École 2600

Cours Zero Trust

Implémentation 2

Juillet 2023

Feuille de route Zero Trust

Bénéfices attendus du Zero Trust

- Renforcement et rationalisation de la cybersécurité
  - Remise à plat du modèle existant ⇒ mise en évidence des points forts/faibles
    - Maturité de la gestion des identités
    - Robustesse de l'authentification
    - Sécurité/gestion des appareils à l'extérieur du réseau d'entreprise
    - Capacité de supervision / détection / réaction / anticipation globale interne + Cloud
  - Vision globale et cohérente, structuration de l'approche ⇒ meilleure pertinence des investissements (*vs* « empilage » de solutions de sécurité)
- Conformité & confiance des parties prenantes (clients, partenaires, usagers, etc.)
  - LPM, NIS2, RGPD, ISO 27001, HDS, etc. ⇒ l'approche Zero Trust permet de constituer un référentiel de processus, d'applications, d'outils et de bonnes pratiques en ligne avec les exigences des règlements, normes et standards de sécurité de l'information

Bénéfices attendus du Zero Trust

- Bénéfices techniques
  - Supervision, analyse dynamique et automatisation : une meilleure administration
  - Gestion des autorisations : une granularité plus fine
  - Une meilleure protection des ressources du système d'information
  - Un contrôle dynamique des applications et des données
- Possibilité de nouveaux scénarios business : ouvrir son système d'information aux clients et partenaires sans risquer la compromission
  - Ex. modèle commercial ou administratif orienté services, 5G
  - Mise à disposition du moteur d'accès conditionnel pour les nouveaux projets
- Projet d'entreprise, donc qui implique tous les acteurs dans l'amélioration de la posture de cybersécurité
- Augmentation de la résilience du SI et donc de la confiance que lui porte l'organisation

Zero Trust implique-t-il abandon du VPN ?

- Selon l'ANSSI, certainement pas !

https://www.ssi.gouv.fr/uploads/2021/08/anssi-article-systemes_information_hybrides_et_securite_un_retour_a_la_realite.pdf

« *L'usage d'un tunnel VPN est incontournable pour les usages les plus sensibles (ex. administration de SI)*

- *Dans ce cas précis, le tunnel doit aboutir sur une zone de confiance restreinte du SI, pour garantir que tous les flux applicatifs soient protégés et ce, quel que soit le réseau sur lequel ils sont transportés*
- *Le risque d'une attaque de type homme-du-milieu est considérablement réduit par rapport à l'utilisation seule de HTTPS*
- *En effet, les postes de travail et les navigateurs Web disposent par défaut d'une liste conséquente d'autorités de certification de confiance, contrairement à un client VPN IPsec censé faire confiance à un nombre très limité d'autorités de confiance configurées spécifiquement* »

Feuille de route Zero Trust

- Comment initier un projet de transformation Zero Trust ?
  - Étape 1 : Définition de la stratégie Zero Trust
  - Étape 2 : Évaluation de l'existant
  - Étape 3 : Définition des étapes du projet
  - Étape 4 : Sensibilisation et acculturation cybersécurité

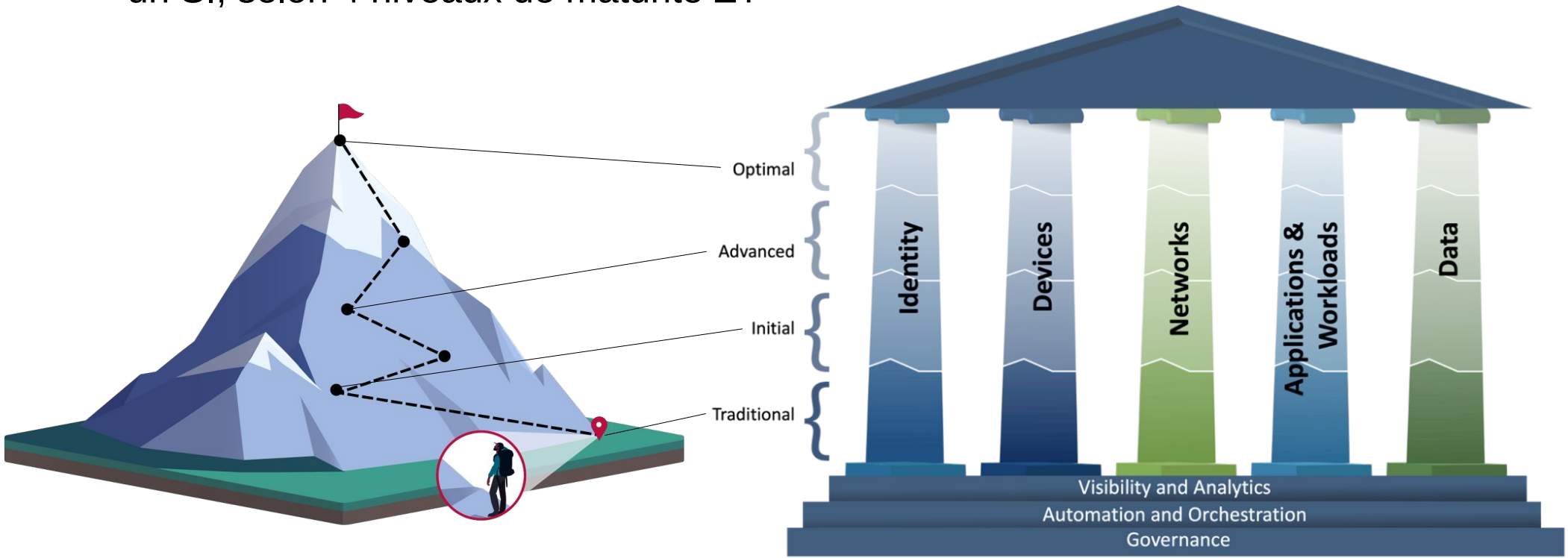
- Attention à ne pas se laisser influencer par les discours marketing
  - Risque de vision partielle du Zero Trust
- Si toutes les briques ne sont pas correctement implémentées, le résultat pourrait être catastrophique

Définition de la stratégie Zero Trust

- Zero Trust : à la fois modèle et programme
  - 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**
- Par son périmètre et les nombreux sujets à aborder, prendre en compte les concepts du Zero Trust s'apparente plus à mettre en place un **programme**
  - Ensemble de projets qui se développent dans le temps
  - Programme transversal devant impliquer l'organisation au-delà des seules équipes sécurité et réseau, exemples :
    - Ressources humaines
    - Gestion des postes de travail
    - Supervision du SI
    - Responsables applicatifs

Évaluation de l'existant

- Le « *Zero Trust Maturity Model* » du CISA propose aux organisations une approche pragmatique pour inventorier et catégoriser les éléments présents sur un SI, selon 4 niveaux de maturité ZT



Source : CISA https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Modèle de maturité Zero Trust du CISA

	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
	Visibility and Analytics		*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Source : CISA

Définition des étapes du projet

- La transformation ne peut se faire que progressivement
- L'approche doit être globale, cohérente et intégrée dans l'architecture SI, avec une coordination des équipes autour de cet objectif commun
- Conseil : commencer par des gains rapides (*quick wins*)
  - Ex. généralisation du MFA sur les applications sensibles
  - Résultats rapidement visibles ⇒ confiance des utilisateurs et soutien du management
- Le plus difficile sera de rendre des applications existantes (le *legacy*) compatibles avec les principes du Zero Trust et la classification des données
- Mettre en place une gouvernance qui permettra de définir les exigences propres au respect des règles d'intégration des nouvelles applications dans les briques Zero Trust
  - Par exemple définir des indicateurs de conformité ZT dans les projets, en plus de la classification DICT des applications
- Mise à contribution du DPO pour les données à caractère personnel

Sensibilisation et acculturation cybersécurité

- Un projet Zero Trust n'est pas *que* technique, il nécessite :
  1. Une évolution de la « culture » sécurité de ses acteurs principaux
  2. Le soutien du projet par l'organisation jusqu'au plus haut niveau (direction)
  3. La classification des informations en vue de déterminer leur besoin de protection
  4. L'implication des équipes métiers et la gestion du changement auprès des utilisateurs
- Il faut s'assurer que d'un point de vue organisationnel et opérationnel :
  - Les ressources humaines sont en place pour garantir le bon fonctionnement du modèle
    - Ex. 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 sont respectés
    - Principe de moindre privilège, besoin d'en connaître, séparation des responsabilités, etc.

Maturité Zero Trust
Modèle CISA

Niveaux de maturité

Niveau	Définition
Traditionnel	Cycles de vie (c'est-à-dire depuis l'établissement jusqu'au décommissionnement) et affectation d'attributs (sécurité et journalisation) configurés manuellement
	Politiques et solutions de sécurité statiques qui traitent un pilier à la fois avec des dépendances séparées vis-à-vis des systèmes externes
	Moindre privilège établi uniquement lors du provisionnement
	Application des politiques cloisonnée par pilier
	Déploiement manuel de la réponse aux incidents et remédiation
	Corrélation limitée des dépendances, des journaux et de la télémétrie
Initial	Début de l'automatisation de l'affectation des attributs et de la configuration des cycles de vie, des décisions et application des politiques, et solutions initiales inter-piliers avec intégration de systèmes externes
	Quelques changements réactifs apportés au moindre privilège après le provisionnement
	Visibilité agrégée pour les systèmes internes

Niveaux de maturité

Avancé	Dans la mesure du possible, contrôles automatisés dans le cycle de vie et l'attribution des configurations et politiques, avec coordination inter-piliers
	Visibilité et contrôle des identités centralisés
	Application des politiques intégrée dans tous les piliers
	Processus pré-définis de remédiation et réponse aux incidents
	Changements apportés au moindre privilège en fonction de l'évaluation des risques et de la posture
	S'orienter vers une vision précise sur l'ensemble des ressources de l'entreprise (incluant celles hébergées en externe)
Optimisé	Automatisation complète en temps réel des cycles de vie et des affectations d'attributs aux actifs et ressources qui s'auto-déclarent, avec des politiques dynamiques basées sur des déclencheurs automatisés/observés
	Accès dynamiques avec moindre privilège (seulement ce qui est nécessaire et dans des limites définies) pour les actifs et leurs dépendances à l'échelle de l'entreprise
	Interopérabilité inter-piliers avec surveillance continue
	Visibilité centralisée avec une connaissance précise et exhaustive de la situation

Pilier **identité**

Une identité fait référence à un attribut ou à un ensemble d'attributs décrivant de manière unique un utilisateur ou une entité

Fonction	Traditionnel	Initial	Avancé	Optimal
Authentification	Mot de passe ou MFA avec droits d'accès statiques en fonction de l'identité de l'entité	Authentification par MFA pouvant comporter un mot de passe et validation éventuelle de plusieurs attributs de l'entité (ex. localisation ou activité)	Début de l'authentification de toutes les identités par MFA résistant au phishing et validation d'attributs, incluant une implémentation initiale de MFA sans mot de passe (ex. FIDO2)	Validation de l'identité par MFA résistant au phishing, en continu et pas seulement lors de l'accès initial
Référentiel des identités	Sur site et géré en interne (c'est-à-dire planifié, déployé et entretenu par l'entreprise)	Combinaison entre géré en interne sur site et hébergé (ex. Cloud ou autre entreprise) avec un minimum d'intégration entre les différents référentiels (ex. SSO)	L'entreprise commence à consolider et intégrer de façon sécurisée des référentiels gérés en interne ou hébergés	L'entreprise intègre de façon sécurisée et appropriée les référentiels d'identité de tous les environnements et partenaires

Pilier **identité**

Fonction	Traditionnel	Initial	Avancé	Optimal
Évaluation des risques	Évaluation limitée des risques liés aux identités (ex. vraisemblance d'une compromission)	L'entreprise détermine les risques liés aux identités en utilisant des méthodes manuelles et des règles statiques pour assister la visibilité	L'entreprise détermine les risques liés aux identités en utilisant certaines méthodes automatisées et des règles dynamiques pour assister les activités de décision d'accès et de réponse aux incidents	Détermination des risques liés aux identités en temps réel sur la base d'une analyse continue et de règles dynamiques pour délivrer une protection permanente
Gestion des accès	Autorisations d'accès permanentes avec révision périodique pour les comptes privilégiés et non privilégiés	Autorisations, y compris pour les demandes d'accès privilégiés, qui expirent via une revue automatisée	Autorisations, basées sur les besoins et les sessions, adaptées aux actions et ressources, y compris pour les demandes d'accès privilégiés	Utilisation de l'automatisation pour autoriser des accès « just-in-time / just-enough » adaptés aux besoins individuels d'actions et de ressources

Pilier **identité**

Fonction	Traditionnel	Initial	Avancé	Optimal
Visibilité et analyse	Collecte de journaux d'activité utilisateurs et entités, en particulier pour les comptes privilégiés, et quelques analyses manuelles régulières	Collecte de journaux d'activité utilisateurs et entités, et analyses manuelles régulières plus quelques analyses automatisées, avec une corrélation limitée entre les différents types de journaux	Analyse automatisée de certains types de journaux d'activités utilisateurs et entités, et intensification de la collecte pour combler les lacunes de visibilité	L'entreprise maintient une visibilité et une connaissance exhaustives de la situation en réalisant une analyse comportementale automatisée des journaux d'activités utilisateurs
Automatisation et orchestration	Orchestration manuelle des identités gérées en interne (onboarding, offboarding et désactivations des utilisateurs et entités), avec peu d'intégration et des revues régulières	Orchestration manuelle des identités privilégiées et externes, et orchestration automatisée des utilisateurs non privilégiés et des entités gérées en interne	Orchestration manuelle des identités privilégiées et orchestration automatisée de toutes les identités sur tous les environnements	Orchestration automatisée de toutes les identités avec une intégration complète de tous les environnements, basée sur les comportements, les enrôlements et les besoins de déploiement

Pilier **identité**

Fonction	Traditionnel	Initial	Avancé	Optimal
Gouvernance	Politiques de gestion des identités (authentification, informations d'identification, accès, cycle de vie, etc.) avec application via des mécanismes techniques statiques, et revues manuelles	Définition et début de mise en œuvre de politiques de gestion des identités appliquées à l'ensemble de l'entreprise, avec un minimum d'automatisation et des mises à jour manuelles	Implémentation de politiques de gestion des identités appliquées à l'ensemble de l'entreprise avec automatisation et mises à jour périodiques	Implémentation et automatisation totale de politiques de gestion des identités pour l'ensemble de l'entreprise, utilisateurs et entités sur tous les systèmes, avec application en continu et mises à jour dynamiques

Pilier **appareils**

Un appareil fait référence à tout actif (y compris son matériel, ses logiciels, son micrologiciel, etc.) pouvant se connecter à un réseau, y compris les serveurs, machines de bureau et portables, imprimantes, téléphones mobiles, objets connectés, équipements réseau, etc.

Fonction	Traditionnel	Initial	Avancé	Optimal
Gestion des risques liés aux actifs et à la chaîne d'approvi-sionnement	Actifs physiques ou virtuels non suivis à l'échelle de l'entreprise ou des fournisseurs, et chaîne d'approvi-sionnement des appareils et services gérée de manière ad hoc avec une vision limitée des risques pour l'entreprise	Tous les actifs physiques et certains actifs virtuels sont suivis, et les risques liés à la chaîne d'approvi-sionnement sont gérés dans un cadre robuste en établissant des politiques et des contrôles conformément aux bonnes pratiques	Début du développement d'une cartographie des actifs physiques et virtuels de l'entreprise, via des processus automatisés pouvant couvrir de multiples fournisseurs, dans un but de contrôle des acquisitions, de suivi des cycles de développement et d'évaluation des tiers	Cartographie en temps réel ou quasi-réel de tous les actifs, fournisseurs et prestataires de services, si possible gestion automatisée des risques de la chaîne d'approvi-sionnement, processus opérationnels conçus pour tolérer les défaillances de la chaîne d'approvisionnement, tout ceci conformément aux meilleures pratiques

Pilier **appareils**

Fonction	Traditionnel	Initial	Avancé	Optimal
Application de la politique & surveillance de la conformité	Visibilité sur la conformité des appareils (capacité d'inspecter leur comportement) limitée voire inexistante, avec peu de méthodes d'application des politiques ou de gestion des logiciels, des configurations et des vulnérabilités	Collecte de caractéristiques auto-déclarées par les appareils (ex. clés, jetons, utilisateurs locaux, etc.) mais mécanismes d'application des politiques limités	Informations sur l'appareil vérifiées (c'est-à-dire qu'un administrateur peut inspecter et vérifier les données) lors de l'accès initial et application de la conformité, pour la plupart des appareils et actifs virtuels	Vérification continue des informations sur l'appareil et application de la conformité tout au long de la durée de vie des appareils et des actifs virtuels
		Début de mise en œuvre d'un processus basique d'approbation des logiciels et de mise à jour et configuration des appareils	Méthodes automatisées pour gérer les appareils et les actifs virtuels, approuver les logiciels, identifier les vulnérabilités et installer les correctifs	Intégration de la gestion des appareils, des logiciels, de la configuration et des vulnérabilités dans tous les environnements, y compris pour les actifs virtuels

Pilier **appareils**

Fonction	Traditionnel	Initial	Avancé	Optimal
Accès aux ressources	L'accès aux ressources ne nécessite pas une visibilité sur la conformité des appareils ou actifs virtuels utilisés	Quelques appareils ou actifs virtuels doivent déclarer leurs caractéristiques, cette information étant utilisée pour contrôler l'accès à certaines ressources	L'accès initial aux ressources prend en compte les informations vérifiées sur les appareils ou les actifs virtuels	L'accès aux ressources tient compte de l'analyse des risques en temps réel au sein des appareils et des actifs virtuels
Protection contre les menaces sur les appareils	Moyens de protection contre les menaces déployés manuellement sur certains appareils	Quelques processus automatisés pour le déploiement et la mise à jour de moyens de protection contre les menaces sur les appareils et les actifs virtuels, avec une intégration limitée de l'application des politiques et de la surveillance de la conformité	Début de la consolidation dans des solutions centralisées des moyens de protection contre les menaces sur les appareils et les actifs virtuels, et intégration de la plupart de ces moyens avec l'application des politiques et la surveillance de la conformité	Solution(s) centralisée(s) de protection contre les menaces déployée(s) avec des fonctionnalités avancées pour tous les appareils et actifs virtuels, et approche unifiée de la protection contre les menaces sur les appareils, l'application des politiques et la surveillance de la conformité

Pilier **appareils**

Fonction	Traditionnel	Initial	Avancé	Optimal
Visibilité et analyse	Inventaire avec étiquetage physique des appareils, surveillance logicielle limitée pour revue régulière complétée par quelques analyses manuelles	Identifiants numériques (ex. adresses d'interfaces, balises numériques) en complément de l'inventaire manuel, et surveillance « endpoint » des appareils sur lesquels c'est possible	L'entreprise automatise à la fois la collecte d'inventaire (comprenant une surveillance « endpoint » sur tous les appareils utilisateur standards, ex. ordinateurs de bureau et portables, téléphones mobiles, tablettes et actifs virtuels, etc.) et une détection d'anomalies visant à découvrir les appareils non autorisés	Collecte automatisée de l'état de tous les appareils et actifs virtuels connectés au réseau tout en établissant une corrélation avec les identités, avec surveillance « endpoint » et détection d'anomalies pour informer le module de contrôle d'accès aux ressources
		Certains appareils et actifs virtuels font l'objet d'une analyse automatisée (ex. logicielle) pour une détection d'anomalies basée sur le risque		Pistage des provisionnements et/ou déprovisionnements d'actifs virtuels en vue de détecter des anomalies

Pilier **appareils**

Fonction	Traditionnel	Initial	Avancé	Optimal
Automatisation et orchestration	Provisionnement, configuration et/ou enregistrement des appareils effectués manuellement au sein de l'entreprise	Début de mise en œuvre d'outils et de scripts pour automatiser les processus de provisionnement, de configuration, d'enregistrement et/ou de déprovisionnement des appareils et des actifs virtuels	Mécanismes de surveillance et procédures pour identifier et déconnecter ou isoler manuellement les appareils et actifs virtuels non conformes (ex. certificat vulnérable ou non vérifié, adresse MAC non enregistrée, etc.)	Processus entièrement automatisés pour le provisionnement, l'enregistrement, la surveillance, l'isolement, la correction et le déprovisionnement des appareils et des actifs virtuels
Gouvernance	Quelques politiques concernant le cycle de vie des appareils informatiques traditionnels et leurs périphériques, processus manuels pour maintenir (ex. mettre à jour, corriger, assainir) ces appareils	Politiques (et application de celles-ci) concernant l'approvisionnement de nouveaux appareils, le cycle de vie des appareils informatiques non traditionnels et des actifs virtuels, et pour effectuer régulièrement une surveillance et une analyse de sécurité des appareils	Politiques à l'échelle de l'entreprise pour le cycle de vie des appareils et des actifs virtuels, y compris leur énumération et leur justification, avec quelques mécanismes d'application automatisés	Politiques et application entièrement automatisées pour le cycle de vie de tous les appareils et actifs virtuels connectés au réseau dans l'entreprise

Pilier **réseaux**

Un réseau fait référence à un support de communication ouvert comprenant des canaux tels que les réseaux internes, les réseaux sans fil et Internet, ainsi que d'autres supports potentiels tels que les canaux cellulaires et applicatifs utilisés pour transporter les messages

Fonction	Traditionnel	Initial	Avancé	Optimal
Segmentation réseau	Architecture réseau définie par larges périmètres et macro-segmentation avec des restrictions minimales d'accessibilité entre les segments de réseau, pouvant également s'appuyer sur des interconnexions multi-services (par exemple des tunnels VPN à large bande)	Début de déploiement d'une architecture réseau avec isolation des zones de travail critiques, limitation de la connectivité selon le principe de besoin minimal et transition vers des interconnexions spécifiques à chaque service	Déploiement sur une plus grande partie de l'architecture réseau de mécanismes d'isolation des extrémités (ex. terminaux et serveurs) et des applications avec des micro-périmètres d'entrée/sortie et des interconnexions spécifiques à chaque service	Architecture réseau composée de micro-périmètres d'entrée/sortie entièrement distribués et d'une micro-segmentation étendue basée sur des profils d'applications avec une connectivité dynamique « just-in-time / just-enough » pour des interconnexions spécifiques à chaque service

Pilier **réseaux**

Fonction	Traditionnel	Initial	Avancé	Optimal
Gestion du trafic réseau	Implémentation manuelle de règles et de configurations réseau statiques pour gérer le trafic lors de l'établissement des services, avec des capacités de surveillance limitées (ex. surveillance des performances des applications ou détection d'anomalies) et des audits et examens manuels des modifications de profil pour les applications critiques	Établissement de profils d'applications avec des fonctionnalités de gestion du trafic distinctes et début du mapping de toutes les applications sur ces profils Mise en œuvre de règles statiques étendue à toutes les applications et audits manuels périodiques des profils d'applications	Mise en œuvre de règles et de configurations réseau dynamiques pour l'optimisation des ressources, qui sont périodiquement adaptées sur la base d'évaluations des risques et de surveillance automatisée des profils d'applications	Mise en œuvre de règles et de configurations réseau dynamiques qui évoluent en permanence pour répondre aux besoins des profils d'applications et reprioriser les applications en fonction de la criticité de la mission, des risques, etc.

Pilier **réseaux**

Fonction	Traditionnel	Initial	Avancé	Optimal
Chiffrement des communications	Chiffrement minimal du trafic qui s'appuie sur des processus manuels ou ad hoc pour gérer et sécuriser les clés de chiffrement	L'entreprise commence à chiffrer tout le trafic vers les applications internes, à privilégier le chiffrement pour le trafic vers les applications externes (ex. HTTPS plutôt que HTTP), à formaliser les politiques de gestion des clés et à sécuriser les clés de chiffrement des serveurs/services	Chiffrement de toutes les communications internes et externes possibles, gestion de l'émission et de la rotation des clés et des certificats, et début de l'intégration des meilleures pratiques d'agilité cryptographique	L'entreprise continue d'étendre le chiffrement des communications selon les besoins, applique le principe de moindre privilège pour une gestion sécurisée des clés à l'échelle de l'entreprise et intègre les meilleures pratiques d'agilité cryptographique aussi largement que possible

Pilier **réseaux**

Fonction	Traditionnel	Initial	Avancé	Optimal
Résilience du réseau	Capacités réseau configurées au cas par cas pour répondre uniquement aux besoins de disponibilité individuels des applications, avec des mécanismes de résilience limités pour les charges de travail jugées non critiques	Début de la configuration des capacités réseau pour gérer les besoins de disponibilité d'applications supplémentaires et étendre les mécanismes de résilience à des charges de travail jugées non critiques	Capacités réseau configurées pour gérer dynamiquement les besoins de disponibilité et les mécanismes de résilience pour la majorité des applications	L'entreprise intègre une démarche holistique en s'adaptant aux changements des besoins de disponibilité pour toutes les charges de travail, et assure une résilience proportionnée

Pilier **réseaux**

Fonction	Traditionnel	Initial	Avancé	Optimal
Visibilité et analyse	Intégration de capacités limitées de surveillance périmétrique du réseau avec un minimum d'analyse pour commencer à développer une connaissance centralisée de la situation	Utilisation des capacités de surveillance du réseau basées sur des indicateurs de compromission connus (y compris l'énumération du réseau) pour développer une connaissance de la situation dans chaque environnement, et début de corrélation de la télémétrie entre les différents types de trafic et les environnements pour les activités d'analyse et de lutte contre les menaces	L'entreprise déploie des capacités de détection réseau basées sur les anomalies pour développer une connaissance de la situation dans tous les environnements, commence à corréler la télémétrie à partir de plusieurs sources pour l'analyse et intègre des processus automatisés pour lutter efficacement contre les menaces	L'entreprise assure une visibilité des communications sur tous les réseaux et environnements tout en permettant une connaissance de la situation à l'échelle de l'entreprise et des capacités de surveillance avancées qui automatisent la corrélation de télémétrie entre toutes les sources de détection

Pilier **réseaux**

Fonction	Traditionnel	Initial	Avancé	Optimal
Automatisation et orchestration	Processus manuels pour gérer la configuration et le cycle de vie des ressources pour les réseaux et environnements de l'entreprise avec intégration périodique des exigences des politiques et connaissance de la situation	Début de l'utilisation de méthodes automatisées pour gérer la configuration et le cycle de vie des ressources pour certains réseaux ou environnements de l'entreprise et garantir que toutes les ressources ont une durée de vie définie en fonction des politiques et de la télémétrie	Utilisation de méthodes automatisées de gestion des changements (Ex. CI/CD) pour gérer la configuration et le cycle de vie des ressources pour tous les réseaux et environnements de l'entreprise, en répondant et en appliquant des politiques et des protections contre les risques perçus	Réseaux et environnements définis à l'aide d'une « infrastructure-as-code » managée par des méthodes automatisées de gestion des changements, y compris l'instanciation et l'expiration automatisées pour s'aligner sur l'évolution des besoins

Pilier **réseaux**

Fonction	Traditionnel	Initial	Avancé	Optimal
Gouvernance	Politiques réseau implémentées statiquement (accès, protocoles, segmentation, alertes et remédiation) avec une approche centrée sur les protections périmétriques	Définition et début de mise en œuvre de politiques adaptées aux différents segments et ressources du réseau tout en héritant de règles à l'échelle de l'entreprise (le cas échéant)	L'entreprise intègre l'automatisation dans la mise en œuvre de politiques personnalisées et facilite la transition des protections basées sur un modèle périmétrique	Mise en œuvre de politiques réseau à l'échelle de l'entreprise permettant des contrôles locaux personnalisés, des mises à jour dynamiques et des connexions externes sécurisées basées sur les workflows des applications et des utilisateurs

Pilier **applications et « *workloads* »**

Les applications et « *workloads* » comprennent les systèmes de traitement, les programmes informatiques et les services qui s'exécutent sur site, sur périphériques mobiles et dans les environnements Cloud

Fonction	Traditionnel	Initial	Avancé	Optimal
Contrôle d'accès aux applications	Contrôle d'accès aux applications principalement basé sur des autorisations locales et des attributs statiques	Début de mise en œuvre de capacités d'autorisation d'accès aux applications qui intègrent des informations contextuelles (ex. l'identité, la conformité de l'appareil et/ou d'autres attributs), pour chaque requête et avec une durée d'expiration	Automatisation des décisions d'accès aux applications à partir d'informations contextuelles étendues et application de conditions d'expiration, en respectant le principe de moindre privilège	Contrôle permanent et continu de l'accès aux applications, en intégrant des analyses de risque en temps réel et des facteurs tels que le comportement ou les modèles d'utilisation

Pilier **applications et « *workloads* »**

Fonction	Traditionnel	Initial	Avancé	Optimal
Protections contre les menaces applicatives	Protections contre les menaces ayant une intégration minimale avec les workflows d'application, appliquant des protections génériques contre des menaces connues	Intégration de protections contre les menaces dans les workflows des applications critiques, en appliquant des protections contre les menaces connues et certaines menaces spécifiques aux applications	Intégration de protections contre les menaces dans tous les workflows d'application, protégeant contre certaines menaces spécifiques aux applications et ciblées	Intégration de protections avancées contre les menaces dans tous les workflows applicatifs, offrant une visibilité en temps réel et des protections sensibles au contenu contre les attaques sophistiquées adaptées aux applications
Accessibilité des applications	Quelques applications critiques sont disponibles uniquement sur des réseaux privés ou via des connexions au réseau public protégées (ex. par VPN), avec surveillance	Certaines applications essentielles sont accessibles depuis des réseaux publics, pour les utilisateurs autorisés qui en ont besoin et via des connexions « négociées »	La plupart des applications essentielles possibles sont accessibles depuis des réseaux publics, pour les utilisateurs autorisés, selon les besoins	Toutes les applications possibles sont accessibles depuis des réseaux publics, pour les utilisateurs et appareils autorisés, selon la pertinences et les besoins

Pilier **applications et « *workloads* »**

Fonction	Traditionnel	Initial	Avancé	Optimal
Développement et déploiement sécurisés des applications	Environnements de développement, de test et de production ad hoc avec des mécanismes de déploiement de code non robustes	Mise en place d'une infrastructure pour les environnements de développement, de test et de production (y compris l'automatisation) avec des mécanismes formels de déploiement de code via des pipelines CI/CD et les contrôles d'accès requis à l'appui du principe du moindre privilège	Équipes distinctes et coordonnées pour le développement, la sécurité et les opérations tout en supprimant l'accès des développeurs à l'environnement de production pour le déploiement du code	Exploitation de charges de travail immuables dans la mesure du possible, permettant uniquement aux modifications de prendre effet via un redéploiement, et suppression des accès administrateur aux environnements de production au profit de processus automatisés pour le déploiement du code

Pilier **applications et « *workloads* »**

Fonction	Traditionnel	Initial	Avancé	Optimal
Test de la sécurité des applications	Tests de sécurité des applications effectués avant le déploiement, principalement via des méthodes de test manuelles	Début de l'utilisation de méthodes de test de sécurité statiques et dynamiques (c'est-à-dire pendant que l'application s'exécute), comprenant une analyse manuelle par des experts, avant le déploiement des applications	Intégration de tests de sécurité dans les processus de développement et de déploiement des applications, comprenant l'utilisation de méthodes de tests dynamiques périodiques	Intégration de tests de sécurité des applications tout au long du cycle de vie du développement logiciel dans toute l'entreprise, avec des tests automatisés réguliers des applications déployées
Visibilité et analyse	Une certaine surveillance des performances et de la sécurité des applications critiques avec des capacités d'agrégation et d'analyse limitées	Début d'automatisation des profils d'applications (ex. l'état, la santé et les performances) et de surveillance de la sécurité pour une meilleure collecte, agrégation et analyse des journaux	Automatisation de la surveillance des profils et de la sécurité pour la plupart des applications avec des heuristiques pour identifier les tendances spécifiques aux applications et à l'échelle de l'entreprise et affiner les processus au fil du temps pour combler les lacunes de visibilité	Surveillance continue et dynamique de toutes les applications pour maintenir une visibilité complète à l'échelle de l'entreprise

Pilier **applications et « *workloads* »**

Fonction	Traditionnel	Initial	Avancé	Optimal
Automatisation et orchestration	L'entreprise établit manuellement l'emplacement d'hébergement statique des applications et l'accès au provisionnement avec une maintenance et un examen limités	Modification périodique de la configuration des applications (y compris l'emplacement et l'accès) pour répondre aux objectifs de sécurité et de performance pertinents	Automatisation de la configuration des applications pour répondre aux changements opérationnels et environnementaux	Automatisation de la configuration des applications pour optimiser en permanence la sécurité et les performances

Pilier **applications et « *workloads* »**

Fonction	Traditionnel	Initial	Avancé	Optimal
Gouvernance	L'entreprise s'appuie principalement sur l'application manuelle de politiques pour l'accès aux applications, le développement, le déploiement, la gestion des actifs logiciels, les tests de sécurité et l'évaluation lors de l'introduction de nouvelles technologies, l'application des correctifs et le suivi des dépendances logicielles	Début de l'automatisation de l'application des politiques pour le développement d'applications (y compris l'accès à l'infrastructure de développement), le déploiement, la gestion des actifs logiciels, les tests de sécurité et l'évaluation lors de l'introduction de nouvelles technologies, l'application des correctifs et le suivi des dépendances logicielles, en fonction des besoins (ex. avec une nomenclature des logiciels)	Mise en œuvre de politiques à plusieurs niveaux, adaptées aux besoins de l'ensemble de l'entreprise, pour les applications et tous les aspects des cycles de développement et de déploiement, et si possible automatisation de l'application de ces politiques	Complète automatisation des politiques régissant le développement et le déploiement des applications, incluant l'intégration de mises à jour dynamiques via le pipeline CI/CD

Pilier **données**

Les données comprennent tous les fichiers et fragments structurés et non structurés qui résident ou ont résidé dans les systèmes, appareils, réseaux, applications, bases de données, infrastructure et sauvegardes (comprenant les environnements sur site et virtuels), ainsi que les métadonnées

Fonction	Traditionnel	Initial	Avancé	Optimal
Gestion de l'inventaire des données	Identification et inventaire manuels de certaines données (par exemple les données essentielles de l'entreprise)	Début d'automatisation des processus d'inventaire des données pour les environnements sur site et dans le Cloud, couvrant la plupart des données de l'entreprise, et commencement d'intégration de protections contre la fuite de données	Automatisation de l'inventaire et du suivi des données à l'échelle de l'entreprise, couvrant toutes les données possibles, avec des stratégies de prévention des fuites de données basées sur des attributs et/ou des étiquettes statiques	Inventaire continu de toutes les données d'entreprise possibles, et stratégies robustes de prévention des fuites de données qui bloquent dynamiquement toute exfiltration suspectée de données

Pilier **données**

Fonction	Traditionnel	Initial	Avancé	Optimal
Classification des données	Classification ad hoc des données avec des capacités limitée	Début de mise en œuvre d'une stratégie de classification des données avec des étiquettes définies et des mécanismes d'application manuelle	Automatisation de certains processus de classification et d'étiquetage des données, de manière cohérente, hiérarchisée et ciblée avec des formats simples et structurés et un examen régulier	Automatisation de la classification et de l'étiquetage des données à l'échelle de l'entreprise grâce à des techniques robustes, des formats granulaires et structurés, et des mécanismes pour traiter tous les types de données
Disponibilité des données	Données mises principalement à disposition à partir de moyens de stockage sur site, avec quelques sauvegardes hors site	Certaines données disponibles à partir de moyens de stockage redondants et hautement disponibles (ex. Cloud), et sauvegardes hors site pour les données hébergées sur site	Données principalement disponibles à partir de moyens de stockage redondants et hautement disponibles, et accès aux historiques de données assuré	Utilisation de méthodes dynamiques pour optimiser la disponibilité des données, y compris les historiques de données, en fonction des besoins de l'utilisateur et de l'entité

Pilier **données**

Fonction	Traditionnel	Initial	Avancé	Optimal
Accès aux données	Accès des utilisateurs et des entités aux données (ex. autorisations de lire, d'écrire, de copier, d'accorder l'accès à d'autres, etc.) régit via des contrôles d'accès statiques	Début de déploiement dans toute l'entreprise de contrôles d'accès aux données automatisés qui intègrent des éléments de moindre privilège	Contrôles d'accès aux données automatisés qui tiennent compte de divers attributs tels que l'identité, le risque de l'appareil, l'application, la classification des données, etc., avec si possible des autorisations limitées dans le temps	Utilisation de l'automatisation pour autoriser des accès « just-in-time / just-enough » adaptés aux besoins individuels d'actions et de ressources

Pilier **données**

Fonction	Traditionnel	Initial	Avancé	Optimal
Chiffrement des données	L'entreprise chiffre un minimum de données au repos et en transit et s'appuie sur des processus manuels ou ad hoc pour gérer et sécuriser les clés de chiffrement	Chiffrement de toutes les données en transit et, si possible, des données au repos (ex. données critiques ou stockées dans des environnements externes), début de formalisation de politiques de gestion des clés de chiffrement et sécurisation de celles-ci (ce qui devrait inclure des efforts pour consolider les magasins de clés et réduire la dépendance à des magasins de clés uniques ou cloisonnés)	Chiffrement de toutes les données possibles au repos et en transit dans l'entreprise, début d'intégration de l'agilité cryptographique et protection des clés de chiffrement (secrets non codés en dur et renouvelés régulièrement)	Chiffrement de toutes les données utilisées possibles, application du principe de moindre privilège pour la gestion sécurisée des clés à l'échelle de l'entreprise, et moyens de chiffrement utilisant des normes à jour et si possible l'agilité cryptographique

Pilier **données**

Fonction	Traditionnel	Initial	Avancé	Optimal
Visibilité et analyse	Visibilité limitée sur les données (emplacement, accès et utilisation), avec une analyse consistant principalement en des processus manuels	Visibilité basée sur la gestion de l'inventaire des données, la classification, le chiffrement et les tentatives d'accès, avec une analyse et une corrélation automatisées	L'entreprise assure la visibilité des données d'une manière plus complète à l'échelle de l'entreprise avec une analyse et une corrélation automatisées et commence à utiliser l'analyse prédictive	Visibilité sur l'ensemble du cycle de vie des données grâce à des analyses robustes, comprenant des analyses prédictives, qui intègrent une cartographie complète des données de l'entreprise et une évaluation continue de la posture de sécurité

Pilier **données**

Fonction	Traditionnel	Initial	Avancé	Optimal
Automatisation et orchestration	Politiques de cycle de vie et de sécurité des données (ex. accès, utilisation, stockage, chiffrement, configuration, protection, sauvegarde, classification, effacement) implémentées par le biais de processus manuels et potentiellement ad hoc	Utilisation de processus automatisés pour mettre en œuvre des politiques de cycle de vie et de sécurité des données	Mise en œuvre de politiques de cycle de vie et de sécurité des données principalement par le biais de méthodes automatisées pour la plupart des données de manière cohérente, hiérarchisée et ciblée dans toute l'entreprise	Automatisation, dans la mesure du possible, des politiques de cycle de vie et de sécurité pour toutes les données de l'entreprise
Gouvernance	L'entreprise s'appuie sur des politiques de gouvernance des données ad hoc (par exemple, pour la protection, la classification, l'accès, l'inventaire, le stockage, la récupération, la suppression, etc.) avec une mise en œuvre manuelle	L'entreprise définit des politiques de gouvernance des données de haut niveau et s'appuie principalement sur une mise en œuvre manuelle et segmentée	Début de l'intégration d'une application de la politique de cycle de vie des données dans toute l'entreprise, permettant des définitions de politiques de gouvernance des données plus unifiées	Les politiques de cycle de vie des données sont unifiées dans la mesure du possible et appliquées de manière dynamique dans toute l'entreprise

Socle (transverse)

Fonction	Traditionnel	Initial	Avancé	Optimal
Visibilité et analyse	Collecte manuelle de journaux limités dans toute l'entreprise avec une faible fidélité et une analyse minimale	L'entreprise commence à automatiser la collecte et l'analyse des journaux et des événements pour les fonctions critiques et évalue régulièrement les processus pour détecter les lacunes de visibilité	Extension de la collecte automatisée de journaux et d'événements à l'échelle de l'entreprise (y compris les environnements virtuels) pour une analyse centralisée en corrélation avec plusieurs sources	Maintien d'une visibilité complète à l'échelle de l'entreprise via une surveillance dynamique centralisée et une analyse avancée des journaux et des événements
Automatisation et orchestration	L'entreprise s'appuie sur des processus statiques et manuels pour orchestrer les opérations et la réponse aux incidents avec une automatisation limitée	Début d'automatisation des activités d'orchestration et de réponse aux incidents à l'appui des fonctions critiques de l'entreprise	Automatisation des activités d'orchestration et de réponse aux incidents à l'échelle de l'entreprise, en tirant parti des informations contextuelles provenant de plusieurs sources pour éclairer les décisions	Les activités d'orchestration et de réponse aux incidents s'adaptent de manière dynamique aux modifications d'exigences à l'échelle de l'entreprise et aux changements environnementaux

Socle (transverse)

Fonction	Traditionnel	Initial	Avancé	Optimal
Gouvernance	Mise en œuvre de politiques de manière ad hoc dans toute l'entreprise, les politiques étant appliquées via des processus manuels ou des mécanismes techniques statiques	Définition et début d'application de politiques à l'échelle de l'entreprise, avec un minimum d'automatisation et des mises à jour manuelles	Mise en œuvre de politiques personnalisées à plusieurs niveaux à l'échelle de l'entreprise, tirant parti de l'automatisation (dans la mesure du possible) pour en soutenir l'application Les décisions de politique d'accès intègrent des informations contextuelles provenant de plusieurs sources	Mise en œuvre entièrement automatisée de politiques à l'échelle de l'entreprise, permettant des contrôles locaux personnalisés avec une application continue et des mises à jour dynamiques