Ayez confiance en votre sécurité. Ayez confiance en votre personnel. Avec Lenovo.

Comment assurer la sécurité de votre personnel dans un environnement de cybersécurité en constante évolution

Smarter technology for all

Lenovo

L’évolution irréversible vers le travail hybride a créé un environnement de cybersécurité difficile.

Aujourd’hui, la plupart des membres du personnel doivent être équipés pour le travail hybride. Par conséquent, la protection contre les menaces doit être étendue à plusieurs Clouds et différentes plateformes.

Cela crée un environnement numérique complexe qui peut être un refuge caché pour des menaces inconnues. L’application de stratégies de sécurité sur les appareils et les différentes couches numériques est une tâche véritablement colossale. Ce sont des nuits blanches pour ceux qui ont la responsabilité de la protection.

Matériel sécurisé et Cloud dans l’équation – un partenariat unique : Lenovo a un partenariat unique avec Microsoft, dans lequel le matériel équipé de la solution ThinkShield est combiné aux services de sécurité du Cloud Microsoft.

Sécurité dès la conception avec Lenovo ThinkShield

Chez Lenovo, nous comprenons le besoin urgent d'une protection complète. Reflétant les meilleures pratiques de protection, nous conduisons notre approche de sécurité ThinkShield avec pour objectif d'accroître la sécurité de notre portefeuille d'appareils dès la conception.

Cela va de la sécurisation des chaînes d'approvisionnement au développement de nouveaux produits Lenovo sécurisés et conçus par les fabricants de PC professionnels les plus fiables au monde.

Notre portefeuille unique de matériel, de services, de logiciels et de processus ThinkShield offre la protection nécessaire et s'étend à tous les niveaux de l'entreprise. Nos partenariats avec les principaux fournisseurs de solutions de sécurité du secteur permettent des défenses radicales qui encapsulent, contiennent et pilotent une stratégie Zero Trust, optimisées par les solutions de sécurité Microsoft.

Zero Trust. L'avenir de la cyberprotection. Le concept d'une nouvelle direction.

Le concept Zero Trust est une rupture majeure entre la sécurité réseau traditionnelle dans laquelle il existe un « périmètre dans l'entreprise » et des appareils connectés via un VPN, ce qui est généralement la norme aujourd'hui.

Les principes directeurs du Zero Trust sont : « Ne jamais faire confiance. Toujours vérifier. »

Dans le monde du travail hybride d'aujourd'hui, il ne faut pas faire confiance aux appareils par principe, même s'ils sont connectés à un réseau « autorisé ».

Le concept Zero Trust suppose qu'un pirate se trouve à l'intérieur du réseau. La confiance est établie en fonction du **contexte**, tel que **l'identité et l'emplacement de l'utilisateur, l'état de sécurité de l'appareil** et **l'application ou le service demandé(e)**. Des contrôles de stratégie ont lieu à chaque étape.

Cela garantit que seules **les bonnes personnes disposant des bonnes ressources sur des appareils sécurisés peuvent accéder à vos données.**

Le besoin du concept Zero Trust n'a jamais été aussi urgent :

81 %
des entreprises ont amorcé leur transition vers le travail hybride[1]

50 %
de diminution du risque de violation de données[3]

1 070 %
d'augmentation des rançongiciels entre juillet 2020 et juin 2021[4]

55 %
des entreprises déclarent avoir détecté une attaque par hameçonnage au cours des 18 derniers mois[2]

50 %
de diminution des appels passés aux services et supports informatiques[3]

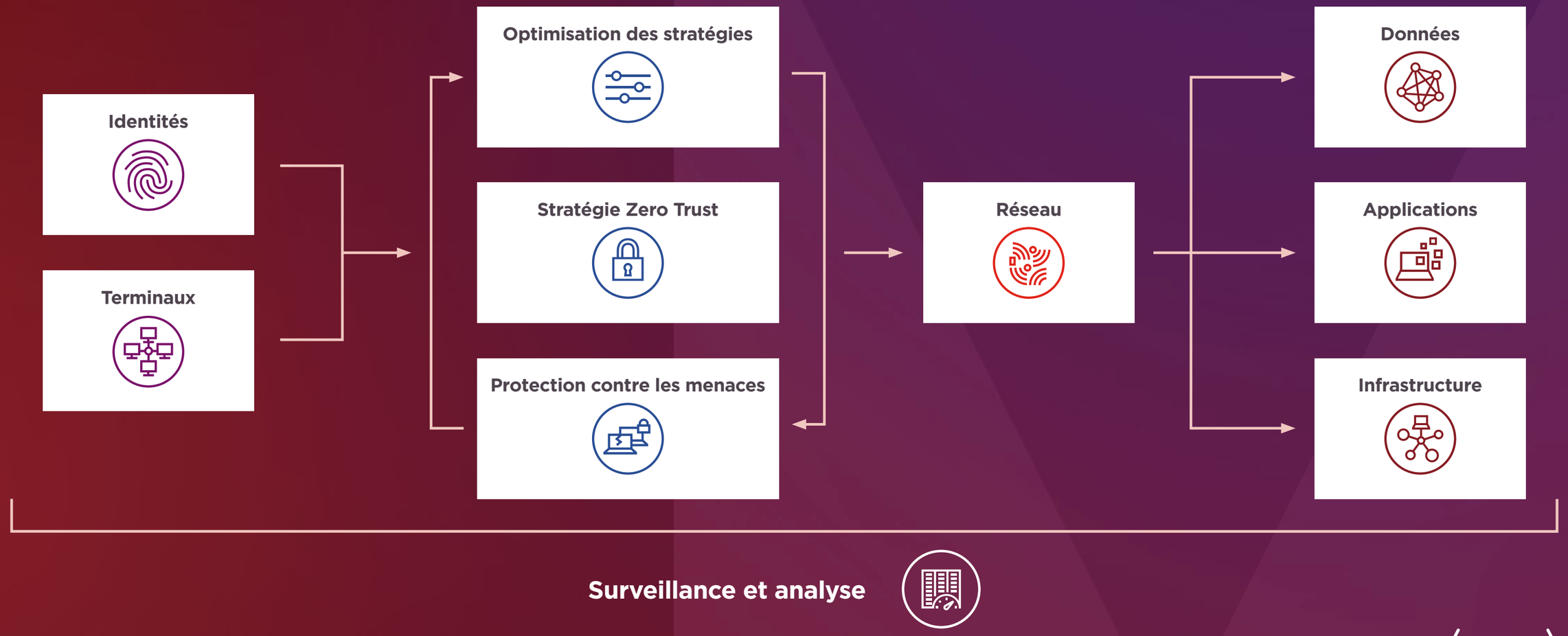
50 %
de réduction du temps consacré à la gestion grâce à l'amélioration des processus de sécurité[3]

Le portefeuille Lenovo ThinkShield et les solutions de sécurité Microsoft sont spécifiquement et résolument conçus pour vous aider à mettre en œuvre une **stratégie Zero Trust de bout** en bout et à protéger votre entreprise à tous les niveaux.

[1] Microsoft Zero Trust Adoption Report, 2021
[2] IBM Cost of a Data Breach Report 2021
[3] The Total Economic Impact™ of Zero Trust solutions from Microsoft, décembre 2021. Étude réalisée par Forrester Consulting pour Microsoft.
[4] 1H Global Threat Landscape Report from FortiGuard Labs

Voici à quoi ressemble l'architecture Zero Trust.

Le concept Zero Trust s'étend à de nombreux domaines de l'informatique, mais la protection commence par les appareils modernes dotés de Windows 11, les identités des utilisateurs et la surveillance des terminaux.



Améliorez et sécurisez l'expérience de travail hybride de vos collaborateurs avec les appareils Lenovo dotés de Windows 11 Professionnel

Windows 11 Professionnel, le système Windows le plus sécurisé à ce jour, vous aide à **rationaliser la gestion** de votre espace de travail hybride tout en **protégeant les données et en y accédant** où que vous soyez.

Conçu pour les appareils modernes optimisés pour la sécurité, il vous offre les derniers avantages de la **protection matérielle**, étroitement intégrée au logiciel. Windows 11 Professionnel est spécialement conçu pour un **travail hybride sécurisé** avec une **base de sécurité plus élevée que Windows 10**. Cela inclut de nouvelles exigences de protection, intégrées et activées par défaut.

ThinkPad X1 Carbon

Améliorez la sécurité de votre appareil Lenovo ThinkShield doté de Windows 11 Professionnel avec la gestion du Cloud

La protection des identités et des terminaux est la première étape essentielle dans la mise en place d'une stratégie Zero Trust. Les identités et les appareils sont les deux principaux domaines ciblés par les voleurs d'identifiants, les e-mails d'hameçonnage, les rançongiciels, ainsi que d'autres types de logiciels malveillants et de menaces avancées.

Associez des appareils Lenovo dotés de Windows 11 avec des solutions de sécurité du Cloud Microsoft afin de déployer une stratégie Zero Trust.

Gestion des identités

- Active l'authentification multifacteur (MFA) qui peut arrêter 99,9 % des attaques via les identités.
- Fournit un moteur « intelligent » d'application de stratégie d'accès conditionnel qui vous permet de définir des règles spécifiques pour la « connexion » des utilisateurs. Lorsqu'il est associé à la MFA, il offre un solide équilibre entre la sécurité et la productivité de l'utilisateur.

Gestion des terminaux

- Assurez-vous que les applications sont conformes aux protocoles de sécurité de votre entreprise à l'aide de Mobile Access Management (MAM).
- Assurez-vous que les appareils sont conformes aux protocoles de sécurité de votre entreprise à l'aide de Mobile Device Management (MDM) sur les appareils de l'entreprise ou appartenant aux collaborateurs (BYOD).

Contrôler, protéger et gérer en tirant parti des avantages des solutions de sécurité du Cloud

Gestion des identités avec Azure Active Directory

- Azure Active Directory est un service simple et efficace, basé sur le Cloud, de gestion des identités et des accès qui fournit une authentification multifacteur et un accès conditionnel.
- Combine services de répertoires de base, gestion de l'accès aux applications et protection des identités en une seule solution.
- Aide vos collaborateurs à accéder en toute sécurité à des ressources externes, telles que Microsoft 365, le portail Azure et des milliers d'autres applications SaaS.
- Sécurise les ressources internes telles qu'un intranet et des applications Cloud développées par votre organisation.

Microsoft Defender pour terminaux

Cette solution de sécurité pour terminaux basée sur le Cloud à la pointe du secteur :

- Aide à se protéger contre les rançongiciels, les logiciels malveillants sans fichier et d'autres attaques sophistiquées sur Windows, Mac OS, Linux, Android et iOS.
- Découvre les menaces cachées en surveillant, en permanence et en temps réel, le comportement du code et les techniques des pirates, permettant une détection et une réponse rapides.
- Réponse et correction automatisées des incidents 24 h/24 et 7 j/7. Aide les équipes de sécurité à passer immédiatement des alertes à la correction pilotée par l'IA.
- Service de chasse aux menaces géré par des experts Microsoft « à la demande ».

Microsoft Endpoint Manager

Bénéficiez de la gestion et de la sécurité des terminaux au sein d'une plateforme de gestion unifiée :

- Sécurise, déploie et gère tous les utilisateurs, applications et terminaux sans perturber les processus de travail existants.
- Aide à passer à un espace de travail et une gestion modernes, permettant d'assurer la sécurité des données, dans le Cloud et sur site.
- Combine des services que vous connaissez et utilisez peut-être déjà, notamment Microsoft Intune, Configuration Manager, Desktop Analytics, la cogestion et Windows Autopilot.

Le bon appareil, au bon endroit, au bon moment avec la solution de déploiement Zero-Touch de Lenovo

Une technologie moderne et sécurisée est la clé du succès de toute entreprise. Mais l'approche manuelle traditionnelle du déploiement est complexe, chronophage et source d'erreurs.

Il existe désormais un moyen plus simple de s'assurer que vos collaborateurs hybrides et distants sont immédiatement opérationnels : **le déploiement Zero-Touch de Lenovo avec Autopilot**.

Il dynamise le travail hybride, augmente la productivité et libère vos équipes informatiques pour qu'elles se concentrent sur l'innovation afin de faire avancer l'entreprise.

Avec **Windows Autopilot**, les services informatiques n'ont plus besoin de réinstaller d'image ni de configurer manuellement de nouveaux appareils. Tout se fait à distance. Les appareils Lenovo dotés de Windows 11 sont livrés avec Autopilot préconfiguré. Les responsables informatiques peuvent personnaliser l'utilisateur et appliquer des configurations depuis n'importe où.

- **Prêt à l'emploi immédiatement** – L'utilisateur n'a qu'à allumer l'appareil et en quelques clics simples, il est prêt à travailler.
- **Gestion des profils simple** – Créez, gérez et attribuez jusqu'à 350 profils différents pour définir les paramètres d'un utilisateur et son expérience avec un PC.
- **Transition aisée vers le Cloud** – Ajoutez automatiquement des appareils à Azure Active Directory et intégrez-les à la gestion des appareils mobiles.
- **Provisionnement sans problème** – Configuration personnalisée et rationalisée.
- **Suivi de la progression** – À l'aide d'Autopilot, les utilisateurs peuvent suivre la progression de la configuration de l'appareil.
- **Enregistrement de produit** – Appareils automatiquement enregistrés auprès du service de déploiement Cloud Autopilot.

Adopter une démarche de « véritable symbiose »

Sécurité prête à l'emploi

- **Protection au cœur** du système avec la sécurité matérielle TPM 2.0, ainsi que les sauvegardes des données et identités.
- Connexion plus simple et plus sécurisée à l'aide de **méthodes d'authentification** sans mot de passe, telles que Windows Hello Entreprise.
- Aide à bloquer les logiciels malveillants avec **la protection intégrée déjà activée**.
- Pour vous aider à **bénéficier de la sécurité dès le début**, Windows 11 empêche le chargement des logiciels malveillants au démarrage.
- Protection des données et du réseau prise en charge par **une racine de confiance reposant sur le matériel**, qui aide à maintenir et à vérifier l'intégrité des appareils.

Protégez-vous contre les menaces en constante évolution

- Protégez les informations d'identification avec une **protection contre l'hameçonnage améliorée** dans Microsoft Defender SmartScreen.
- Bénéficiez d'une connexion sans les mains grâce à la **détection de présence** : connexion lorsque vous approchez, verrouillage lorsque vous partez.
- Protégez vos données les plus sensibles avec les PC **« Secured-core » (à noyau sécurisé) de Lenovo**.
- Bénéficiez d'une protection des informations d'identification basée sur le matériel avec **Microsoft Pluton**.
- Tirez parti de la **détection intelligente des menaces et de réponses rapides** informées par 43 000 milliards de signaux de sécurité analysés quotidiennement.
- Le chiffrement BitLocker permet de **protéger les informations de votre entreprise**, même sur les appareils perdus ou volés.
- Obtenez plus de **protection contre les sources non fiables** : ouvrez des fichiers et des sites Web dans un conteneur isolé avec Microsoft Defender Application Guard.

Gestion moderne de la sécurité

- **Maintenez les fonctionnalités de sécurité à jour** avec Windows Update pour Entreprise.
- Activez l'adoption de cadres de **sécurité Zero Trust**.
- **Assurez la conformité aux stratégies pour les collaborateurs sur site et à distance** avec Microsoft Endpoint Manager.
- Déployez des appareils **préconfigurés avec des stratégies de sécurité d'entreprise** à l'aide de Windows Autopilot et du déploiement Zero-Touch.
- Gagnez en sécurité et en visibilité en activant **l'authentification unique sécurisée** sur toutes vos applications avec Azure Active Directory.
- **La conception axée sur le Cloud permet une extensibilité facile** avec Microsoft 365, Microsoft Defender pour le Cloud et Microsoft Defender pour les terminaux.
- Aidez à **lutter contre les codes malveillants**, protégez-vous contre les logiciels malveillants et autres logiciels non fiables avec Windows Defender Application Control.

Lenovo – votre partenaire de confiance pour la mise en œuvre d'une stratégie Zero Trust et du travail hybride

Pourquoi choisir Lenovo ?

Expérience, expertise, capacité à l'échelle de l'entreprise et équipe d'experts dédiée pour soutenir l'adoption de Clouds, la définition de stratégies de sécurité et leur mise en œuvre. En tant que fournisseur de solutions Cloud Microsoft (CSP) autorisé, Lenovo propose le portefeuille complet de services Cloud de Microsoft, y compris les services Microsoft 365 et Azure.

Microsoft Partner

Microsoft

2022 Partner of the Year Winner
Device Award

Gold Partner et partenaire de l'année Microsoft dans le domaine des appareils

Répondant aux exigences strictes de Microsoft, Lenovo est reconnu comme Gold Partner, ce qui confirme que Lenovo possède l'expertise et les capacités nécessaires pour vous fournir des solutions haut de gamme et sécurisées pour le télétravail.

En outre, Lenovo a reçu le prestigieux prix de partenaire de l'année Microsoft dans le domaine des appareils. Il récompense l'excellence dans la conception, le marketing ou la vente d'appareils et de solutions informatiques qui soutiennent la technologie basée sur Microsoft.

Ce prix vient récompenser les performances de Lenovo en matière de fourniture de solutions et de services intégrés, de façon cohérente, flexible et prévisible, afin de répondre à la demande actuelle de transformation numérique de ses clients et de pérenniser l'activités de ses derniers.

Notre stratégie Cloud : tout auprès d'un seul fournisseur

L'objectif de Lenovo est devenir une véritable organisation hybride, capable de déployer un Cloud sur site, privé et public en répondant aux besoins des clients en matière de stockage, de logiciels et de solutions. C'est lié à notre capacité à proposer du matériel, des services, des logiciels, des appareils As-a-Service et une assistance, le tout en tant que fournisseur unique.

Voilà comment nous faisons en sorte que votre solution de stratégie Zero Trust fonctionne pour votre entreprise

Les services externalisés et gérés de Lenovo vous mettent sur la bonne voie pour une mise à niveau fluide et sans problème vers les défenses Zero Trust.

- De la conception de la solution à l'intégration, en passant par la migration finale, Lenovo répond à tous vos besoins.
- Si vous avez une licence Microsoft 365, nous actualisons simplement les appareils Windows 11 et Microsoft 365, et nous incluons Azure Active Directory, Microsoft Defender et Endpoint Manager.
- Premier Support – hotline dédiée aux utilisateurs, 24 h/24, 7 j/7 et 365 jours par an.
- Des experts dédiés – des experts locaux prêts à vous accompagner dans votre transition vers un travail hybride sécurisé.
- Sécurité de niveau professionnel – les meilleures défenses de cybersécurité pour repousser la vague croissante de logiciels malveillants et d'attaques ciblées.

Smarter technology for all

Lenovo

Contactez-nous dès aujourd'hui pour découvrir comment Lenovo peut vous aider à élaborer la stratégie de sécurité Zero Trust de votre organisation.

Prendre rendez-vous

Microsoft 365