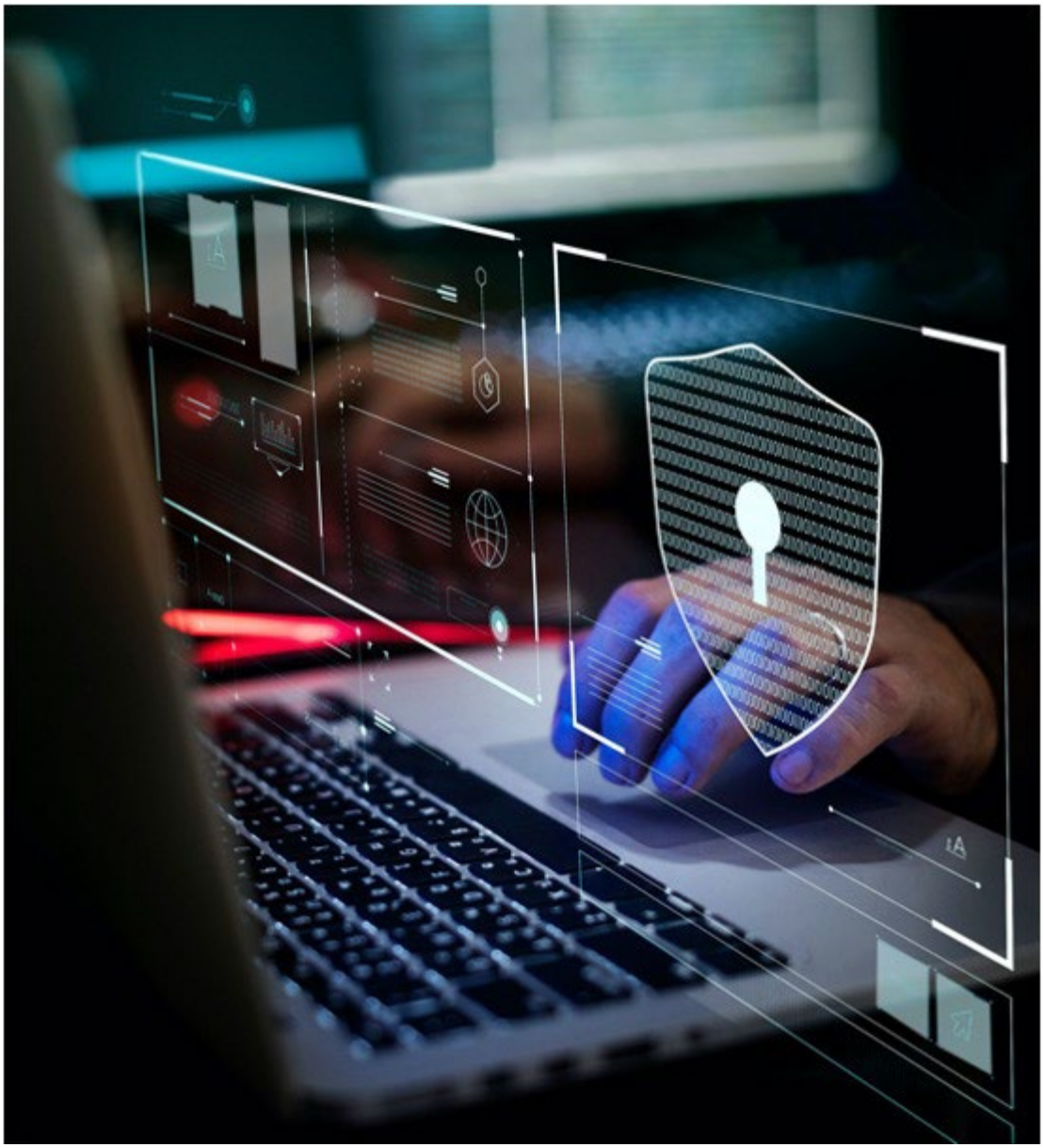


Sécurité Xerox de nouvelle génération : le partenariat avec Trellix[1]

Livre blanc

[1]Trellix : anciennement une société de McAfee

xerox™

Contexte

Les imprimantes multifonctions (MFP) actuelles sont des systèmes intégrés complexes. Elles combinent une multitude de composants, tels que systèmes d'exploitation complets, serveurs Web intégrés, supportent différentes piles de protocoles, offrent des interfaces matérielles et logicielles externes et des interfaces de programmation d'applications (API) pour interagir avec les systèmes d'entreprise. Du fait même de leurs vastes capacités et de leur puissance, ces imprimantes multifonctions constituent un risque grave pour votre réseau et vos systèmes d'entreprise, si elles ne sont pas correctement protégées.

Les fabricants investissent constamment des efforts considérables pour renforcer les contrôles de sécurité et améliorer la protection, notamment :

- Chiffrement du disque dur avec écrasement des données pour protéger la confidentialité de l'utilisateur final
- Activation de protocoles chiffrés tels que Transport Layer Security (TLS), Internet Protocol Security (IPsec) et Simple Network Management Protocol Version 3 (SNMPv3) pour protéger toutes les données transmises dans les deux sens par le périphérique
- Authentification utilisateur pour la plupart des tâches
- Contrôle d'accès avec des pare-feu et des groupes Active Directory (AD) définis par des rôles
- Journaux d'audit pour la traçabilité
- Programmes d'évaluation de sécurité tels que la certification Critères communs

Les imprimantes multifonctions sont-elles des systèmes intégrés ou ouverts ? Ces systèmes ont-ils besoin d'une couche de sécurité supplémentaire ? Dans ce cas, quelle est la solution appropriée pour protéger les serveurs, les postes de travail et les réseaux contre les menaces actuelles et futures ? Cette question cruciale concentre les efforts continus des spécialistes de la sécurité informatique.

Nous savons que les technologies de sécurité traditionnelles, telles que les anti-virus, ont une efficacité limitée par rapport aux menaces persistantes avancées (APT) et aux botnets.

En réalité, malgré la protection supplémentaire ajoutée par les fournisseurs de multifonctions, des incidents de sécurité continuent de se produire. Ces incidents de sécurité ont tous un point commun : ils ne peuvent être découverts qu'a posteriori. Le fournisseur et le client ne peuvent alors que se précipiter pour réduire les dommages, trouver une solution et la déployer. Comme si on était obligé d'attendre que le coffre-fort soit percé et l'argent envolé pour évaluer les dégâts et renforcer la porte de la banque.

[1]Trellix : anciennement une société de McAfee

DISPOSITIFS INTÉGRÉS

Un système intégré est un système informatique conçu pour fournir des fonctions fixes. Les systèmes intégrés sont présents dans tous les aspects de la vie moderne : distributeurs automatiques, appareils médicaux, imprimantes, périphériques de point de vente, kiosques, etc.

Toutefois, les multifonctions modernes assurent bien plus qu'une fonction seule fixe. Ce sont de véritables solutions hybrides entre fonction fixe et serveur réseau informatique. Ces deux rôles utilisent leur propre disque dur, système d'exploitation, serveur Web, interfaces et connexions d'entrée et de sortie, et traitent plusieurs types d'informations. Ces systèmes ont-ils besoin d'une couche de sécurité supplémentaire ? Quelles sont les meilleures solutions pour protéger les serveurs, les ordinateurs de bureau et les réseaux contre les menaces actuelles et futures ? Cette question cruciale concentre les efforts continus des spécialistes de la sécurité informatique.

Nous savons que les technologies de sécurité traditionnelles, telles que les logiciels antivirus, ne peuvent pas lutter contre toute une catégorie d'attaques, telles que les menaces avancées persistantes (APT) et les botnets. Les experts reconnaissent que la technologie des listes blanches/ listes d'autorisations peut être la bonne réponse pour lutter contre ces menaces.

Commençons par les listes blanches/ listes d'autorisations et listes noires/ listes de blocages.

LISTES NOIRES/ LISTES DE BLOCAGES

Pour lutter contre les accès non autorisés, l'utilisation abusive des informations et les logiciels malveillants, les administrateurs de sécurité informatique s'appuient généralement sur divers outils, comme les logiciels antivirus, les anti-malware et les contrôles des accès réseau et la surveillance du contenu. La plupart des outils peuvent être divisés en deux modèles : listes noires/ listes de blocages et listes blanches/ listes d'autorisations.

Un anti-virus utilise principalement les définitions des logiciels malveillants connus. Dès qu'une variante particulière d'un virus est détectée, sa définition est ajoutée à la liste noire. Ces listes de blocage sont distribuées sous forme des fichiers .dat qui doivent être téléchargés quotidiennement. Le problème est qu'il faut en moyenne quatre jours aux fournisseurs d'anti-virus pour isoler le virus et publier une mise à jour des fichiers .dat. Tout ordinateur uniquement protégé par un anti-virus reste vulnérable pendant cette durée.

Le principal inconvénient de cette approche est d'être seulement réactive, de toujours suivre les menaces. Plus important encore, les outils basés sur une liste noire sont totalement inefficaces contre les attaques zéro-jour.

Attaques zéro-jour

Une attaque de type zéro-jour (zero-day) exploite des vulnérabilités encore dépourvues d'une protection spécifiquement adaptée. Généralement, lorsqu'un éditeur de logiciels détecte un bogue ou un problème dans un logiciel après sa diffusion, il développe et distribue un correctif spécialement adapté. Une attaque de type zéro-jour exploite ce problème avant la création et l'installation d'un correctif spécifique. S'il détecte des vulnérabilités avant le développeur du logiciel, un programmateur peut créer un virus ou un ver pour les exploiter et attaquer un système avec différentes méthodes ou robots.

[1]Trellix : anciennement une société de McAfee

LISTE BLANCHE/ LISTE D'AUTORISATIONS

L'approche par liste blanche est fondamentalement basée sur l'identification des fichiers normalement utilisés dans un environnement informatique. Son rôle consiste donc à uniquement autoriser l'exécution de tous les fichiers prédéfinis et inscrits. Fondamentalement, elle n'autorise que ce qui est connu et interdit tout ce qui est inconnu. La politique par défaut consiste à refuser toute exécution à moins qu'un programme logiciel n'ait été explicitement ajouté à la liste blanche. La plupart des outils de surveillance utilisés aujourd'hui sont basés sur une liste blanche, car ils « autorisent uniquement » des utilisateurs désignés, des adresses IP spécifiques ou des types prédéfinis de services à transmettre ou exécuter sur le système. Vous pouvez alors avoir la certitude qu'une armée de robots ne pourra pas recruter de force vos multifonctions pour lancer des attaques !

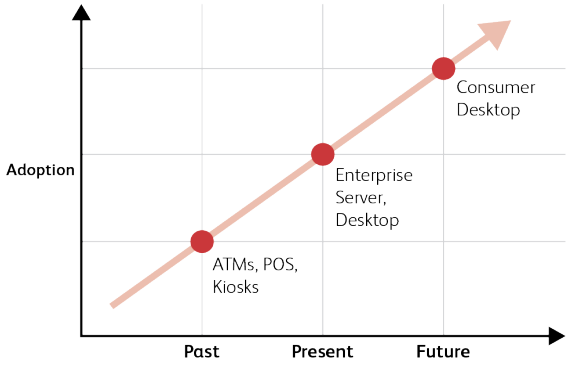
Les botnets sont connus pour être composés de milliers d'ordinateurs infectés. Un botnet est une collection d'ordinateurs infectés par des logiciels malveillants qui asservissent l'ordinateur sous la commande centrale et le contrôle d'un botmaster. Chaque ordinateur infecté est appelé un zombie. Le logiciel malveillant botnet réside sur l'ordinateur infecté, souvent à l'insu de son propriétaire et sans interférer avec ses opérations. Le botmaster vend les services du botnet à un client qui souhaite envoyer par e-mail de la publicité, sous forme de courrier indésirables/ spam, ou lancer une attaque par déni de service distribué (DDOS). Pendant une DDOS, tous les zombies tentent d'accéder simultanément à un site Web particulier, saturant ainsi ses capacités et forçant sa fermeture. Pensez à l'attaque anonyme d'un site Web gouvernemental ou d'un site média. Le logiciel Trellix[1] Embedded Control intégré dans les systèmes Xerox® empêche les logiciels malveillants de s'approprier le périphérique, évitant ainsi toute possibilité d'être recruté dans un botnet.

Voyons la différence entre la liste blanche installée sur un ordinateur de bureau ou dans un système intégré. Sur un ordinateur personnel, l'utilisateur peut installer les logiciels de son choix pour répondre à des besoins spécifiques. Le logiciel de liste blanche installé demandera alors à l'utilisateur de confirmer l'autorisation d'accès pour chaque nouveau logiciel. Par contre, dans un système intégré, son développeur est seul à savoir exactement ce qui doit être autorisé, et il peut efficacement bloquer tout le reste.

À l'aide d'une liste blanche, nous définissons ce qui doit et ne doit pas se produire. Le chaos commence lorsque quelque chose qui ne devrait pas se produire devient possible, comme une application Adobe® Flash® Player accédant à un système central. Avec la technologie des listes blanches, vous pouvez empêcher une application autrement autorisée d'accéder aux fichiers de base auxquels elle ne devrait pas avoir droit.

Adoption d'une liste blanche

Il est largement reconnu que la technologie des listes blanches est un outil très efficace pour contrer les menaces zéro-day.



COMMENT XEROX PEUT-IL VOUS AIDER ?

Quelle est la prochaine étape de l'évolution de la sécurité pour limiter les attaques sur votre réseau par l'intermédiaire d'une imprimante multifonction ? Xerox a toujours été à l'avant-garde de la sécurité des imprimantes et des multifonctions.

Conformément à notre objectif de sécurité continue, Xerox s'est associé à Trellix[1] pour garder une longueur d'avance sur les menaces croissantes qui ciblent les systèmes intégrés. Ensemble, nous avons intégré l'auto-surveillance et l'auto-protection dont chaque unité a besoin pour résister aux attaques malveillantes. En outre, l'agent Trellix[1] intégré est capable de communiquer directement avec la console de gestion de sécurité centrale Trellix[1] ePolicy Orchestrator, pour offrir aux utilisateurs d'imprimantes et de multifonctions une gestion semblable à celle dont ils ont l'habitude sur un ordinateur de bureau.

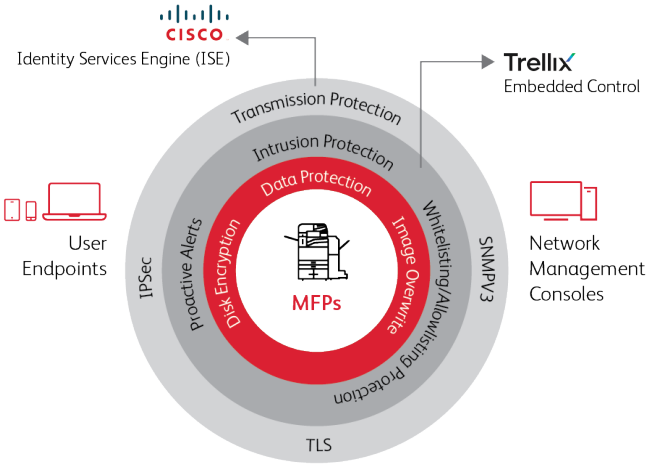
Les événements de sécurité Trellix[1] générés sur toutes les multifonctions prises en charge sont communiqués au Trellix[1] ePolicy Orchestrator configuré. Cette méthode simplifie la surveillance de toutes les multifonctions avec Trellix[1] ePolicy Orchestrator.

Voyons ce que Trellix[1] met en place pour garantir la meilleure sécurité possible sur les imprimantes multifonctions Xerox®.

[1]Trellix : anciennement une société de McAfee

TECHNOLOGIE TRELLIX[1] EMBEDDED CONTROL

Grâce à la technologie apportée par Trellix[1] Embedded Control dans les périphériques Xerox®, les clients de toutes tailles, allant des petites et moyennes entreprises, dont les ressources informatiques sont limitées, jusqu'aux grandes entreprises internationales, peuvent avoir l'esprit tranquille, sachant que leurs multifonctions sont sécurisées, dès leur livraison et sans configuration supplémentaire.



Trellix[1] Embedded Control utilise une technologie des liste blanches pour protéger vos périphériques Xerox® contre les attaques. Elle verrouille les systèmes critiques et empêche les modifications non autorisées. Seuls les programmes figurant sur la liste blanche créée par Xerox peuvent être exécutés. D'autres programmes, tels que .exes, .dlls et scripts, sont exclus car non autorisés. Les tentatives d'écriture dans des fichiers à lecture seule, ou de lecture de fichiers ou de dossiers à écriture seule, sont impossibles. Elles ne font que générer l'enregistrement d'un événement dans le journal d'audit interne. Si SIEM est configuré (nativement sur la gamme AltaLink® 8100 ou via Xerox® Device Manager pour les VersaLink®), tous les événements de journal d'audit sont transférés hors zone vers un serveur SIEM pour l'enregistrement et l'analyse. En outre, lorsque des alertes par e-mail sont configurées sur un périphérique Xerox®, un message envoyé à l'adresse désignée résume tous les détails de l'événement.

Le concept de liste blanche est simple : Xerox prédéfinit une liste limitée d'applications de confiance, et seules ces applications sont autorisées et peuvent être exécutées. C'est une solution idéale pour les systèmes intégrés à fonction fixe. Cette même technologie est aussi déployée dans les distributeurs automatiques de billets.

Les fonctions classiques telles que l'impression, la copie, la numérisation et la télécopie font partie d'une liste blanche couvrant les applications de confiance. Les tâches administratives, y compris les mises à jour micrologicielles et logicielles, le chargement des formulaires et des polices, les changements d'attributs de configuration et les diagnostics des techniciens Xerox, sont tous traités comme opérations de confiance.

Le logiciel Trellix[1] est conçu pour empêcher les attaques qui tentent de corrompre le logiciel interne ou d'installer des logiciels non autorisés. Dans le langage de la sécurité, il s'agit d'attaques « d'injection de code » ou « d'exécution de code à distance ». Contrairement à d'autres logiciels qui effectuent des analyses périodiques pour valider l'intégrité des fichiers du système d'exploitation, chaque tentative de lecture, d'écriture et d'exécution est vérifiée en temps réel. En outre, le logiciel Trellix[1] Embedded Control fonctionne sous le système d'exploitation afin que tout élément étranger soit détecté, tels que les Rootkits, dès qu'ils tentent de lancer une dissimulation d'activité à ce niveau.

Avantages attendus de la cyber-défense :

- Élimination des correctifs d'urgence
- Réduction du nombre et de la fréquence des cycles de correction
- Réduction du risque de sécurité lié aux attaques polymorphes à zéro-jour par le biais de logiciels malveillants tels que vers, virus, chevaux de Troie et injections de code, avec dépassement de tampon, débordement de tas et dépassement de la capacité de la pile
- Confiance dans l'intégrité des fichiers autorisés, avec la certitude que le système est dans un état connu et vérifié
- Réduction des coûts d'exploitation liés aux temps d'arrêt non planifiés.
- Augmentation de la disponibilité du système

Trellix[1] Embedded Control détecte les tentatives de modification en temps réel. Elles incluent en particulier les tentatives de modification du code, de la configuration, de l'état et du registre du système. Tous les événements de changement sont consignés en temps réel et envoyés au contrôleur du système.

SÉCURITÉ RENFORCÉE TRELLIX[1]

La sécurité avancée Trellix[1], en standard sur les nouvelles multifonctions, est installée et activée par défaut. Elle bloque les attaques générales, telles que les lectures/ écritures non autorisées de fichiers et de dossiers protégés, et met à jour la liste des éléments à protéger. L'intégrité de la multifonction est assurée en autorisant uniquement l'exécution des codes autorisés et l'application des modifications approuvées. Grâce à l'image de référence du système, toute tentative de modification des applications système est immédiatement détectée et signalée à l'administrateur par e-mail. Ces tentatives sont enregistrées dans les journaux d'audit. Selon la configuration du client, elles peuvent ensuite être signalées via Xerox® CentreWare® Web Software ou Xerox® Device Manager et Trellix[1] ePolicy Orchestrator® (ePO), s'il a été installé. Si SIEM est configuré (nativement sur la gamme AltaLink 8100 ou via Xerox Device Manager pour VersaLink), tous les événements de journal d'audit sont transférés hors zone vers un serveur SIEM pour l'enregistrement et l'analyse.

Les mises à jour des listes blanches sont fournies par Xerox, mais ne sont exécutées qu'avec l'actualisation du logiciel intégré. Par conception, certaines fonctions du logiciel sont déjà sécurisées, y compris le processus de mise à jour des logiciels. Une signature numérique garantit l'intégrité et l'authenticité du logiciel Xerox®. Le nouveau logiciel est uniquement installé avec une nouvelle liste blanche lorsque sa signature est valide.

Quel que soit votre fournisseur de sécurité, vous bénéficierez toujours des fonctionnalités de sécurité Xerox et Trellix[1] intégrées sans nécessiter de logiciel supplémentaire. La fonction de liste blanche est indépendante de tout logiciel externe. Elle est conçue pour fonctionner sans interférer avec les performances du système.

[1]Trellix : anciennement une société de McAfee

La sécurité avancée Trellix[1] est conçue pour éliminer les problèmes liés aux risques de sécurité accrus par l'adoption de systèmes d'exploitation commerciaux dans des systèmes intégrés. Avec son faible encombrement et ses frais d'utilisation réduits, cette solution indépendante des applications offre la sécurité ultra efficace et sans maintenance dont vous avez besoin.

Vous vous demandez peut-être comment un nouveau logiciel peut être installé sur la machine, puisque la liste blanche n'autorise que des éléments déjà connus. Tous les logiciels autorisés sont signés numériquement par Xerox. Le processus d'installation du logiciel vérifie la signature numérique avant de procéder à une installation, et si la signature est bonne, il informe Trellix[1] Enhanced Security que le nouveau logiciel est sûr et peut être installé. Comme Xerox définit l'ensemble de logiciels autorisés pendant le développement, chaque jeu de logiciels contient sa liste blanche. Après l'installation du logiciel, Trellix[1] Enhanced Security utilise la nouvelle liste blanche pour actualiser les éléments autorisés.

Rapports des alertes de menace

Les alertes de menace peuvent être communiquées de différentes manières en fonction de chaque configuration :

- **Journal d'audit** – Généré à partir de l'interface utilisateur sur l'imprimante multifonction, activé par défaut
- Si SIEM est configuré (nativement sur AltaLink® 8100 ou via Xerox® Device Manager pour VersaLink®), tous les événements de journal d'audit sont transférés hors zone vers un serveur SIEM pour l'enregistrement et l'analyse
- **Alerte par e-mail depuis le périphérique** – Configurée via l'interface utilisateur des services Internet CentreWare® de Xerox®
- **Alertes et rapports par e-mail via le logiciel Xerox® CentreWare Web Software et Xerox® Device Manager** – Configurés sur l'interface utilisateur de Xerox® CentreWare® Web Software et de Xerox® Device Manager
- **Alertes et rapports par e-mail via Trellix[1] ePolicy Orchestrator** – Configuré via le logiciel de gestion de la sécurité Trellix[1] ePolicy Orchestrator disponible sur Trellix[1]
- Les événements de sécurité Trellix[1] générés sur toutes les multifonctions provisionnées sont communiqués au Trellix[1] ePolicy Orchestrator. Cela permet de simplifier la surveillance de toutes les multifonctions grâce au Trellix[1] ePolicy Orchestrator

CONTRÔLE D'INTÉGRITÉ PAR TRELLIX[1].

Trellix[1] Integrity Control est un logiciel en option, vendu séparément, qui combine des fonctions de sécurité avancées standard avec des fonctions de détection et de prévention des attaques ciblées, de blocage de fichiers exécutables non autorisés sur tout emplacement par des processus non vérifiés. Il empêche aussi l'écriture de fichiers exécutables protégés qui ne font pas partie du logiciel standard fourni par Xerox®. Ce niveau de sécurité est le plus élevé, vous permettant de bénéficier de la meilleure protection possible sur votre imprimante multifonction Xerox®.

Trellix[1] Integrity Control ajoute une couche de sécurité qui bloque l'exécution de nouveaux fichiers depuis n'importe quel emplacement autre qu'une source fiable. Il empêche l'écriture de fichiers exécutables protégés ce qui interdit toute possibilité d'écrasement malveillant des exécutables fournis par Xerox. Il arrête l'exécution de tout code non autorisé ou toute modification du système par tout logiciel malveillant, vers, chevaux de Troie, attaques zéro-jour et même attaques ciblées. Seuls les logiciels approuvés peuvent être exécutés, ce qui prévient les attaques sur des vulnérabilités non identifiées et encore dépourvues de contre-mesures.

Xerox et Trellix[1] offrent une technologie des listes blanches qui garantit que seul un code vérifié et approuvé peut être appliqué sur des systèmes protégés. Cela garantit que vos périphériques exécutent uniquement les services que vous souhaitez utiliser tout en empêchant un attaquant d'installer un code malveillant. Cette même technologie protège les serveurs, les distributeurs automatiques, les terminaux de points de vente et les systèmes intégrés, tels qu'imprimantes et périphériques mobiles.

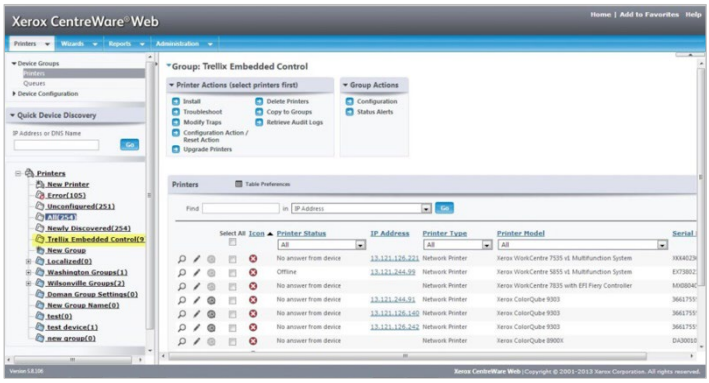
Comme indiqué précédemment, la sécurité avancée de Trellix[1] est disponible de série, entièrement installée et activée, sur certains modèles. Le logiciel Trellix[1] Integrity Control, disponible en option, ne nécessite aucune procédure d'installation. Son activation est basée sur un processus avec clé de licence.

GESTION DES PÉRIPHÉRIQUES TRELLIX[1] EMBEDDED CONTROL

Plusieurs options sont disponibles pour gérer des systèmes dotés de Trellix[1] Embedded Control :

Logiciel Web Xerox® CentreWare® et Xerox® Device Manager

CentreWare® Web de Xerox® est un outil logiciel innovant basé sur un navigateur qui installe, configure, gère, contrôle et crée des rapports sur les imprimantes et les multifonctions connectées à un réseau, quel que soit leur fabricant. Xerox® Device Manager est un outil unique conçu pour installer les files d'impression, configurer, gérer, surveiller et créer des rapports sur des appareils locaux et en réseau, quel que soit leur fabricant, à tous les niveaux de votre entreprise. Ses fonctions incluent la découverte, la configuration et la gestion des périphériques, le suivi et la visualisation des travaux, la surveillance proactive, les diagnostics et le dépannage à distance et la création des rapports.



Trellix[1] ePolicy Orchestrator®

Ce logiciel permet aux administrateurs informatiques d'unifier la gestion de la sécurité entre les terminaux, les réseaux, les données et les solutions de conformité des logiciels Trellix[1] et tiers.

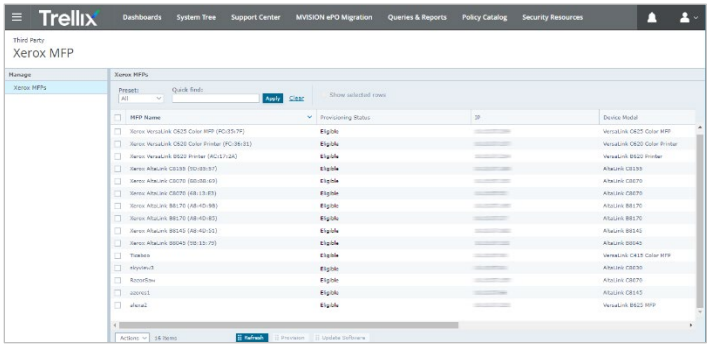
Trellix[1] ePolicy Orchestrator (ePO) est un logiciel de gestion de la sécurité vendu séparément, qui facilite la gestion des risques et de la conformité pour les entreprises de toutes tailles. Ses tableaux de bord par glisser-déposer fournissent des informations de sécurité sur les terminaux, les données, les appareils mobiles et les réseaux, pour bénéficier d'éclairages exploitables immédiats et des temps de réponse plus courts. Trellix[1] ePO tire parti des infrastructures informatiques existantes en connectant la gestion des solutions de sécurité Trellix[1] et tierces au protocole LDAP, aux opérations informatiques et aux outils de gestion des configurations.

[1]Trellix : anciennement une société de McAfee

Grâce à une visibilité de bout en bout et à des automatisations puissantes qui réduisent considérablement les temps de réponse aux incidents, le logiciel Trellix[1] ePO améliore la protection des dispositifs intégrés, réduit les coûts et la complexité de la gestion des risques et de la sécurité.

Ses fonctionnalités de reporting complètes offrent des requêtes préconfigurées et des questions personnalisées. Elles permettent de collecter des informations précises sur les produits gérés sur votre réseau ou les actions des utilisateurs sur votre serveur ePO.

Les résultats des rapports peuvent être affichés dans différents formats, tableaux ou diagrammes, et exportés pour créer des rapports PDF.

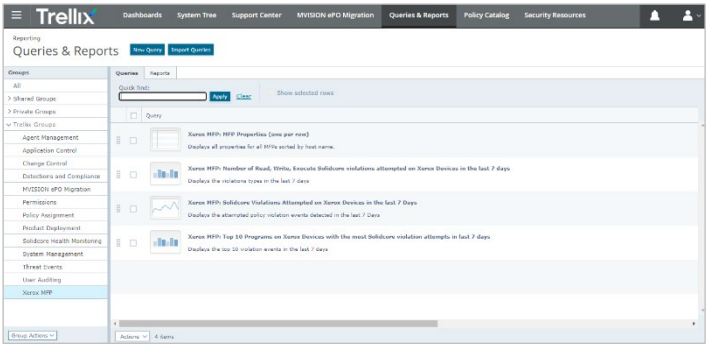


EXTENSION ePO[2] MFP DE XEROX® ET ePOLICY ORCHESTRATOR® DE TRELLIX[1]

Trellix[1] ePO est vendu directement par Trellix[1] et ne fait pas partie de l'installation des systèmes intégrés. Toutefois, si vous êtes actuellement client de Trellix[1], vous pouvez déjà utiliser Trellix[1] ePO. Dans ce cas, avec l'extension ePO MFP de Xerox®, vous bénéficiez d'une visibilité très pratique sur les périphériques Xerox® éligibles et les conditions pour recevoir des événements de sécurité. Vous avez accès à 60 attributs supportant une meilleure gestion et des informations plus détaillées sur les configurations de sécurité.

En outre, l'extension ePO MFP de Xerox® vous donne :

- Une réponse automatisée permettant aux administrateurs de recevoir automatiquement des notifications par e-mail
- Une visibilité basée sur 60 attributs de configuration de sécurité et leurs paramètres actuels
- La possibilité de vérifier la mise à jour du micrologiciel du périphérique
- La possibilité de télécharger le micrologiciel du périphérique dans ePO et de mettre à niveau un ou plusieurs périphériques Xerox®
- L'affichage en temps réel des ports actifs sur le périphérique Xerox®
- L'affichage des ports non autorisés
- L'affichage des événements de sécurité d'un périphérique Xerox® sur le tableau de bord fourni
- L'utilisation des requêtes et rapports fournis par Xerox
- La personnalisation des requêtes ou des rapports, pour effectuer rapidement des vérifications de conformité de sécurité sur l'ensemble de votre parc de services



[1]Trellix : anciennement une société de McAfee
[2]Xerox® AltaLink®, Xerox® WorkCentre® iSeries et Xerox® EC7800/ 8000

APPAREILS PRIS EN CHARGE

Trellix[1] Embedded Control est disponible pour Xerox® AltaLink®, Xerox® VersaLink® 7100, WorkCentre® iSeries et EC7800 et 8000. D'autres produits seront ajoutés à l'avenir.

RESSOURCES SUPPLEMENTAIRES

- Sécurité des données Xerox et Trellix[1]
  https://www.xerox.fr/fr-fr/connectkey/infos-complementaires/securite-trellix
- Foire aux questions sur la sécurité Xerox et Trellix[1]
  https://www.xerox.fr/bureau/latest/SECFS-14F.pdf
- Xerox, Trellix[1] et Cisco® : forment un nouveau partenariat pour fournir des réponses en temps réel aux cybermenaces
  https://www.xerox.fr/fr-fr/connectkey/infos-complementaires/securite-imprimante-reseau
- Fiche de données Trellix[1] Embedded Control
  https://www.trellix.com/en-us/assets/data-sheets/trellix-embedded-control-datasheet.pdf
- Sécurité « Zéro confiance »
  https://www.xerox.fr/fr-fr/qui-sommes-nous/solutions-de-securite/securite-zero-trust
- Solutions de sécurité Xerox
  https://www.xerox.fr/fr-fr/qui-sommes-nous/solutions-de-securite

[1]Trellix : anciennement une société de McAfee

AUTEURS

- Zia Masoom, Responsable marketing produit mondial, Xerox
- Doug Tallinger, Responsable planification des plateformes mondiales, Xerox

Pour en savoir plus sur les produits Xerox® avec Trellix[1] Embedded Control, veuillez contacter un représentant Xerox ou vous rendre sur **www.xerox.fr/fr-fr/connectkey/infos-complementaires/securite-trellix**.

© 2023 Xerox Corporation. Tous droits réservés. Xerox®, CentreWare®, AltaLink®, VersaLink® et WorkCentre® sont des marques de Xerox Corporation aux États-Unis et/ou dans d'autres pays. Toutes les autres marques sont la propriété de leurs fabricants respectifs. Les informations contenues dans cette brochure peuvent être modifiées sans préavis. TSK-3919 03/23 BR38619 SECWP-03FB