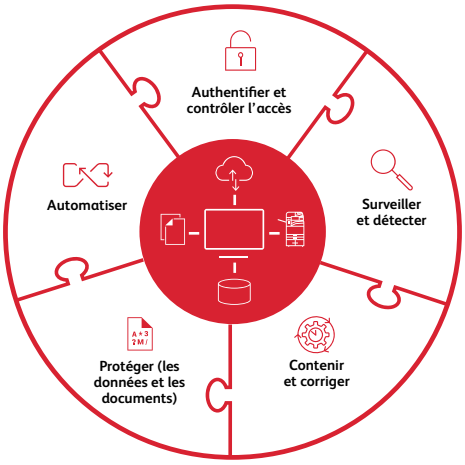
Zero Trust

La cybercriminalité a atteint un niveau record dans le monde et devrait continuer de croître. Les entreprises ont besoin de nouvelles stratégies et de bonnes pratiques pour se protéger contre ces menaces.

Le personnel décentralisé actuel doit pouvoir accéder à son infrastructure informatique à tout moment, où qu'il soit. Un nombre croissant d'initiatives de transformation numérique concourt à faciliter l'accès aux données d'entreprise. Une multitude d'appareils IoT sont désormais connectés à des systèmes métier essentiels, qui constituent l'épine dorsale de toute entreprise. Ces tendances exercent une pression de plus en plus forte sur les professionnels de la sécurité, qui doivent s'adapter à l'environnement de travail moderne tout en réduisant la surface d'attaque de la sécurité de l'entreprise.

Le Zero Trust s'est imposé comme une méthode puissante visant à fournir un accès sécurisé aux utilisateurs et aux appareils autorisés, tout en améliorant la sécurité de l'entreprise.

La sécurité complète étant une priorité pour Xerox, nous avons fourni à nos clients des produits et des services qui soutiennent les initiatives Zero Trust. Des concepts tels que ne jamais faire confiance, toujours vérifier, le moindre privilège, la détection et la résolution proactives des menaces, le chiffrement et les certifications de sécurité ne sont pas nouveaux. Cependant, lorsqu'ils sont utilisés dans le cadre d'une stratégie de sécurité cohérente, ils représentent des éléments essentiels d'un programme efficace de sécurité Zero Trust.



Mise en œuvre de Zero Trust

Nous soutenons vos initiatives Zero Trust avec les bonnes pratiques et recommandations suivantes :

AUTHENTIFICATION ET CONTRÔLE DE L'ACCÈS

Commencez par la politique « aucune confiance implicite » et assurez-vous que tous les accès utilisateur sont vérifiés.

Les imprimantes Xerox® sortent d'usine avec des mots de passe uniques et sécurisés pour le compte administrateur. Les contrôles d'accès basés sur les rôles peuvent être mis en œuvre avec des noms d'utilisateur locaux, un accès par code PIN, une authentification sécurisée par carte et une authentification sécurisée CAC/PIV. L'accès au moindre privilège et la revalidation continue peuvent être mis en œuvre au moyen de minuteries ou de déconnexions d'inactivité. L'authentification multifacteur est prise en charge via les fournisseurs d'identité cloud (IDPs) tels que Ping Identity, Okta, Microsoft Azure Identity Services, ainsi que via les solutions Xerox® Workplace Cloud/Xerox® Workplace Suite.

Les solutions de gestion des impressions Xerox® Workplace Cloud et Xerox® Workplace Suite étendent les fonctionnalités des imprimantes Xerox® à l'ensemble d'un parc afin de fournir une approche cohérente. Elles appliquent une posture de sécurité reposant sur la non-confiance absolue, en demandant aux utilisateurs de déverrouiller les imprimantes à l'aide de cartes/badges, d'appareils mobiles ou de codes PIN avant d'accéder aux services des imprimantes.

Les Managed Print Services (services de gestion déléguée des impressions) de Xerox® mettent en œuvre l'authentification obligatoire à chaque nouvelle connexion, au niveau de l'utilisateur et du système. Ils établissent un accès défini basé sur les rôles aux utilisateurs et assurent la gestion des mots de passe avec les méthodes approuvées NIST 800-171R2. La gestion des CA/Certificats garantit que les imprimantes autorisées communiquent en toute sécurité sur le réseau.

SURVEILLER ET DÉTECTER

Surveillez et détectez en permanence les menaces de sécurité (potentielles).

Les imprimantes Xerox® sont équipées d'un micrologiciel signé numériquement et chiffré. Grâce à la vérification du micrologiciel, elles sont conçues pour se protéger contre les tentatives de falsification du logiciel système. La Trellix*[1] Liste blanche/Autoriser surveille les logiciels malveillants en temps réel, rejetant les activités malveillantes et envoyant des notifications aux utilisateurs. Trusted Boot[4] assure l'intégrité du processus de démarrage du système.

La génération de données de journaux Syslog/d'audit et leur intégration avec des outils SIEM[2] tels que LogRhythm, Splunk et Trellix* Security Manager fournissent des informations utiles pour détecter et atténuer les menaces de sécurité. Avec l'aide de Cisco Identity Services Engine (ISE), nous pouvons détecter les imprimantes non autorisées et les empêcher de se connecter à votre réseau.

Xerox® Workplace Cloud et Xerox® Workplace Suite s'intègrent à votre système de gestion des identifiants pour garantir une opération d'accès et d'authentification transparente. Cela permet d'éviter les problèmes de synchronisation entre le mécanisme de contrôle d'accès et le fournisseur d'identifiant. Au niveau local/de l'appareil, nous utilisons des outils tels que reCAPTCHA pour surveiller et bloquer les tentatives d'entrée par force brute détectées.

Les Managed Print Services (services de gestion déléguée des impressions) de Xerox® fournissent une cadence de surveillance de la sécurité définie par le client. Nous mettons en place une gestion des appareils à l'échelle du parc avec le Service de vérification de la sécurité de l'imprimante de Xerox®. Il permet de gérer intuitivement la configuration de l'ensemble du parc en définissant à distance les politiques d'impression et de sécurité. Il sert également de base à la génération de rapports sur les données en temps réel, sous forme de tableaux de bord interactifs. Les correctifs de sécurité et les mises à jour des micrologiciels sont appliqués conformément à la politique de sécurité du client.

CONTENIR ET CORRIGER

En cas de compromission potentielle, contenez la menace et fournissez des mesures correctives rapides pour l'éliminer.

Xerox conçoit ses imprimantes selon une approche qui donne la priorité à la sécurité et qui empêche les menaces de les infecter. Des couches de fonctionnalités de sécurité permettent de contenir davantage d'éventuelles failles de sécurité. Par exemple, la fonction d'imprimante Configuration Watchdog (Surveillance des configurations)[3] permet aux administrateurs système de mettre en œuvre jusqu'à 75 paramètres de sécurité et de les corriger (réinitialiser) de manière proactive en cas de modification.

Au niveau du parc, les Services de vérification de la sécurité de l'imprimante de Xerox® maintiennent la conformité aux politiques et corrigent de manière proactive les appareils non conformes. Nous examinons régulièrement les politiques de configuration pour nous assurer qu'elles sont conformes aux exigences de sécurité. Nous conseillons le client et lui fournissons des recommandations permanentes en matière de sécurité.

PROTÉGER (LES DONNÉES ET LES DOCUMENTS)

Utilisez des techniques de chiffrement des données et des solutions logicielles pour protéger les données et les documents contre toute divulgation intentionnelle et non intentionnelle.

Les disques durs de nos imprimantes sont protégés par un chiffrement 256 bits. Les données stockées qui ne sont plus requises peuvent être supprimées à l'aide d'algorithmes approuvés par le National Institute of Standards and Technology (NIST) et par le ministère américain de la Défense. La sortie des impressions est protégée par l'utilisation d'un système de libération par code PIN ou carte. Et nous empêchons que les informations de numérisation ne parviennent à des destinataires non autorisés en utilisant des formats de fichiers signés numériquement, chiffrés et protégés par mot de passe.

Nos imprimantes[4] vous permettent de verrouiller les champs de courrier électronique « à/cc/bcc », limitant les destinations de numérisation aux domaines désignés uniquement, tels que les domaines internes. Grâce à la fonction de sécurité de l'imagerie, les imprimantes Xerox® AltaLink® utilisent la technologie IR (infrarouge) pour marquer et détecter les documents sensibles. Cela empêche leur duplication involontaire et crée des alertes et des journaux d'audit pour suivre les tentatives de duplication.

Les services réseau non utilisés peuvent être désactivés pour réduire la surface d'attaque du réseau. Le filtrage IP peut limiter l'accès au réseau aux seuls clients approuvés pour la numérisation, l'impression et la gestion des appareils. Les protocoles sécurisés tels qu'IPsec, HTTPS, LDAPS et SFTP protègent les données en transit. Le mode FIPS peut être activé pour garantir que seuls les protocoles les plus sûrs sont autorisés à interagir avec l'appareil.

La solution Xerox® Workplace Cloud chiffre le contenu en transit et au repos. Le contenu stocké dans le cloud de Xerox peut être chiffré à l'aide de la propre clé du client. En utilisant sa propre gestion du chiffrement, le client bénéficie de tous les avantages liés à la migration vers une gestion de l'impression dans le cloud, et garde le contrôle des personnes qui peuvent voir le contenu de ses données. La fonction de sécurité du contenu des solutions Xerox® Workplace Cloud et Workplace Suite permet de détecter des contenus sensibles prédéfinis et de générer des alertes et rapports basés sur l'utilisation de ces données.

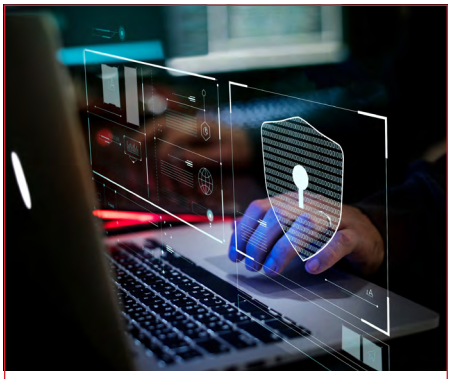
Les Services de vérification de la sécurité de l'impression de Xerox® permettent de s'assurer que les fonctions de protection des données et des documents sont activées au niveau du parc, de remédier aux violations des politiques et d'établir des rapports de conformité

AUTOMATISER

Rationalisez la politique de sécurité pour obtenir de meilleurs résultats.

L'automatisation mène à la simplicité et permet aux équipes de sécurité de se concentrer sur les questions importantes. La fonction Orchestrateur de parc des imprimantes Xerox® automatise la configuration des appareils et applique les mises à jour des micrologiciels à un réseau d'imprimantes. Cela permet de garantir la conformité tout en réduisant la charge de travail du personnel informatique. Grâce à l'intégration de Cisco ISE et de Trellix* ePolicy Orchestrator, toute imprimante peut être automatiquement mise en quarantaine dès qu'une menace est détectée. Cela évite les dommages à l'imprimante et protège le réseau et autres points terminaux.

Les Services de vérification de la sécurité de l'imprimante de Xerox® utilisent un mécanisme de politique centralisée et un regroupement de périphériques pour rationaliser la gestion du parc avec un minimum d'efforts. L'application et la validation de la conformité sont entièrement automatisées. Les tableaux de bord présentent les informations sur la conformité du parc, des politiques et des appareils dans un format graphique facile à lire.



La réussite d'un programme de sécurité repose sur une politique de sécurité simple et applicable, étayée par des fonctionnalités et services produits qui garantissent la conformité. Zero Trust est en train de devenir rapidement le modèle de sécurité préféré des entreprises de toutes tailles. En mettant en œuvre les recommandations de sécurité de Xerox évoquées dans ce rapport, les entreprises peuvent en toute sécurité accorder l'accès aux utilisateurs autorisés, limiter l'exposition en cas de violation des données et automatiser les réponses aux menaces de sécurité potentielles.

[1] Imprimantes multifonctions Xerox®AltaLink® série EC et Xerox® VersaLink® série 7100.
[2] Intégration directe de SIEM à AltaLink®, tous les autres appareils par le biais des services de gestion déléguée des impressions de Xerox®.
[3] Imprimantes multifonctions Xerox® AltaLink®8000 et 8100.
[4] Xerox® AltaLink®et Xerox® VersaLink.®
* Trellix anciennement connu sous le nom de McAfee.

Pour en savoir plus sur la sécurité Xerox, rendez-vous sur **www.xerox.fr/fr-fr/qui-sommes-nous/solutions-de-securite**.