je évaluer mon niveau de maturité Zero Trust par rapport à l'existant en sécurité ?

Déterminer le niveau de maturité du SI par rapport au modèle Zero Trust est un prérequis pour établir un plan d'action. Plusieurs approches complémentaires permettant d'évaluer ce niveau de maturité peuvent être utilisées.

Une première manière serait de s'appuyer sur le *Zero Trust Maturity Model* du CISA[55] (référentiel reposant sur cinq piliers, quatre niveaux de maturité définis), qui propose aux organisations une approche pragmatique pour catégoriser et inventorier les éléments présents sur un SI. Néanmoins, ce modèle aborde le concept du Zero Trust à un niveau trop abstrait pour savoir si les briques de sécurité mises en place sont suffisantes pour bien respecter les préconisations du modèle. L'approche du CISA n'est pas suffisamment détaillée pour aider une entreprise à rajouter les briques manquantes ou les éléments permettant de construire un plan d'action.

Une seconde approche serait d'identifier précisément les produits déjà en place dans le SI. En effet, une architecture Zero Trust est constituée d'un assemblage de briques techniques (IAM, MFA, EDR, etc.) dont certaines sont probablement préexistantes dans le SI. Les responsables des SI ou RSSI doivent en établir la liste : existe-t-il un gestionnaire d'identité pour accéder aux ressources du SI ? Y a-t-il un contrôle sur la provenance des connexions entrantes (établissement d'un contexte) avant d'autoriser l'accès au SI ? Les données stockées sont-elles chiffrées au repos ? En fonction des réponses, il est alors possible de déterminer le niveau de maturité du SI.

Enfin, rappelons que le Zero Trust est aussi un paradigme centré autour de la gouvernance. En complément de ces approches très techniques, on pourrait donc également s'assurer que d'un point de vue organisationnel ou opérationnel :

- les bonnes ressources humaines et processus sont bien en place pour garantir le fonctionnement de ce modèle. Avoir une architecture Zero Trust sans agir sur les alertes remontées revient à ne pas en appliquer le concept.
- les principes du Zero Trust en matière de gestion des droits et habilitations (IAM/IAG) sont respectés : principe de moindre privilège, besoin d'en connaître, séparation des responsabilités, etc. En bref, toute mesure partant du postulat de limiter la confiance accordée à un utilisateur identifié sur un réseau, un des principes fondamentaux du Zero Trust.

Chacune de ces trois approches permettra ainsi de cartographier l'ensemble des solutions tant techniques qu'organisationnelles en place sur le SI, et de définir un niveau de maturité global.

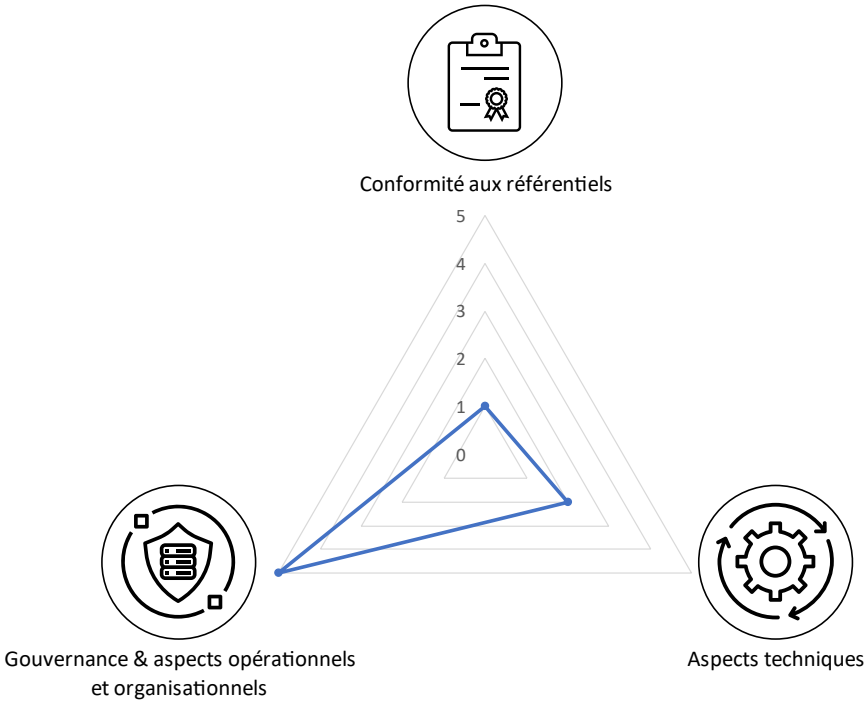
[55] Le CISA est aujourd'hui l'une des seules administrations à proposer des référentiels à suivre, en dehors des entreprises privées, et en ne prenant pas en compte la note de l'ANSSI, « Le Modèle Zero Trust », parue en avril 2021.

6.2 Finalement, faites-vous du Zero Trust sans le savoir ?

Nous avons donc vu que trois indicateurs de maturité peuvent accompagner les directions des SI et les RSSI à définir leur niveau de maturité Zero Trust :

1. un indicateur sur la conformité aux référentiels existants (*Zero Trust Network Architecture*, *Zero Trust Maturity Model* du CISA) ;
2. un indicateur sur la gouvernance, les aspects opérationnels et organisationnels ainsi que le niveau d'adhésion aux principes du Zero Trust ;
3. un indicateur sur les aspects techniques, évaluant le degré de mise en œuvre des briques Zero Trust sur un SI.

Il est possible d'avoir les prémices de l'approche Zero Trust même si certains composants ou concepts organisationnels ou opérationnels de votre SI ne sont pas explicitement identifiés comme tels. Si ces éléments répondent à l'un des concepts définis précédemment, cela facilite ensuite la mise en place de l'approche complète.



Ci-dessus, un schéma sous forme de graphique radar qui montre un niveau de maturité selon les trois indicateurs. Les échelles de notes sont à définir en fonction de l'organisation de l'entreprise.

Il devient alors plus facile d'identifier les lacunes ou les éléments manquants et ainsi prioriser les axes de travail pour atteindre un modèle Zero Trust complet. La démarche consiste à définir, pour chaque indicateur, un questionnaire qui permettra de déterminer le niveau de maturité. Pour chaque question, un nombre de points est « gagné » si la mesure est appliquée. Le score total obtenu en additionnant les points permet de placer le SI dans un niveau de maturité (niveau standard/avancé/optimal).

Le tableau suivant donne un exemple pour le critère « aspects techniques » sur les thèmes de l'identité (pilier du CISA). Un tableau similaire est à créer pour l'ensemble des piliers et des indicateurs.

Aspects techniques

Questions sur l'identité	Points	Score obtenu
Disposez-vous d'un moyen d'authentification fiable ?		3
Je dispose d'une authentification multifacteurs	1	1
Je dispose d'une authentification multifacteurs fondée sur un dispositif matériel	3	0
Mon dispositif matériel pour le MFA est délivré en face à face	3	0
Mon organisation met en œuvre une politique stricte de renouvellement des moyens d'authentification	2	2
Analysez-vous le contexte de connexion de vos utilisateurs avant de leur donner accès à vos ressources ?		3
Je n'autorise que certaines IP à accéder à mon SI, dans des plages horaires bien définies.	1	1
J'utilise une analyse de la « e-réputation » des utilisateurs pour cibler mes actions de contrôle	3	0
Je vérifie que l'emplacement de connexion de l'utilisateur est vraisemblable (problème du « voyage impossible »)	2	2
J'utilise un moteur d'analyse des accès fondé sur l'intelligence artificielle pour disposer d'un « profil de connexion » des utilisateurs autorisés	3	0
Standard : de 1 à 6 pts / Avancé : de 7 à 12 pts / Optimal : de 13 à 18 pts	Total	6
	Niveau obtenu	STANDARD

Les notes obtenues ici permettent de déduire un plan d'action comprenant les principaux thèmes lacunaires identifiés, en fonction des objectifs stratégiques.

6.3 Migration progressive vers le Zero Trust : comment, quelles briques, quel périmètre ?

L'approche Zero Trust, comme abordée dans les questions précédentes, suppose de pouvoir déterminer les habilitations d'un utilisateur en fonction de son identité, de son contexte de connexion. Elle suppose aussi qu'il est possible de protéger les ressources du SI et particulièrement les données, y compris vis-à-vis d'un accès par des acteurs « en interne » (dans le langage de la protection périmétrique).

Bien que la mise en œuvre du Zero Trust, notamment via une architecture conforme aux standards NIST/CISA, ne se limite pas à la mise en place d'outils et de fonctions de confiance isolées, mais requiert des logiciels spécifiques, on en déduit que certaines briques « de base » sont pour le moins indispensables :

- comment identifier à coup sûr un utilisateur, si le système d'authentification repose sur un mot de passe partagé ?
- comment déterminer si le comportement de connexion de l'utilisateur est anormal, si aucune solution de traçabilité/analyse des accès n'est déployée ?
- comment assurer le principe du besoin d'en connaître ou le principe de moindre privilège si les données circulent en clair sur des réseaux partagés ?

On peut arriver à la conclusion que le déploiement de briques technologiques permettant de répondre à ces questions, comme des systèmes d'authentification forte, des communications chiffrées de bout en bout, des systèmes d'analyse des traces d'accès, etc., peut constituer une avancée vers le Zero Trust.

Sans être suffisantes, ces briques et fonctions de sécurité augmentent néanmoins le niveau de maturité en proposant une base saine pour l'atteinte de la cible Zero Trust.

En résumé :

- l'approche doit être progressive ; on ne peut pas repenser la sécurité d'un SI en imaginant qu'une simple brique technique va permettre de « devenir » Zero Trust.
- on doit prendre en compte l'existant (détermination de son niveau de maturité, cf. section « 6.1 Puis-je évaluer mon niveau de maturité Zero Trust par rapport à l'existant en sécurité ? ») et définir quels sont les thèmes à traiter en priorité.
- on définira si possible des *quick wins* pour lancer et crédibiliser le projet, par exemple la mise en place d'une authentification multifacteur sur les applications critiques.
- on doit ensuite définir les briques techniques (telles que décrites précédemment) à utiliser pour implémenter en s'appuyant sur le découpage en piliers tel que défini en section « 2.4 Existe-t-il un modèle d'architecture Zero Trust ? ».
- on devra finalement définir une feuille de route qui présentera les différents projets à mener, calés dans le temps en fonction des priorités définies.
- on pourra alors lancer les différents projets en définissant et en suivant les indicateurs de progression (KPI) pour suivre le déroulement de chaque projet et justifier du travail accompli.

6.4 En conclusion, quels sont les points d'attention (à quelles difficultés peut-on s'attendre) ?

L'obstacle majeur auquel vont se confronter les organisations est la compréhension, la traduction en déclinaison opérationnelle et en matière de conformité de ce qu'est le Zero Trust. C'est exactement l'objectif de ce document : vous aider au fil des pages à avoir une vision plus claire de ce paradigme.

Un des premiers défis opérationnels est d'avoir une excellente connaissance de son SI, avec notamment l'ensemble des référentiels à jour des actifs, utilisateurs, outils et applications. Cet exercice fastidieux demande beaucoup de temps et de rigueur pour être efficace dans la durée.

En effet, l'aspect primordial du Zero Trust est de repenser et renforcer la gestion des accès et des identités. Et c'est sur ces actifs, utilisateurs, outils et applications, qu'il va être appliqué. Il est donc primordial de tenir continuellement à jour l'inventaire de ces éléments.

Un autre défi majeur est d'être en mesure d'authentifier l'ensemble des accès (utilisateurs, machines, robots) de manière systématique. De nombreux systèmes ou méthodes de travail n'ont pas été pensés initialement avec cette approche, et il est parfois difficile – voire impossible –, de pouvoir authentifier un utilisateur ou un système.

Repenser cette nouvelle gestion demande donc beaucoup de temps, aussi bien dans la mise en place au travers des évolutions de processus et des outils, que de la culture d'entreprise. Aujourd'hui, encore de trop nombreuses organisations ont, par exemple, des développeurs avec les droits « administrateur » sur le poste, car c'est plus « facile et rapide pour travailler ».

Ainsi, l'accompagnement au changement va être primordial dans le cadre du déploiement et de l'adoption du Zero Trust par les entreprises. Cela permettra une compréhension et adhésion forte des collaborateurs et évitera aussi les déviances d'utilisation du système par les utilisateurs réfractaires.

Pour examiner et détecter les anomalies, il sera nécessaire d'être en mesure d'analyser les événements de sécurité, notamment à l'aide d'un SIEM ou d'un XDR.

Un autre défi pour les entreprises sera de constituer une équipe d'experts dans un marché hypertendu où les compétences disponibles sont rares.

Et comme brièvement abordé précédemment, un dernier défi sera de composer avec le temps.

Rappelons-le, le Zero Trust est avant tout une évolution du prisme « sécurité » renforçant notamment l'approche de l'identification, de l'authentification et des autorisations d'accès à une ressource ou une donnée. Cette évolution est la réponse à la nature actuelle du paysage cyber où nous devons faire face à des menaces d'attaques régulières. Et nous avons besoin de renforcer nos systèmes d'information le plus rapidement possible.

Or l'adoption et la mise en place du Zero Trust demandent beaucoup de temps d'analyse, de conception, de préparation et de ressources (humaines et financières). Et ces évolutions ne peuvent voir le jour au sein des grandes organisations que sous forme de projets pluriannuels.

7 Glossaire

API	Une API, ou interface de programmation d'applications, est un ensemble de règles et de protocoles qui définissent la manière dont deux programmes logiciels peuvent communiquer entre eux. Elle spécifie comment les composants logiciels doivent interagir et permet l'interopérabilité entre différents systèmes.
APT	Une menace persistante avancée (APT – *Advanced Persistent Threat*) est un type de cyberattaque dans laquelle un attaquant obtient un accès non autorisé à un réseau et reste non détecté pendant une période prolongée pendant laquelle il recueille des informations sensibles ou perturbe les opérations. Les attaques APT sont généralement ciblées et sophistiquées, et sont souvent menées par des acteurs étatiques ou d'autres organisations hautement qualifiées et bien financées.
CASB	Le *Cloud Access Security Broker* (CASB) est un type de logiciel de sécurité qui aide les organisations à se protéger contre les menaces et à appliquer des politiques de sécurité lorsqu'elles utilisent des services en nuage. Les solutions CASB offrent généralement une gamme de fonctionnalités telles que la prévention des pertes de données (voir DLP), la protection contre les cybermenaces et les politiques pour aider les organisations à sécuriser leur utilisation des services en nuage.
CIEM	La gestion des droits de l'infrastructure en nuage (CIEM – *Cloud Infrastructure Entitlement Management*) est un ensemble de processus et d'outils utilisés pour gérer et contrôler l'accès aux ressources en nuage. Un CIEM aide les organisations à s'assurer que seuls les utilisateurs autorisés ont accès à leurs ressources en nuage, et qu'ils ne peuvent effectuer que les actions qu'ils sont autorisés à effectuer.
CNAPP	Une plateforme de protection des applications natives du cloud (CNAPP – *Cloud Native Application Platform*) est un type de solution de sécurité conçue pour protéger les applications natives du cloud contre les cybermenaces. Les applications natives du cloud sont conçues pour être construites, déployées et exécutées dans un environnement cloud, et elles utilisent souvent les technologies de microservices et de conteneurisation.
CSPM	La gestion de la posture de sécurité du cloud (CSPM – *Cloud Security Posture Management*) est un ensemble de processus et d'outils qui sont utilisés pour garantir que les ressources disponibles dans le cloud d'une organisation sont sécurisées et conformes aux normes et politiques de sécurité pertinentes. Le CSPM aide les organisations à évaluer la sécurité de leur infrastructure dans le cloud et à identifier toute vulnérabilité ou mauvaise configuration qui pourrait compromettre la sécurité de leurs ressources.
CWPP	Une plateforme de protection des charges de travail en cloud (CWPP – *Cloud Workload Protection Platform*) est un type de solution de sécurité conçue pour protéger les charges de travail en cloud contre les cybermenaces. Les CWPP offrent généralement un éventail de fonctionnalités, notamment la possibilité de rechercher les failles de sécurité dans les systèmes en cloud, de contrôler la conformité des configurations des ressources en cloud avec les normes de sécurité et d'alerter les administrateurs des risques de sécurité potentiels.

DevSecOps	DevSecOps est un ensemble de pratiques et de principes qui visent à intégrer la sécurité dans le processus de développement des applications logicielles. Il implique la collaboration du développement, de la sécurité et de l'administration des systèmes d'information ainsi que des équipes d'exploitation tout au long du cycle de vie du développement logiciel afin de garantir que la sécurité est prise en compte à chaque étape du processus.
DLP	La prévention de la perte de données (DLP – *Data Loss Prevention*) est une technologie de sécurité conçue pour empêcher l'utilisation non autorisée des données, la divulgation de données sensibles ou confidentielles. Les systèmes DLP comprennent généralement une série de fonctionnalités telles que l'inspection du contenu, le chiffrement et le blocage pour aider à se protéger contre les fuites de données.
EDR	La détection et la réponse aux attaques pour les points d'extrémité, c'est-à-dire les ordinateurs des utilisateurs (EDR – *Endpoint Detection and Response*), est un type de solution de sécurité conçu pour protéger les dispositifs d'extrémité, tels que les ordinateurs mais aussi les serveurs, contre les cybermenaces.
HSM	Boitier matériel destiné au stockage, à la gestion et à l'utilisation sécurisés de clés cryptographiques, un HSM (*Hardware Security Module*) est un composant externe pouvant être directement relié à un système hôte ou partagé entre plusieurs hôtes, au sein d'un centre de données, par exemple.
IaaS	L'infrastructure en tant que service (IaaS – *Infrastructure as a Service*) est un type de service d'informatique en cloud qui permet aux utilisateurs d'accéder à un large éventail de ressources informatiques, notamment des serveurs, du stockage et des réseaux, par l'intermédiaire de l'Internet.
IAM / IAG	L'IAM (*Identity and Access Management*), ou gestion des identités et des accès, est un ensemble de services et de fonctionnalités qui vous permettent de gérer l'accès aux ressources de manière sécurisée et centralisée. L'IAG traite de la gouvernance de l'IAM.
IDaaS	IDaaS est l'abréviation de *Identity as a Service* (identité en tant que service). Il s'agit d'un type de service basé sur le cloud qui fournit une plateforme pour gérer et sécuriser les identités des utilisateurs et l'accès aux ressources.
IGI 1300	Consécutive au décret n° 2019-1271 du 2 décembre 2019 relatif aux modalités de classification et de protection du secret de la défense nationale, l'instruction générale interministérielle du 9 août 2021 sur la protection du secret de la défense nationale (IGI 1300) détermine les rôles et responsabilités ainsi que les exigences liées à la gestion du cycle de vie d'une information ou d'un support classifié.
II 901	Cette instruction définit les objectifs et les règles relatifs à la protection des systèmes d'information sensibles, notamment ceux traitant des informations portant la mention « Diffusion Restreinte ».
LPM	Loi de programmation militaire (voir OIV / SIIV).
Micro-services	Les microservices sont un paradigme architectural informatique permettant de créer des applications logicielles composées de petits services, indépendants et modulaires qui travaillent ensemble pour atteindre un objectif plus large. Chaque microservice est conçu pour être autonome et pour gérer un ensemble spécifique de tâches, et peut être développé, déployé et mis à l'échelle indépendamment des autres services.

MFA	L'authentification multifacteur (MFA – *Multi Factor Authentication*) est un processus de sécurité qui exige plus d'une méthode d'authentification à partir de catégories indépendantes d'informations d'identification pour vérifier l'identité de l'utilisateur.
NAC	Le contrôle d'accès au réseau (NAC – *Network Access Control*) est une technologie de sécurité utilisée pour s'assurer que seuls les dispositifs autorisés peuvent accéder à un réseau. Les systèmes NAC comprennent généralement une série de fonctions telles que l'authentification, l'application de politiques et des capacités de quarantaine pour aider à sécuriser un réseau et empêcher tout accès non autorisé.
NIS / NIS 2	La directive européenne NIS, adoptée par les institutions européennes en 2016 et désormais retranscrite dans le droit français, édicte des règles qui doivent être respectées par l'ensemble des OSE (voir ce terme) de l'UE. NIS 2, publiée en décembre 2022, remplace et abroge la directive NIS de 2016. Elle renforce la gestion des risques liés à la cybersécurité et introduit des obligations de déclaration dans des secteurs tels que l'énergie, les transports, la santé et les infrastructures numériques.
NIST	*National Institute of Standards and Technology*, agence gouvernementale américaine établissant des normes et bonnes pratiques technologiques, notamment dans le domaine de la cybersécurité.
OIV / OSE	Les OIV (opérateurs d'importance vitale) opèrent des installations « jugées indispensables pour la survie de la nation » et doivent se conformer à un ensemble de règles émises par l'État français, au travers de la LPM. Les OSE (opérateurs de services essentiels) fournissent « un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société » et doivent quant à eux se conformer aux réglementations émises par l'Union européenne au travers de la directive NIS/NIS 2 (voir ce terme).
On-premises	Le terme « *on-premises* » (sur site) fait référence à une infrastructure qui est installée et fonctionne sur du matériel appartenant à l'organisation qui l'utilise et exploité par celle-ci. Les systèmes sur site sont généralement situés dans les locaux de l'organisation, comme un centre de données (datacenter) ou une salle de serveurs.
PaaS	La plateforme en tant que service (PaaS – *Platform as a Service*) est un type de service de *cloud computing* qui fournit aux utilisateurs une plateforme pour développer, déployer et exécuter des applications. Les fournisseurs de PaaS proposent généralement une gamme d'outils et de services, tels que des environnements de développement, des bases de données et des intergiciels (*middleware*), que les développeurs peuvent utiliser pour créer et déployer des applications.
RGPD	Règlement général sur la protection des données (RGPD) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Ses dispositions sont directement applicables dans l'ensemble des 27 États membres de l'Union européenne depuis le 25 mai 2018.

SaaS	Le logiciel en tant que service (*SaaS – Software as a Service*) est un type de service informatique en nuage qui permet aux utilisateurs d'accéder à des applications logicielles et de les utiliser sur Internet, généralement sur la base d'un abonnement. Les applications SaaS sont hébergées par le fournisseur de services et sont accessibles via un navigateur internet, plutôt que d'être installées localement sur l'ordinateur de l'utilisateur.
SAML	SAML (*Security Assertion Markup Language*) est un protocole standard utilisé pour l'échange sécurisé d'informations sur la sécurité, les données d'authentification et d'autorisation entre les systèmes. SAML est souvent utilisé pour permettre l'authentification unique (SSO) entre différents systèmes, ce qui permet aux utilisateurs d'utiliser un seul ensemble d'informations d'identification pour accéder à plusieurs applications.
SCIM	SCIM (*System for Cross-domain Identity Management*) est un protocole standard utilisé pour automatiser l'échange d'informations sur l'identité des utilisateurs entre les systèmes. SCIM est conçu pour simplifier le processus de gestion des identités des utilisateurs dans différents systèmes et organisations, et réduire la complexité et les frais liés à cette gestion.
SIEM	La gestion des informations et des événements de sécurité (SIEM – *Security Incidents and Events Management*) est un type de logiciel de sécurité qui collecte et analyse les données provenant de diverses sources (telles que les journaux, le trafic réseau et les mises à jour du système) afin d'identifier les menaces potentielles pour la sécurité.
SIIV / SIIE	Système d'information d'importance vitale ou essentielle (voir OIV / OSE).
SOC	Un centre d'opérations de sécurité (SOC – *Security Operation Center*) est une équipe ou une installation spécialisée chargée de surveiller et d'analyser le dispositif de sécurité d'une organisation, d'identifier les menaces potentielles pour la sécurité et de répondre aux incidents de sécurité.
SSO	L'authentification unique (SSO – *Single Sign On*) est un processus d'authentification qui permet aux utilisateurs d'accéder à plusieurs applications ou systèmes à l'aide d'un seul ensemble d'informations d'identification. Le SSO simplifie le processus de connexion pour les utilisateurs, qui ne doivent saisir leurs informations d'identification qu'une seule fois afin d'accéder à plusieurs applications ou systèmes.
TPM	Composant matériel destiné principalement au stockage sécurisé de clés cryptographiques, un TPM (*Trusted Platform Module*) est une puce intégrée dans le système qu'elle protège contrairement à un HSM (voir ce terme) qui est un composant externe beaucoup plus puissant.
VPN	Un réseau privé virtuel (VPN – *Virtual Private Network*) est une technologie qui crée une connexion sécurisée entre deux ordinateurs ou appareils sur Internet. Les VPN utilisent le chiffrement pour sécuriser les données qui sont transmises entre les deux points et pour masquer l'adresse IP de l'utilisateur, ce qui rend la communication plus sûre et plus privée.
XDR	*Extended Detection and Response* – Évolution de l'EDR qui collecte et met automatiquement en corrélation des données sur plusieurs couches de sécurité.
ZTA / ZTNA	Zero Trust Architecture / Zero Trust Network Architecture (cf. section 4.4.)

Tour Eria – 5, rue Bellini
92821 Puteaux Cedex
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

clusif.fr