Prevention First :

Comment une défense proactive peut réduire les risques d'attaque et combler les lacunes en matière de conformité.

Digital Security
Progress. Protected.

Table des matières

Introduction

Le document qui suit examine les risques auxquels les organisations sont confrontées via divers vecteurs de menace. Il décrit aussi comment une stratégie de prévention à plusieurs niveaux peut être mise en œuvre efficacement.

Avec la montée de la complexité informatique et l'augmentation des menaces, il est crucial de les gérer à partir d'une seule plateforme intégrée. Dans un monde en constante évolution, il est essentiel de choisir un partenaire en cybersécurité digne de confiance.

Le monde évolue rapidement. Et La technologie est le moteur de ce changement, modifiant profondément la manière dont les entreprises à l'échelle mondiale fonctionnent et interagissent avec leurs clients. Dans la quasi-totalité des secteurs verticaux, les services, les applications et infrastructures sont orientés vers l'informatique en cloud. Il s'agit d'environnements informatiques distribués conçus pour faciliter le travail à distance. Ces environnements intègrent de plus en plus l'IA pour optimiser la productivité et améliorer les expériences client, mais cette transformation numérique accroît rapidement la surface d'attaque. Les courriels, terminaux, applications SaaS, appareils mobiles et réseaux deviennent des cibles croissantes pour les menaces. De nombreuses organisations s'efforcent de gérer un ensemble dynamique de risques. Selon une estimation, un actif sur dix exposé à Internet avait une vulnérabilité non corrigée en 2023, et 70 milliards de fichiers étaient exposés à un vol potentiel ou à un ransomware. Une autre étude révèle que (52 %) des organisations ne savent pas dans quelle mesure leur surface d'attaque est sécurisée, **et qu'aucune n'est sûre de maîtriser totalement cette surface d'attaque.**

Plus de

52%

des entreprises

ne savent pas dans quelle mesure leur surface d'attaque est sécurisée.

Les acteurs de menaces prospèrent dans ces conditions. Il y a cinq ans, les cyberattaques sérieuses étaient automatisées. Mais avec l'évolution des défenses, les tactiques offensives ont aussi changé. Aujourd'hui, les menaces les plus préjudiciables sont les attaques « hands-on-keyboard » qui peuvent faire appel à une ingénierie sociale sophistiquée, à des logiciels malveillants sans fichier et à bien d'autres choses encore. **Les défenseurs des réseaux doivent améliorer leur protection contre les menaces, leur détection et les efforts de réponse en tandem.**

QU'EST-CE QUE CELA SIGNIFIE EN PRATIQUE ?

Une approche axée sur la prévention et multi-couches réduira les chances qu'un adversaire s'infiltre dans le réseau de l'entreprise et limitera les dommages qu'il peut causer en cas de réussite. Les équipes de sécurité ne se **concentreront donc plus sur la remédiation et la récupération**, **mais sur la surveillance proactive du réseau,** la détection des intrusions et la gestion des risques liés à la surface d'attaque. Une approche proactive, axée sur la prévention, aidera les organisations à :

- **Atténuer les risques des menaces avancées comme les ransomwares et les "zero-day"**
- **Identifier et neutraliser les menaces émergentes avant leur exécution**
- **Poser les bases d'un cadre de confiance zéro**
- **Réduire les coûts et l'impact d'éventuelles violations de données**
- **Réduire le temps des équipes de sécurité pour la réponse aux incidents et la remédiation.**
- **Combler les lacunes de conformité et satisfaire les exigences strictes de cyber-assurance**
- **Assurer la conformité de l'entreprise**

Une protection multicouche contre les vecteurs d'attaques

Les organisations font face quotidiennement à des tentatives de vol de données internes sensibles, de données clients ou d'employés, et de détournements d'actifs informatiques ou de chiffrements de systèmes critiques. Grâce à des plateformes cloud unifiées, elles atténuent ces cybermenaces en couvrant les multiples aspects de leur surface d'attaque.

ENDPOINT

Le endpoint où l'homme et la machine se rencontrent, est une cible privilégiée pour les attaques. Les cybercriminels cherchent à exploiter les vulnérabilités des dispositifs/machines du endpoint, ou les erreurs humaines (comme le l'hameçonnage), afin d' obtenir des informations sensibles et infiltrer les réseaux. Les logiciels malveillants sans fichier sont dangereux car ils n'exploitent pas les fichiers exécutables traditionnels, ce qui signifie qu'il n'y a pas de signature à détecter pour les antivirus traditionnels. Une étude de 2023 a enregistré une augmentation de 1400 % de ces attaques pendant six mois.

LA PRÉVENTION AU NIVEAU DU ENDPOINT

La protection des endpoints doit dépasser l'antivirus traditionnel en intégrant une analyse comportementale alimentée par l'IA, capable de stopper les exploits sans fichier exécutés via des scripts. Cette technologie examine et classe les échantillons suspects à grande échelle, optimisant ainsi la prévention des menaces. Ces solutions se **mettent constamment à jour en temps réel** et protégent contre les nouvelles menaces offrant plusieurs couches de protection, incluant l'analyse du trafic réseau et le blocage des menaces sur les disques amovibles. La protection des endpoints doit également être compatible avec divers systèmes d'exploitation et types d'appareils, tels que les ordinateurs de bureau, les ordinateurs portables et les serveurs. **La détection et l'élimination des vulnérabilités, ou leur atténuation** par l'application des derniers correctifs pour les applications et systèmes d'exploitation, sont des mesures préventives cruciales... Il est indispensable de surveiller et de corriger les vulnérabilités sur tous vos points d'accès car les équipes informatiques prennent parfois du retard dans l'application des correctifs. Les organisations devraient prévenir tout risque potentiel causé par le report des correctifs et rechercher une **solution automatisée** qui détecte en permanence les vulnérabilités et simplifie le processus de correctifs en priorisant les actifs critiques dans toutes les applications et tous les systèmes d'exploitation.

OFFRE D'ESET ESET offre diverses fonctionnalités de sécurité des endpoints de nouvelle génération. **ESET LiveGuard® Advanced** offre une défense proactive contre les menaces zero day et celles inédites, en s'appuyant sur le sandboxing dans le cloud pour analyser et isoler les fichiers suspects en masse et rapidement. **ESET Endpoint Security** compatible avec Windows, macOS et Linux, protège contre les attaques de logiciels malveillants basées sur les fichiers, détecte les activités malveillantes, et fournit des outils pour une réponse rapide aux incidents de sécurité. **ESET Vulnerability and Patch Management** surveille activement les vulnérabilités dans les systèmes d'exploitation et les applications, et fournit des correctifs automatisés ou manuels pour combler les lacunes de sécurité et répondre aux exigences de conformité.

MOBILE

Le travail hybride et à distance augmente le nombre d'utilisateurs accédant aux ressources de l'entreprise via leurs appareils mobiles. Or, ceux-ci sont de plus en plus ciblés par des attaques de phishing et des logiciels malveillants et sont davantage exposés au risque de perte ou de vols. Un rapport de 2023 a révélé que 1 appareil sur 20 était compromis par des logiciels malveillants.

2 LA PRÉVENTION SUR LE MOBILE

Les entreprises ont besoin d'une protection multicouche couvrant tous leurs appareils. Cette protection doit idéalement inclure des mesures **contre le vol** (comme l'effacement et le verrouillage à distance), **le contrôle des applications, la sécurité web**, **l'anti-phishing**, ainsi que de pouvoir appliquer des **mots de passe à distance**, etc. Tout cela doit être centralisé et géré à partir d'une seule console pour garantir une visibilité et un contrôle accrus.

OFFRE D'ESET **ESET Mobile Threat Defense** fonctionne sur Android et iOS, et offre une prévention des logiciels malveillants basée sur le cloud et des défenses multicouches basées sur l'IA, le tout à partir d'un endpoint avec une performance inégalée. Il prend en charge plusieurs options de gestion des appareils mobiles (MDM) pour faciliter la protection de l'ensemble de la flotte.

APPLICATIONS DE PRODUCTIVITÉ EN CLOUD ET EMAIL

L'email reste un canal privilégié pour des menaces telles que les attaques par hameçonnage, les ransomwares sophistiqués, la compromission des courriels d'entreprise (BEC) et autres. En 2023, le phishing a d'ailleurs été le vecteur d'accès initial le plus courant dans les violations de données.

Les plateformes de messagerie et de productivité en cloud les plus répandues, comme Microsoft 365 et Google Workspace, offrent une gamme étendue d'applications telles que le stockage en nuage et les outils de collaboration. Ces applications peuvent être des cibles pour des vols de données et des extorsions. Les organisations ne devraient pas se reposer uniquement sur les contrôles de sécurité fournis par les fournisseurs de services en nuage pour garantir leur protection.

3 PRÉVENTION AU NIVEAU DE L'APPLICATION EN CLOUD ET DU COURRIER ÉLECTRONIQUE

Les meilleures pratiques recommandent de compléter les contrôles intégrés de Microsoft ou de Google par une protection dédiée et multicouche pour les services de messagerie, de collaboration et de stockage en nuage. L**a sécurité intégrée pour la messagerie électronique en nuage**, qu'elle soit native ou basée sur une API, devrait inclure le filtrage du **spam, l'analyse anti-malware, l'anti-phishing et l'analyse comportementale**. Elle doit surveiller automatiquement les fichiers nouveaux ou modifiés dans le stockage partagé pour prévenir l'exécution ou la propagation de logiciels malveillants. Idéalement, cette protection devrait être gérée depuis une console unique et centralisée.

OFFRE D'ESET **ESET Cloud Office Security** offre une protection avancée pour les applications Microsoft 365 et Google Workspace. Les nouveaux utilisateurs sont automatiquement protégés par une analyse adaptative avancée, un apprentissage automatique de pointe, un sandboxing dans le cloud et une analyse comportementale approfondie.

4 PRÉVENTION AU NIVEAU DES EMAILS SUR SITE

Les organisations qui continuent d'utiliser des serveurs de messagerie sur site doivent mettre en place des systèmes complets pour lutter contre le phishing, le spam et les logiciels malveillants afin de **filtrer les messages non sollicités ou malveillants**. De plus, elles doivent assurer la protection du serveur en tant qu'hôte. Les meilleures solutions combinent l'IA avec l'expertise humaine et intègrent le clustering, permettant aux produits de communiquer entre eux, d'échanger des configurations, des notifications, des listes grises, et bien plus encore, pour offrir une protection de niveau entreprise.

OFFRE D'ESET **ESET Mail Security** offre une protection avancée pour les serveurs MS Exchange, grâce à la technologie 64 bits qui accélère la prévention des menaces par courriel. Il prend aussi en charge les entreprises qui utilisent Microsoft Exchange dans une configuration hybride.

MATÉRIEL ET DISPOSITIFS

La multiplication des terminaux augmente la surface d'attaque des entreprises, rendant leurs données particulièrement vulnérables. Les acteurs malveillants cherchent souvent à accéder à ces données en exploitant des vulnérabilités ou, plus fréquemment, en utilisant des informations d'identification légitimes. Une telle violation coûterait en moyenne 4,5 millions de dollars aujourd'hui et peut susciter la réaction des autorités de réglementation.

5 LA PRÉVENTION AU NIVEAU DU MATÉRIEL

Les organisations peuvent mettre en place une protection par couches, mais elle n'est pas infaillible à 100%. En cas de scénario extrême, elles doivent aussi recourir à un **chiffrement robuste des données** pour les rendre inutilisables par tout voleur potentiel. Cela contribuera également à assurer la conformité avec le RGPD et d'autres réglementations en matière de cyberassurance. Les organisations devraient choisir une solution appliquant la norme de chiffrement avancé (AES) de 256 bits aux disques système, aux partitions et aux lecteurs entiers, garantissant ainsi qu'aucune donnée ne soit exposée. Pour simplifier l'administration et l'utilisation, la solution doit être compatible avec Windows et macOS, et permettre de gérer plusieurs appareils à partir d'une seule console.

OFFRE D'ESET **ESET Full Disk Encryption** propose un chiffrement AES 256 bits robuste, conforme à la norme FIPS 140-2, pour les systèmes d'exploitation de disques, les partitions et les disques durs. Avec un déploiement en un clic et une gestion centralisée, il simplifie le travail des équipes informatiques et assure tranquillité d'esprit.

IDENTITÉ

Les acteurs malveillants abandonnent de plus en plus les logiciels malveillants et l'exploitation des vulnérabilités pour utiliser des identifiants légitimes afin de se faire passer pour des utilisateurs et contourner les protections des endpoints. Un rapport indique une augmentation annuelle de 71% des attaques utilisant des identifiants valides. Ces informations d'identification sont souvent acquises sur le dark web ou volées à l'aide de logiciels malveillants. Le recours à ces méthodes a augmenté de 266 % en 2023, selon le même rapport. Les acteurs malveillants profitent largement de la réutilisation et de la mauvaise gestion des mots de passe.

6 PREVENTION AU NIVEAU DE L'IDENTITÉ

L'authentification multifactorielle (MFA) est essentielle pour protéger les informations d'identification, surtout pour les comptes privilégiés. Les solutions doivent offrir une **authentification mobile en une touche,** compatible avec Android et iOS, intégrant la biométrie et l'authentification push pour une meilleure expérience utilisateur. Elles devraient supporter l'accès au réseau, les VPN, le protocole de bureau à distance (RDP), Outlook Web Access, VMware Horizon View et les services basés sur RADIUS pour optimiser l'efficacité du back-end. Les solutions de MFA complètes doivent aussi être compatibles avec les jetons matériels si nécessaire.

OFFRE D'ESET **ESET Secure Authentication** propose une solution de MFA mobile en une seule touche, facile à installer sans matériel nécessaire. Elle prend en charge diverses méthodes d'authentification, y compris les applications mobiles, les notifications push, les jetons matériels, les clés de sécurité FIDO et les méthodes personnalisées.

Au-delà de la protection des endpoints avec XDR

En plus de protéger chaque espace de la surface d'attaque, les entreprises doivent aussi considérer l'importance de la détection et de la réponse étendues (XDR). Contrairement à une idée reçue, ces capacités ne servent pas juste à accélérer la détection et la réponse aux incidents. Elles peuvent également jouer un rôle dans une approche proactive axée sur la prévention. En effet, les capacités de détection de l'XDR peuvent révéler des systèmes mal configurés, des vulnérabilités non corrigées et des menaces dissimulées, permettant ainsi aux organisations de prendre des mesures rapides et de renforcer leur cyber-résilience. Les avantages de l'XDR sont :

- **Visibilité accrue du réseau de l'entreprise**
- **Enquêtes sur les incidents de sécurité, les menaces avancées et les attaques ciblées stacks**
- **Une surveillance plus efficace des incidents et activités inhabituels et suspects**
- **Exécution plus précise de la réponse aux incidents**
- **Support pour la détection aux menaces proactive, permettant d'intercepter les attaques avant que les logiciels malveillants ne soient déployés.**

OFFRE D'ESET ESET Inspect fournit des services uniques basés sur le comportement et la réputation, avec des informations en temps réel grâce aux renseignements sur les menaces du système mondial de réputation ESET LiveGrid®. Il est capable de détecter et de bloquer les menaces persistantes avancées, les attaques sans fichier, les menaces de zero day, les rançongiciels, et les violations des politiques de l'entreprise.

LE POUVOIR DU MDR

Les services de gestion de la détection et de la réponse (MDR) permettent aux équipes internes des clients de se concentrer sur des tâches à plus forte valeur ajoutée. En accélérant la détection et la réponse aux menaces, ils contribuent également à mettre en place une stratégie de prévention en identifiant les failles de sécurité et les problèmes dans les systèmes d'information. Le MDR aide les organisations à :

- **Renforcer la préparation en matière de sécurité grâce à des capacités immédiates de détection des menaces, d'investigation et de réponse, tout en bénéficiant d'une expertise en cybersécurité.**
- **Assurer une surveillance des menaces rentable, continue, 24/7, dirigée par des experts.**
- **Réduire les coûts liés à l'embauche de personnel qualifié tout en diminuant le temps de réponse aux incidents à quelques minutes.**
- **Se préparer à la conformité : les systèmes EDR/XDR et MDR deviennent essentiels pour l'assurance cybersécurité et les exigences réglementaires.**

OFFRE D'ESET ESET propose des services gérés adaptés aux PME et aux grandes entreprises. ESET MDR et ESET Detection & Response Ultimate offrent une gestion des menaces 24/7, combinant l'IA et l'expertise humaine pour fournir une protection de premier ordre contre les ransomwares, sans nécessiter de spécialistes de la sécurité en interne. Selon le niveau de service choisi, ESET met à disposition des chasseurs de menaces expérimentés pour une surveillance et une détection proactive des menaces.

Conclusion : L'importance de la prévention unifiée

Les organisations mondiales tentent de maîtriser les risques d'une surface d'attaque en expansion, aggravée par le travail hybride et la transformation numérique. La solution est de se **concentrer proactivement sur la prévention**. Pourquoi ? Parce que cela permet de réduire les coûts opérationnels associés à la détection des menaces et à la réponse aux incidents, tout en optimisant la productivité des équipes de sécurité.

> **Lorsque la plateforme de protection des endpoints bloque une attaque, les experts peuvent se concentrer sur l'exploration des voies par lesquelles la menace a contourné les autres défenses, plutôt que de passer leur temps à nettoyer les endpoints.**

Source: Forrester: The Forrester Wave™: Endpoint Security, Q4 2023. Paddy Harrington, 19 Octobre, 2023.

La meilleure façon de rendre opérationnelle la cybersécurité axée sur la prévention est d'utiliser une plateforme unique. Cela permettra d'assurer :

- **Moins de silos de sécurité entre les produits et réduction des lacunes potentielles dans la protection.**
- **Économies sur les licences qui seraient autrement consacrées à des produits ponctuels**
- **Réduction de la charge administrative pour les équipes de sécurité étendues, grâce à l'utilisation d'un seul produit/interface à maîtriser.**
- **SecOps plus efficace (avec moins de travail en alternance)**

La plateforme **ESET PROTECT** offre précisément ces avantages grâce à une gamme complète de capacités de prévention des menaces de nouvelle génération, consolidées en une seule solution. S'appuyant sur trois décennies d'expertise en cybersécurité et une veille mondiale avancée sur les menaces, ESET offre **une protection transparente et automatisée contre divers vecteurs d'attaque**. Conçu pour allier haute détection des menaces, faible taux de faux positifs et impact minimal sur les ressources informatiques, il vise à **réduire la surface d'attaque, atténuer les risques réglementaires** et garantir la continuité des activités.

Découvrez ce qui rend la **plateforme ESET PROTECT** idéale pour votre entreprise.

EN SAVOIR PLUS

Nous sommes ESET

Une défense proactive. Notre activité consiste à minimiser la surface d'attaque.

Gardez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre approche axée sur la prévention, alimentée par l'IA et l'expertise humaine.

Profitez d'une protection de premier ordre grâce à nos renseignements sur les cybermenaces, accumulés et analysés depuis plus de 30 ans. Notre réseau étendu de recherche et développement, dirigé par des experts reconnus, assure la sécurité de votre entreprise pour qu'elle puisse exploiter pleinement le potentiel de la technologie.

La prévention d'abord, en multi-couche

L'IA de pointe rencontre l'expertise

Renseignements sur les menaces de renommée mondiale

Support hyperlocal et personnalisé

ESET
Digital Security
Progress. Protected.