Les nouveaux axes d'amélioration de la sécurité des terminaux

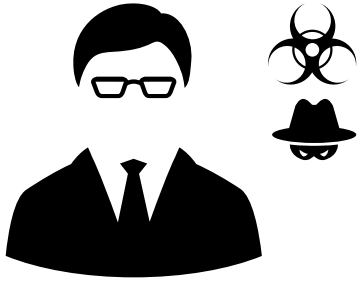
Une infrastructure IT qui protège les terminaux et renforce la productivité opérationnelle

Table des matières

Synthèse

Les terminaux (endpoints) restent une cible privilégiée des cyberattaques. Un PC portable, un smartphone ou un objet connecté piraté constitue, pour les menaces et les assaillants, une opportunité de se mouvoir au sein d'un réseau, d'infecter d'autres terminaux et d'accéder à des ressources internes critiques. Si elles pèsent sur la sécurité, les intrusions mobilisent par ailleurs les équipes et freinent leurs initiatives permettant de renforcer les performances réseau et de simplifier l'opérationnel.

Pour répondre à ces défis, les responsables d'infrastructures IT ont besoin de solutions intégrées réseau et sécurité, de maîtriser l'impact opérationnel d'une surface d'attaque en expansion et de dimensionner leur équipe de manière appropriée. Une interconnexion étroite entre la sécurité des terminaux et le réseau, renforce la protection globale de l'entreprise, grâce à une visibilité sur les risques qui pèsent sur tous les terminaux, un contrôle d'accès basé sur des règles, un partage en temps réel d'informations de veille sur les menaces et une automatisation des workflows et processus de sécurité.



Seuls 26% des responsables IT se déclarent « bien préparés » face aux cyberattaques.[1]

Introduction : le responsable de l'infrastructure IT et la sécurité des terminaux

La surface d'attaque associée aux terminaux progresse, tirée par la croissance exponentielle des dispositifs pour end-users. D'autre part, ce sont les dispositifs connectés qui prolifèrent, à l'instar des capteurs IoT, des « wearables », des systèmes de contrôles industriels ou encore des voitures autonomes. Il en résulte des cyberattaques plus nombreuses : la moitié des entreprises ont subi un piratage de terminaux au cours des 12 derniers mois.[2] La majorité des entreprises comptent sur leur équipes IT pour gérer cette problématique : 73% d'entre elles sont d'ailleurs directement responsables de la sécurité des terminaux.[3]

Au-delà de ces menaces, c'est la sécurité du réseau et des terminaux qui se révèle problématique : les outils de sécurité, cloisonnés, ne communiquent pas entre eux. Les approches traditionnelles à la sécurité du réseau et des terminaux peinent à intégrer les multiples composants de sécurité en place. Les responsables IT doivent décloisonner et évoluer vers une architecture de sécurité qui intègre les éléments réseau et sécurité (des terminaux notamment) au sein d'une plateforme intelligente. Cette transformation exige quatre axes essentiels d'amélioration : une visibilité renforcée sur les risques, un contrôle d'accès dynamique, un partage de veille des informations sur les menaces et une automatisation des workflows de sécurité.

56%

des responsables d'infrastructures IT consacrent plus de la moitié de leur temps à la cybersécurité.[4]

Axe 1 : améliorer la visibilité sur les risques

La visibilité est un prérequis essentiel de la sécurité des terminaux : vous ne pouvez protéger ce qui vous est invisible. Les équipes en charge des infrastructures IT doivent parfaitement connaître le statut des terminaux présents sur et hors du réseau corporate, et notamment les vulnérabilités non patchées, les logiciels obsolètes, les applications indésirables et les transgressions de règles. Une visibilité sur les risques implique une bonne compréhension des risques potentiels en matière d'identité des utilisateurs, de statut de protection et d'évènements de sécurité.

Pour les responsables IT, l'objectif est de retenir des solutions de sécurité qui partagent en temps réel des indicateurs avec d'autres outils de sécurité. Les pare-feux, les sandbox et les filtres web font partie de ces solutions. D'autre part, les workflows de sécurité et les processus de prise en charge des menaces doivent interagir de manière transparente entre chaque élément. Ainsi, une solution de sécurité des terminaux de nouvelle-génération doit permettre d'évaluer en un clin d'œil le statut de sécurité, via des outils de gestion proposés via une interface unique.

$8,19M

Le coût total moyen d’un piratage de données aux USA[5]

Axe 2 : un contrôle d'accès actualisé

Une fois la visibilité sur les risques actée, les responsables IT ont besoin d’un contrôle plus granulaire et dynamique des accès. La sécurité des terminaux doit évaluer l'application des règles et contrôles sur l’ensemble des dispositifs et juguler les attaques menées via des terminaux. Pour tenir cet objectif, la sécurité des terminaux se doit d'assurer que ces derniers respectent toutes les normes de conformité et de sécurité avant de leur accorder un accès. D'autre part, les terminaux indésirables et piratés doivent également pouvoir être mis en quarantaine lorsque nécessaire.

Le regroupement des terminaux au sein de segments de type intent-based permet de définir un contrôle d'accès dynamique. Ceci implique des fonctionnalités simplifiées de déploiement et de gestion, avec notamment des tâches et un reporting de conformité, pour des équipes IT souvent fortement mobilisées et incapables de mener ces activités manuellement.

67%

des responsables IT estiment que la pénurie de compétences empêche leur entreprises de s’adapter au changement.[6]

Axe 3 : une veille partagée des menaces

Face aux attaques toujours plus ciblées et virulentes, le délai pour traiter efficacement les menaces se réduit. Pour accélérer ces opérations, il s'agit de partager de manière instantanée et bidirectionnelle les informations de veille, grâce à une intégration étroite entre les terminaux et les outils de sécurité réseau. Lorsqu'un composant réseau intercepte une nouvelle menace, il relaye cette information à d'autres outils de sécurité des terminaux, en temps réel et sur l'ensemble du périmètre organisationnel.

Le partage en temps réel d'informations permet aux équipes IT de disposer d'une image globale et précise de la posture de sécurité du réseau. La sécurité des terminaux corrèle les évènements avec le trafic réseau et les flux de veille pour vérifier les alertes, identifier les menaces et repérer les piratages potentiels. Une intégration étroite améliore le ratio signal/bruit, minimise le taux de faux-positifs et offre une image plus précise de la posture de sécurité du réseau.

Pour optimiser la productivité des équipes, les responsables IT sont invités à renforcer la sécurité de leurs terminaux en s'abonnant à un service de notation de la sécurité. Ils disposent ainsi d'outils leur offrant ces services pour mieux comprendre le niveau de sécurité de leur entreprise et l'évaluer par rapport à celui de leurs pairs et à des normes reconnues. Ils peuvent également disposer d'un accompagnement pertinent et d'une checklist de mesures à prendre pour améliorer systématiquement leur posture de sécurité et notifier les dirigeants de ces améliorations.

206 jours

Le délai moyen pour identifier un piratage de données, soit +5% par rapport à l'an dernier.[7]

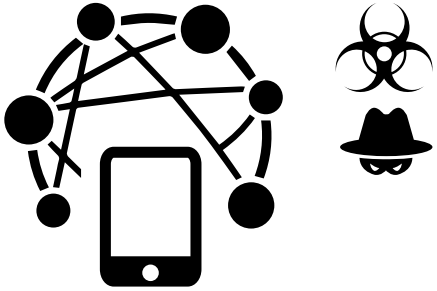
Axe 4 : Automatiser les workflows de sécurité

L'automatisation des principaux workflows de sécurité est nécessaire pour permettre aux professionnels IT d'assurer une sécurité efficace des terminaux, tout en allégeant le poids qui pèse sur des équipes fortement mobilisées et souvent limitées. L'automatisation de la sécurité des terminaux renforce la sécurité des entreprises grâce à la gestion des vulnérabilités, une prise en charge automatisée des incidents et de la conformité des terminaux. Voici quelques-unes des fonctionnalités clés nécessaires pour optimiser la sécurité des terminaux :

Gestion des vulnérabilités. La gestion des vulnérabilités vise à automatiser le patching des logiciels et systèmes d'exploitation des terminaux, et à proposer une remédiation flexible et automatisée des problématiques de sécurité mineures, sans intervention humaine. Cette approche pallie les failles l'arsenal de défense des terminaux tout en réduisant les tâches manuelles et répétitives des équipes IT.

Automatisation de la réponse aux incidents. Une prise en charge automatisée des incidents accélère les opérations de restauration et élimine les délais associés aux tâches manuelles dans les workflows de sécurité. La sécurité des terminaux doit être capable d'isoler automatiquement les terminaux suspects ou piratés pour prévenir toute infection d'autres dispositifs, ainsi que la propagation des menaces au sein d'une entreprise. Cette approche permet également de garder la main sur les erreurs humaines et d'assurer la conformité des terminaux à des normes et réglementations toujours plus strictes en matière de confidentialité de données.

Architecture Open API. Pour optimiser l'interopérabilité des fonctions d'automatisation de la solution de sécurité des terminaux sur l'ensemble de l'architecture, les responsables IT ont besoin d'une solution de sécurité basée sur une architecture ouverte et sur des API, compatibles avec des produits de sécurité tiers. Ceci permet de renforcer le niveau d'intégration de la sécurité et aide à tirer parti des investissements existants dans d'autres solutions antivirales et produits de sécurité.



"Avec une armée de dispositifs connectés et une surface d’attaque qui intègre tous les partenaires de l’écosystème d’une entreprise, les cybercriminels disposent d’un véritable avantage"[8]

Synthèse : perspectives

L'expansion rapide de la surface d'attaque qui résulte de la croissance rapide des terminaux connectés ou actifs sur le réseau, ne facilite en rien la lutte contre les cyberattaques. D'autre part, elle alourdit la charge de travail des équipes pour gérer les terminaux.

Les équipes IT et de sécurité ne disposent que trop rarement d'une visibilité complète sur les terminaux et les vulnérabilités devant être restaurées. Ce qui incite à repenser la sécurité des terminaux. Celle-ci doit éviter de consacrer plus de temps à gérer cette sécurité. Au contraire, il s'agit de décloisonner les terminaux, entre eux et vis-à-vis du réseau. C'est à ce titre qu'un partage en temps réel des données sur les menaces devient possible, tout comme le contrôle d'accès centralisé, l'automatisation des audits et du reporting de conformité, ainsi que les workflows associés aux patching et à la prise en charge des incidents.

[1] Anna Frazzetto, et al., « A Changing Perspective: CIO Survey 2019, » Harvey Nash/KPMG, 2019.

[2] Lee Neely, « Endpoint Protection and Response: A SANS Survey, » SANS Institute, 12 juin 2018.

[3] « The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges, » Fortinet, 18 août 2019.

[4] Idem.

[5] « Cost of a Data Breach Report 2019, » IBM Security and Ponemon Institute, Avril 2019.

[6] Anna Frazzetto, et al., « A Changing Perspective: CIO Survey 2019, » Harvey Nash/KPMG, 2019.

[7] « Cost of a Data Breach Report 2019, » IBM Security and Ponemon Institute, Avril 2019.

[8] « The Post-Digital Era is Upon Us: Are You Ready for What's Next?, » Accenture, 2019.

www.fortinet.com/fr

446935-B-1-FR

mai 26, 2021 3:29 PM

eb-next-generation-endpoint-security_FR