# Mise en place d'un réseau Zero Trust économique

## Maximiser la sécurité du réseau et minimiser les coûts

Fiche solution

Alcatel·Lucent Enterprise


# Cybersécurité et Zero Trust

La cybersécurité est une préoccupation de plus en plus importante car la technologie ne cesse de progresser et le nombre et la complexité des cybermenaces continuent d'augmenter. Les menaces évoluant rapidement, il est difficile pour les organisations de les prévoir et de s'en défendre, ce qui oblige les experts en cybersécurité à restés à l'affût des dernières tendances et vulnérabilités.

En raison de la diversité et de l'explosion du nombre de sources et de vecteurs d'attaque, tels que les e-mails d'hameçonnage, l'ingénierie sociale et les vulnérabilités logicielles, la défense contre les cybermenaces nécessite une approche unique pour chaque type d'attaque.

Il peut être difficile d'identifier et de protéger toutes les vulnérabilités potentielles d'un système complexe. Il est donc essentiel que les experts en cybersécurité comprennent comment les différents systèmes et réseaux fonctionnent ensemble afin de mettre au point des mesures de sécurité efficaces.

L'erreur humaine constitue une cause fréquente de violation de la cybersécurité et, d'ici 2025, on estime que le manque de compétence ou la défaillance humaine seront à l'origine de plus de la moitié des cyberincidents importants.[1]

Le respect des réglementations et des normes complexes en matière de cybersécurité, telles que le règlement général sur la protection des données (RGPD) et la loi Health Insurance Portability and Accountability Act (HIPAA), représente un autre défi qui nécessite des connaissances et une expertise spécialisées.

1 Gartner® Prévoit 2023: L'industrie de la cybersécurité se concentre sur la transaction humaine| Bitsight, janvier 2023.

# Processus en cas de violation de la cybersécurité

La figure suivante illustre les étapes suivies par un cyberattaquant pour pénétrer dans un réseau et voler des données précieuses. La première étape est la reconnaissance : les attaquants recherchent, identifient et sélectionnent des cibles, et recherchent les vulnérabilités du réseau.

L'étape suivante est celle de l'armement : les attaquants déterminent comment compromettre un point de terminaison cible et délivrer une charge utile armée.

Vient ensuite l'exploitation : l'attaquant déclenche la charge utile militarisée et escalade les privilèges sur le point de terminaison compromis pour se déplacer latéralement dans le réseau.

L'étape suivante est l'installation : les attaquants établissent un accès à distance et installent des logiciels malveillants afin d'établir une persistance.

Au stade du commandement et du contrôle, les attaquants établissent des canaux de communication chiffrés vers des serveurs de commandement et de contrôle afin de diriger l'attaque à distance et d'exécuter les objectifs.

La dernière étape est le mouvement latéral et l'exfiltration : les attaquants peuvent avoir des objectifs multiples, notamment le vol de données, la destruction ou la modification de systèmes critiques et le déni de service.

La clé pour arrêter les attaquants est de détecter rapidement les différentes étapes du cycle de vie de l'attaque et d'interrompre leur progression.

Afin d'éviter cela, vous devez prendre une série de mesures telles que la gestion des vulnérabilités et des correctifs, la détection et la prévention des logiciels malveillants, le blocage des applications et des services à risque, ainsi que l'enregistrement et la surveillance de toutes les activités du réseau, des terminaux et, bien sûr, du cloud.

Du côté du réseau, vous devez mettre en œuvre des technologies qui permettent un contrôle granulaire des applications et qui surveillent le trafic entre les zones ou les segments dans un modèle Zero Trust (confiance zéro). La confiance zéro part du principe que, par défaut, tout doit être considéré comme non fiable.

Le concept Zero Trust a été développé en réponse au nombre croissant de cyberattaques sophistiquées sur les réseaux informatiques. Traditionnellement, les organisations s'appuyaient sur des solutions de sécurité basées sur le périmètre, telles que les pare-feu et les logiciels antivirus, pour protéger leurs réseaux. Cependant, les cyberattaques étant devenues plus avancées et plus complexes, ces solutions se sont révélées insuffisantes, et chaque demande d'accès doit être vérifiée et authentifiée avant d'accorder l'accès aux ressources.


Source : XDR pour les nuls, Palo Alto Networks Edition Spéciale, 2022

# Dynamiser votre stratégie Zero Trust

Alcatel-Lucent Enterprise aide ses clients à renforcer leur sécurité et à évoluer vers un environnement Zero Trust avec simplicité et rentabilité. Chez ALE, nous comprenons l'importance de l'implémentation d'un modèle Zero Trust pour garantir la sécurité du réseau et des données de nos clients. Nous proposons une gamme de solutions conçues pour aider les organisations à mettre en œuvre un réseau Zero Trust et à relever les défis posés par les cybermenaces.

## Durcissement du réseau

Nous offrons un **réseau robuste, tant à l'intérieur qu'à l'extérieur**. Cela commence par une infrastructure sécurisée et la garantie que l'appareil lui-même n'est pas compromis. Notre gamme de produits Alcatel-Lucent OmniSwitch® fonctionne avec le système d'exploitation sécurisé Alcatel-Lucent (AOS), qui utilise un code diversifié sécurisé pour protéger les réseaux contre les vulnérabilités et les attaques potentielles. Le code est continuellement mis à jour afin de se prémunir des menaces actuelles et futures, avec une diversification des logiciels grâce à la randomisation de l'espace d'adressage (ASLR, Address Space Layout Randomisation) utilisée pour se protéger contre les attaques par débordement de mémoire tampon. La vérification et la validation indépendantes (IV&V) permettent également d'analyser et de tester le code source de l'AOS afin de détecter les vulnérabilités potentielles, les portes dérobées, les logiciels malveillants et les exploits du système. Des experts en cybersécurité tiers effectuent ces tests, qui sont exécutés sur des images de logiciels à disponibilité générale afin de garantir l'intégrité des logiciels.

Nous appliquons une macro et une micro-segmentation pour garantir l'accès au réseau Zero Trust. Ces deux éléments sont des composants essentiels d'une stratégie de sécurité Zero Trust. **Macro-segmentation** désigne le cloisonnement du réseau en zones ou domaines distincts sur la base d'une fonction, d'une application ou d'un groupe d'utilisateurs. Il en résulte un niveau élevé de segmentation du réseau, qui permet aux organisations d'isoler les ressources et les équipements critiques du reste du réseau. **La micro-segmentation**, quant à elle, se concentre sur la segmentation du réseau à un niveau plus granulaire, jusqu'à l'utilisateur ou l'appareil individuel. Cette approche offre un contrôle plus fin de l'accès au réseau, permettant aux organisations d'appliquer des politiques de sécurité au niveau de l'utilisateur individuel ou de l'appareil.

Shortest Path Bridging (SPB) et les **profils réseau universel** (UNP, Universal Network Profiles) offrent une solution puissante pour aider à la macro- et micro-segmentation des réseaux, ce qui améliore la sécurité et la performance en limitant la portée des attaques potentielles.

SPB est un protocole de réseau de Couche 2 qui permet le routage à trajets multiples dans les grands réseaux tout en simplifiant la configuration et la gestion de l'infrastructure de réseau. Des fonctionnalités, telles que la segmentation virtuelle du réseau, offrent une protection supplémentaire contre les accès non autorisés et les cyberattaques. Lorsqu'elles utilisent SPB dans leur infrastructure de réseau, les organisations peuvent bénéficier d'une efficacité et d'une sécurité accrues du réseau, ce qui leur permet d'atteindre leurs objectifs commerciaux en toute confiance.

L'UNP d'ALE est un contrôle d'accès basé sur le profil, une fonctionnalité puissante des commutateurs Alcatel-Lucent Enterprise qui permet aux administrateurs de réseau de créer et de gérer les profils d'utilisateurs pour l'accès au réseau en fonction de l'identité, de l'emplacement et de l'appareil. Ils peuvent mettre en œuvre une gestion centralisée des politiques de réseau, simplifiant alors la configuration et l'application des politiques. En mettant en œuvre l'UNP d'ALE, les entreprises sont en mesure d'améliorer la visibilité, la sécurité et le contrôle de leur réseau, tout en optimisant ses performances, en protégeant les équipements et en réduisant les temps d'arrêt.

**Ensemble, le SPB et l'UNP permettent aux administrateurs de réseaux de gérer et de sécuriser efficacement leur infrastructure réseau afin de :**

- **Constamment appliquer les politiques sur l'ensemble du réseau**
- **Segmenter et isoler les appareils IoT des autres appareils**
- **Réduire la surface d'attaque du réseau**

## Authentification solide

ALE fournit une authentification solide par le biais d'un gestionnaire d'authentification de politiques unifiées (UPAM).

L'un des éléments clés de la cybersécurité est l'authentification, qui consiste à vérifier l'identité d'un utilisateur, d'un appareil ou d'un système. Cela implique de confirmer qu'un utilisateur ou un appareil est bien celui qu'il prétend être, généralement en fournissant une forme d'identification, comme un nom d'utilisateur et un mot de passe.

La solution ALE prend en charge un certain nombre de méthodes d'authentification des utilisateurs.

- **802.1X**, un protocole d'authentification réseau, permet aux appareils de se connecter à un réseau sécurisé en fournissant des informations d'identification, telles qu'un nom d'utilisateur et un mot de passe. Lorsqu'un appareil tente de se connecter à un réseau en utilisant 802.1X, il est tout d'abord authentifié avant d'être autorisé à accéder au réseau. Dans un monde idéal, l'appareil est authentifié à l'aide de 802.1x. L'authentification génère un enregistrement qui peut être partagé avec un pare-feu.
- Si l'appareil ne prend pas en charge 802.1x, l'authentification **adresse MAC** constitue une option. Une adresse MAC est une carte d'identité numérique pour chaque appareil d'un réseau. Elle est unique, identifie chaque appareil et permet les communications entre eux, tout comme un badge pour votre ordinateur ou votre téléphone.
- ALE prend en charge **l'empreinte numérique des dispositifs et des systèmes**. Si aucun profil n'est renvoyé avec l'autre 802.1X ou l'authentification MAC, nous tentons d'obtenir une empreinte numérique. Dans le domaine de la sécurité informatique, l'empreinte numérique est le processus de collecte d'informations sur un appareil ou un système, comme son système d'exploitation, ses logiciels et ses ports ouverts, afin de l'identifier, de le classer et d'évaluer les risques et les vulnérabilités potentiels. Elle peut également être utilisée pour établir une correspondance avec le profil d'un appareil enregistré dans la base de données de l'inventaire de l'IoT.
- ALE propose également par défaut une règle « Tout capturer » au cas où un profil ne serait pas renvoyé. La règle « Tout capturer » par défaut peut autoriser un accès limité ou refuser complètement l'accès en cas d'échec de l'authentification principale.

Pour exécuter ces différents types d'authentification, il vous faut un endroit où créer et gérer les informations d'identification des utilisateurs et des appareils. L'UPAM, un composant de la solution accès unifié d'ALE, est nécessaire. Il fournit des services centralisés d'authentification, d'autorisation et de comptabilisation (AAA, Authentification Autorisation et Comptabilité) pour le réseau. Il permet aux administrateurs de réseaux de créer et de gérer les profils d'utilisateurs pour l'accès au réseau, sur la base de l'identité et de la localisation, entre autres. L'UPAM peut être configuré et géré par l'intermédiaire du système de gestion du réseau Alcatel-Lucent OmniVista®, ce qui permet aux administrateurs de réseau de définir et d'appliquer des politiques d'accès au réseau.

## Réactivité en cas d'incident

Répondre rapidement aux incidents de réseau constitue un facteur essentiel de la réduction des dommages aux systèmes et aux réseaux, ainsi que de la réduction des temps d'arrêt causés par des attaques de sécurité telles que le déni de service distribué (DDoS).

Minimisez les risques, maximisez la qualité d'expérience (QoE) et renforcez la sécurité grâce à Alcatel-Lucent OmniVista Network Advisor. **OmniVista Network Advisor** est un système intelligent et autonome basé sur l'IA qui permet de surveiller le réseau en temps réel, d'émettre des alertes lorsque des problèmes surviennent et de suggérer des solutions pour divers problèmes liés au réseau et à la sécurité, notamment les attaques DDoS. Il effectue en permanence des audits de configuration et des analyses de performance du réseau, ce qui lui permet d'**identifier** rapidement les problèmes potentiels, de les **atténuer** et d'**optimiser** le réseau avec une intervention informatique minime, voire inexistante.

## Partenariats et intégrations

Un aspect important de l'authentification est l'intégration avec les pare-feu. Par exemple, grâce à l'intégration avec Fortinet, les utilisateurs ou les dispositifs authentifiés sur les réseaux LAN et/ou WLAN peuvent également être authentifiés simultanément et de manière transparente sur le pare-feu Fortinet.

Avec l'intégration du pare-feu de nouvelle génération de Palo Alto Networks (PAN), les utilisateurs ou les dispositifs authentifiés sur les réseaux LAN et/ou WLAN peuvent également l'être simultanément et de manière transparente sur le pare-feu PAN.

Notre partenariat avec Versa Networks permet un accès sécurisé aux ressources critiques, quel que soit l'emplacement des utilisateurs, des données, des applications ou des appareils. Cette solution est particulièrement avantageuse pour les entreprises dont les bureaux régionaux ou les succursales sont éloignés du site central ou du centre de données. Contrairement aux réseaux étendus (WAN) traditionnels qui nécessitent plusieurs sauts de réseau et qui peuvent entraîner des coûts supplémentaires, le SASE et le SD-WAN offrent une solution rentable et sécurisée pour l'ère du client vers le cloud. En combinant ces deux solutions, les entreprises peuvent simplifier la gestion de l'infrastructure informatique et permettre un accès sécurisé à Internet et aux applications métiers dans le cadre de scénarios de travail en tout lieu, notamment dans les entreprises et les centres de distribution, les bureaux régionaux et les succursales, ainsi que pour les télétravailleurs/travailleurs mobiles.

L'offre Versa Titan d'ALE est une solution complète qui combine la solution Secure Access Service Edge (SASE) et le SD-WAN à partir du cloud. Elle comprend le SD-WAN de Versa Titan, qui fournit un SD-WAN dans le cloud pour le Lean IT, ainsi que la solution Versa Secure Access (VSA), qui offre des capacités de pare-feu nouvelle génération et de blocage géographique, ainsi qu'un accès réseau Zero Trust (ZTNA) pour les scénarios de travail en tout lieu. De plus, la solution Secure Web Gateway (SWG) de Versa offre une navigation web sécurisée et un accès aux applications Internet (SaaS) pour une connectivité sécurisée entre le bureau à distance/domicile. Le portail web et l'application Versa Titan offrent des services intégrés de mise en réseau et de sécurité sur une plateforme unique, tous les composants SASE étant fournis par le même fournisseur. Grâce à un registre unique de politiques qui couvrent les règles de réseau et de sécurité, les entreprises peuvent simplifier la gestion informatique et garantir un accès sécurisé aux ressources stratégiques.

## La stratégie Zero Trust

Pour mettre en œuvre un modèle Zero Trust, les organisations doivent d'abord s'attaquer aux problèmes de leur infrastructure de sécurité existante, tels que les politiques incohérentes, la confiance implicite et les appareils IoT vulnérables. L'objectif est de mettre en place des capacités de contrôle d'accès au réseau et d'accès basé sur les rôles, de segmentation et de surveillance pour remédier à ces problèmes, une segmentation adéquate permettant de cloisonner les ressources sensibles et de limiter l'accès aux seules personnes qui en ont besoin. Les capacités de surveillance et de mise en quarantaine permettent aux clients d'identifier et d'isoler les menaces potentielles.

Une stratégie simple mais puissante pour construire un réseau Zero Trust avec des solutions ALE comporte plusieurs étapes.

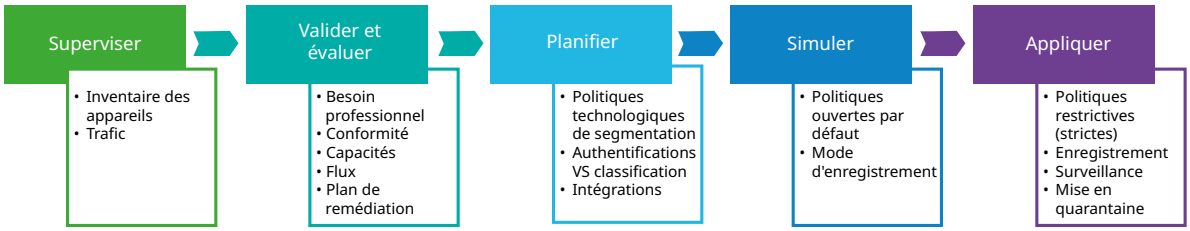
- **Contrôler** : une surveillance doit être effectuée, y compris l'inventaire des dispositifs et le trafic
- **Valider et évaluer** : la validation et l'évaluation impliquent l'analyse des besoins de l'entreprise, des exigences de conformité, des capacités et des flux
- **Planifier** : un plan de remédiation doit être élaboré sur la base des résultats de l'évaluation. La planification comprend la sélection de la bonne technologie de segmentation et des bonnes politiques, ainsi que la prise en compte de l'authentification par rapport à la classification, et des intégrations
- **Simuler** : dans la phase de simulation, les politiques sont ouvertes par défaut et en mode de journalisation, et d'autres fonctionnalités seront testées
- **Appliquer** : l'étape d'application consiste à mettre en œuvre des politiques restrictives, à enregistrer, à surveiller et à prendre des mesures de quarantaine

## Coût total de propriété

Le coût total de possession (TCO) couvre toutes les dépenses associées à la possession et à l'exploitation d'un produit ou d'un service tout au long de sa durée de vie. Il s'agit notamment du prix d'achat, de la maintenance, de l'assistance et des mises à niveau. Il est important de choisir des solutions rentables qui offrent une valeur à long terme, ce qui permet d'atténuer les dépassements de budget et de fournir un retour sur investissement (RSI) plus précis.

Il convient de faire la distinction entre l'investissement initial et les dépenses courantes nécessaires pour maintenir le système sous licence et opérationnel. Si certains composants, tels que les pare-feu, sont purement axés sur la sécurité, d'autres sont également essentiels à l'élaboration d'une stratégie de sécurité plus approfondie. Il s'agit notamment de la gestion des politiques, de la technologie de séparation efficace des réseaux (macro- et micro-segmentation avancée et automatisée), de l'attribution automatique de réseaux virtuels (VLAN), du protocole de chiffrement du réseau, de la visibilité des applications ainsi que de la validation et de l'attestation indépendantes du code du système d'exploitation.

La stratégie de cybersécurité du réseau d'ALE aborde gratuitement les éléments essentiels de la sécurité du réseau mentionnés ci-dessus, alors que les solutions proposées par d'autres fournisseurs exigent une expertise spécifique et de nombreux éléments et licences coûteux pour l'exploitation et la maintenance. L'approche d'ALE offre aux clients des avantages économiques substantiels tout en garantissant une cybersécurité des réseaux solide et efficace.



# Conclusion

Il est évident que la mise en œuvre d'un réseau Zero Trust pour une sécurité solide peut présenter plusieurs défis, tels que la complexité et le coût en termes de création et de maintenance. Cependant, ALE offre une approche unique et rentable pour résoudre ces problèmes. Les technologies avancées de macro- et micro-segmentation, en plus des autres composants présentés dans ce document, fournissent un moyen simple et abordable de mettre en œuvre un réseau Zero Trust capable de répondre aux exigences modernes en matière de cybersécurité. Nous nous engageons à aider nos clients à répondre à leurs préoccupations en matière de cybersécurité, et nous pensons que notre approche peut contribuer à atteindre cet objectif.

Les solutions d'ALE comprennent nos solutions résilientes et sécurisées intelligent Fabric (iFab) et uNP, ainsi qu'un contrôle d'accès réseau (NAC) robuste avec l'UPAM, qui fournit un contrôle d'accès basé sur le profil. Notre solution innovante OmniVista Network Advisor garantit un fonctionnement fluide, une récupération rapide et la prévention des attaques. En outre, nous nous associons à des fournisseurs de SASE tels que Versa Networks, et nous intégrons des fournisseurs de pare-feu tels que Palo Alto Networks afin d'offrir à nos clients des solutions de sécurité plus complètes et intégrées.



Alcatel·Lucent Enterprise