Microsoft

Comment initier votre projet de transformation Zero Trust ?

En 11 conseils simples et pratiques

Juillet 2021

Microsoft France

Rédaction : Equipe « Initiative Zero Trust », France

Contributeurs/Relecteurs : Jean-Yves Grasset, Arnaud Jumelet, Félix Ndouga, Maxime Roques, Guillaume Aubert, Bastien Simon, Guillaume Bordier, India Giblain, Marc Gardette, Etienne Lacour, Jean-Marc Guégan, Martin Flichy

Table des matières

Introduction

La période actuelle est propice à la remise en cause de la manière dont la sécurité est prise en charge par les entreprises, car il est flagrant que l'empilement des solutions de sécurité ne protège plus contre la prolifération des attaques en raison de leur plus grande complexité. De plus, les attaquants profitent de la pandémie COVID-19 pour mener des attaques opportunistes qui collent à l'actualité comme le détaille le document MICROSOFT DIGITAL DEFENSE REPORT de septembre 2020.

L'extension de la menace est malheureusement confirmée par la recrudescence des attaques auxquelles font face les organisations. Selon un communiqué de presse commun de l'ANSSI et son homologue allemand le BSI de décembre 2020[1], je cite : « *dans la continuité d'une trajectoire initiée en 2019, le nombre de cyberattaques a explosé : le nombre de victimes a ainsi été multiplié par 4 en un an* ». L'agence (ANSSI) a dénombré 200 cyberattaques contre des opérateurs d'importance vitale (OIV) en 2020, soit quatre fois plus qu'en 2019. "*Ces attaques visent des entreprises du public ou du privé*".

L'autre élément majeur est la bascule généralisée des employés en télétravail, un scénario qui, pour de nombreuses entreprises et organisations, n'avait pas été anticipé. Ceci a bousculé les principes bien acquis de la sécurité périmétrique par une exposition plus forte des postes de travail situés en-dehors des frontières physiques de l'entreprise.

La prise en compte du modèle Zero Trust

Comme l'analyse très justement L'ESSENTIEL DE LA SECURITE NUMERIQUE POUR LES DIRIGEANTS ET LES DIRIGEANTES, « *Avec un système d'information totalement étendu et très fragmenté, désormais porté par le cloud et avec des équipements mobiles dispersés, la sécurité numérique fait face à une nouvelle difficulté pour repenser ses modes de contrôle et de protection en profondeur* ». Il est impératif de revoir en profondeur la sécurité de son système d'information étendu pour passer d'un modèle périmétrique à un modèle Zero Trust.

Le modèle Zero Trust reçoit un accueil beaucoup plus attentif de la part des responsables sécurité car ils sont conscients que les réflexes acquis depuis des décennies ne fonctionnent plus. Le monde d'aujourd'hui n'est plus celui d'il y a simplement 10 ans, voire 5 ans. Pour étayer cette prise en compte, on peut se référer au BAROMETRE DE LA CYBER-SECURITE DES ENTREPRISES, VAGUE 6 du CESIN-Opinionway,

[1] L'ANSSI ET LE BSI ALERTENT SUR LE NIVEAU DE LA MENACE CYBER EN FRANCE ET EN ALLEMAGNE DANS LE CONTEXTE DE LA CRISE SANITAIRE

daté de janvier 2021, qui indique que 75% des personnes interrogées sont en train d'étudier la façon dont le modèle Zero Trust va se traduire, ont déjà mis en place des briques du modèle ou sont déjà très engagées.

Au-delà de l'hexagone, une étude menée dans le cadre du rapport MICROSOFT DIGITAL DEFENSE REPORT cité précédemment, a évalué que 94% des répondants ont déjà commencé à déployer des briques Zero Trust et que 55% sont dans l'optique d'accélérer ce déploiement du fait de la pandémie.

L'ANSSI a publié récemment un AVIS SCIENTIFIQUE ET TECHNIQUE SUR LE MODELE ZERO TRUST dans lequel il est admis que « *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* ». Il est ensuite recommandé que « *si une mise en œuvre du modèle est envisagée, elle ne peut être que progressive* », ce qui va strictement dans le sens de ce document.

En effet, la transition vers Zero Trust est un objectif ambitieux, un projet de refonte qui doit s'envisager dans la durée, mais aussi une réelle opportunité d'adaptation à un contexte qui a profondément changé depuis la dernière décennie.

Les principes du Zero Trust

Le modèle Zero Trust s'appuie sur le principe que l'on ne peut plus faire confiance au réseau ou à l'emplacement depuis lequel l'accès est demandé ; c'est d'autant plus évident dans le nouveau contexte de télétravail généralisé où les employés se connectent à travers leur connexion Internet personnelle et n'utilisent plus obligatoirement le VPN, ou uniquement pour les accès aux ressources internes. Il est alors nécessaire de s'assurer dynamiquement du contexte d'accès (identité de l'accédant, statut de l'appareil, localisation, etc.) avant d'autoriser éventuellement et sous conditions l'accès à la ressource (application ou service).

De plus, cette approche sécurité prend pour hypothèse que le risque est omniprésent : on acte pour principe de « Présumer la compromission » (ou « Assume Breach ») qui admet, quelles que soient les protections mises en place, que l'on peut être compromis à tout moment. Dans ce cas, il faut être en mesure de détecter et réagir le plus rapidement et efficacement possible.

Approche d'un projet Zero Trust

Une fois ce constat admis, la question qui suit immédiatement est : « par où puis-je commencer et comment mener à bien ce projet vers le modèle de sécurité Zero Trust ? ». De fait, il s'agit plus d'un « voyage » que d'un projet car les organisations ne vont pas pouvoir basculer du jour au lendemain : il y a un existant à prendre en compte et il ne s'agit pas de vouloir tout remplacer. Des actifs sensibles et des applications critiques resteront encore en interne pendant une longue période. Les autres données de l'organisation seront mises à disposition au travers d'applications

SaaS et les applications internes pourront profiter d'une migration dans le cloud. Le défi est donc d'adapter le modèle de sécurité pour ce mode hybride.

Pour citer le livre blanc du NIST CHAPITRE 7 : MIGRATING TO A ZERO TRUST ARCHITECTURE « *La mise en œuvre d'une ZTA [Zero Trust Architecture] est un voyage plutôt qu'un remplacement complet de l'infrastructure ou des processus. Une organisation doit chercher à mettre en œuvre progressivement les principes de Zero Trust, les changements de processus et les solutions technologiques qui protègent ses actifs de données de plus grande valeur. La plupart des entreprises continueront à fonctionner dans un mode hybride zéro confiance / périmétrique pendant une période indéterminée tout en continuant à investir dans des initiatives de modernisation informatique en cours* ».

Objectif de ce livre blanc

L'objectif de ce livre blanc est de vous guider dans la structuration de votre projet Zero Trust en s'appuyant sur des retours d'expérience. Il s'agit de vous aider dans le démarrage de « votre » propre projet Zero Trust en prenant en compte votre existant, les points à résoudre en priorité et les scénarios que vous voudrez privilégier. Des ressources complémentaires sont indiquées pour vous permettre d'approfondir.

S'agissant d'un livre blanc Microsoft, nous déclinerons l'architecture Zero Trust avec comme exemple les briques technologiques de nos solutions : Azure Active Directory comme brique centrale de l'identité, Microsoft Endpoint Manager pour la brique de gestion des appareils, Microsoft Defender for Endpoint pour la sécurité des appareils Windows 10/Windows 11, Azure Sentinel pour la brique SIEM, etc.

Cependant, déployer une architecture Zero Trust ne vous impose pas d'adopter uniquement des briques Microsoft, ni de remplacer tous les systèmes de sécurité qui sont actuellement en place. À vous de construire votre propre architecture en prenant comme but de réduire de manière drastique le nombre de solutions de sécurité pour faciliter leur intégration, éviter les redondances et en optimiser l'administration.

L'idée est de préconiser une approche pragmatique pour l'adoption du Zero Trust telle que résumée par le slogan « Think big, start small, move fast » (Pensez grand, commencez petit, avancez vite) que vous trouverez dans le livre blanc Microsoft « ZERO TRUST BUSINESS PLAN, A PRACTICAL GUIDE TO IMPLEMENTING THE ZERO TRUST FRAMEWORK AT YOUR ORGANIZATION".

1 Comprendre la vision Zero Trust

Démarrer un projet Zero Trust nécessite une bonne compréhension des concepts Zero Trust et des briques technologiques qui vont permettre de mettre en œuvre dans la réalité ces grands principes. L'objectif est de décliner la vision par rapport à son propre existant. Cette première étape est une introduction à Zero Trust et une découverte des briques technologiques associées à six grands thèmes (ou piliers) décrits ci-dessous qui structurent l'approche Zero Trust. Il s'agit de comprendre les principes de Zero Trust qui devront servir de guide dans toute la suite du projet, mais sans entrer dans un premier temps dans les détails des technologies. Le choix des technologies utilisées et leur approfondissement seront effectués sous forme d'ateliers dédiés tel qu'expliqué plus loin dans l'étape 4 DECLINER EN BRIQUES TECHNOLOGIQUES.

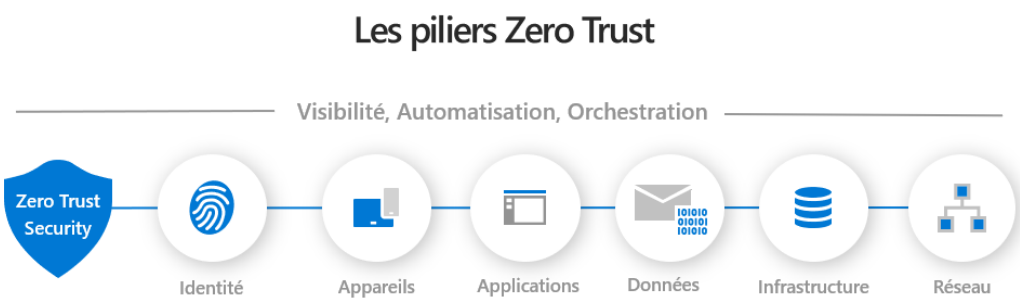
Principes

Pour résumer en une phrase : le principe de Zero Trust décrit le fait que « tous les utilisateurs et appareils doivent pouvoir accéder aux bonnes ressources depuis n'importe quel endroit avec les mêmes conditions de sécurité ». Ceci se décline en trois piliers :

1- Vérifier explicitement : contrôler dynamiquement le contexte de l'accédant – identité, l'endroit depuis lequel se fait l'accès, l'appareil utilisé et son état de santé, etc.
2- Implémenter l'accès à moindre privilège : s'assurer en fonction de ce contexte que l'accédant aura uniquement les privilèges nécessaires pour accéder à l'application. Cela peut être affiné en attribuant une fenêtre temporelle pour l'accès.
3- Présumer la compromission : adopter une posture où on admet que l'on pourra être compromis et s'assurer qu'on est en mesure de détecter les attaques et de les circonscrire rapidement pour en limiter les impacts.

Piliers technologiques

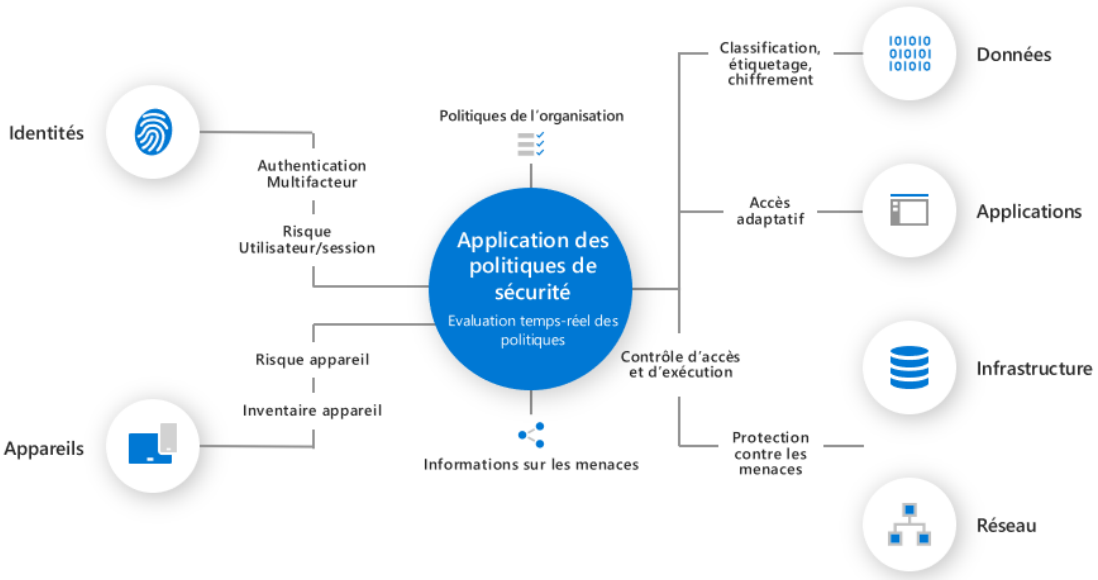
Au-delà de la compréhension de ces principes simples, on s'aperçoit que la déclinaison dans le monde réel couvre un ensemble très large de sujets (ou piliers) depuis l'identité, les terminaux, les données jusqu'aux applications, l'infrastructure et le réseau, selon la catégorisation proposée dans le ZERO TRUST DEPLOYMENT CENTER.



La pré-étude devra s'intéresser à ces 6 grands piliers, sachant que certains sont à traiter en priorité comme l'identité, que tous sont reliés et que le niveau maturité de votre organisation ne sera pas le même selon le sujet. Vous pourrez très bien avoir un bon niveau de maturité sur le pilier de l'identité en ayant déjà mis en place un référentiel hybride (avec une synchronisation entre votre référentiel d'identité interne et le référentiel cloud), mais être moins mature sur la gestion et la sécurité des postes de travail.

L'architecture Zero Trust

Le schéma ci-dessous répartit les 6 piliers autour d'un élément central pour comprendre comment s'articule l'ensemble.



On trouve sur la gauche l'identité de l'accédant, (classiquement l'utilisateur) auquel on imposera une authentification forte – multifacteur – et dont on pourra estimer dynamiquement le risque. Ensuite, l'appareil utilisé pour accéder à la ressource visée (une application ou un service) dont on sera en mesure d'identifier le niveau de risque associé : par exemple, un niveau de risque peu élevé si l'appareil est géré par l'entreprise, évalué en conformité aux politiques de sécurité, à jour des correctifs de

sécurité, etc., contrairement à un appareil personnel dont l'état de santé ne peut être mesuré.

Le nœud central, qui est très précisément décrit dans la vision Zero Trust, est le moteur d'évaluation de l'accès en temps réel. Il s'appuie sur des éléments du contexte d'accès liés à l'identité et l'appareil et sur l'évaluation dynamique de l'état des menaces. En se basant sur les politiques de sécurité définies par l'organisation, il autorise l'accès total, partiel, sous condition à l'application demandée ou impose un refus. Ceci reprend strictement la modélisation définie dans le livre blanc ZERO TRUST ARCHITECTURE du NIST, où l'utilisateur est le sujet qui accède à la ressource depuis un appareil et dont le contexte est évalué dynamiquement pour lui donner ou non accès à la ressource. Ces accès peuvent être révoqués automatiquement lorsque le contexte de sécurité évolue sans nécessiter de se réauthentifier. Cette évaluation repose sur un module appelé *Policy Enforcement Point* qui constitue « le cœur du réacteur ».

Les autres piliers concernent les Données avec la classification et la protection des données les plus sensibles par chiffrement. On peut y inclure la protection contre la fuite d'information.

Vient ensuite l'Infrastructure que ce soit cloud (Azure et autres cloud) ou on-premises pour la protection des composants des applications : les VM, containers, les microservices, etc. Enfin le Réseau, avec tout ce qui est lié à la sécurisation réseau comme le filtrage des flux, le chiffrement des communications, l'exposition des points de terminaison, la micro-segmentation…

On voit qu'au-delà de ces principes, il est nécessaire de s'appuyer sur des briques technologiques, mais que cette vision est « disruptive » par rapport à la sécurité périmétrique comme on l'entendait jusqu'à maintenant.

Déclinaison en briques technologiques

Chaque sujet sera associé à une ou plusieurs briques technologiques, lesquelles offriront plusieurs fonctionnalités. Par exemple la brique Identité – assurée en environnement Microsoft par Azure Active Directory – offrira entre autres le SSO, l'accès conditionnel, l'authentification multifacteur qui rentreront dans l'ensemble des fonctions et contrôles concourant à la mise en œuvre du Zero Trust. La brique Données – basée sur Microsoft Information Protection – intégrera les fonctions de classification et de protection des données sensibles par chiffrement.

Vous devrez profiter de ce projet de refonte de la sécurité Zero Trust pour minimiser le nombre de solutions utilisées. On constate qu'avec une approche tendant à choisir au coup par coup les « meilleures » solutions du marché, les entreprises en viennent à empiler plusieurs dizaines de solutions de sécurité dont l'intégration et l'exploitation s'avèrent problématiques autant du point de vue de la mise en place que du retour sur investissement. Cependant, rien n'impose de faire table rase de

l'existant comme on le verra plus loin dans la détermination du niveau de maturité Zero Trust au chapitre 5 IDENTIFIER SON NIVEAU DE MATURITE.

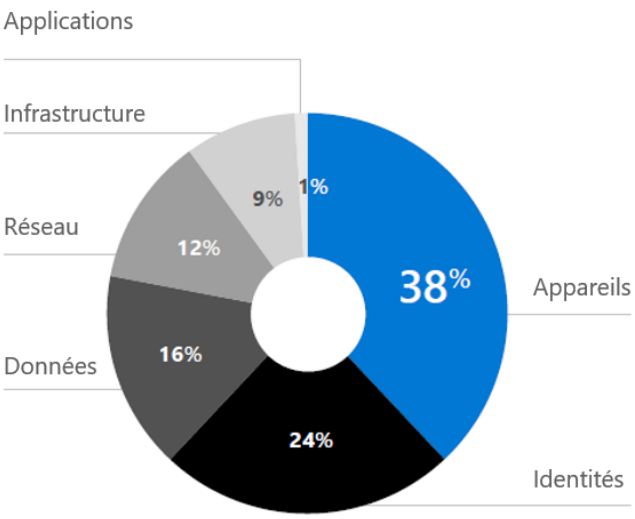
La plus grande partie des briques technologiques de sécurité s'appuient désormais sur le cloud, ce qui offre comme avantages d'être accessible depuis n'importe quel endroit disposant d'une connexion Internet (plus de nécessité d'un VPN), de ne pas nécessiter de déploiement d'infrastructure, et enfin de s'appuyer sur la puissance de l'Intelligence Artificielle (IA) en profitant de l'effet d'échelle pour la détection et la réaction aux menaces cyber.

Pour plus d'informations, vous pouvez consulter les liens :

- CHIEF INFORMATION SECURITY OFFICER (CISO) WORKSHOP TRAINING
- CISO WORKSHOP MODULE 3: IDENTITY AND ZERO TRUST USER ACCESS
- ZERO TRUST EBOOK

Importance des piliers

Tous les piliers ne sont pas forcément perçus avec la même importance. Une enquête menée début 2020 dont vous trouverez les chiffres dans l'infographie SECURING IDENTITY WITH ZERO TRUST, posait la question « Quel est le pilier le plus important dans votre modèle de sécurité Zero Trust ? ». Les 2 piliers cités en priorité sont Appareils à 38% et Identités à 24%.



On peut l'interpréter par le fait que les responsables IT interrogés sont plus sensibles à la sécurité des appareils car le télétravail a mis ce sujet au-devant de la scène, et à la prise de conscience de l'importance de la protection de l'identité avec la recrudescence des attaques dont le vecteur d'entrée reste l'usurpation d'identité et plus particulièrement le phishing. Quant aux autres piliers, il semble étonnant que les applications soient reléguées à simplement 1% des préoccupations. Sans doute

est-ce lié au fait que les entreprises utilisent de plus en plus d'applications SaaS ou que les applications internes n'ont pas encore migré massivement vers le cloud ?

2 Former une équipe transverse

La mise en place d'un modèle Zero Trust n'est pas un simple projet au sens où il s'agit d'un véritable changement de modèle de sécurité par rapport au modèle précédent qui n'a pas évolué depuis des décennies. Certes, on ne remet pas en cause les fondamentaux de la sécurité mais on doit changer la manière de les mettre en œuvre pour s'adapter aux nouvelles menaces et aux nouveaux besoins de l'entreprise. Il faut également prendre en compte que les « armes » qui sont à notre disposition se sont considérablement renforcées, faut-il au moins les connaitre et savoir en tirer le meilleur profit.

Vous allez devoir considérer cette transition de modèle comme un projet ou un ensemble de projets qui s'étaleront sur plusieurs mois voire plusieurs années : on a tendance à dire qu'il s'agit plus d'un « voyage ». Depuis plusieurs années, la sécurité revient au cœur des organisations et implique toutes les entités. Pour citer l'un des principes fondamentaux de L'ESSENTIEL DE LA SECURITE NUMERIQUE POUR LES DIRIGEANTS ET LES DIRIGEANTES : « *La cybersécurité est gérée comme un* ***élément transversal dans l'entreprise****. Elle concerne tout le monde, à tous les niveaux, depuis la conception d'un projet jusqu'à son exécution et la vente*. ». Cela est d'autant plus vrai pour un projet de refonte du modèle de sécurité qui devra impliquer de bâtir une équipe dont les membres intégreront les équipes réseau, sécurité et IT (infrastructure, annuaire, postes de travail…), mais également les métiers, le juridique, etc.

Comme tout projet qui impacte fortement l'entreprise, il faudra lui trouver un sponsor, c'est-à-dire quelqu'un d'assez haut placé dans la hiérarchie, qui croit au projet et saura le défendre au plus haut niveau. Si votre entreprise dispose déjà d'un CYBER-COMEX, il est clair qu'il faudra vous appuyer sur ses membres pour mener à bien votre projet Zero Trust.

Les métiers vous seront des alliés sûrs si vous leur prouvez qu'avec cette transformation vous pourrez plus facilement déployer de nouvelles applications ou rendre possible des scénarios qui n'étaient pas autorisés jusqu'à présent. Ces équipes vous seront indispensables pour définir quels scénarios sont les plus intéressants à considérer. C'est vrai à la fois pour la reprise en main des solutions SaaS utilisées – en les autorisant désormais en toute conscience –, mais aussi pour le développement de nouvelles applications ou services mis à disposition de l'interne ou de clients de l'entreprise.

Cette nouvelle approche de la sécurité que vous allez proposer doit être vue non plus comme un frein, mais comme pouvant au contraire faciliter le business, le travail

au quotidien pour l'ensemble des utilisateurs de votre SI, et la fluidité des échanges en interne comme avec les partenaires/sous-traitants.

Vous devrez choisir des personnes motivées par le sujet dans une équipe resserrée qui formera le noyau dur du projet. Inutile de multiplier les membres pour se retrouver dans des réunions de travail pléthoriques qui seront le meilleur moyen de noyer le projet. En revanche, il sera nécessaire d'impliquer plus largement des personnes avec les compétences nécessaires, sur un sujet technique ou sur l'existant et avec la connaissance de l'entreprise, lors de réunions de travail pour recueillir les éléments sur l'existant, proposer et discuter des directions, évaluer la complexité de mise en œuvre, etc.

L'un des critères de choix des personnes de l'équipe est un minimum de connaissance en sécurité ou au moins une appétence sur le sujet. En effet, la pré-étude nécessite une connaissance sur le modèle Zero Trust et passera par une étape de formation. De plus, les personnes devront être ouvertes aux idées nouvelles pour construire la vision Zero Trust et capable ensuite de la porter auprès de leurs équipes et collègues.

L'équipe resserrée (la « Core Team ») et le sponsor seront tout naturellement impliqués dans la suite du projet Zero Trust. Ne pas oublier que le voyage vers le Zero Trust en lui-même nécessitera un engagement sur la durée de l'équipe et des dirigeants.

Mais n'oublions pas l'objectif : il s'agit dans un premier temps d'un cadrage du projet qui ne nécessite pas que tout soit défini dans les moindres détails (techniques, organisationnels, …) mais que les grands sous-projets ou chantiers soient identifiés, estimés en coût, mis en relation les uns avec les autres et positionnés sur une échelle de temps.

3 Pourquoi un projet Zero Trust ?

Avant de s'embarquer dans le voyage Zero Trust, il faut être en mesure d'identifier quelles sont les attentes autour de ce projet, quels sont les problèmes à résoudre, quelles améliorations sont attendues tout en s'assurant que cela s'inscrit dans la vision Zero Trust. Partant d'une approche générale qui consiste à vouloir transformer le modèle de sécurité pour rendre le système d'information étendu mieux adapté aux nouvelles menaces, il faut ensuite se focaliser sur des objectifs plus précis pour définir des priorités dans les briques que l'on mettra en place.

La question de base va donc être : quels sont les problèmes à résoudre et selon quelle priorité ?

Pour y répondre, la méthode consiste à « brainstormer » lors d'ateliers non-techniques pour identifier les attentes en les formulant sous la forme de souhaits de « haut niveau », c'est-à-dire sans rentrer dans les considérations techniques. La liste suivante non-exhaustive vous donne quelques exemples :

- Je veux pouvoir migrer ou développer des applications dans le cloud tout en m'assurant qu'elles seront correctement protégées ;
- Je veux permettre aux employés de travailler depuis la maison avec les mêmes conditions de sécurité et les mêmes performances ;
- Je veux conserver des applications sur site mais qu'elles soient accessibles de l'extérieur sous conditions strictes ;
- Je veux pouvoir m'assurer que mes données critiques (par exemple mes secrets de fabrication) soient correctement protégées et me garantir contre leur fuite ou vol ;
- Je veux pouvoir me protéger efficacement contre les rançongiciels (j'ai déjà subi une attaque qui m'a coûté cher) ;
- Je veux pouvoir faciliter le travail avec des partenaires sur des projets sensibles ;
- Je veux renforcer l'authentification des utilisateurs pour sécuriser l'accès aux applications externes et internes ;
- Je veux minimiser la surface d'attaque de mon annuaire Active Directory ;
- Je veux m'assurer que mes sites de production sont correctement protégés et resteront disponibles ;

- Je veux rationaliser mes solutions de sécurité pour en réduire les coûts et faciliter les opérations ;
- Je veux m'assurer que je suis conforme au RGPD pour limiter les risques d'une amende en cas de fuite de données personnelles ;
- Je veux pouvoir limiter les outils et les contraintes d'infrastructure (type VPN, réseau de connexion) pour permettre à mes utilisateurs de travailler de façon sécurisée ;
- Je veux offrir plus de flexibilité à mes utilisateurs et minimiser mon empreinte sur les infrastructures ;
- Etc.

De la liste que vous aurez construite, il faudra ensuite affecter à chaque attente une priorité. Par exemple, vous pourriez mettre en priorité la protection contre les rançongiciels ou la protection des données critiques. Les solutions pour couvrir chaque attente pourront concerner plusieurs piliers, plusieurs technologies par piliers et être plus ou moins difficiles à mettre en place.

On remarquera que certaines attentes peuvent être plus précises comme « *Je veux minimiser la surface d'attaque de mon annuaire Active Directory* » car elles correspondent à un vécu ou un risque évalué comme fort (compromission de l'annuaire d'entreprise on-premises Active Directory).

Les attentes se divisent en deux catégories : un renforcement de la sécurité et l'ouverture raisonnée à de nouveaux scénarios, en phase avec les nouveaux défis. L'aspect sécurité est, de facto, prédominant puisque Zero Trust est un nouveau modèle de sécurité, mais il faut considérer également les bénéfices au sens du business. Il est important de changer la vision négative et anxiogène de la sécurité pour la faire voir comme un moyen de s'adapter tout en protégeant les actifs et le fonctionnement de son entreprise dans un environnement qui s'est éminemment complexifié.

Parmi les arguments à avancer :

Sécurité Une meilleure résistance aux attaques tant issues d'organisations cybercriminelles (le MICROSOFT DIGITAL DEFENSE REPORT SEPTEMBER 2020 cite 13 milliards de mails malveillants dont 1,6 milliards contenant des URL d'hameçonnage) que d'états nations ciblant très largement tous les secteurs d'activité tant privés, gouvernementaux, les ONG, ou l'éducation. Le pilier « Assume Breach » de la stratégie Zero Trust prend en compte ces menaces.

Adaptabilité Une opportunité de répondre à des scénarios beaucoup plus ouverts. Les entreprises ayant déjà adopté au moins en partie Zero Trust ont pu mesurer l'intérêt avec les exigences créées par la pandémie et la généralisation du télétravail. Mais on peut envisager des scénarios allant bien au-delà : une meilleure gestion des identités – y compris des identités externes – avec un accès facilité aux

ressources de l'organisation dans un respect du principe de « moindre privilège » permet d'intégrer facilement de nouveaux partenaires ou de réaliser plus efficacement des fusions/acquisitions tout en respectant ses propres standards de sécurité.

Opportunités Une implémentation plus adaptée de la sécurité permet de saisir plus facilement les opportunités à travers le développement de nouvelles applications à mettre à disposition de l'interne ou de ses propres clients, ou la mise à disposition plus rapide de nouvelles applications SaaS.

Contrôle des données Les données sont les actifs les plus précieux de l'entreprise : faut-il être en mesure d'identifier celles qui sont les plus sensibles à travers une classification. Ces données sensibles doivent bénéficier d'une protection adaptée qui garantira leur confidentialité y compris en cas de fuite (intentionnelle ou non) à l'extérieur. La garantie de leur intégrité et disponibilité est cruciale par exemple en cas d'attaque de rançongiciel.

Conformité Une meilleure protection des données adaptée à leur sensibilité facilite le respect des réglementations tout en limitant les risques de fuite d'information et leurs impacts financiers comme en termes d'image. Plus particulièrement si vous mettez en place des processus et des briques de sécurité pour assurer la protection des données, le respect du RGPD[2] n'en sera que plus aisé.

Intégration du cloud Le cloud est devenu un élément incontournable tant pour l'utilisation par les métiers des applications SaaS disponibles que pour les applications développées en interne. Les organisations pour lesquelles l'intégration du cloud s'est faite de manière moins contrôlée doivent saisir l'opportunité du Zero Trust pour reprendre le contrôle en limitant le Shadow IT. L'identité est l'un des piliers du Zero Trust : la mise en place d'une gestion et d'une protection fortes de l'identité dans un environnement hybride est un sujet à considérer en priorité.

[2] REGLEMENT GENERAL POUR LA PROTECTION DES DONNEES

4 Décliner en briques technologiques

A l'étape précédente, vous avez défini les attentes et affecté des priorités. Maintenant, il s'agit d'identifier et de bâtir les solutions technologiques qui vont vous permettre de satisfaire ces attentes en puisant dans les briques technologiques à votre disposition telles qu'elles ont été étudiées en étape 1 1 COMPRENDRE LA VISION ZERO Trust.

Certaines attentes se déclineront de manière simple car elles ne feront référence qu'à un seul pilier et un nombre restreint de briques technologiques dans ce pilier. Par exemple, si on considère l'attente « *Je veux renforcer l'authentification des utilisateurs pour sécuriser l'accès aux applications externes et internes* », ceci concerne le pilier Identité et deux technologies de renforcement de l'authentification que sont l'authentification multifacteur et l'authentification sans mot de passe.

D'autres attentes seront plus complexes à décliner car impliquant plusieurs piliers et plusieurs technologies parmi ces piliers. Par exemple, l'attente « *Je veux pouvoir me protéger efficacement contre les rançongiciels* » s'intéressera à plusieurs piliers dont principalement le pilier Données avec la protection de l'accès aux données, la sauvegarde-restauration, mais aussi la détection des attaques (dans une vision « Assume breach »), la protection contre le phishing, la protection des identités et des appareils, le durcissement de l'Active Directory, et le renforcement des pratiques d'administration.

Autre exemple, l'attente « *Je veux permettre aux employés de travailler depuis la maison avec les mêmes conditions de sécurité et les mêmes performances* » sera encore plus transversale en impliquant les piliers Identité (gestion des identités, authentification forte), Appareils (gestion de la sécurité des appareils), Données (protection/classification des données), Réseau (accès performant aux applications de collaboration), et Applications (accès conditionnel lié à l'identité et au contexte, sécurité des applications). On voit dans ce cas que l'on devra faire des choix dans le calendrier de déploiement des briques, par exemple s'attaquer en premier à la sécurisation de l'identité, puis à la sécurisation des appareils, etc.

Enfin, dans les solutions à mettre en place pour répondre aux attentes, des briques technologiques seront communes (à terme toutes devraient être utilisées) ; par exemple l'authentification forte sera une brique de base que l'on retrouvera dans de nombreux scénarios puisqu'il s'agit d'une fondation de la sécurisation des identités. Le contrôle d'accès conditionnel sera aussi une brique centrale, comme moteur du Zero Trust pour autoriser les accès de manière intelligente en fonction du contexte.

Une chose est certaine, l'Identité est un pilier qui sera commun à quasiment tous les scénarios.

Cette étape de construction sera conduite sous forme d'ateliers de travail que vous pourrez construire et animer vous-mêmes en vous basant sur les nombreuses documentations existantes, ou en vous faisant aider par des ressources de conseil extérieures. Dans ces réunions de travail devront être impliqués les personnes de la Core Team mais également des représentants des équipes internes. Par exemple, sur le sujet des appareils (PC, mobiles) vous devrez faire appel à des personnes de l'IT interne qui ont la connaissance de la gestion et du déploiement des appareils, et qui pourront imaginer avec vous les transformations à opérer pour s'intégrer au modèle Zero Trust.

Enfin, il vous faudra être ambitieux pour envisager le changement de modèle dans son ensemble, mais ensuite définir un étagement dans le déploiement des briques technologiques en fonction des priorités de vos attentes.

5 Identifier son niveau de maturité

Dans votre voyage vers Zero trust, vous ne partez pas de rien : vous avez un existant à prendre en compte et il se peut que vous ayez déjà déployé des mécanismes ou technologies qui correspondent à une première avancée vers le modèle Zero Trust. Par exemple si vous avez déjà déployé Office 365, vous disposez d'une architecture d'identité hybride avec Azure Active Directory comme référentiel d'identités dans le cloud synchronisé avec Active Directory, le référentiel d'identité on-premises. Peut-être avez-vous déjà mis en œuvre quelques règles de contrôle d'accès conditionnel pour sécuriser l'accès à certaines applications ou déployé l'authentification multifacteur pour une partie de vos employés ? Ou encore avez-vous déployé une solution de CASB pour limiter le Shadow IT en contrôlant l'accès aux solutions cloud SaaS ?

Evaluer son niveau de maturité

Pour vous permettre d'évaluer votre niveau de maturité Zero Trust, vous pouvez en premier lieu consulter le livre blanc (synthétique) ZERO TRUST MATURITY MODEL dont le tableau ci-dessous donne un aperçu pour les piliers Identités et Appareils.

	Traditionnel	Avancé	Optimal
Identités	Le référentiel d'identité est on-premises Pas de SSO entre le cloud et les applications on-premises Visibilité limitée sur les risques liés à l'identité	L'identité Cloud est fédérée avec le système on-premises Les politiques d'accès conditionnel contrôlent l'accès et fournissent des actions correctives L'analyse des signaux améliore la visibilité	L'authentification sans mot de passe est activée L'utilisateur, l'appareil, l'emplacement et le comportement sont analysés en temps réel pour déterminer les risques et fournir une protection continue
Appareils	Les appareils sont joints au domaine et gérés avec des solutions telles que Group Policy Object ou Config Manager Les appareils doivent être connectés au réseau pour accéder aux données	Les appareils sont enregistrés auprès du fournisseur d'identité cloud Accès uniquement accordé aux appareils gérés et conformes dans le cloud Les stratégies DLP sont appliquées pour les appareils d'entreprise et BYO	Un EDR (Endpoint threat detection) est utilisée pour surveiller les risques liés aux appareils Le contrôle d'accès est basé sur le risque de l'appareil pour les appareils d'entreprise et BYO

Selon les fonctionnalités que vous avez déjà mises en œuvre, vous pourrez vous situer dans un niveau Traditionnel, Avancé ou Optimal selon les piliers. Par exemple, si vous déjà mis en place une solution cloud de gestion des appareils (mobiles et PC) comme Microsoft Intune, que vous vérifiez la conformité des appareils avant de donner l'accès aux applications par une politique de contrôle d'accès conditionnel, vous vous situez pour le pilier Appareil dans le niveau Avancé.

Pour aller plus loin, l'outil en ligne ÉVALUATION DU MODELE DE MATURITE ZERO TRUST vous propose, pour chaque pilier, d'évaluer votre niveau de maturité à partir d'un ensemble de questions sur votre existant, et vous fournit ensuite des recommandations pour augmenter votre niveau de maturité Zero Trust et des liens pour la description technique des solutions à utiliser.

Cette analyse du niveau de maturité vous permet de faire un premier passage sur votre existant. Cet exercice est important car il vous permet d'inventorier les solutions déjà existantes qui pourraient s'intégrer dans la vision Zero Trust, l'éventuel niveau de difficulté pour leur intégration, les solutions à remplacer, etc. Il faut garder à l'esprit les attentes que vous avez définies pour vous focaliser en priorité sur les briques technologiques que vous avez identifiées à l'étape précédente. Même s'il faut être ambitieux pour bâtir une vision d'ensemble, il faut éviter de se disperser et surtout de rentrer à cette étape dans des détails techniques.

Exemples d'évaluation

Si on reprend le cas concret de la protection contre les rançongiciels, on évaluera les sujets suivants par rapport à son existant pour en déduire, par exemple :

- La protection contre les emails de phishing : OK, même si on devra renforcer la sensibilisation des employés et tester par des campagnes.
- La protection des postes de travail : les postes sont tous gérés par un outil interne avec des configurations de sécurité appliquées, une mise à jour des correctifs de sécurité régulière, et un anti-virus/anti-malware, mais un EDR (Endpoint Detection and Response) apporterait un plus.
- La détection des attaques de rançongiciel : c'est actuellement le point faible : notre SIEM ne permet pas d'identifier efficacement ce type d'attaque et de réagir sans délai. Un EDR devrait être envisagé éventuellement couplé à un SIEM qui pourrait détecter rapidement des postes compromis et les isoler pour éviter la propagation.
- La reconstruction des postes de travail : c'est un autre point faible. On ne serait pas capable de reconstruire un nombre important de postes dans un délai court. Une solution automatisée et performante, idéalement sous forme de service cloud serait à envisager.
- La restauration des données : beaucoup de données sont hébergées dans SharePoint Online et pourraient être restaurées sur des versions antérieures en cas de chiffrement, mais il reste encore des serveurs on-premises dont on est moins sûr des capacités de restauration.
- La protection des applications : les applications vitales reposent sur des solutions SaaS qui ne sont pas sensibles aux rançongiciels.

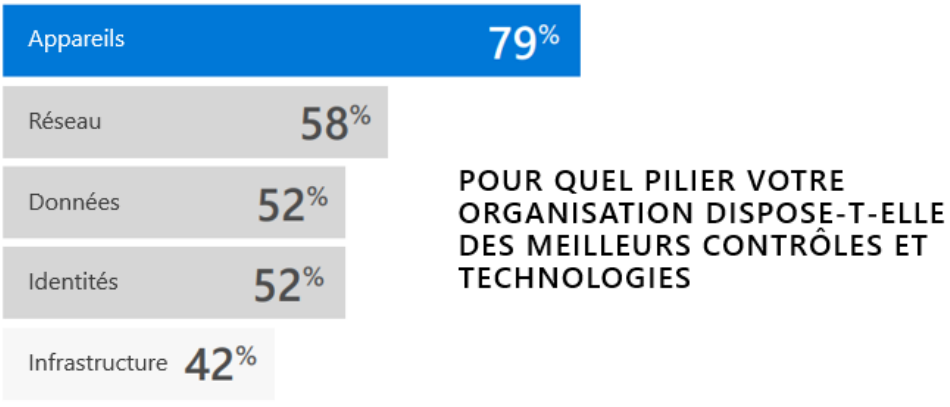
Prenons comme deuxième exemple la volonté de migrer ou développer des applications dans le cloud en s'assurant qu'elles soient correctement protégées : on va s'intéresser aux piliers Identité, Applications mais également Appareils pour faire le constat suivant par rapport à son existant :

- Gestion et protection des identités : Azure Active Directory a été déployé et synchronisé avec l'Active Directory interne, mais le SSO n'a pas été généralisé pour les applications SaaS et n'est pas utilisé pour les applications développées en interne. L'authentification multifacteur n'est pas encore utilisée de manière généralisée.
- Sécurisation de l'accès aux applications : l'accès conditionnel n'est pas utilisé pour s'assurer du contexte de l'utilisateur, de l'appareil, etc. avant d'autoriser ou non l'accès aux applications au moins les plus critiques qui sont disponibles depuis Internet.
- La protection des postes de travail : les postes sont tous gérés par un outil interne avec des politiques de sécurité appliquées, une mise à jour des correctifs de sécurité régulière, un anti-virus/anti-malware, mais leur statut de santé ne peut pas utilisé comme paramètre dans l'accès conditionnel.

En résumé, cet examen du niveau de maturité est un exercice qui permet de réaliser un état des lieux de haut niveau en gardant à l'esprit les attentes prioritaires. Il permet d'identifier les points sur lesquels il est possible de progresser en avançant dans la direction d'un modèle Zero Trust et de commencer à avoir les idées plus claires sur les technologies à mettre en œuvre, sur celles à remplacer ou à intégrer.

Enquête sur le niveau de maturité

Pour vous donner une idée du niveau de maturité des entreprises, une enquête menée début 2020, dont vous trouverez les chiffres dans l'infographie SECURING IDENTITY WITH ZERO TRUST, précise que les entreprises interrogées considèrent à 79% qu'elles sont le mieux armées sur le pilier Appareils. Les piliers Réseau, Données et Identités suivent avec des scores quasi-identiques, puis en dernier le pilier Infrastructure.



Ces résultats mettent en évidence que la sécurité des appareils est un sujet qui a été traité en priorité. Le réseau est classiquement un sujet sur lequel la sécurité est maîtrisée au moins sur la partie on-premises, même s'il ne faut pas négliger l'importance qu'il faudra lui apporter sur l'architecture des applications cloud et sur

les impacts liés à la généralisation du télétravail. Quant aux piliers Données et Identités, même si les technologies sont disponibles (respectivement classification, chiffrement, DLP, etc. et authentification multifacteur, contrôle d'accès conditionnel, protection des comptes à privilèges, etc.), la moitié des entreprises considèrent qu'elles ont encore du chemin à faire pour en tirer parti.

Le pilier infrastructure qui concerne la sécurité des serveurs on-premises ou les composants IaaS dans le cloud (pour la détection des attaques ou des anomalies de configuration) reste le sujet sur lequel les entreprises se sentent le plus vulnérables et le moins outillées.

6 Identifier les quick wins

Le slogan « Think big, start small, move fast » (Pensez grand, commencez petit, avancez vite)[3] vous recommande d'être ambitieux pour considérer d'embarquer l'ensemble du système d'information dans votre vision Zero Trust, de démarrer par des étapes courtes mais marquantes – les quick wins ou victoires rapides – et d'être rapides dans l'exécution.

Les quicks wins ont un côté positif : ils sont à la fois motivants pour les équipes et apportent rapidement des résultats tangibles. Ils rassurent également au niveau plus haut sur la viabilité et les impacts positifs du projet Zero Trust. Le revers de la médaille est qu'ils peuvent apporter un faux sentiment de fin de projet et laisser penser que « ça y est, on est Zero Trust », « finalement ce n'était pas plus compliqué que ça, maintenant passons à autre chose et cessons d'investir ».

C'est pour cela que les quick wins doivent être choisis avec précaution et être présentés comme points de départ tout en étant intégrés dans la feuille de route complète du projet, qui lui ne s'étalera pas sur quelques semaines mais sur le plus long terme. Le choix des quick wins doit s'intégrer dans les briques techniques qui correspondent aux attentes déterminées précédemment.

Certains quick wins sont mis en avant car ils correspondent à des briques Zero Trust incontournables comme l'Identité. Le gain rapide systématiquement mis en avant est la généralisation de l'authentification multifacteur ou mieux, sans mot de passe. Mais c'est loin d'être le seul : par exemple la mise en place du SSO pour les applications les plus populaires ou les plus critiques serait visible et pas obligatoirement complexe. Si on considère l'objectif de la lutte contre les rançongiciels, la mise en place d'un EDR tel que Microsoft Defender for EndPoint, apportera rapidement une visibilité sur les menaces provenant des postes et permettra de réagir en conséquence.

Un quick win peut être défini par rapport à un périmètre de mise en œuvre, par exemple en s'intéressant en priorité aux actifs les plus critiques de l'entreprise. On pourra choisir de traiter prioritairement le renforcement de l'accès aux applications les plus critiques, la sécurisation des données les plus sensibles, la protection des comptes à privilèges, etc. Ensuite, on pourra généraliser en avançant par phases lorsque la solution aura été éprouvée. Cette idée de se concentrer en premier lieu

[3] A retrouver dans le livre blanc Microsoft ZERO TRUST BUSINESS PLAN, A PRACTICAL GUIDE TO IMPLEMENTING THE ZERO TRUST FRAMEWORK AT YOUR ORGANIZATION

sur les actifs critiques permet d'augmenter rapidement le niveau de sécurité et de résilience de l'entreprise/organisation vis-à-vis d'attaques cyber.

Un quick win peut être visible (par exemple un déploiement de l'authentification multifacteur ou le SSO), ou non (déploiement d'un système EDR – Endpoint Detection and Response), mais se doit d'être mesurable pour évaluer la progression et démontrer que les bénéfices attendus sont bien au rendez-vous, que ce soit au niveau sécurité ou sur un éventuel retour sur investissement. On abordera ce sujet dans le chapitre 8 DEFINIR ET UTILISER DES INDICATEURS).

Enfin, un quick win reste une étape tactique, c'est-à-dire un avantage immédiat et visible, mais qui doit s'inscrire dans une démarche stratégique que représente le basculement dans modèle Zero Trust. De plus, on s'efforcera de respecter le principe de minimiser le nombre de solutions pour limiter les problèmes d'intégration, diminuer les coûts et faciliter l'administration.

7 Traiter en priorité le pilier Identité

L'identité est l'élément fondamental dans le modèle Zero Trust, associé à l'appareil depuis lequel s'effectue l'accès. On affirme même que « l'identité est le nouveau périmètre » puisque la plupart des compromissions impliquent des vols d'identifiants ou des usurpations d'identité.

Dans la terminologie du NIST, l'élément central est le composant appelé *Policy Enforcement Point* (PEP) qui évalue dynamiquement le contexte et prend les décisions d'accorder ou non l'accès. Dans l'environnement Microsoft, ce rôle est dévolu à Azure Active Directory qui implémente la fonction de PEP via le contrôle d'accès conditionnel et joue également le rôle de référentiel des identités.

Comme le recommande le livre blanc 10 TIPS FOR ENABLING ZERO TRUST SECURITY, « *l'identité est le meilleur point de départ pour le Zero Trust* » puisque « *l'utilisation de l'identité comme point de contrôle permet aux entreprises de traiter chaque demande d'accès comme non fiable jusqu'à ce que l'utilisateur, le dispositif et d'autres facteurs soient entièrement vérifiés* ».

La compromission de l'identité est le point d'entrée de la plus grande majorité des attaques perpétrées sur les entreprises ou organisations : rien qu'en mars 2020, Microsoft a détecté 4,9 milliards tentatives de connexions liées à des attaques et plus de 150 000 comptes compromis, selon les chiffres spécifiés dans le document UNDERSTANDING IDENTITY THREAT PROTECTION. La protection de l'identité est donc une priorité pour faire face à la recrudescence de ce type d'attaques souvent initiées par des campagnes de phishing.

Pour renforcer encore le message, citons le document EXAMINING ZERO TRUST AN EXECUTIVE ROUNDTABLE DISCUSSION qui résume le tour de table entre la Cloud Security Alliance et Microsoft en décembre 2020, qui préconise de « *considérer l'identité comme le nouveau périmètre* » en arguant que « *les organisations doivent d'abord s'attacher à renforcer l'authentification des utilisateurs et la vérification de leur identité, car la plupart des violations de la sécurité impliquent le vol d'informations d'identification* ».

Une identité gérée dans le Cloud

La mise en œuvre d'Azure Active Directory, que l'on doit considérer comme le « cœur du réacteur », nécessite que les identités soient créées dans Azure AD, soit directement, soit par synchronisation avec l'annuaire on-premises Active Directory (cas le plus courant). Cette étape de synchronisation doit être mise en place à travers l'utilisation du connecteur Azure AD Connect, mais est déjà effective si vous avez

déployé Office 365. Il est en effet indispensable que les identités soient présentes dans l'annuaire cloud pour lui permettre de prendre en charge l'authentification et le contrôle d'accès conditionnel.

Une migration d'Active Directory vers Azure Active Directory

Active Directory est depuis deux décennies l'annuaire interne utilisé par la quasi-totalité des entreprises. Même si les bonnes pratiques de sécurisation et d'administration sont disponibles de longue date, l'historique et la vie des entreprises (fusion, acquisition) ont pu le rendre complexe à sécuriser. De plus, les attaques dont le scénario est maintenant bien connu (compromission d'un compte utilisateur, déplacement latéral et élévation de privilège) visent à prendre possession de l'annuaire en tant qu'administrateur et ainsi s'accorder tous les droits sur les ressources internes.

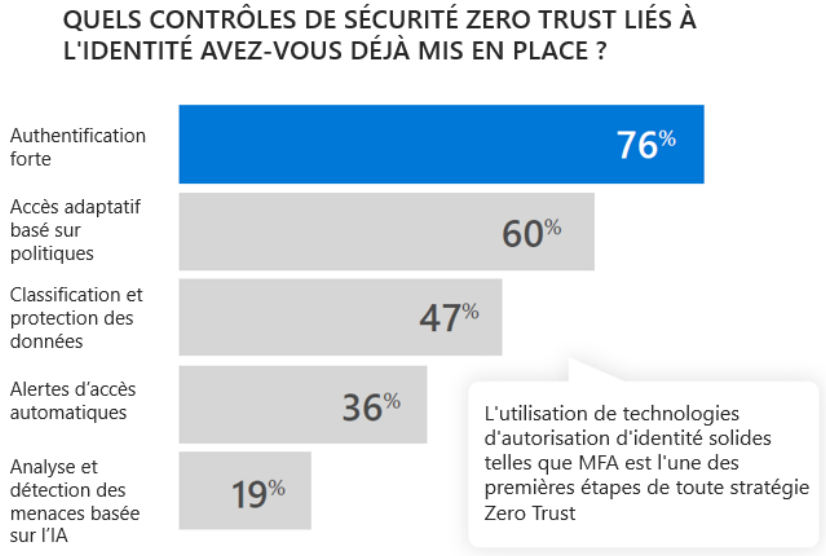
Dans une approche Zero Trust, la recommandation de Microsoft est à terme de dépeupler Active Directory au fur et à mesure que les applications et ressources internes seront disponibles depuis le cloud, que ce soient les applications SaaS, les applications et données ayant migré dans le cloud. Alors que les identités vont migrer dans Azure AD, les postes de travail vont quitter Active Directory pour être gérés depuis un service MDM dans le cloud dans un mode de « management moderne ». Cette bascule vers un dépeuplement de l'Active Directory interne va avoir pour effet de limiter grandement son exposition aux attaques. Cela va de pair avec la mise en place des technologies associées aux autres piliers Zero Trust sur le renforcement de la sécurité des postes de travail, des capacités de détection, le renforcement de l'authentification lié à Azure Active Directory, etc.

En cible, Active Directory devrait être réduit à l'administration des ressources internes n'ayant pas vocation à migrer dans le cloud (par exemple, systèmes industriels) avec des stations d'administration renforcées, une segmentation réseau et des systèmes de détection garants de la sécurité sur un périmètre désormais excessivement restreint.

Un renforcement de l'authentification

Selon une enquête réalisée par Microsoft auprès de responsables informatiques de plusieurs pays ayant entamé leur voyage Zero Trust[4], il ressort que 76% ont implémentés en premier lieu une authentification forte et 60% l'accès conditionnel basé sur des politiques.

[4] ZT_One_Minute_Identities (microsoft.com)



Rien d'étonnant quand on sait que les mots de passe sont responsables de 80% des portes d'entrée pour les pirates [5] et qu'on estime que la généralisation de l'authentification multifacteur réduit le risque de compromission de 99,9%[6]. D'autant que sa mise en œuvre est largement simplifiée par un paramétrage unique qui regroupe plusieurs options de sécurité préconfigurées[7].

L'étape suivante, le nec plus ultra de l'authentification, est l'authentification sans mot de passe qui supprime de facto les faiblesses liées à l'utilisation des mots de passe. L'authentification peut s'appuyer sur une caractéristique biométrique telle qu'un visage ou une empreinte digitale, ou un code confidentiel propre à un appareil et qui n'est pas transmis sur le réseau. Vous aurez le choix entre l'utilisation de votre ordinateur Windows avec biométrie et/ou code PIN, la connexion par clé de sécurité FIDO2 ou l'application Microsoft Authenticator pour les appareils mobiles[8].

Un contrôle d'accès sous conditions

A l'authentification forte s'ajoute l'élément clé du Zero Trust, le contrôle d'accès conditionnel, qui prend en temps-réel les décisions d'accès aux ressources en prenant en compte le contexte de la requête : utilisateur avec évaluation du risque sur l'identité ; appareil avec évaluation de la conformité, de l'état de santé ; endroit depuis lequel est effectuée la demande et l'ensemble de signaux collectés par le Graphe de Sécurité Microsoft. Ces éléments sont examinés, en considérant les politiques que vous définissez, pour prendre la décision d'accès à la ressource ou de son refus. Un exemple de politique d'accès est de définir que « l'accès à l'application

---

[5] Email: Is the Digital Door Propped Open for Identity Hijackers? Multi-Factor Authentication Helps Shut Cyber Criminals Out, CHUBB/Microsoft.

[6] Flash whitepaper: Why MFA is a top priority in 2020

[7] Présentation des paramètres de sécurité par défaut

[8] Planifier un déploiement d'authentification sans mot de passe dans Azure Active Directory

des Ressources Humaines n'est possible que pour les groupes d'utilisateurs appartenant à ce service, à condition que l'accès s'effectue depuis un poste géré par le MDM de l'entreprise et avec authentification multifacteur imposée quel que soit l'endroit ».

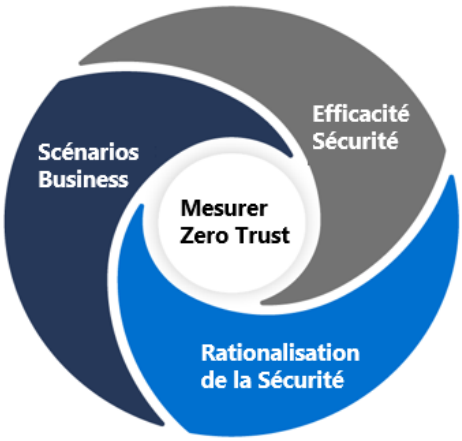
La recommandation est de commencer avec quelques politiques simples en les déployant par paliers, sur un périmètre réduit avant de les généraliser. Une fois que le processus est pris en main et testé, on peut augmenter le nombre de politiques d'accès en ayant soin de s'appuyer sur des indicateurs pour en suivre l'application, ce qui fait la transition vers le chapitre suivant.

Pour conclure, la démarche complète de prise en compte du pilier Identité est décrite dans l'article SECURING IDENTITY WITH ZERO TRUST | MICROSOFT DOCS.

8 Définir et utiliser des indicateurs

Pour introduire l'importance de cette étape, on peut mentionner cette courte citation extraite du document 10 TIPS FOR ENABLING ZERO TRUST SECURITY qui résume bien l'objectif : « *Montrer la valeur tout au long de la route* »[9] pour détailler ensuite que « *L'un des moyens les plus efficaces de susciter un soutien à long terme pour une initiative Zero Trust est de démontrer la valeur progressive de chaque investissement* ». Ceci ne fait que renforcer le fait que Zero Trust est un projet de transition qui doit se penser stratégiquement sur le moyen terme avec une mise en œuvre progressive et des avancées mesurables. Et comment évaluer l'avancement et les bénéfices au fur et à mesure de votre projet Zero Trust ? : en définissant des indicateurs pour mesurer l'atteinte des objectifs dans le déploiement des fonctionnalités couvrant les attentes que vous avez définies.

Dans son approche pour mesurer l'avancée du projet Zero Trust, le livre blanc Microsoft « ZERO TRUST BUSINESS PLAN, A PRACTICAL GUIDE TO IMPLEMENTING THE ZERO TRUST FRAMEWORK AT YOUR ORGANIZATION », définit trois grandes catégories d'indicateurs qui correspondent à trois objectifs globaux à toute vision Zero Trust que l'on a déjà abordé en étape 3 : le renforcement et l'efficacité de la sécurité, l'ouverture à de nouveaux scénarios business et la simplification de l'implémentation de la sécurité en limitant le nombre de solutions hétérogènes à intégrer (i.e. sortir de l'approche « Best of breed »).



[9] « *Show value along the way.* »

Dans la première catégorie scénarios business, on s'attachera à offrir une expérience la plus transparente et sans anicroches aux utilisateurs en définissant des indicateurs comme le nombre d'authentifications multifacteur rejetées (à minimiser), le pourcentage d'utilisateurs accédant à des applications en SSO, le nombre de demandes de réinitialisation de mots de passe. On s'intéressera également au ressenti de l'utilisateur au quotidien sur les scénarios liés à la mobilité, par exemple le nombre d'accès aux applications depuis des appareils mobiles personnels ou gérés par l'entreprise, mais aussi les performances d'utilisation à distance des outils collaboratifs devenus indispensables avec le télétravail.

La deuxième catégorie, concentrée sur l'efficacité de la sécurité, s'appuiera sur des indicateurs plus techniques comme le nombre et la criticité des incidents de sécurité, le nombre d'incidents détectés et résolus automatiquement, le nombre d'équipements gérés et conformes aux politiques de sécurité, etc.

Enfin, la catégorie concernant la simplification des solutions de sécurité sera évaluée par des indicateurs comme le nombre total de produits de sécurité (souvent plusieurs dizaines initialement), le nombre de solutions nécessitant une intégration et le coût associé, le temps et le coût de leur exploitation, le nombre d'étapes d'un processus de gestion d'incidents et le temps moyen de résolution d'un incident, le pourcentage de faux-positifs…

Ces indicateurs seront synthétisés dans des tableaux de bord pour être présentés régulièrement à la Core Team et relayés vers les instances dirigeantes. Ces éléments constitueront des preuves mesurables de l'avancement du projet, de son efficacité et valideront l'intérêt de continuer dans la transformation Zero Trust.

Les indicateurs seront choisis avec pertinence parmi les informations remontées par une télémétrie qui devra être omniprésente : c'est l'un des retours d'expérience de l'implémentation du modèle Zero Trust par l'informatique interne de Microsoft tel que décrit sur la page IMPLEMENTING A ZERO TRUST SECURITY MODEL AT MICROSOFT. Selon cet article, « *Les données et la télémétrie sont utilisées pour comprendre l'état de sécurité actuel, identifier les lacunes dans la couverture, valider l'impact des nouveaux contrôles et corréler les données de toutes les applications et services de l'environnement. Des capacités d'audit, de surveillance et de télémétrie solides et standardisées sont des exigences essentielles pour les utilisateurs, les appareils, les applications, les services et les modèles d'accès.* »

D'une manière plus générale, la télémétrie aura une couverture plus importante car elle englobe un ensemble plus large d'informations permettant de valider le bon fonctionnement des services et fonctionnalités déployés, et autorisant une vision et un suivi plus fins. Seuls quelques indicateurs seront choisis pour figurer dans les tableaux de bord.

En environnement Microsoft, vous disposez nativement de l'outil SECURE SCORE pour vous aider à évaluer votre posture de sécurité courante et de vous donner une liste

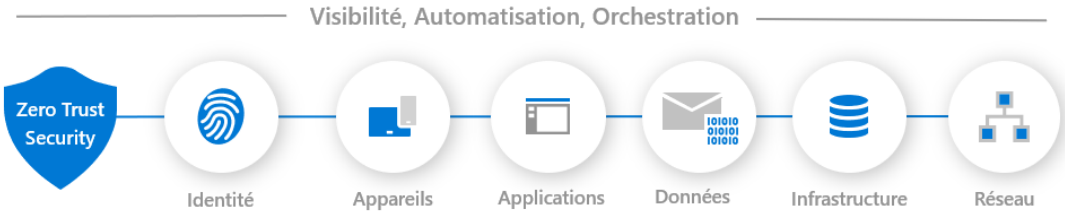
de recommandations pour l'améliorer de manière proactive. Cette fonctionnalité se décline en deux variantes : Secure Score applicable aux charges de travail PaaS, IaaS, hybrides et multi-cloud, et Microsoft Secure Score applicable aux applications travail Microsoft SaaS.

9 Superviser la sécurité

Un des principes de Zero Trust est le fait de présupposer la compromission (« Assume Breach »), c'est-à-dire d'assumer que, malgré tous les contrôles de sécurité mis en place, une attaque pourra se réaliser et fournir une entrée dans le système d'information.

Dans son article Zero Trust Doesn't Mean Zero Breaches, Forrester répond à une question qui leur est couramment posée : Zero Trust aurait-il empêché telle ou telle attaque (SolarWinds, NOELIUM, etc.) ? La réponse est que « *Zero Trust reconnaît que de mauvaises choses arrivent aux bonnes personnes et prescrit la mise en place de techniques pour limiter le rayon de l'explosion, détecter l'incident et réagir automatiquement* ». Cette affirmation met en évidence l'intérêt d'une détection précoce de l'incident, d'une réaction rapide – si possible automatique – pour limiter les impacts de la déflagration.

Si la supervision de la sécurité n'est pas spécifiée comme pilier du Zero Trust, elle n'en constitue pas moins une composante transversale tel qu'indiqué sur le schéma ci-dessous. Il faudra l'envisager sur l'ensemble du périmètre intégrant la partie on-premises et la partie cloud.



L'identité étant le « nouveau périmètre » et la cible privilégiée des attaques, sa surveillance devient une nécessité. Par exemple, vous pouvez remonter les journaux d'activité d'Azure AD dans Azure Monitor ou les transférer dans votre propre SIEM[10] pour traitement. Vous pouvez aussi vous appuyer sur Identity Protection qui se charge d'analyser les signaux, de détecter et de remédier aux risques sur l'identité[11].

Pour superviser la sécurité des postes Windows, vous pourrez vous appuyer sur votre propre EDR ou choisir d'utiliser Microsoft Defender for Endpoint. Pour étendre la

[10] Journaux d'activité Azure Active Directory dans Azure Monitor
[11] Qu'est-ce qu'Identity Protection ?

supervision au-delà, vous pouvez optez soit pour des solutions par services ou fonctions et effectuer le traitement et la corrélation dans votre SIEM (Security Information and Event Management), soit pour un premier niveau d'intégration avec une suite comme Microsoft 365 Defender[12] qui intègre plusieurs outils (Microsoft Defender for Endpoint, Defender for Office 365, Defender for Identity, etc.).

La supervision des ressources cloud est une nécessité, que ce soit pour Azure ou les autres fournisseurs cloud, pour vos applications IaaS, PaaS et sous forme de conteneurs. Par exemple Azure Defender[13] sera en mesure de détecter des menaces dans votre environnement et de générer des alertes de sécurité.

L'élément de la supervision de plus haut niveau reste le SIEM qui collecte les signaux en provenance d'une multitude de sources hétérogènes pour tenter d'en extraire les signaux faibles, remonter des alertes significatives et donner la possibilité d'investiguer sans jongler entre les consoles. Malheureusement, les solutions SIEM classiques ont tendance à multiplier les faux-positifs à cause de l'augmentation exponentielle des signaux à traiter. Des solutions plus récentes s'appuyant sur le cloud et l'Intelligence Artificielle (IA) s'avèrent plus efficaces pour traiter ces masses de signaux, limiter le nombre de faux-positifs et offrir des possibilités d'orchestration et de réponse automatique. On peut citer Microsoft Azure Sentinel[14] qui s'appuie sur l'IA pour identifier rapidement les menaces et supprimer le défaut des SIEM traditionnels en éliminant le besoin de configuration, de maintien et d'évolution de de l'infrastructure.

En résumé, la supervision de la sécurité est composant majeur d'une architecture Zero Trust d'autant que son périmètre va bien au-delà de ce que l'on devait surveiller précédemment puisqu'il s'étend sur les six piliers dont les appareils, l'identité hybride et les applications on-premises et cloud, etc. Un projet Zero Trust est l'opportunité de reconsidérer certains choix avec la possibilité de conserver des solutions de supervision toujours pertinentes à condition de les faire évoluer ou, au contraire, de les remplacer par des solutions plus adaptées profitant des avancées technologiques plus récentes.

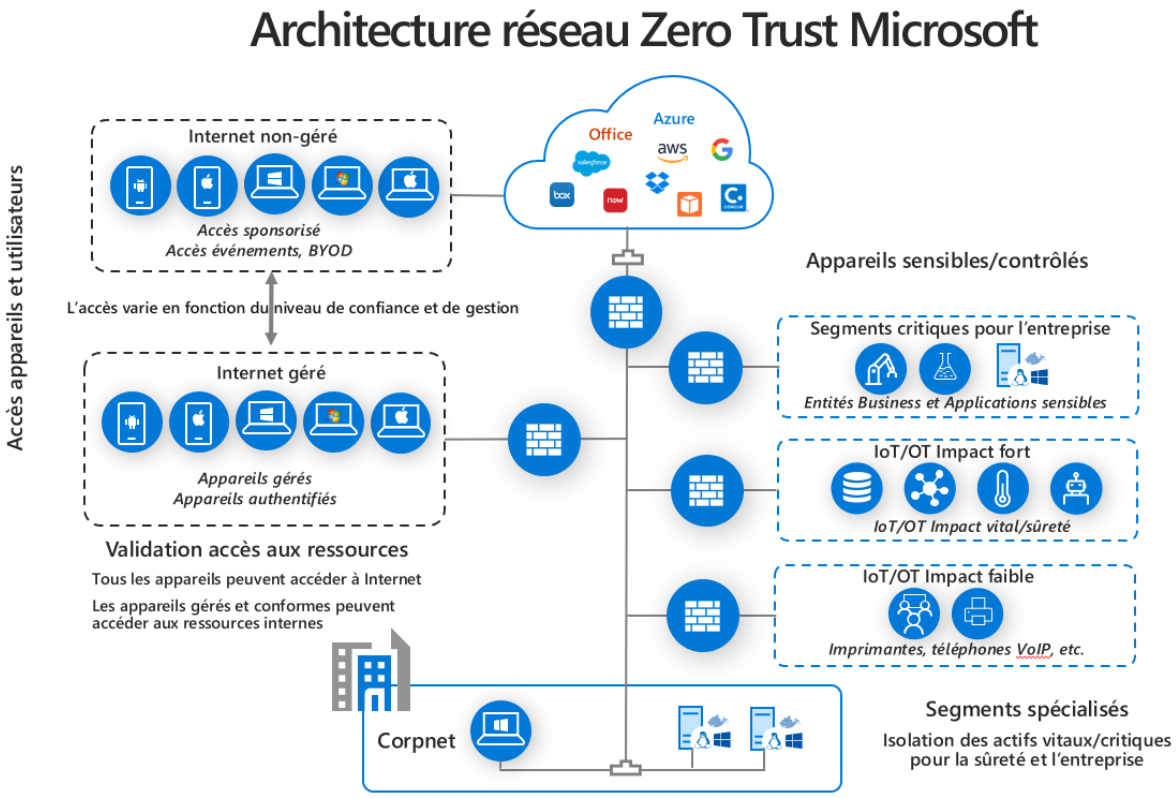
[12] Microsoft 365 Defender
[13] Présentation d'Azure Defender
[14] Qu'est-ce qu'Azure Sentinel ?

10 Internet comme réseau d'entreprise

L'extension du système d'information vers le cloud et les nouveaux scénarios de travail à distance ont bouleversé la manière de penser le réseau d'entreprise. L'époque où le VPN était le seul moyen de se connecter au réseau pour accéder aux applications et à Internet de manière contrôlée est révolue. Un des principes de Zero Trust est de garantir le même niveau de sécurité quel que soit l'endroit depuis lequel l'utilisateur et l'appareil accèdent à l'application ou au service. De plus, la plupart des applications sont désormais accessibles depuis Internet, qu'il s'agisse d'applications d'éditeurs en mode SaaS ou d'applications de l'organisation ayant migré dans le cloud. Les services de gestion des appareils (MDM pour appareils mobiles et PC), les services de sécurité (XDR, etc.), les services d'annuaire (Azure Active Directory) sont également disponibles sous forme de services SaaS permettant ainsi une gestion de la sécurité accessible avec une simple connexion Internet.

Tout ceci concourt au fait que, d'un point de vue IT, « Internet devient le réseau de l'entreprise ». En effet, lorsque les identités sont gérées dans votre annuaire cloud Azure AD, que tous les postes sont pilotés depuis des services cloud, que les applications sont accessibles depuis l'extérieur, et que les systèmes de sécurité sont eux-mêmes capables de fonctionner depuis le cloud, la notion de réseau se banalise. Peu importe où se situe l'appareil de l'utilisateur, il lui suffit d'être en mesure de se connecter à Internet pour accéder avec le même niveau de sécurité à l'ensemble des ressources nécessaires à son travail.

C'est le choix adopté par l'informatique interne de Microsoft qui fournit sur site deux types d'accès à Internet : le réseau appelé « Unmanaged Internet » est réservé aux personnes (invités, participants à des séminaires…) ou aux appareils utilisés en mode BYOD ; le réseau « Managed Internet » est réservé aux employés qui accèdent depuis un appareil géré par l'entreprise. Ce dernier réseau offre, en plus de l'accès Internet, la possibilité d'accéder à des ressources sur site comme les imprimantes. Ces deux réseaux sont accessibles à travers le wifi sur chaque site Microsoft.



Le réseau interne (Corpnet) qui hébergeait auparavant les postes de travail et l'ensemble des ressources (serveurs applicatifs, serveurs de collaboration, serveurs de fichiers, etc.), le tout sous le contrôle de l'annuaire interne Active Directory, s'est fortement réduit suite à ce dépeuplement. Il n'héberge plus que quelques serveurs Windows et Linux et des stations d'administration dûment renforcées et accessibles uniquement par des administrateurs enregistrés. Des segments réseau particuliers ont été créés pour héberger des ressources IoT/OT selon leur niveau de sensibilité et quelques applications critiques conservées en interne[15]. Pour donner une échelle, le nombre de serveurs on-premises a été réduit de 80%, en phase avec la migration des applications puisque 96% sont désormais hébergées dans notre Cloud Azure, dont 65% en PaaS, le reste en IaaS.

Les bénéfices en termes de sécurité sont évidents : la surface d'attaque du réseau interne est fortement réduite suite à la contraction du réseau interne ; les attaques venant principalement des postes de travail compromis et ciblées sur Active Directory deviennent inopérantes ; le rôle de l'annuaire Active Directory devient mineur du fait de son dépeuplement et le rend moins critique ; l'utilisation de stations d'administration strictement sécurisées limite les possibilités de compromission ; enfin, l'isolation des ressources critiques dans des segments réseau renforce leur insensibilité aux attaques.

[15] Implementing a Zero Trust security model at Microsoft

Les bonnes pratiques d'architecture de sécurité réseau que l'on respectait pour les applications internes s'appliquent aussi aux applications hébergées dans le cloud, pour la segmentation des sous-réseaux, les DMZ, l'utilisation des contrôles réseau, etc.[16]

Cet exemple sera certainement à adapter en fonction de votre propre existant mais il constitue une cible et dresse les grands principes :

- La transition se fait par une contraction du réseau interne au profit d'un basculement vers des liens Internet ;
- Il est préconisé de mettre en place une segmentation réseau pour les ressources qui restent hébergées en interne et de prendre en compte les ressources OT/IoT[17]. Concernant les systèmes OT et IoT, il est recommandé d'utiliser des segments réseau différents. Pour les systèmes OT, une granularité plus fine dans la segmentation est conseillée en appliquant plusieurs niveaux en respect du modèle Purdue[18].
- Les applications ayant migré dans le cloud ou développées spécifiquement doivent respecter les bonnes pratiques d'architecture de sécurité réseau.

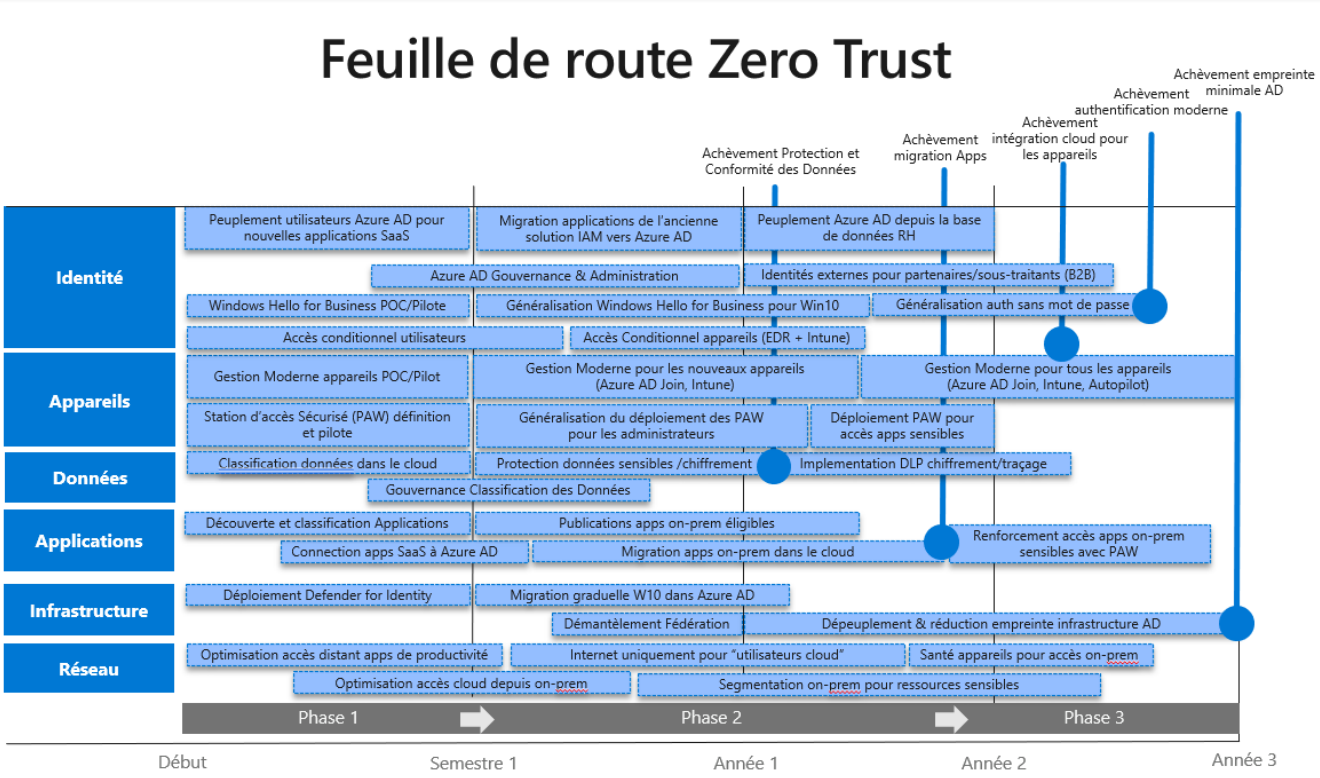
[16] MEILLEURES PRATIQUES AZURE POUR LA SECURITE RESEAU
[17] How to apply a Zero Trust approach to your IoT solutions
[18] Purdue Enterprise Reference Architecture - Wikipedia

11 Définir une feuille de route

La feuille de route (roadmap) constitue l'aboutissement de vos réflexions de cette phase d'initiation de votre projet Zero Trust. C'est le livrable que vous devez construire pour positionner l'ensemble des sujets qui devront être traités, les ordonner et en évaluer la durée. Vous devez prendre en compte les attentes prioritaires (définies au chapitre 3 POURQUOI UN PROJET ZERO TRUST ?), les quick wins – même s'ils n'apparaissent pas directement dans la vision globale – et indiquer les étapes importantes. Les sujets seront répartis selon les six grands piliers du Zero Trust. La figure représentera une vue synthétique de l'ensemble des chantiers qui vous attendent, et prendra en compte les sujets liés à l'intégration dans l'existant et les impacts sur les briques de sécurité déjà en place : certaines briques seront reconduites et devront être prises en compte dans l'intégration avec les autres briques Zero Trust, alors que d'autres disparaîtront ou, a minima, seront conservées dans un périmètre nettement plus réduit. Cette roadmap n'aura pas la précision d'un plan projet détaillé mais fournira une vision globale suffisamment précise pour aller défendre votre projet de transformation.

Pour rentrer dans le concret, prenons un exemple de roadmap basé sur des cas réels de clients ayant mené cette phase de cadrage Zero Trust. Vous remarquerez que de nombreuses briques font appel à des solutions Microsoft, ce qui a été un choix dicté par une volonté de limiter les coûts d'intégration et de simplifier l'administration de la sécurité en limitant, entre autres, le nombre de portails d'administration.

On apporte dans la suite du chapitre une description rapide de chaque chantier et des briques technologiques mises en œuvre.



Tout d'abord, remarquez la structuration selon les six piliers du Zero Trust qui apparaissent sur la gauche.

Le pilier Identité est, sans surprise, assez riche, avec l'annuaire Azure AD qui devient l'annuaire de référence des identités après la migration de la précédente plateforme de gestion des identités on-premises puis sa suppression[19]. A terme, les liens de synchronisation avec Active Directory sont dévalidés avec l'approvisionnement des identités depuis le système de Ressources Humaines. L'accès conditionnel est mis en place dès le départ pour les utilisateurs (c'est un quick-win) puis étendu aux appareils qui sont gérés depuis le MDM Microsoft Intune[20] et dont la sécurité et l'état de santé sont transmis par l'EDR en place. Le chantier d'authentification biométrique Windows Hello for Business[21] est lancé dès le démarrage sous la forme d'une preuve de concept (autre quick win) avant d'être généralisé puis associé à l'authentification sans mot de passe disponible nativement avec Azure AD. L'étape « *Achèvement de l'authentification moderne* » est indiquée sur la roadmap, étant jugée importante dans la sécurisation des accès des utilisateurs. Enfin, le chantier *Azure AD Gouvernance & Administration* est crucial dès lors que l'annuaire devient la référence

[19] On parle de la plateforme de gestion des identités et non d'Active Directory dont l'empreinte sera réduite mais qui ne sera pas supprimé.
[20] Documentation de Microsoft Intune
[21] Vue d'ensemble de Windows Hello for Business

des identités et qu'il convient de mettre en place dès le départ les bonnes pratiques d'administration et de sécurisation de l'accès à ce composant.

Le pilier Appareils enchaîne trois phases dans le chemin vers une gestion « moderne » en démarrant avec un pilote où les postes et mobiles dans ce premier périmètre sont joints à Azure AD puis enregistrés et gérés dans Microsoft Intune. La phase suivante procède à l'extension du périmètre pour les nouveaux appareils en y adjoignant le processus de construction rapide des postes avec Windows Autopilot[22] dont l'implémentation a été jugée nécessaire pour couvrir le scénario du télétravail.

Les réflexions sur la sécurité de l'administration de l'ensemble des applications et services ont mené à considérer le déploiement de stations d'administration sécurisées (Privileged Access Workstation ou PAW[23]) ; ces postes sont construits sur un socle Windows 10/Windows 11 contraint et contrôlé, réservé aux tâches d'administration. Le socle héberge une machine virtuelle Windows avec l'image d'un poste « classique » permettant d'utiliser les applications de productivité Office et d'accéder à Internet sans les restrictions imposées sur le socle. C'est la solution qui a été retenue pour reprendre le contrôle des postes d'administration et limiter le risque de compromission des comptes à privilège.

Le pilier Données débute par la mise en place de la classification des données hébergées dans le cloud, une grande partie des données ayant migré sur SharePoint Online. Certaines données sensibles resteront on-premises, hébergées sur des serveurs sécurisés dans des segments réseau isolés avec des contraintes d'accès exigeantes. Le chantier de *Gouvernance de la Classification des Données* sera enclenché pour définir les processus de gestion des données en fonction de leur sensibilité. Le chantier de protection des données suivra pour appliquer un chiffrement sur les données en fonction de la sensibilité basée sur l'étiquetage suite à la classification, qu'elle soit automatique ou sous la responsabilité du créateur/possesseur de l'information.

L'atteinte de l'étape « *Achèvement de la Protection et Conformité des Données* » scelle un moment important du projet Zero Trust, puisque ce dernier aura fourni l'occasion de mettre en place une solution de classification souvent reportée faute de solutions techniques adaptées.

Enfin, la fonctionnalité de DLP (Data Loss Prevention) sera ensuite activée et paramétrée au niveau des CASB (Cloud Access Security Broker) déjà déployés par l'entreprise (voir ci-dessous).

Le pilier Applications commence par le déploiement de la fonction de CASB au niveau de l'entreprise, le choix ayant été fait d'utiliser la solution

---

[22] Vue d'ensemble de Windows Autopilot
[23] Protecting high-risk environments with secure admin workstations

Microsoft Cloud App Security[24]. Le CASB sera en mesure de découvrir l'ensemble des applications cloud utilisées, dont certaines applications SaaS non référencées par l'informatique interne (« Shadow IT »). Il sera possible de leur assigner un niveau de risque et d'en approuver ou non leur utilisation. Les applications SaaS seront ensuite progressivement connectées à Azure AD (pour celles qui ne le sont pas nativement[25]) pour s'appuyer sur le référentiel des identités de l'annuaire et profiter du SSO[26]. Deux chantiers seront menés en parallèle : le premier pour migrer dans le cloud les applications historiques éligibles ; le second pour publier les applications Web plus anciennes à travers des reverse-proxies en s'appuyant sur les authentifications Azure AD.

L'étape « *Achèvement migration Applications* » est importante puisque toutes les applications éligibles à une bascule dans le cloud ont été migrées. Seules restent hébergées on-premises les applications et ressources considérées comme spécialement critiques au regard de la politique de sécurité de l'entreprise ou des exigences réglementaires. Le dernier chantier consiste à imposer l'utilisation de stations sécurisées PAW pour l'accès à ces ressources particulières.

Le pilier Infrastructure se lance par le déploiement de la solution Microsoft Defender for Identity[27] pour surveiller l'Active Directory et être en mesure de détecter les attaques ou compromissions en attendant de réduire drastiquement sa surface d'attaque. Les postes Windows 10/Windows 11 vont ensuite progressivement migrer vers Azure AD en relation avec Windows Intune pour leur gestion. La fonction de fédération entre Active Directory (et éventuellement les autres annuaires internes) et Azure Active Directory sera supprimée dès lors que toutes les applications auront basculé sur l'authentification Azure AD (voir pilier Applications).

Le dernier chantier prend en charge le dépeuplement progressif d'Active Directory au fur et à mesure où les utilisateurs et comptes machines migrent vers Azure : l'infrastructure, qui peut comprendre de nombreuses forêts et une multitude de contrôleurs de domaine, va pouvoir être réduite à une taille minimale qui resterait nécessaire pour administrer les ultimes ressources internes. Cette diminution de l'empreinte d'Active Directory a pour avantage de réduire de manière radicale la surface d'attaque du SI, limitant ainsi la probabilité de compromission avec les scénarios d'attaque utilisés communément. La surveillance restera de mise pour continuer à protéger les ressources internes.

Le dernier pilier Réseau se focalisera en priorité sur l'optimisation des accès distants aux applications et services de productivité, comme par exemple les outils collaboratifs Office 365. Dans un contexte où le télétravail est devenu la nouvelle norme, il est nécessaire d'offrir aux utilisateurs les moyens de travailler efficacement

---

[24] Microsoft Cloud App Security
[25] Liste des applications intégrées nativement à Azure AD
[26] Didacticiels pour l'intégration d'applications SaaS avec Azure Active Directory
[27] Qu'est-ce que Microsoft Defender pour Identity ?

depuis chez eux. L'ère du tout VPN est révolue et les accès distants doivent concilier performance et respect du niveau de sécurité[28]. On devra prendre en compte plus particulièrement les flux audio et vidéo qui imposent des conditions de quasi-temps réel pour offrir une expérience utilisateur optimale.

L'architecture réseau interne devra être revue pour assurer une connexion performante au cloud que ce soit à travers Internet ou par le biais de connexions directes aux fournisseurs de cloud. Les sites de l'entreprise devront être adaptés pour accueillir les postes dans des segments réseau différenciés (voir le chapitre 10) avec l'objectif de faire d'Internet le réseau par défaut de l'entreprise pour la plus grande partie des utilisateurs. Enfin, la segmentation du réseau interne sera adaptée pour héberger les ressources internes en fonction de leur sensibilité, avec des accès contrôlés prenant de plus en compte le niveau de santé et de conformité des postes.

La manière dont les chantiers seront menés – par exemple sous forme de sprints dans le cadre d'une approche agile – n'est pas détaillée à ce niveau pour laisser la liberté à chaque chantier de choisir la meilleure méthode.

[28] Voir le livre blanc Optimiser le télétravail Office 365 avec le split-tunneling Q-A disponible en versions française et anglaise.

Conclusion

Pour conclure, on peut citer cette description extraite du document EXAMINING ZERO TRUST AN EXECUTIVE ROUNDTABLE DISCUSSION, « *La sécurité Zero Trust n'est pas un produit ou une solution. Il s'agit d'une stratégie plus large de sécurité moderne qui s'adapte à la complexité de l'environnement business actuel, prend en compte la main-d'œuvre mobile et protège les personnes, appareils, applications et données, où qu'ils se trouvent* ».

Cette citation qui résume l'âme du Zero Trust doit cependant se décliner à travers un véritable projet de transformation du modèle de sécurité, induit par une façon nouvelle dont la sécurité doit être adressée pour faire face aux nouvelles menaces cyber. Aller vers le Zero Trust, ce n'est pas qu'une simple révision de la sécurité réseau : six piliers doivent être considérés avec en priorité l'identité. En effet, « l'identité est le nouveau périmètre » : l'accent doit être porté sur le renforcement de l'authentification et un contrôle d'accès conditionnel basé sur l'identité, le niveau de risque associé et plus largement sur le contexte d'accès – incluant l'appareil et son statut.

Pour démarrer un projet Zero Trust, il faut être ambitieux dans la vision, commencez par des étapes raisonnables tout en étant rapide dans l'exécution, ce qui peut se résumer par la formule « Think big, start small, move fast » (Pensez grand, commencez petit, avancez vite). Il faut voir grand car il s'agit d'un projet de transformation : l'établissement de la feuille de route doit développer cette vision en la déclinant technologiquement sur l'axe des temps. Vous devrez définir quelles sont vos attentes prioritaires dans les deux catégories que sont le renforcement de la sécurité et l'ouverture de nouveaux scénarios business ; des étapes rapides avec des gains visibles vous permettront de montrer rapidement les bénéfices de votre projet Zero Trust.

Il n'est pas question de repartir de zéro mais de prendre en compte l'existant en évaluant votre niveau de maturité et en construisant votre propre solution : certaines briques seront conservées et adaptées, d'autres seront remplacées par des solutions plus performantes avec, comme objectif, de limiter le nombre d'outils de sécurité disparates pour gagner en efficacité tout en réduisant les coûts.

Pour conclure, à l'heure où la cybersécurité devient un enjeu majeur dans la vie des entreprises, il est temps d'assumer que l'ancienne vision d'une sécurité périmétrique est désormais obsolète, et que l'adoption du nouveau modèle de sécurité Zero Trust vous permettra de résoudre les défis d'aujourd'hui.