GUIDE

Maîtriser la protection des terminaux modernes

Six étapes pour une protection renforcée des entreprises, aujourd'hui comme demain

Pour garder une longueur d'avance sur les dernières cyberattaques, les entreprises n'ont cessé de multiplier les niveaux de protection. En théorie, elles devraient donc être mieux protégées. En réalité, les équipes de sécurité croulent sous les outils et les interfaces. D'après le rapport ***Mastering the Endpoint*** (Pour une maîtrise totale des terminaux) publié par Forrester en 2017, les entreprises surveillent aujourd'hui en moyenne 10 agents de sécurité différents et jonglent avec au moins cinq interfaces différentes pour analyser et corriger les incidents.

Il est cependant possible d'aborder la sécurité des terminaux de façon originale. L'expérience de terrain de plus de 250 décideurs chargés de la sécurité et les informations recueillies par Forrester et McAfee ont permis de définir six étapes essentielles pour maîtriser les terminaux modernes et protéger les entreprises, aujourd'hui comme demain.

1. Mise en œuvre d'un cadre de sécurité capable de s'adapter à l'évolution du paysage des menaces

De plus en plus de décideurs en matière de sécurité informatique s'intéressent aux défenses intégrées et privilégient un système unique coordonné. Cependant, à peine un tiers (35 %) d'entre eux ont automatisé et opérationnalisé la cyberveille sur les menaces au sein de leur architecture.

Le concept de la superposition des niveaux de protection s'est aujourd'hui généralisé, mais pour tirer le meilleur parti de ces différentes couches, il est indispensable de les connecter au sein d'un cadre de sécurité flexible et évolutif. En implémentant des niveaux de protection qui communiquent les uns avec les autres, vous améliorerez considérablement l'efficacité. Le cadre idéal doit également être extensible et vous permettre d'ajouter de nouveaux niveaux à la structure à mesure que vos besoins métier et en sécurité évoluent.

2. Intégration de fonctionnalités de détection et de réponse aux opérations quotidiennes

Selon le rapport, la majorité des entreprises ont été victime d'une compromission au cours des 12 derniers mois, et la plupart peinent à corriger tous les terminaux infectés. Les administrateurs doivent pouvoir remonter rapidement la trace de la menace et nettoyer tous les terminaux infectés. Malheureusement, ces capacités sont généralement l'apanage d'enquêteurs spécialisés, lesquels ne sont tout simplement pas suffisamment nombreux pour répondre aux besoins des entreprises.

Le déploiement d'une énième suite d'investigation avancée ne résoudra pas le problème. En implémentant une solution qui intègre des fonctionnalités de détection et de réponse aux opérations quotidiennes des terminaux, les administrateurs de première ligne peuvent intervenir rapidement lors des inévitables attaques.

3. Réduction des faux positifs afin de permettre aux équipes de sécurité de se concentrer sur les tâches critiques

Les répondants à l'enquête ont classé la précision et l'élimination des faux positifs en tête des fonctionnalités de sécurité des terminaux les plus importantes. La possibilité de neutraliser totalement les infections lors de leur première apparition suivait de près en deuxième position. Toutefois, plus de 80 % de répondants sont confrontés à des obstacles majeurs qui limitent leur capacité à gérer les risques, notamment le temps et les efforts nécessaires pour gérer les solutions de sécurité, et la difficulté de prioriser les nouvelles vulnérabilités.

La meilleure réponse consiste à améliorer la coordination entre les outils de sécurité afin de réduire le nombre de faux positifs. Les défenses qui partagent les informations de cyberveille peuvent confirmer ou exonérer automatiquement une menace potentielle, évitant ainsi aux administrateurs humains de devoir le faire. En éliminant la complexité et les efforts manuels, les équipes de sécurité de première ligne peuvent faire le tri entre les informations superflues et les données pertinentes, et agir plus rapidement. Vous pouvez optimiser davantage encore l'efficacité en faisant remonter automatiquement les incidents les plus critiques et en définissant un workflow de résolution clair.

4. Partage des informations de cyberveille en temps réel et application immédiate des enseignements tirés

Une cyberveille actualisée en permanence est essentielle pour une protection efficace contre les logiciels malveillants furtifs. D'après les résultats de l'enquête, 48 % des entreprises s'appuient sur la cyberveille pour identifier les menaces qui ont contourné les dispositifs de prévention. Un pourcentage presque identique utilise les flux de cyberveille pour traquer les menaces dans leur environnement, bénéficier d'une visibilité accrue et obtenir des informations contextualisées.

La stratégie idéale en matière de cyberveille combine sources externes et informations recueillies au sein de votre propre environnement. Votre plate-forme doit communiquer automatiquement les informations de cyberveille aux différents niveaux de protection en temps réel, sans obliger les administrateurs à basculer constamment d'une interface à l'autre. Elle doit ensuite appliquer immédiatement les informations glanées lors d'une infection à tous les autres systèmes de sécurité de votre environnement.

5. Utilisation de l'apprentissage automatique avancé et du cloud pour une vitesse et une évolutivité accrues

Les répondants à l'enquête ont cité le temps nécessaire pour obtenir les nouvelles signatures et mettre manuellement à jour les terminaux comme la principale difficulté en matière de gestion de la sécurité des terminaux.

Les stratégies modernes reposent sur une approche plus intelligente. L'implémentation et l'exploitation de fonctionnalités d'apprentissage automatique avancé, tant au niveau local que dans le cloud, vous permettent d'effectuer une comparaison statistique des fichiers exécutables suspects avec des milliers d'attributs de menaces connues, le tout sans signature. La possibilité d'analyser non seulement les caractéristiques statiques du code mais également le comportement réel d'un fichier exécutable vous permet ainsi d'identifier les menaces dissimulées en quelques secondes.

6. Consolidation des agents et des processus manuels

Les administrateurs responsables de la sécurité des terminaux ont, à juste titre, le sentiment que leur vie devient de plus en plus compliquée : 81 % des répondants estiment que certains obstacles limitent leur capacité à gérer efficacement les risques.

La consolidation des divers outils, systèmes et rapports au sein d'une console de gestion unique réduit considérablement le nombre de processus manuels. En adoptant une approche consolidée, vous pouvez réduire le nombre d'agents administrés par votre équipe et automatiser les tâches manuelles dans le cadre de workflows rationalisés. Au lieu de passer des heures à jongler entre des interfaces disparates, votre équipe de sécurité peut ainsi contrôler plusieurs niveaux de protection des terminaux au moyen de fonctionnalités automatisées faisant uniquement l'objet d'une configuration initiale.

En savoir plus

Pour en savoir plus sur la façon dont d'autres entreprises font face à leurs propres failles de sécurité des terminaux et obtenir des recommandations de Forrester pour les combler, **téléchargez le rapport**.

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr

2974_0417
AVRIL 2017