CISCO
SECURE

Guide Cisco sur la maturité de la sécurité Zero Trust

Identifier les actions à effet rapide

cisco SECURE

Sommaire

I. Synthèse

La sécurité Zero Trust n'est plus seulement une tendance, c'est une obligation internationale. Les gouvernements des États-Unis, du Royaume-Uni et de l'Australie ont tous annoncé des engagements qui reposent sur le credo : « ne jamais présumer de la fiabilité, toujours la vérifier ».

Les dirigeants d'entreprise qui adoptent le modèle Zero Trust constatent que leur système de sécurité gagne en résilience. En fait, les clients de Cisco ont réduit de moitié les risques et les coûts liés aux violations de données, tandis que d'autres ont atteint un ROI de 191 % en mettant en place le travail hybride et en optimisant les performances des équipes de sécurité.

Parce qu'il améliore l'efficacité, le modèle Zero Trust accélère la réponse des équipes SOC. Nous avons augmenté de 90 % l'efficacité de notre SOC pour nos clients. De toute évidence, le modèle Zero Trust apporte une valeur ajoutée.

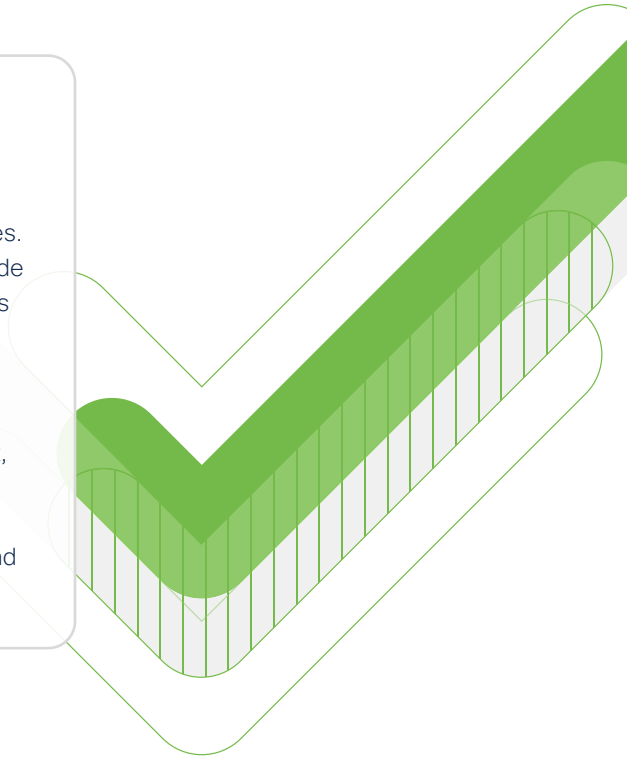
Malgré tout, certaines entreprises doutent encore de l'approche à privilégier pour que la mise en œuvre des principes Zero Trust soit rentable. Pourtant, Cisco et bien d'autres entreprises ont fait des progrès significatifs dans leur parcours d'adoption de la sécurité Zero Trust tout en pouvant démontrer des bénéfices financiers.

En quoi ces entreprises sont-elles différentes ? Quels sont les secrets de leur réussite ?

À propos des données utilisées dans ce guide

Nous avons utilisé les résultats de l'étude Cisco sur les objectifs en matière de sécurité, volume 2, un rapport vérifié par une instance indépendante qui se propose d'expliquer « pourquoi » certaines pratiques de sécurité sont si efficaces. Dans le cadre de l'étude, plus de 5 000 professionnels de l'IT, de la sécurité et de la confidentialité des données de tous secteurs d'activité ont été interrogés dans 27 pays pour comprendre comment améliorer les capacités et les résultats en matière de sécurité.

Cisco organise également régulièrement des ateliers Zero Trust qui permettent aux participants de comprendre le parcours d'adoption de la sécurité Zero Trust, d'effectuer des activités pratiques, de procéder à une analyse des écarts et de développer un plan d'action. À ce jour, environ 3 000 responsables de l'IT et de la sécurité, ainsi que des experts se sont inscrits à ces ateliers. Ce guide reprend les réponses à l'enquête recueillies lors de ces ateliers.



Nous avons exploité les données collectées et analysées par l'équipe en charge de l'étude Cisco sur les objectifs en matière de sécurité, volume 2, ainsi que les réponses des participants aux nombreux ateliers « Zero Trust » organisés par Cisco au cours de l'année passée.

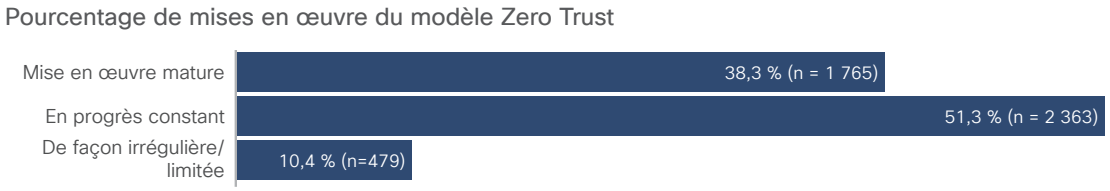


Figure 1 : Progrès des personnes interrogées sur l'adoption de la sécurité Zero Trust

Les résultats de l'analyse de ces données fournissent un éclairage aux équipes qui cherchent à mettre en œuvre un modèle Zero Trust :

- **Une approche Zero Trust est possible, indépendamment de la taille de l'entreprise ou du niveau de complexité de son infrastructure IT.** Nous avons découvert que les entreprises de toutes tailles pouvaient réussir à déployer progressivement une sécurité Zero Trust, que leur environnement IT soit simple ou complexe.
- Les entreprises qui déclarent que leur mise en œuvre du modèle Zero Trust est mature sont plus de **deux fois** plus nombreuses à avoir renforcé **leur résilience** (63,6 %) que celles dans lesquelles la mise en œuvre du Zero Trust est limitée.
- Les entreprises dont les mises en œuvre de la sécurité Zero Trust sont matures sont **deux** fois plus nombreuses à exceller dans les **cinq pratiques de sécurité suivantes** :
  - Détection précise des menaces
  - Remplacement proactif des technologies
  - Accélération de la reprise après sinistre
  - Réponse rapide aux incidents
  - Intégration des technologies
- Les entreprises dont la mise en œuvre du modèle Zero Trust est, selon elles, mature, sont **2 fois** plus nombreuses à se démarquer dans des domaines tels que le **renforcement de la confiance des dirigeants** (47 %), **l'adhésion des collaborateurs** (45 %), **l'adaptation à l'évolution de l'activité** (46 %) et la **création d'une culture de la sécurité**.
- Les entreprises dotées d'une **infrastructure IT moderne** sont **plus de deux fois** plus nombreuses à être parvenues à une mise en œuvre de la sécurité Zero Trust mature.
- **Les intégrations favorisent la maturité Zero Trust**. Parmi les entreprises ayant choisi les intégrations, celles dont la mise en œuvre du modèle Zero Trust est à maturité sont plus nombreuses (**51 %**) à avoir privilégié une approche basée sur la plateforme avec achat des **technologies intégrées auprès d'un fournisseur favori**, qu'à avoir opté pour des intégrations prêtes à l'emploi (**28,8 %**).
- Les entreprises dont les mises en œuvre du modèle Zero Trust sont à maturité tirent parti de **l'automatisation** (64,4 %) pour améliorer les mesures dont leur modèle de sécurité est capable.

Le but de ce guide sur la maturité Zero Trust est de vous aider à savoir où vous en êtes dans votre mise en œuvre du modèle Zero Trust, à identifier les actions à effet rapide, à passer à la vitesse supérieure et à continuer à progresser vers la sécurité Zero Trust.

II. Introduction

La sécurité Zero Trust n'est pas prête de disparaître. Mais pourquoi pose-t-elle tant de difficultés ? Où les équipes peuvent-elles trouver la motivation nécessaire pour s'attaquer à une tâche aussi herculéenne ?

Nous pensons que les entreprises ont beaucoup à apprendre des équipes qui sont parvenues à une mise en œuvre du modèle Zero Trust plus mature. Quels sont leurs secrets ? Que font-elles que nous pouvons partager avec le reste du monde ?

Et plus précisément :

1. Quels sont les résultats obtenus par ces équipes en termes de sécurité et quel est leur pourcentage de réussite ?
2. Quelles sont leurs priorités lors de la sélection des fournisseurs et prestataires d'architectures Zero Trust ?
3. Quelle est leur stratégie d'intégration et d'automatisation pour déployer un modèle Zero Trust ?
4. Sur quels standards de la sécurité Zero Trust s'appuient-elles ?
5. Dans quelle mesure ont-elles automatisé leurs processus de sécurité ?

III. Qu'est-ce que la sécurité Zero Trust ?

La sécurité Zero Trust est une **approche stratégique** qui repose sur le concept de **l'élimination de toute confiance implicite** dans l'environnement d'une entreprise.

La confiance n'est ni binaire ni permanente. Aujourd'hui, il n'est plus possible de partir du principe que toutes les entités internes sont fiables, qu'il est possible de les gérer directement afin de réduire les risques ou qu'il suffit de les contrôler une fois.

Le modèle Zero Trust implique de **se méfier de tout et de vérifier** toutes les tentatives d'accès, quelle que soit leur provenance.

Une stratégie Zero Trust déploie une politique qui « ne fait jamais confiance d'emblée, vérifie toujours et applique le principe du moindre privilège » pour chaque demande de connexion à chaque ressource de l'entreprise. En vérifiant toujours la fiabilité avant d'accorder l'accès à vos applications, à vos équipements et à vos réseaux, vous vous assurez que seuls les utilisateurs autorisés ont accès aux informations.

Ce sont les points de décision des politiques et les points d'application des politiques qui prennent et appliquent ces décisions. En fait, ils font toute la différence dans l'architecture. Ils appliquent les principes Zero Trust et étendent ou annulent les limites de confiance en fonction de ce qui est observable lors de la connexion.

La sécurité Zero Trust n'est PAS :

- Un seul produit ou une seule technologie, mais un modèle de sécurité
- Quelque chose à « acheter » ou à « vendre », mais une opportunité de positionner une solution dans le cadre du modèle
- Un projet mené à son terme, mais un effort continu pour améliorer la sécurité

En vérité, les entreprises évoluent trop vite pour prendre le temps d'adapter leur sécurité. Mais en dépit des innovations dans ce domaine, les risques n'ont jamais été aussi importants. Trop souvent, un seul incident de cybersécurité suffit à menacer l'avenir d'une entreprise.

Chez Cisco, nous pensons qu'une stratégie de sécurité Zero Trust doit permettre de sécuriser l'accès d'une manière qui complique la vie des hackers, pas celles des utilisateurs.

A. Pourquoi maintenant ?

La sécurité Zero Trust n'est pas un nouveau concept. Mais le fait qu'elle soit de plus en plus adoptée témoigne d'une nouvelle réalité : les périmètres qui sécurisaient autrefois l'accès aux données de l'entreprise n'existent plus. Les entreprises fonctionnent maintenant comme des écosystèmes intégrés avec leurs fournisseurs, leurs partenaires et leurs clients. Ces relations étendent la surface d'exposition aux attaques, augmentant les risques et la complexité, et compliquant la reprise de l'activité après une attaque.

Les cyberattaques ont un tel impact sur les résultats de leur entreprise que les dirigeants sont prêts à envisager une nouvelle façon de mettre en œuvre une sécurité de bout en bout, guidée par les principes d'accès Zero Trust, à condition que ces changements ne ralentissent pas la productivité ou les opérations.

Les enjeux sont si importants et les impacts matériels si potentiellement dévastateurs qu'ils sont désormais impatients d'entamer cette transformation. Les principes de la sécurité Zero Trust sont globalement acceptés.

Une approche Zero Trust est envisageable, quel que soit le niveau de complexité de l'infrastructure IT des entreprises. Elles peuvent se lancer dans la mise en œuvre du modèle Zero Trust et améliorer leurs résultats, que leurs environnements IT soient simples ou complexes.

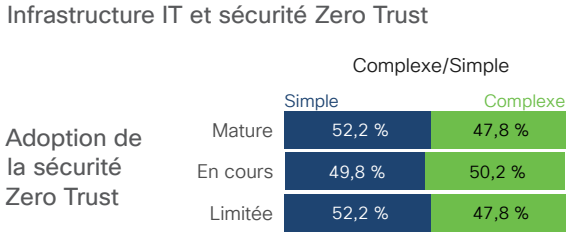


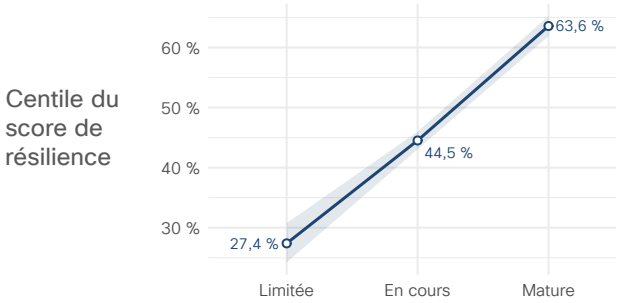
Figure 2 : Adoption de la sécurité Zero Trust dans les entreprises avec une infrastructure simple et complexe

La sécurité Zero Trust accroît la résilience de l'entreprise. La sécurité Zero Trust n'est pas une tendance marketing. Concrètement, la migration vers une architecture Zero Trust permet de sécuriser toute l'entreprise, d'améliorer ses performances et de répondre plus rapidement aux menaces.

Nous avons constaté que les entreprises dont la mise en œuvre du modèle Zero Trust est à maturité sont deux fois plus nombreuses à renforcer leur résilience que celles dont la mise en œuvre du Zero Trust est limitée.

Nous avons créé un « score de résilience » en utilisant 4 des 12 résultats de sécurité les plus pertinents en matière de résilience :

- S'adapter à l'évolution de l'activité (la sécurité doit améliorer, pas entraver)
- Éviter les incidents majeurs (et l'impact sur l'entreprise qui en découle)
- Assurer la continuité des activités (continuer à fonctionner en cas de sinistre)
- Fidéliser les talents en interne (il est impossible de rester performant quand les meilleurs collaborateurs s'en vont)



Mise en œuvre de la sécurité Zero Trust

Plus le score de résilience est élevé, plus les taux de réussite sont importants pour ces résultats.

Le problème est que les entreprises ne savent pas comment s'y prendre ni par où commencer. Elles craignent que la mise en œuvre de la sécurité Zero Trust affecte leur productivité ou compromette leur agilité et leur résilience opérationnelle.

Pour éviter ce scénario, elles doivent se lancer en se concentrant sur les pratiques qui fonctionnent. Nous avons identifié une corrélation claire entre les mises en œuvre du modèle Zero Trust matures et cinq pratiques de sécurité désignées dans l'étude Cisco sur les objectifs en matière de sécurité, volume 2 comme les « 5 facteurs de réussite » d'un programme de sécurité :

- Détection précise des menaces
- Remplacement proactif des technologies
- Accélération de la reprise après sinistre
- Réponse rapide aux incidents
- Intégration des technologies

Les entreprises dont les mises en œuvre du modèle Zero Trust sont matures sont deux fois plus nombreuses à exceller dans ces cinq pratiques de sécurité.

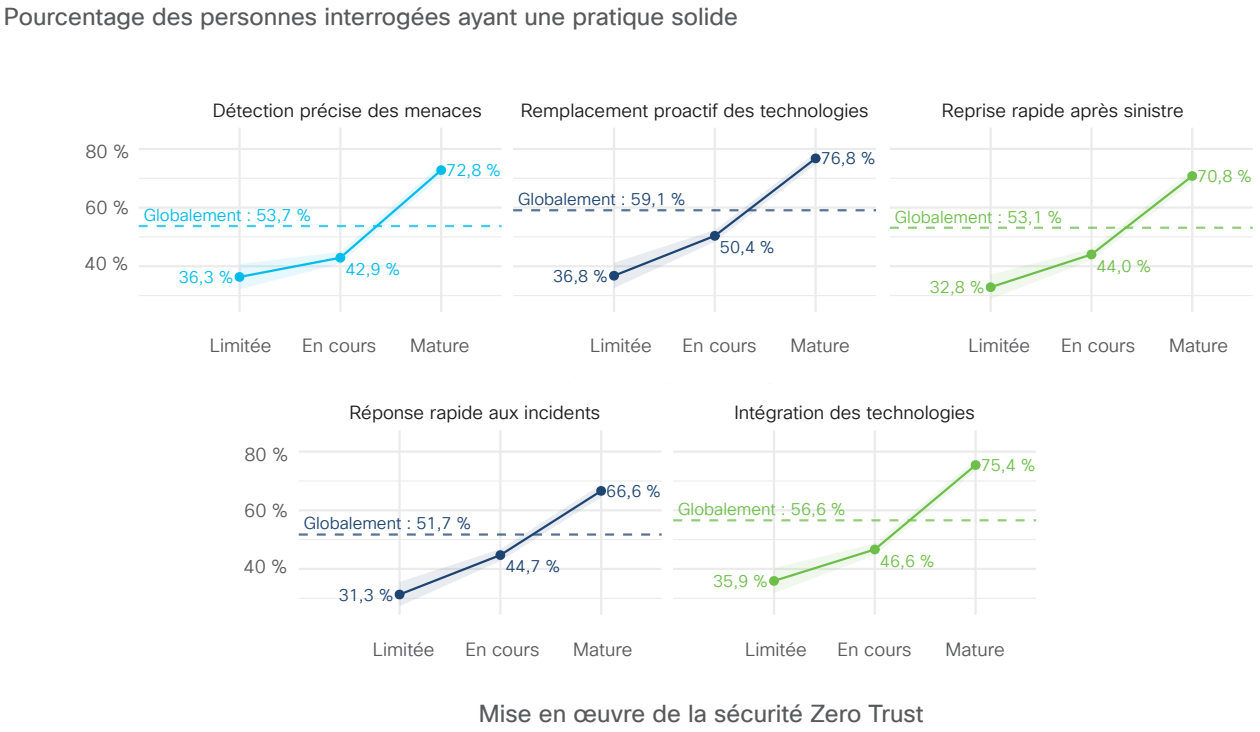


Figure 3 : Niveau d'adoption du modèle Zero Trust et pratiques de sécurité

Conseil d'expert : à l'heure ou la sécurité Zero Trust représente une part de marché de 20 milliards de dollars (en croissance constante)[1], vous devez choisir un partenaire qui pourra répondre à vos besoins où que vous soyez, qui saura intégrer les piliers du modèle Zero Trust et qui aura lui-même progressé dans sa transition.

[1]Selon Grandview Research, le marché mondial de la sécurité Zero Trust était évalué à 19,8 milliards de dollars en 2020 et devrait connaître une croissance annuelle moyenne de 15,2 % entre 2021 et 2028.
https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report

IV. Les secrets de la réussite

A. Développez d'abord une culture de la sécurité

La remise en cause de la culture de l'entreprise est un frein à toute initiative.

Les principaux facteurs pour réussir à mettre en œuvre le modèle Zero Trust sont la capacité à obtenir l'adhésion de l'équipe dirigeante, à être soutenu par les collaborateurs et à tirer parti de la culture de la sécurité. Les équipes de sécurité sont en difficulté lorsqu'elles n'ont ni l'adhésion ni le budget, et que le programme de sécurité va à l'encontre de la culture de l'entreprise.

L'étude de cas Cisco montre que ces facteurs étaient tous présents dans l'entreprise, à commencer par l'adhésion des dirigeants et des collaborateurs. L'étude sur les objectifs en matière de sécurité confirme que le **renforcement de la confiance** des dirigeants (47 %) et **l'adhésion des collaborateurs** (45 %) sont caractéristiques des mises en œuvre matures. D'autres tendances sont également déterminantes, comme la capacité à **s'adapter à l'évolution de l'activité** (46 %) et à **créer une culture de la sécurité** (48 %). En fait, **les entreprises dont la mise en œuvre du modèle Zero Trust est mature sont 2 fois plus susceptibles d'exceller dans ces domaines.**

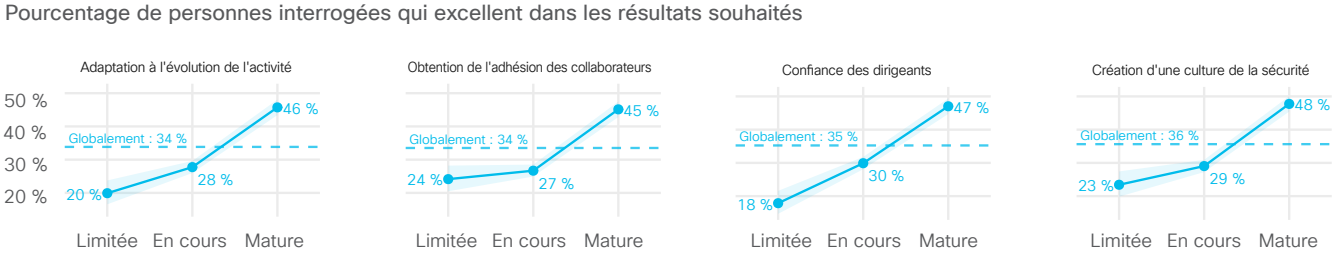


Figure 3 : Niveau d'adoption de la sécurité Zero Trust dans le contexte des résultats souhaités

Les relations stimulent le changement organisationnel. Avant de rédiger votre plan sur un tableau blanc et d'ouvrir la console pour configurer la politique, vous devez renforcer les relations entre l'équipe de sécurité et les dirigeants. Vos homologues en charge de l'IT, du réseau, de l'architecture, de la gestion de projet et de l'audit sont tous concernés. Ces relations permettent de faire mûrir les programmes Zero Trust beaucoup plus rapidement et donc d'atteindre des niveaux de réussite plus élevés, un aspect essentiel de tout changement transformationnel.

Le changement commence au sommet de l'entreprise. Il est plus facile de suivre une voie qui est pleinement soutenue. Lorsque le PDG sollicite la mise en œuvre d'une initiative Zero Trust ou lorsque les clients demandent à en bénéficier dans le cadre de la gestion de leur chaîne d'approvisionnement, l'entreprise n'a pas d'autre choix que de se lancer. Vous devez tirer parti de ce type d'événement et vous en servir comme tremplin pour faire avancer le programme.

Créez une culture de la confiance. Avant d'aborder le sujet de la technologie et d'argumenter en faveur d'une approche Zero Trust, les responsables de la sécurité doivent renforcer la confiance de leurs homologues et obtenir l'adhésion des dirigeants. Le message doit être cohérent avec la culture de l'entreprise.

Cherchez à renforcer les relations. Lors de la conception et de la mise en œuvre de l'architecture Zero Trust, identifiez les moyens de resserrer les liens avec les différentes équipes. Il peut s'agir de cartographier les workflows, de mettre en place des moteurs de politiques, de discuter des répercussions de la sécurité Zero Trust sur l'entreprise ou de développer l'activité de l'entreprise tout en prévenant les menaces.

Les études de cas et les données démontrent que ces facteurs sont essentiels pour la réussite des mises en œuvre du modèle Zero Trust.

B. Faites une solide analyse de rentabilité

Au sein des ateliers Cisco Zero Trust et sur le marché dans son ensemble, nous avons identifié une tendance claire concernant les initiatives Zero Trust.

Les premiers projets Zero Trust étaient des programmes pilotes. Les responsables de la sécurité ont entendu parler de ce modèle et ont voulu l'essayer pour voir ce qui fonctionnait et ce qui ne fonctionnait pas. Ces premiers projets pilotes leur ont permis de voir ce que cela pourrait donner dans leur entreprise. De 2018 à 2020, de nombreuses initiatives Zero Trust ont été lancées à la demande d'un dirigeant ou d'un client, ou en raison d'un besoin de modernisation.

Une nouvelle approche axée sur les résultats. Depuis quelque temps, l'analyse de rentabilité ne porte plus sur des initiatives Zero Trust autonomes, mais sur la satisfaction des besoins de l'entreprise en appliquant les principes Zero Trust. Ces besoins sont notamment la prise en charge des équipes travaillant essentiellement à distance, de la clientèle axée sur le numérique, de la transformation numérique, de la migration vers le cloud et de la modernisation de l'IT. Les programmes Zero Trust efficaces cherchent à améliorer le fonctionnement de l'entreprise tout en augmentant la sécurité.

Priorité à l'expérience utilisateur. Aujourd'hui, l'expérience utilisateur est l'un des principaux aspects étudiés dans les analyses de rentabilité de la sécurité Zero Trust. C'est la notion de « confiance » propre à la sécurité Zero Trust. Les programmes matures améliorent l'expérience utilisateur de manière à ce que la sécurité reste discrète lorsque le personnel effectue ses activités quotidiennes. Les contrôles de sécurité ne doivent interrompre l'activité qu'en cas de risque réel, par exemple lorsqu'une connexion n'est pas fiable ou qu'une attaque malveillante se produit.

Une sécurité plus efficace. La facilité de gestion est un autre facteur à prendre en compte dans l'analyse de rentabilité. **L'étude sur les objectifs en matière de sécurité révèle que les entreprises dont les mises en œuvre du modèle Zero Trust sont matures optimisent les coûts (47 %) tout en minimisant les tâches non planifiées (43 %)**. Les participants aux ateliers Cisco Zero Trust citent régulièrement comme objectif la consolidation des outils, juste derrière l'amélioration de la visibilité. Les entreprises qui réussissent leur mise en œuvre réduisent la charge de travail liée au maintien de la sécurité tout en augmentant leurs fonctionnalités de protection.

En d'autres termes, l'objectif de l'analyse de rentabilité de la sécurité Zero Trust doit être de compliquer la vie des hackers, pas celle des utilisateurs.

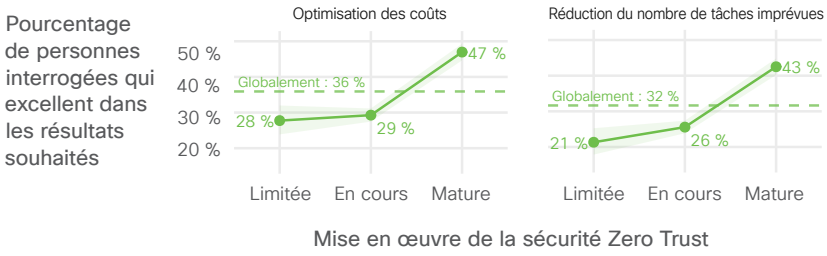


Figure 6 : Rentabilité de la sécurité Zero Trust

Réduction de la surface d'exposition aux attaques. Il s'agit là du composant « zéro » de la sécurité Zero Trust : diminuer la confiance excessive et implicite pour réduire les risques pour la sécurité. La plupart des entreprises pensent aux menaces telles que le phishing et les ransomwares, mais elles utilisent plus généralement le modèle Zero Trust pour réduire la surface d'exposition aux attaques.

Exploitation de l'audit. Les exigences de conformité au modèle Zero Trust sont de plus en plus demandées, en particulier dans le secteur fédéral américain. Selon nous, cette exigence de conformité va gagner du terrain à mesure que les entreprises adopteront la sécurité Zero Trust et la mettront en œuvre dans le cadre de la gestion des risques liés à la chaîne d'approvisionnement.

Conclusion : les analyses de rentabilité doivent avant tout répondre à un besoin de l'entreprise ; en y répondant, l'application des principes de la sécurité Zero Trust permet de renforcer la sécurité.

C. Sécurisez la pile IT

La sécurité Zero Trust consiste à créer un périmètre dynamique éphémère, clairement défini, appliqué par une politique et basé sur la télémétrie et les signaux de confiance. Ce périmètre de confiance est défini entre un sujet (généralement une personne sur son équipement) et une ressource (généralement une application à laquelle cette personne accède).

La pile IT doit prendre en charge l'établissement de ces limites de confiance par session et par connexion.

Les mises en œuvre du Zero Trust matures sont plus souvent modernes qu'obsolètes (68 % contre 31,3 %) et axées sur le cloud que on-premise (46 % contre 23,6 %). Ces piles cloud modernes prennent mieux en charge l'exigence d'établir des limites de confiance par session et par connexion.

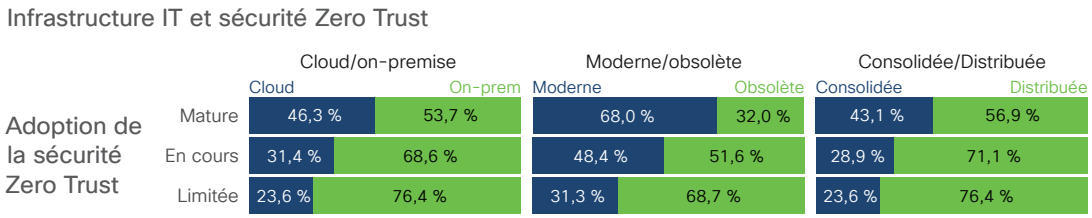


Figure 7 : Adoption de la sécurité Zero Trust dans le contexte des attributs de l'infrastructure IT

Faire le lien entre les différents points. Les points de contrôle de la sécurité Zero Trust sont les personnes, les équipements, les réseaux, les workloads des applications et les données. Lorsqu'ils sont distribués, ces points de contrôle peuvent devenir des silos qui génèrent le double de travail et de coordination. C'est donc sans surprise que les entreprises dont les **mises en œuvre sont matures privilégient l'infrastructure consolidée plutôt que l'infrastructure distribuée (43,1 % contre 23,6 %).** Le principe de l'économie des dispositifs est donc confirmé par les données.

Diffusion des correctifs. Maintenir l'environnement à jour est un facteur de réussite. La sécurité Zero Trust continue de faire évoluer les modèles d'architecture, les normes, les protocoles d'authentification et d'autorisation, ainsi que les protocoles de partage des signaux de confiance.

Les entreprises dont les mises en œuvre du modèle Zero Trust sont plus matures s'appuient sur la stratégie de leur fournisseur pour les mises à niveau plutôt que sur des mises à niveau proactives (45,8 % contre 30,9 %). Au lieu d'attendre une mise à jour planifiée et de laisser la technologie stagner pendant plusieurs années avec une stratégie de mise à jour pluriannuelle classique, les entreprises qui profitent des mises à jour automatiques de leurs applications SaaS bénéficient d'une plus grande flexibilité et d'un meilleur contrôle de la politique liée à ces applications SaaS dans le cloud.

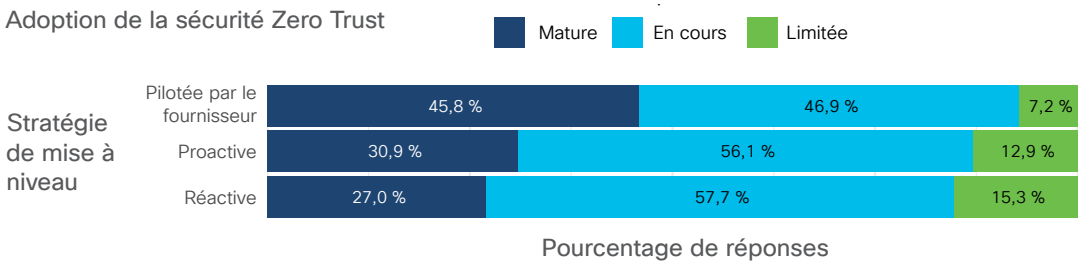


Figure 8 : Niveau d'adoption de la sécurité Zero Trust dans le contexte de la stratégie de mise à niveau

Centralisation des identités. Les entreprises qui fédèrent les identités sur une pile technologique moderne ont plus de facilité à atteindre la maturité. Cependant, celles qui sont en train de mettre en place une telle pile pourront appliquer très tôt dans leur processus de transition les principes et les modèles d'architecture Zero Trust.

Aucune technologie existante n'est négligée. L'application de ces principes Zero Trust aux environnements existants et aux environnements de pointe constitue un défi constant. Trop souvent, les contrôles de sécurité de pointe ciblent uniquement les environnements IT de pointe, qui sont pourtant loin d'être majoritaires.

Résultat : tout comme la transition vers le cloud, la transition vers la sécurité Zero Trust exige d'adopter une approche hybride combinant les anciens et les nouveaux modèles de sécurité.

D. Commencez par les utilisateurs, les applications et les équipements

Le programme de sécurité Zero Trust est destiné à des cas d'usage spécifiques. Ces cas d'usage, très présents parmi les entreprises qui ont réussi leur mise en œuvre, sont les suivants :

- Protection des collaborateurs
- Modernisation des applications
- Sécurisation des systèmes IoT (Internet des objets), IT et OT (technologies opérationnelles)

...et ces protections doivent être fournies dans un contexte permettant à un moteur de politiques de tout gérer et exécuter.

Par ailleurs, d'autres programmes de sécurité complémentaires, également conformes aux principes de sécurité Zero Trust, doivent être pris en compte. Commençons par les domaines opérationnels fondamentaux :

- Gestion des identités et des accès : qui sont mes utilisateurs autorisés, comment le savoir et à quelles ressources (par exemple les applications) ont-ils besoin d'accéder ?
- Gestion des ressources : quels équipements sont présents dans mes environnements IoT, IT et OT ? Comment savoir s'ils sont configurés de manière sécurisée ?

Il n'est pas simple d'obtenir des réponses à ces questions.

Par exemple, les participants aux **ateliers Cisco Zero Trust** ont souvent des difficultés avec leur programme de gestion des identités. **74 % des participants ont indiqué que la stratégie de gestion des identités de leur entreprise n'était pas définie, pas claire ou peu claire.** Dans la mesure où l'identité est, selon nous, le nouveau périmètre, le manque de contrôles des identités est problématique.

Les programmes de gestion des actifs posent également un défi constant pour la mise en œuvre de la sécurité Zero Trust. **55 % des participants ont indiqué qu'ils n'avaient pas de visibilité sur les équipements, ou seulement une visibilité faible ou partielle.** La limite de confiance est établie entre une personne, ses équipements et son application. En l'absence de visibilité ou de base de données de gestion de la configuration appropriée, comment pouvons-nous assurer la sécurité Zero Trust ?

Il faut notamment cesser de considérer la gestion des identités et des équipements comme un exercice ponctuel pour en faire une activité à la demande, exécutée chaque fois que les utilisateurs s'authentifient ou que l'équipement accède à une ressource.

En revanche, certains programmes de sécurité prenant en charge la sécurité Zero Trust connaissent un grand succès. **Les entreprises dont la mise en œuvre du modèle Zero Trust est mature font état de meilleurs résultats avec leurs programmes de gestion des risques (49 %)**. Elles correspondent et collaborent pour s'assurer que la sécurité Zero Trust applique (via une politique) la bonne approche des risques et les bonnes décisions identifiées par un programme de gestion des risques.

Nous constatons également que **les entreprises dont la mise en œuvre du modèle Zero Trust est mature obtiennent de meilleurs résultats avec leurs programmes de réponse aux incidents (43 %) et de continuité de l'activité (41 %).**

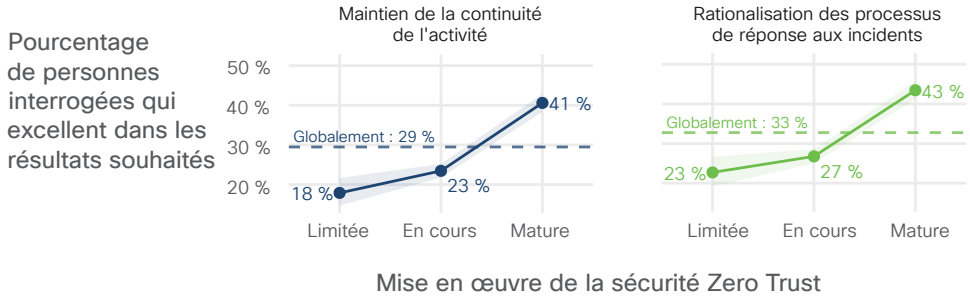


Figure 9 : Niveau d'adoption de la sécurité Zero Trust, continuité de l'activité et gestion des incidents

De plus en plus, le programme Zero Trust est associé à d'autres programmes de sécurité pour obtenir de meilleurs résultats. Les équipes de sécurité renoncent peu à peu aux processus manuels classiques pour la gestion des ressources, la gestion des identités ou les activités de détection et de réponse. En cas de non-conformité à la politique, lorsque le contexte et les conditions indiquent qu'un utilisateur ou un équipement n'est pas fiable, la réponse doit être automatique.

Résultat : les mises en œuvre de la sécurité Zero Trust réussies tirent parti des atouts des autres programmes via la collaboration et l'intégration technique.

E. Zoom sur les fonctionnalités Zero Trust

Concentrez-vous sur les fonctionnalités Zero Trust lorsque vous effectuez l'analyse de rentabilité, que vous créez le programme et que vous l'appliquez à une pile technologique moderne.

Soyez ambitieux : analyse, intégration et automatisation. La visibilité, l'intégration, ainsi que l'automatisation et l'orchestration des workflows sont les fonctionnalités Zero Trust présentes dans les mises en œuvre « optimales », telles que décrites dans les modèles de maturité et les architectures de référence. Ce sont ces fonctionnalités que vous devez chercher à déployer.

Les entreprises matures mettent l'accent sur l'intégration. Les données reflètent le débat qui anime les entreprises : est-il préférable d'acheter des technologies permettant des intégrations prêtes à l'emploi dans l'infrastructure existante (28,8 %) ou d'établir une sécurité Zero Trust en achetant auprès d'un fournisseur unique des solutions intégrées de façon native ou qui font partie d'une plateforme plus vaste (51 %) ? **Selon les entreprises, les deux approches sont efficaces, ce qui indique une évolution des produits sur le marché.**

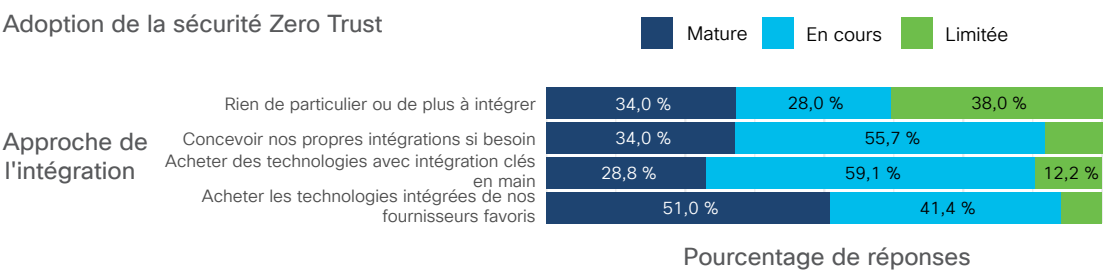


Figure 10 : Adoption de la sécurité Zero Trust dans le contexte de la stratégie d'intégration

Le partage des signaux permet d'élaborer une politique éclairée. Pour que votre mise en œuvre du modèle Zero Trust parvienne à maturité, vous devez renforcer l'intégration avec d'autres signaux de confiance pour **détecter** les menaces, **identifier** les vulnérabilités, **protéger** les ressources, **répondre** aux incidents et **rétablir** rapidement le fonctionnement. En d'autres termes, du point de vue de l'application de la politique, que consommez-vous et utilisez-vous pour prendre des décisions basées sur la confiance ? Quels signaux utilisez-vous et appliquez-vous pour étendre cette limite de confiance ? Pour répondre à ces questions, vous devez disposer de technologies bien intégrées, qui sont généralement bien plus présentes dans les entreprises matures.

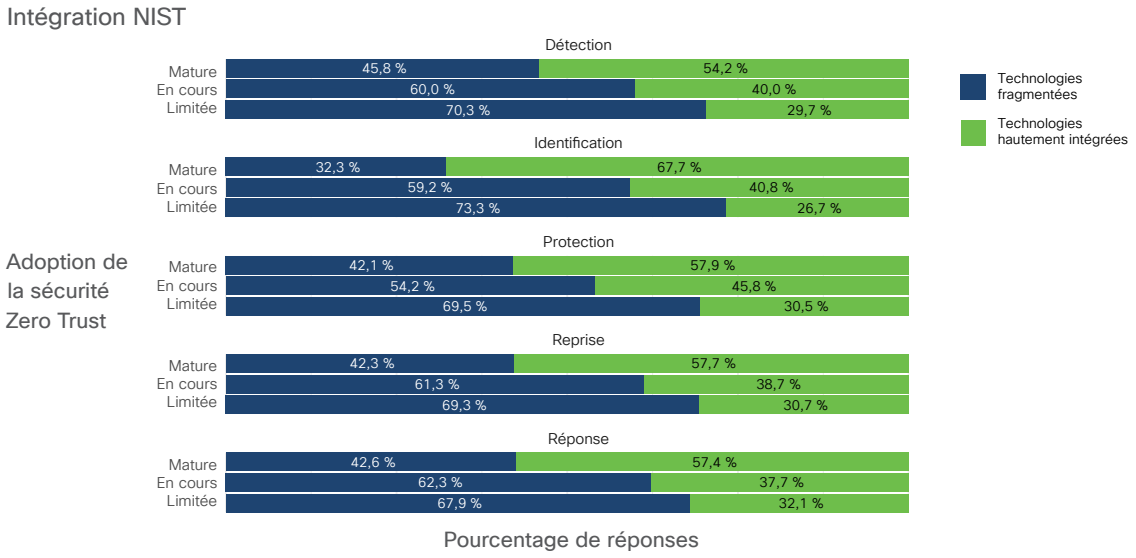
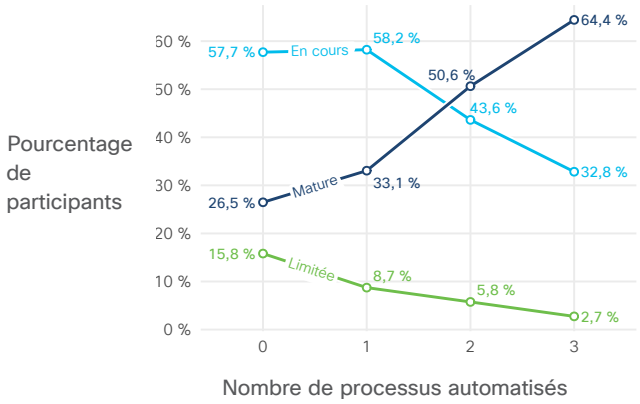


Figure 10 : Adoption de la sécurité Zero Trust dans le contexte de la stratégie d'intégration

L'automatisation et l'orchestration rendent la sécurité Zero Trust exploitable à grande échelle. Si l'intégration améliore la prise de décision en matière de politiques, l'automatisation et l'orchestration améliorent les mesures prises dans le cadre d'une sécurité Zero Trust. **Les entreprises dont les mises en œuvre du modèle Zero Trust sont matures sont celles qui automatisent le plus la supervision des menaces, l'analyse des événements et la réponse aux incidents (64,4 %).** Ces intégrations se font au fur et à mesure que les décisions des politiques sont prises et que les données sont mises à disposition pour une inspection rétroactive, ou une prévention proactive, d'une menace continue.



Plus les processus sont automatisés, mieux c'est. L'automatisation et l'orchestration peuvent s'appliquer à un certain nombre d'éléments tels que la modification des limites de confiance, la modification des niveaux de privilège, l'ajustement des rôles et l'ajustement du contexte dans lequel l'identité fonctionne, jusqu'à ce que la confiance soit améliorée.

Figure 12 : Les entreprises dont les mises en œuvre du modèle Zero Trust sont matures tirent parti de l'automatisation

Nous constatons que les entreprises dont les mises en œuvre de la sécurité Zero Trust sont matures automatisent davantage leur processus, ce qui confirme que l'orchestration et l'automatisation à tous les niveaux se généralisent.

Principaux points à retenir : pour les fonctionnalités Zero Trust, commencez par mettre en place une politique de base. Ensuite, assurez la visibilité sur ces points d'application des politiques. Planifiez les intégrations entre les moteurs de politiques et le nombre croissant de signaux de confiance. Enfin, augmentez l'automatisation et l'orchestration pour pouvoir agir dans un plus grand nombre d'environnements. Procédez étape par étape.

F. Préparez la transition à venir

Si vous présentez le programme de sécurité comme une transition, vous risquez d'avoir des difficultés à conserver le soutien des dirigeants et l'adhésion des collaborateurs sur le long terme.

Ce n'est ni un marathon ni un sprint : les programmes Zero Trust permettent d'intégrer la sécurité dans votre façon de travailler.

Alignez-vous sur les valeurs et les priorités de l'entreprise. Pour réussir, les initiatives Zero Trust doivent s'appuyer sur des principes Zero Trust qui accroissent la valeur commerciale, présentent un intérêt pour l'équipe dirigeante et vos collègues, et renforcent la sécurité. Ainsi, les entreprises obtiennent des résultats rapidement.

Tirez parti des architectures de référence et des cadres de gestion de projet. Cet effort de transformation doit s'appuyer sur l'architecture de l'entreprise et la gestion de projet. Ces fonctions définissent une méthode cohérente de mise en œuvre des principes Zero Trust dans divers environnements, avec des identités variées (personnes, services et équipements, par exemple). Pour mettre en œuvre la sécurité Zero Trust, vous devez commencer par définir la gouvernance.

Connectez votre architecture à votre gouvernance. Si votre entreprise dispose d'une équipe de gestion de l'architecture d'entreprise, commencez par définir une architecture de référence pour la sécurité Zero Trust. Si votre entreprise dispose d'une équipe GRC (gouvernance, gestion des risques et de la conformité), commencez à réfléchir à l'application des principes Zero Trust conformément aux directives, aux normes et, éventuellement, à la codification de la politique. Utilisez des points de décision des politiques Zero Trust et un moteur de décision des politiques pour définir et appliquer les politiques GRC.

Définissez et communiquez les indicateurs clés de performance (KPI). Si vous souhaitez que les contrôles Zero Trust soient bien compris des auditeurs, vous devez les relier aux objectifs de gouvernance avant de leur en parler. La fonction GRC peut, dans le cadre d'un audit interne, déterminer la manière dont la sécurité Zero Trust sera mesurée et documentée, pour communiquer ces informations aux auditeurs tiers et externes. Les analyses de rentabilité en lien avec les facteurs de conformité ou les demandes de clients exigent ce type d'approche. Déterminez très tôt comment la sécurité Zero Trust sera évaluée et mesurée par des tiers, et discutez-en avec vos homologues et les dirigeants.

Tirez parti de vos points forts. Dans toutes les entreprises, les piles de sécurité présentent des forces et des faiblesses. Si vous disposez d'une solution CASB (service de sécurité pour l'accès au cloud) très performante, vous pouvez obtenir une liste dynamique d'applications. Si vous disposez d'un dispositif d'authentification unique (SSO) ou d'authentification multifacteur (MFA) très performant, vous pouvez obtenir des données sur les équipements de façon dynamique. L'important est de tirer parti de vos points forts pour gagner en visibilité et mieux prendre en compte le contexte.

La visibilité est primordiale. En gagnant en visibilité et en configurant des processus d'inventaire, vous obtiendrez rapidement des résultats. N'oubliez pas : vous devez vous assurer que l'authentification multifacteur et l'authentification unique sont déployées pour améliorer la visibilité sur l'application des politiques dans ces contrôles. Avec cette approche, vous mettez en place le moteur de politiques pour gagner en visibilité, tout en décidant du niveau d'application des politiques. Ensuite, définissez les points de collaboration avec d'autres programmes de sécurité.

Feuille de route pour passer d'une mise en œuvre du modèle Zero Trust « en cours » à une mise en œuvre « mature »

La transition d'une mise en œuvre en cours vers une mise en œuvre mature repose sur trois points :		
• D'abord, donnez de **l'ampleur à la mise en œuvre**, en augmentant la couverture des contrôles. Vous pouvez par exemple augmenter le nombre de personnes inscrites à l'authentification multifacteur, accroître le nombre d'équipements gérés et protéger un plus grand nombre d'applications.	• Ensuite, **augmentez la profondeur de la politique**. Tirez parti de la télémétrie, du contexte et des conditions au sein du moteur de politiques pour prendre des décisions plus fiables. De là, étendez les intégrations à d'autres technologies de sécurité.	• Enfin, pour évoluer vers une mise en œuvre mature, **augmentez l'automatisation et l'orchestration**. Quelles autres procédures pouvez-vous automatiser pour qu'elles se déclenchent en cas d'identification d'un équipement/utilisateur non fiable ?

Conclusion : il est préférable d'adopter une approche progressive de la mise en œuvre de la sécurité Zero Trust, comprenant plusieurs étapes gérées comme des projets de sécurité individuels.

Chaque étape peut offrir :

- Des opportunités plus nombreuses de renforcer les relations et la culture de la sécurité
- Des moyens de mettre en œuvre les améliorations attendues depuis longtemps, de la gestion des identités à la gestion des ressources, en passant par la réponse aux incidents et la reprise après sinistre
- Des technologies de sécurité peu coûteuses, bien intégrées et automatisées qui apportent une valeur ajoutée à l'entreprise

V. Points à retenir pour la mise en œuvre de la sécurité Zero Trust

A. Utilisation du modèle Zero Trust de l'agence CISA

La sécurité Zero Trust étant une stratégie architecturale, mieux vaut s'appuyer sur l'expertise du secteur pour sa mise en œuvre. La CISA est la référence en matière d'architecture Zero Trust. La CISA, ou Cybersecurity and Infrastructure Security Agency, a été créée en 2018. Elle est le fruit d'un partenariat entre public et privé visant à sécuriser l'infrastructure numérique stratégique au sein du ministère de la Sécurité intérieure américain. Avec ses partenaires, l'agence « collabore à la fourniture d'une protection contre les menaces actuelles et à la création d'une infrastructure plus sécurisée et plus résiliente pour l'avenir[2] ».

> « La sécurité Zero Trust est essentielle pour moderniser et renforcer les défenses de notre pays. » – Jen Easterly, directrice de la CISA

Le modèle de maturité Zero Trust de la CISA fournit une feuille de route aux entreprises qui cherchent à mettre en œuvre la sécurité Zero Trust. Ce cadre présente les cinq piliers de la sécurité Zero Trust :

- Identification
- Équipement
- Réseau (ou environnement)
- Applications (ou workloads)
- Données

[2] https://www.cisa.gov/about-cisa

Chacun de ces piliers comprend des exigences en matière de visibilité et d'analyse, d'automatisation et d'orchestration, et de gouvernance (ou de conformité). En outre, pour chacun de ces piliers, différents niveaux de maturité ont été définis en fonction de la force du contrôle ou de son mode de déploiement : classique, avancé et optimal.

Le modèle de maturité Zero Trust de la CISA témoigne du fait que la sécurité Zero Trust est une quête permanente et non un projet unique. L'utilisation de ce modèle permet aux équipes d'évaluer où elles en sont dans leur transition, où elles présentent des lacunes et comment progresser.

Selon le modèle de la CISA, et conformément aux données de notre enquête, les mises en œuvre du modèle Zero Trust optimales s'appuient sur les éléments suivants :

- Automatisation
- Workflows intégrés
- Validation continue de la fiabilité
- Inventaires de données
- Chiffrement
- Micropérimètres

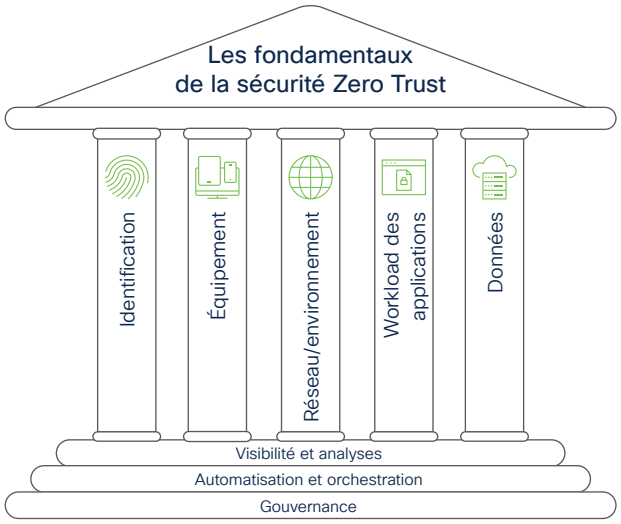


Figure 13 : Les piliers de la sécurité Zero Trust selon la CISA (Cybersecurity and Infrastructure Security Agency) aux États-Unis

Modèle de maturité Zero Trust de la CISA

	Identification	Équipement	Réseau/ Environnement	Workload des applications	Données
Classique	• Mot de passe ou authentification multifacteur (MFA) • Évaluation limitée des risques	• Visibilité limitée sur la conformité • Inventaire simple	• Vaste macrosegmentation • Chiffrement minimum du trafic interne ou externe	• Accès basé sur une autorisation locale • Intégration minimum avec le workflow • Certaine accessibilité au cloud	• Pas bien inventorié • Contrôle statique • Non chiffré
Avancé	• Authentification multifacteur • Relative mutualisation des identités avec des systèmes cloud et on-premise	• Utilisation de la mise en application de la conformité • L'accès aux données dépend du niveau de sécurité de l'équipement lors du premier accès.	• Défini par des micropérimètres d'entrée/de sortie • Analyses basiques	• Accès basé sur l'authentification centralisée • Intégration basique dans le workflow des applications	• Contrôles sur le principe du moindre privilège • Les données stockées dans des clouds ou des environnements distants sont chiffrées au repos.
Optimal	• Validation continue • Analyse de l'apprentissage automatique en temps réel	• Surveillance et validation constantes de la sécurité des équipements • L'accès aux données dépend de l'analyse des risques en temps réel	• Micropérimètres d'entrée/de sortie entièrement distribués • Protection contre les menaces basée sur l'apprentissage automatique • Tout le trafic est chiffré	• L'accès est autorisé en continu • Forte intégration dans le workflow des applications	• Assistance dynamique • Toutes les données sont chiffrées

Visibilité et analyses | Automatisation et orchestration | Gouvernance

Figure 14 : Modèle de maturité Zero Trust de la CISA (Cybersecurity and Infrastructure Security Agency) aux États-Unis

Le gouvernement américain encourage l'adoption du modèle Zero Trust

En mai 2021, le président Biden a signé son premier décret sur la cybersécurité, obligeant le gouvernement fédéral à adopter une architecture Zero Trust. En janvier 2022, le Bureau de la gestion et du budget (Office of Management and Budget, OMB) a publié une note de service réaffirmant cette obligation en précisant les échéances de chaque exigence spécifique. Malgré la portée limitée de cette note de service sur les agences fédérales civiles, de nombreux analystes du secteur se sont appuyés sur le modèle de la CISA pour analyser le marché de la sécurité Zero Trust.

B. Enseignements tirés de l'expérience Zero Trust de Cisco

En 2020, Cisco a décidé de passer d'un modèle classique basé sur le périmètre réseau et le VPN à un modèle Zero Trust. Dès le départ, l'objectif était de proposer une expérience d'accès aux applications sécurisée et uniforme, indépendamment de l'emplacement de l'utilisateur et des applications.

Notre équipe a amélioré la sécurité et l'expérience de nos 100 000 utilisateurs, et a mis en œuvre ce changement radical en moins de cinq mois.

À quoi ressemble la sécurité Zero Trust chez Cisco ? Pour Cisco, la sécurité Zero Trust consiste à déclencher quatre opérations à chaque tentative d'accès à une application :

1. Nous vérifions l'utilisateur à l'aide de l'authentification multifacteur.
2. Nous confirmons que l'équipement est à jour et intègre.
3. Nous confirmons que l'équipement utilisé est géré par Cisco.
4. Nous rendons l'application accessible sans VPN.

Et nous le faisons vraiment systématiquement, pas une seule fois par jour ou pour une seule application, mais en continu.

« Ce n'est pas souvent que vous pouvez vous vanter d'améliorer en même temps la sécurité et l'expérience des utilisateurs, et c'est ce que nous a permis de faire ce déploiement. »
– Josephina Fernandez, directrice IT de Cisco

C. Présentation des actions à effet rapide

Action à effet rapide nº 1 : obtenir l'adhésion avec un message simple. Nous avions constaté lors de précédentes initiatives que l'équipe dirigeante avait du mal à comprendre et soutenir un projet complexe. Notre objectif était donc de simplifier le message, de le préciser et de le cadrer dans le temps, pour que les informations soient faciles à mémoriser et à partager.

Action à effet rapide nº 2 : bien définir le périmètre et communiquer efficacement sur l'état. Nous avons clairement communiqué nos objectifs : améliorer l'expérience utilisateur, réduire les risques et améliorer la gouvernance. Nous avons stoppé net toute tentative d'aller au-delà de ces objectifs et informé régulièrement toutes les parties de l'état du déploiement.

Action à effet rapide nº 3 : créer la demande pour une sécurité Zero Trust. Nous avons commencé par les 10 à 15 applications les plus utilisées pour que l'amélioration de l'expérience utilisateur ait l'impact le plus visible et le plus vaste possible. Lorsque les utilisateurs ont compris combien il était facile d'accéder à leurs applications les plus importantes, les responsables des applications et les chefs de service de toute l'entreprise ont été de plus en plus nombreux à demander la mise en œuvre de la sécurité Zero Trust.

Action à effet rapide nº 4 : commencez par tirer parti de ce que vous avez. Comme le dit notre vice-président et directeur de la sécurité, Brad Arkin : « On ne part jamais de rien ». Notre équipe a identifié les contrôles de sécurité existants qu'elle pourrait utiliser pour atteindre ses objectifs de sécurité Zero Trust et les technologies qui n'étaient plus utiles.

Cliquez ici pour en savoir plus sur le déploiement de la sécurité Zero trust à grande échelle chez Cisco.

La sécurité Zero Trust chez Cisco en chiffres

Indicateurs pilotes	Indicateurs mensuels	Économies annuelles
• Calendrier de 5 mois, incluant les collaborateurs et les sous-traitants dans 98 pays • 10 à 15 applications privées protégées sans VPN (aujourd'hui > 100) • Moins de 1 % d'utilisateurs ont contacté le centre d'assistance (contre 7 %) • 170 000 équipements sécurisés	• 5,76 millions de contrôles d'intégrité • Plus de 86 000 équipements corrigés automatiquement • 410 000 authentifications en moins via le VPN	• 3,4 millions de dollars d'économies grâce aux gains de productivité des collaborateurs • 500 000 dollars d'économies sur les coûts d'assistance IT

D. Renforcement de la résilience : comment Cisco Secure assure la sécurité Zero Trust

Cisco permet aux entreprises d'intégrer la sécurité Zero Trust dans la fabric de leur écosystème IT multi-environnement et de sécuriser l'accès d'une manière qui complique la vie des hackers, pas celle des utilisateurs. Elles protègent ainsi leur intégrité face aux menaces et aux défis imprévisibles, et assurent la résilience de leur système de sécurité.

Grâce aux fonctionnalités Zero Trust indispensables fournies par Cisco, les entreprises peuvent :

L'approche intégrée de Cisco permet aux entreprises de mettre en œuvre une gestion unifiée du cycle de vie des politiques sur leur réseau, leurs équipements, leurs applications et leurs clouds.

Grâce à Cisco, elles dégagent de la valeur et atteignent leurs objectifs (tout en bénéficiant d'une sécurité robuste et d'une productivité élevée), et leurs équipes améliorent la sécurité, augmentent la performance et accélèrent la réponse aux menaces.

En tant qu'entreprise ayant elle-même mis en œuvre la sécurité Zero Trust dans ses opérations mondiales, Cisco apporte une expertise de confiance et aide plus de 300 000 clients à travers le monde à protéger l'intégrité de chaque aspect de leur activité pour faire face aux menaces ou aux changements imprévisibles et en sortir renforcés.

Plateforme Cisco Secure

Principaux atouts de la sécurité Zero Trust

Établir la fiabilité
Visibilité et prise en compte du contexte pour prendre des décisions relatives à la fiabilité au niveau de l'IT et de l'OT

Fournir un accès basé sur la confiance
Vérification unifiée et cohérente basée sur des politiques (personnes/applications/machines)

Vérifier en permanence le niveau de confiance
Adaptation continue de la confiance en fonction de l'évolution du risque

S'adapter aux fluctuations de fiabilité
Réponse automatisée sur l'ensemble du réseau/des appareils/des applications pour rebondir plus rapidement

Nos solutions couvrent les cinq piliers du modèle de maturité Zero Trust de la CISA, fournissant une visibilité et un contrôle sur les réseaux locaux, cloud et on-premise.

cisco SECURE

VI. Étapes suivantes

Les nombreux clients et partenaires avec lesquels nous travaillons sur la sécurité Zero Trust ont plusieurs problèmes critiques à résoudre. Pour certains, la sécurité Zero Trust est un moyen de protéger les ressources contre les menaces ciblées ou d'améliorer les performances de l'entreprise en sécurisant le travail hybride. Pour d'autres, elle est un moyen de réduire les risques liés à la chaîne d'approvisionnement et de protéger les environnements cloud.

Pour faire face à l'essor des menaces, vous devez adopter une nouvelle approche de la sécurité. En s'associant à Cisco pour mettre en œuvre la sécurité Zero Trust, votre entreprise peut accélérer sa réponse aux menaces et renforcer sa résilience grâce à une meilleure visibilité, et réduire l'impact des menaces pour accélérer la reprise des opérations et de l'activité.

Prêt à faire vos premiers pas avec la sécurité Zero Trust ? Assurez-vous que seuls les utilisateurs autorisés et les équipements sécurisés ont accès aux applications, dans le cadre d'une expérience fluide. Essayez gratuitement Cisco Secure Access by Duo.

Pour savoir comment démarrer votre quête de la sécurité Zero Trust, inscrivez-vous à l'un des ateliers Cisco Zero Trust.

cisco.com/go/zero-trust-workshops

DUO

Duo Security, qui fait désormais partie de Cisco, est le principal fournisseur de solutions d'authentification multifacteur et d'accès sécurisé. Duo est un pilier de la solution Zero Trust de Cisco Secure, la plateforme la plus complète pour sécuriser l'accès aux applications et aux environnements IT, quel que soit l'utilisateur ou l'équipement. Duo est le partenaire de confiance de plus de 35 000 clients à travers le monde, parmi lesquels Bird, Facebook, Lyft, l'Université du Michigan, Yelp, Zillow, etc. Fondée à Ann Arbor, dans le Michigan, la société Duo est également présente à Austin, au Texas, à San Francisco, en Californie et à Londres.

Bénéficiez d'un essai gratuit sur duo.com.

cisco SECURE

Cisco s'est imposé depuis longtemps comme le leader des solutions réseau, tout en développant une gamme de solutions ouvertes et intégrées pour la cybersécurité. Cisco Secure repose sur le principe d'une sécurité améliorée, et non augmentée. Il propose une approche rationalisée de la sécurité, centrée sur le client, qui garantit la facilité de déploiement, de gestion et d'utilisation, et de fonctionnement avec tous les autres produits. Les collaborateurs et les clients sont au cœur de nos activités, et c'est ce qui nous motive. Cisco Secure permet aux professionnels de la sécurité de se protéger en toute confiance contre les menaces actuelles et futures grâce à la plateforme Cisco SecureX. Nous aidons l'ensemble des entreprises du classement Fortune 100 à se protéger aujourd'hui comme demain grâce à la plateforme de cybersécurité intégrée la plus complète au monde.

Pour savoir comment nous simplifions les expériences, accélérons la réussite et protégeons l'avenir de nos clients, rendez-vous sur cisco.com/go/secure.