Protégez vos données d'entreprise avec Alcatel-Lucent Enterprise

Anticipez les cybermenaces et gardez le contrôle face à des réglementations en constante évolution

Brochure

Alcatel·Lucent
Enterprise

Introduction

Alors que les entreprises sont confrontées à des changements majeurs, la sécurité est l'un des domaines les plus bouleversés. L'essor de l'IA a bousculé les modèles de sécurité traditionnels, obligeant les entreprises à repenser les pratiques mises en place de longue date.

Pour relever ce défi, notre équipe d'experts en cybersécurité des réseaux, des communications et des solutions cloud s'est mobilisée pour partager des informations essentielles sur les nouveaux risques auxquels les entreprises sont exposées et sur les moyens à leur portée pour mieux se protéger et garder une longueur d'avance.

L'évolution de la cybersécurité

La cybersécurité est confrontée à l'évolution rapide des technologies, à des menaces plus sophistiquées et à l'évolution de la réglementation. Les experts du secteur observent trois grandes tendances qui façonnent actuellement la cybersécurité dans le monde de l'entreprise :

1. Le rôle à double tranchant de l'intelligence artificielle
2. Le nombre croissant de ransomwares et d'attaques au niveau de la chaîne logistique
3. Le besoin d'une gestion solide des identités dans les architectures Zero Trust

Le rôle à double tranchant de l'IA dans le domaine de la cybersécurité

L'IA, une arme pour les attaquants

L'utilisation de l'intelligence artificielle à des fins malveillantes est devenue l'une des menaces les plus importantes pour la sécurité des entreprises. Les cybercriminels s'appuient sur l'IA pour automatiser la reconnaissance, concevoir des campagnes de phishing hyperpersonnalisées et développer des logiciels malveillants adaptatifs capables d'échapper aux systèmes de détection traditionnels.

Des outils pilotés par l'IA analysent des données publiques pour établir le profil des cibles, générer des fichiers audio et vidéo « deepfakes » convaincants et exploiter les vulnérabilités avec une précision chirurgicale. C'est le cas notamment des e-mails de phishing générés par l'IA qui imitent les styles de communication légitimes, avec un taux de réussite de 40 % supérieur aux méthodes traditionnelles. Ce phénomène est amplifié par la normalisation de l'IA, ce qui favorise l'arrivée d'attaquants moins qualifiés.

Le « deepfake » est une technique particulièrement insidieuse basée sur l'IA. Les auteurs de la menace se font passer pour des cadres ou des collègues de confiance lors d'appels vidéo en temps réel afin de les amener à autoriser des transactions frauduleuses ou à communiquer des informations sensibles. Dans un cas documenté, une vidéo « deepfake » d'un directeur financier donnant des instructions pour un virement bancaire a entraîné une perte de 25 millions de dollars pour une société multinationale. Ces incidents soulignent la nécessité de mettre en place des protocoles d'authentification perfectionnés et de former les employés à la reconnaissance des ressources artificielles.

L'IA comme moyen de défense

Paradoxalement, l'IA est aussi le pilier des stratégies de défense modernes en matière de cybersécurité. Les algorithmes d'apprentissage automatique analysent d'importants ensembles de données dans le but de détecter les anomalies, d'anticiper les vecteurs d'attaque et d'automatiser les réactions en cas d'incident. À titre d'exemple, les systèmes de sécurité optimisés grâce à l'IA sont capables d'identifier des vulnérabilités de type « Zero Day » en reconnaissant des modèles subtils de comportement au niveau du trafic réseau, réduisant ainsi les temps de détection moyens de plusieurs semaines à quelques heures. Selon Gartner, les entreprises qui investissent dans des plateformes de renseignement sur les menaces pilotées par l'IA enregistrent 30 % de violations en moins par rapport à celles qui s'appuient sur des systèmes existants[1]. Les systèmes basés sur l'IA sont particulièrement efficaces pour identifier les menaces d'initiés en surveillant le comportement des utilisateurs et en signalant les situations d'accès inhabituelles, ce qui a une importance croissante dans les environnements de travail distants et hybrides actuels.

Défis réglementaires et éthiques

La nature bivalente de l'IA a exigé des réponses réglementaires strictes. La loi européenne sur l'intelligence artificielle, promulguée en février 2025, interdit les systèmes d'IA à haut risque dans des domaines tels que la surveillance biométrique et impose la transparence dans la prise de décision algorithmique. Les entreprises doivent désormais procéder à des audits indépendants des systèmes d'IA, consigner l'origine des données et garantir une utilisation éthique, des opérations complexes compte tenu de l'opacité de nombreux modèles d'apprentissage automatique. Des comités d'éthique transversaux dédiés à l'IA sont mis en place pour maîtriser ces questions. Par ailleurs, les sociétés s'associent aux autorités de réglementation pour définir les futurs cadres.

Remontée des ransomwares et des attaques au niveau de la chaîne logistique.

Les fournisseurs essentiels ciblés

Les attaques par ransomware sont passées de campagnes opportunistes à des opérations stratégiques ciblant des fournisseurs et des prestataires de services essentiels. Les attaques de 2024 contre CDK Global et Change Healthcare ont montré comment une seule victime peut paralyser des secteurs entiers, causant des perturbations opérationnelles et demandant des efforts de rétablissement dont le coût est estimé à des milliards de dollars. En 2025, les attaquants ciblent de plus en plus les fournisseurs de logiciels en tant que service (SaaS) et les entreprises d'infrastructures cloud, en exploitant leur rôle centralisé dans les écosystèmes professionnels. Par exemple, une attaque de ransomware contre un grand fournisseur de services de stockage dans le cloud pourrait priver simultanément des milliers d'entreprises de leurs données, amplifiant ainsi l'effet de l'extorsion.

L'abondance de systèmes interconnectés et une maîtrise insuffisante des risques au niveau de la chaîne logistique facilitent ces attaques. De nombreuses entreprises manquent de visibilité sur les mesures de sécurité de leurs fournisseurs, ce qui les rend vulnérables aux défaillances en cascade. Gartner estime que 60 % des sociétés seront confrontées à une violation importante de la chaîne logistique d'ici 2026, sous l'effet de vulnérabilités tierces au niveau des outils DevOps et des appareils IoT[4].

Écosystèmes de ransomwares en tant que service (RaaS)

L'essor des plateformes de ransomware en tant que service a démocratisé l'accès aux outils d'attaque avancés, permettant ainsi à des criminels peu qualifiés de lancer des campagnes sophistiquées. Les opérateurs RaaS fournissent des logiciels malveillants personnalisables, des portails de paiement et une aide à la négociation en échange d'une partie des rançons, généralement de l'ordre de 20 à 30 %. Ce modèle a entraîné une augmentation de 150 % des incidents de ransomware depuis 2023, avec des demandes de rançon moyennes dépassant les 5 millions de dollars par incident.

Les ransomwares modernes utilisent des techniques d'obscurcissement basées sur l'intelligence artificielle, telles que le code polymorphe et le chiffrement à retardement, afin d'échapper à la détection. Les attaquants exfiltrent également des données avant de déployer le chiffrement, en menaçant de divulguer des informations sensibles s'ils ne sont pas payés, une tactique connue sous le nom de double extorsion. Les entreprises écartent ces menaces en ayant recours à des sauvegardes de type « air-gap », à des solutions de stockage décentralisées et à des systèmes de vérification de l'intégrité basés sur la blockchain.

Elles auront besoin d'une technologie sécurisée à tous les niveaux pour prévenir, contenir et limiter l'impact des ransomwares et des attaques au niveau de la chaîne logistique.

1. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

La gestion des identités et l'impératif Zero Trust

La crise d'identité des machines

Alors que les entreprises adoptent l'IA générative, l'IoT et les architectures cloud natives, les identités des machines (identifiants pour les appareils, les API et les charges de travail automatisées) ont dépassé les identités humaines en termes de volume et de risque. En 2025 Gartner a identifié les identités non gérées des machines comme l'un des principaux vecteurs d'attaque, les clés API et les comptes de service compromis étant à l'origine de 45 % des intrusions sur le cloud[1]. Pour remédier à la situation, les entreprises déploient de plus en plus d'outils de gestion des certificats qui automatisent une rotation plus fréquente des identifiants et renforcent leurs politiques de moindre privilège afin de détecter en temps réel les comportements anormaux des machines.

Architecture Zero Trust dans la pratique

Les cadres Zero Trust, qui partent du principe qu'aucune entité humaine ou machine n'est intrinsèquement digne de confiance, sont passés du statut d'objectif à celui de nécessité opérationnelle. Leur mise en œuvre se concentre sur l'authentification continue, la microsegmentation et le chiffrement des communications. À titre d'exemple, un réseau Zero Trust pourrait exiger une vérification biométrique pour l'accès aux données sensibles, isoler les environnements de développement des systèmes de production et chiffrer tout le trafic est-ouest au sein des centres de données.

Le NIST dans une évaluation de l'efficacité, institut américain des normes et de la technologie, indique que les entreprises qui adoptent le Zero Trust architecture [2] réduisent l'impact des violations de 70 % en moyenne. Le succès dépend de l'intégration des principes du Zero Trust dans l'infrastructure existante, ce qui représente un défi pour les sociétés dotées de systèmes anciens. Les approches hybrides gagnent du terrain, telles que les périmètres définis par logiciel pour les actifs sur site et les solutions Zero Trust pour le cloud.

Facteurs humains et menaces internes

Selon un rapport du Forum économique mondial, 95 % des incidents de cybersécurité sont dus à des erreurs involontaires. Les attaques de phishing utilisant du contenu généré par l'IA contournent les filtres de messagerie 30 % plus efficacement que les méthodes traditionnelles. Par ailleurs, les employés exposant par inadvertance des informations d'identification dans des outils collaboratifs représentent 25 % des violations. Les menaces internes sont exacerbées par les erreurs de configuration de l'accès manuel au réseau et par le télétravail, les appareils personnels et les réseaux non sécurisés créant des points d'entrée pour les attaquants.

Il est devenu essentiel d'aider les utilisateurs à mieux se protéger tout en allégeant les responsabilités liées aux politiques de sécurité de plus en plus restrictives. Pour les administrateurs de réseaux et d'applications, l'automatisation des opérations et l'assistance active de l'IA doivent fournir les outils nécessaires pour se protéger des conséquences d'éventuelles erreurs de configuration.

L'approche d'ALE en matière de sécurisation des communications et des produits de réseau

L'approche d'Alcatel-Lucent Enterprise en matière de sécurité consiste à garantir que les interactions numériques sont efficaces et conformes aux réglementations. La technologie numérique est très répandue, avec l'adoption croissante de l'IA et des appareils IoT (Internet des Objets) qui collectent des données pour prendre en charge les alertes en temps réel et pour la planification future. Il est essentiel de sécuriser et de renforcer les réseaux et les communications qui alimentent les entreprises d'aujourd'hui afin de prévenir les risques d'interruption des services. Les solutions d'ALE pour les communications d'entreprise et l'infrastructure de réseau mettent en œuvre la cybersécurité de bout-en-bout, la seule façon d'assurer une sécurité complète. Cette approche de la cybersécurité aide les entreprises et les institutions publiques à :

- Prévenir les cyberattaques et mettre en œuvre la cybersécurité dans chaque aspect de la conception du produit afin de réduire la surface d'attaque
- Protéger contre les cyberattaques, en mettant en œuvre les normes de sécurité les plus récentes et les bonnes pratiques dans tous les composants de la solution afin d'accroître leur résistance
- Réagir aux cyberattaques, en prenant des mesures rapides et appropriées pour limiter l'impact et améliorer la résilience en cas d'attaque

En tant que constructeur de produits matériels et logiciels, ALE se concentre sur les domaines décrits ci-dessous en matière de cybersécurité afin de cibler les vulnérabilités potentielles dans le paysage des cybermenaces.

1. Sécurité dès la conception

Historiquement, la conception de la plupart des solutions était pilotée par la nécessité d'ajouter de nouvelles fonctionnalités. La sécurité était une considération essentielle, mais secondaire. Le contexte évoluant, les priorités traditionnelles en matière de conception se sont inversées. Les exigences en matière de cybersécurité doivent désormais guider la conception des solutions. Les solutions matérielles et logicielles sécurisées dès la conception prennent en compte la sécurité à chaque étape de la définition, du développement et de la livraison du produit. Tout le hardware et les systèmes d'exploitation sont durcis, la protection contre les dénis de service (DoS) est intégrée et les solutions mettent en œuvre les bonnes pratiques en matière de cybersécurité qui sont les plus importantes de l'industrie.

2. Sécurité de l'accès aux réseaux Zero Trust

Les stratégies de sécurité qui accordent la confiance en fonction de la localisation de l'utilisateur à l'intérieur du pare-feu de l'entreprise, des informations d'identification qu'il saisit ou de l'application ou de l'appareil qu'il utilise ne sont plus suffisantes, même lorsque plusieurs mécanismes de sécurité sont combinés. Aujourd'hui, aucun utilisateur, appareil ou application ne devrait bénéficier d'une confiance implicite. Le modèle de sécurité ZTNA (Zero Trust Network Access) contribue à lutter efficacement contre des menaces en constante évolution. Le modèle ZTNA ne fait confiance à aucun utilisateur, aucun appareil ni aucune application, quelle que soit sa localisation. ALE met en œuvre le modèle ZTNA en permettant l'application de politiques basées sur les rôles, le contrôle d'accès (avec gestionnaire Unified Policy Authentication Manager-UPAM) en fonction de l'emplacement et la segmentation dynamique entre les utilisateurs, les appareils et les applications (avec gestionnaire Unified Policy Authentication Manager-UPAM), qu'ils soient gérés ou non gérés.

3. Macro et microsegmentation

La macro et la microsegmentation permettent une approche granulaire et hautement contrôlée de la cybersécurité pour tous les utilisateurs, appareils et applications qui accèdent au réseau. macrosegmentation sépare les utilisateurs, les appareils et les applications en fonction de leur domaine fonctionnel, de sorte qu'ils ne peuvent pas communiquer avec les éléments d'autres macro-segments. Par exemple, les applications de communications unifiées et de collaboration d'un macro-segment ne peuvent pas communiquer avec les technologies de sécurité, telles que les caméras de vidéosurveillance et les systèmes de verrouillage des portes d'un deuxième macro-segment, ni avec les capteurs et les commandes d'éclairage, de chauffage et de climatisation d'un troisième macro-segment.

La microsegmentation définit la manière dont les utilisateurs, les appareils et les applications au sein d'un macro-segment peuvent interagir les uns avec les autres ; elle est généralement régie par des politiques de sécurité très spécifiques. Par exemple, une caméra de surveillance ne devrait pas être autorisée à s'interfacer avec un verrou de porte, bien qu'ils fassent partie du même macro-segment du point de vue de la sécurité.

4. Chiffrement de bout en bout

Dans les entreprises modernes, les employés, les clients, les partenaires et les fournisseurs peuvent être n'importe où dans le monde. Les solutions qu'ils utilisent pour communiquer et collaborer peuvent être installées dans le bâtiment où ils travaillent, à l'autre bout de la ville ou dans un centre de données à l'autre bout du monde. Dans tous les cas, les échanges d'informations doivent être sécurisés et confidentiels, que ce soit à travers des communications voix, vidéo et texte. Pour que seuls les participants à la conversation puissent accéder aux informations échangées, chaque conversation doit être entièrement chiffrée, de l'origine à la destination. Cela signifie que chaque élément matériel et logiciel impliqué dans les communications de bout en bout doit incorporer nativement des mécanismes de chiffrement approuvés par les agences de sécurité.

5. Certifications en matière de sécurité et de confidentialité, et conformité à la législation

Il y a quelques années à peine, les certifications et accréditations les plus strictes en matière de sécurité n'étaient exigées que pour les produits de sécurité, tels que les pare-feu, ou dans des secteurs particuliers, tels que la défense. Aujourd'hui, des normes de sécurité spécifiques doivent être appliquées à tous les produits technologiques, dans tous les secteurs d'activité. Il est extrêmement important de vérifier que les affirmations en matière de cybersécurité sont étayées par des certifications et des accréditations reconnues.

Voici quelques exemples de conformité à rechercher :

- Normes mondiales en matière de sécurité et de protection de la vie privée, telles que la norme ISO 27001
- Normes sectorielles de sécurité et de protection de la vie privée, telles que la loi HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis et la certification HDS (Hébergeurs de Données de Santé) en France
- Normes régionales de sécurité et de protection de la vie privée, telles que le Règlement général sur la protection des données (RGPD) et la directive NIS 2 dans l'Union européenne

6. Tests de sécurité continus et spécialisés

À l'instar des normes de sécurité, les processus de test de sécurité spécialisés, autrefois réservés aux produits de sécurité, sont désormais obligatoires pour les solutions de communications unifiées et de collaboration. Les tests de pénétration en sont un bon exemple. Ces tests simulent des cyberattaques afin de révéler les vulnérabilités en matière de sécurité et d'y remédier de manière proactive avant que les problèmes ne surviennent. Pour garder une longueur d'avance sur les cybermenaces dans un paysage en constante évolution, les tests de pénétration, qui sont uniquement motivés par des exigences de cybersécurité, doivent être effectués de façon continue. Les fournisseurs de technologie qui s'engagent à aider leurs clients à maintenir une cybersécurité maximale doivent fournir les ressources, les outils et l'expertise nécessaires pour effectuer ces tests de pénétration en continu.

7. Souveraineté des données

La souveraineté des données est devenue une préoccupation majeure pour la plupart des entreprises qui doivent protéger leur propriété intellectuelle, préserver la confiance de leur clientèle et conserver leur avantage concurrentiel. Avec l'adoption de nouvelles technologies, telles que le cloud et, plus récemment, l'IA, l'ouverture des systèmes de communication des entreprises au monde extérieur n'a jamais été aussi importante. L'accès sécurisé au réseau est un sujet tout aussi essentiel. Certaines sociétés opteront pour une solution de cloud public répondant à leurs besoins tout en limitant la surface d'attaque interne de leur système d'information. D'autres choisiront une approche plus traditionnelle, avec des applications de communications unifiées hébergées sur leur réseau privé, soit sur site, soit sur un cloud privé dédié. Quel que soit le choix du client, ALE propose des produits et des services adaptés à tous les contextes de déploiement afin de garantir la souveraineté sur les données critiques.

Brochure
Protégez vos données d'entreprise avec Alcatel-Lucent Enterprise

8. Automatisation intelligente des opérations et de la sécurité

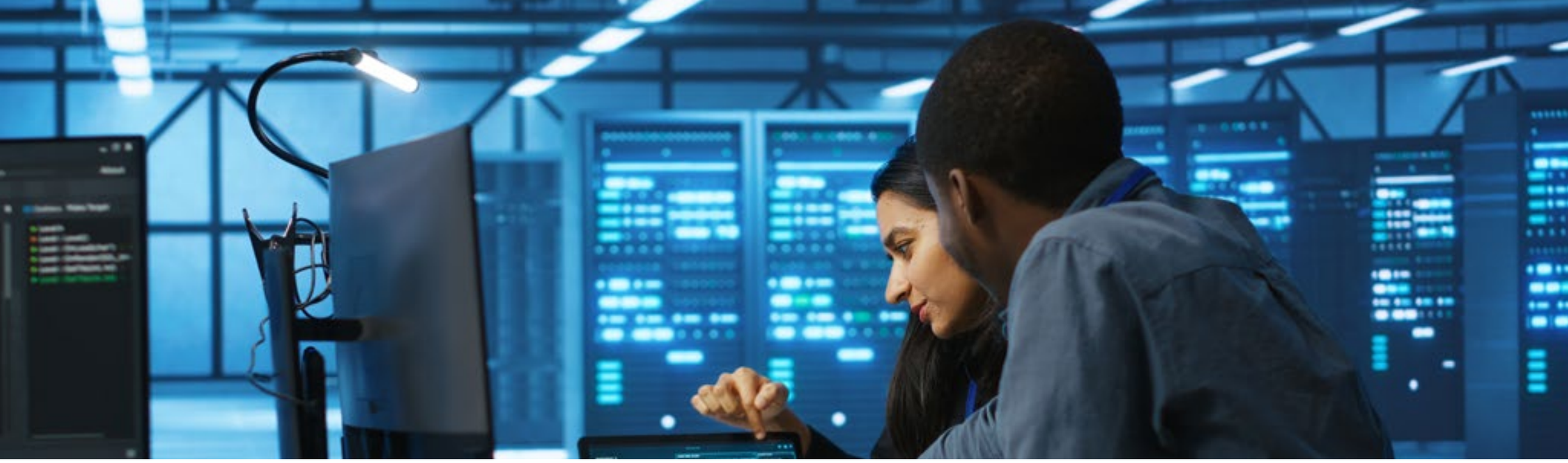
La suite OmniVista et l'application Network Advisor d'ALE offrent une sécurité opérationnelle avancée grâce à une surveillance en temps réel, à des audits de configuration et à l'automatisation de la réaction face aux menaces. Grâce aux outils AIOps intégrés, les anomalies du réseau sont détectées de façon proactive et des mesures correctives guidées sont fournies, corrigeant généralement d'un simple clic les problèmes de qualité de l'expérience ou de conformité. Ces solutions minimisent ainsi les erreurs humaines, accélèrent la réaction en cas d'incident et garantissent la conformité des politiques dans des environnements complexes.

9. Connectivité sécurisée en tout lieu

ALE prend en charge le SD-WAN sécurisé pour les entreprises distribuées et le télétravail en combinant la visibilité du réseau, la sécurité et l'optimisation des performances, et en s'alignant sur les modèles modernes de travail en tout lieu. Grâce au chiffrement MACsec, l'intégrité et la confidentialité des données sont préservées dans les environnements WAN multisites.

10. Confiance dans la chaîne logistique du logiciel

ALE applique des mesures rigoureuses pour sécuriser sa chaîne logistique du logiciel, notamment des images signées de microprogrammes, des processus de démarrage sécurisés, des systèmes d'exploitation renforcés et une validation indépendante du code source. Ces pratiques limitent l'exposition aux menaces logicielles et garantissent des environnements de déploiement fiables.



Pourquoi faire confiance à ALE pour sécuriser votre infrastructure réseau et votre plateforme de communication d'entreprise ?

Si de nombreux fournisseurs de technologie mettent l'accent sur la cybersécurité, tous ne disposent pas de l'expertise nécessaire pour mettre en œuvre une sécurité de bout en bout. Alcatel-Lucent Enterprise va plus loin que les autres fournisseurs en mettant en œuvre toutes les bonnes pratiques requises pour une cybersécurité de bout en bout.

Nous nous engageons à :

- suivre les standards de sécurité lors de l'évaluation des risques liés aux nouvelles fonctionnalités et lors de la mise en œuvre de fonctions de cybersécurité, telles que le chiffrement natif, dans nos produits
- appliquer les normes ISO 27001 à toutes nos solutions
- prendre en charge le modèle ZTNA, correspondant à la segmentation granulaire du réseau et à des politiques de sécurité concrètes afin de réduire le risque d'activités non autorisées
- procéder à des tests hautement spécialisés et spécifiques en matière de sécurité, tels que des tests de pénétration, sur nos produits
- veiller à ce que nos produits obtiennent les principales certifications industrielles, telles que HDS, HIPAA et FERPA (Family Educational Rights and Privacy Act) et FIPS 140-2 pour le gouvernement et la défense
- prendre en compte les certifications régionales pour nos produits, telles que CSPN de l'ANSSI en France, ENS en Espagne, C5 en Allemagne et ANATEL au Brésil.
- respecter les réglementations régionales en matière de sécurité et de protection de la vie privée, telles que le RGPD, CRA et la directive NIS 2 dans l'Union européenne.

Nous contribuons aux propositions de directives de l'Union européenne sur la cybersécurité. Nous mettons également à profit notre expertise pour aider nos clients à choisir et à mettre - avec un coût total de possession le plus bas (30 à 50 % de réduction) - en œuvre la combinaison de solutions de communication et de réseau sécurisées la plus adaptée à leurs besoins, et à former leurs employés aux bonnes pratiques en matière de cybersécurité. Notre approche globale de l’architecture Zero-Trust permet à nos clients de démontrer à leurs assureurs qu’ils adoptent une approche proactive et bénéficient généralement d’une réduction pouvant atteindre 20 à 30 % sur leur assurance cybersécurité.

Conclusion : anticiper les tendances et renforcer la cybersécurité

En 2026, les tendances en matière de cybersécurité exigent un changement de paradigme en ce qui concerne la stratégie des entreprises. Les sociétés doivent concilier le double rôle de l'IA, perçue à la fois comme une menace et un moyen de défense, investir dans des chaînes logistiques résilientes pour résister aux attaques de ransomware et revoir l'architecture des systèmes de gestion des identités dans un environnement Zero Trust. La conformité réglementaire, l'utilisation éthique de l'IA et la collaboration intersectorielle seront essentielles pour atténuer les risques. Alors que les surfaces d'attaque s'étendent à l'ère de l'edge computing et de l'adoption de l'IoT, les entreprises qui donnent la priorité à la défense adaptative, à la formation des employés et à la traque proactive des menaces seront les mieux placées pour prospérer dans ce paysage volatile.

La marche à suivre passe par l'innovation technologique et implique le soutien et l'expertise d'un constructeur de confiance comme ALE.

En savoir plus

Pour en savoir plus, veuillez consulter le site ALE Solutions de Sécurité. Si vous souhaitez échanger avec l'un de nos experts en sécurité, nous vous invitons à nous contacter.

Alcatel·Lucent Enterprise