ÉTUDE DE CAS

La refonte de la protection des terminaux favorise l'innovation et renforce le niveau de sécurité

Une grande entreprise internationale de transformation des processus métier remanie ses propres processus de sécurité avec l'aide de McAfee.

Sutherland Global Services

Profil client
Entreprise multinationale de transformation des processus métier

Secteur d'activité
Services technologiques et professionnels

Environnement informatique
Près de 50 000 terminaux dans 16 pays sur six continents

Sutherland Global Services aide plus de 100 entreprises du classement *Fortune 1000* dans 16 pays à repenser et à remanier leurs processus métier à l'ère numérique, tirant parti de technologies de pointe telles que l'analyse des données, de son expertise en matière de conception créative (design thinking) et de sa connaissance approfondie des secteurs dans lesquels elle intervient. L'entreprise basée à Pittsford, dans l'État de New York, a investi dans la transformation de la protection de ses propres terminaux, ce qui lui a permis d'améliorer considérablement son niveau de sécurité global, mais aussi de gagner du temps et de l'argent. Sutherland Global Services s'appuie en outre sur le projet Open Data Exchange Layer (OpenDXL) afin de créer une défense unifiée permettant à divers systèmes de sécurité de se soutenir et de se renforcer mutuellement.

Gardez le contact

Protection contre les interruptions d'activité et les compromissions

« Chaque minute où un système est indisponible alors qu'un utilisateur professionnel en a besoin nous coûte beaucoup d'argent », explique Prashanth MJ, Responsable mondial de l'infrastructure technologique de Sutherland Global Services. « Les interruptions d'activité et les compromissions de données représentent un risque majeur contre lequel nous voulons nous protéger. Nous veillons constamment à ce que tous les contrôles nécessaires soient en place afin de réduire ces risques et de pouvoir continuer à proposer à nos clients des solutions et des services innovants et personnalisés. »

Avec près de 50 000 postes à protéger, dont 1 000 serveurs, plus de 80 centres de données et de distribution, et une infrastructure numérique répartis dans 16 pays et sur six continents, la réduction des risques de sécurité est une tâche colossale nécessitant de nombreuses solutions de sécurité. L'équipe chargée de l'infrastructure technologique doit notamment s'assurer que les différents systèmes et contrôles communiquent les uns avec les autres et partagent leurs données de cyberveille en vue de protéger l'ensemble de l'entreprise.

Un impératif : des partenaires stratégiques favorisant l'innovation

Compte tenu de sa taille et de son envergure, Sutherland Global Services a besoin de l'aide de partenaires stratégiques tels que McAfee. « Nous avons développé une véritable relation de confiance avec McAfee, qui a toujours su satisfaire nos exigences métier, notamment notre besoin d'innovation constante, indique Prashanth MJ. L'innovation fait la réussite de notre entreprise. »

« Nos services innovent au carrefour de l'entreprise et des technologies, en transformant les processus de nos clients afin de concrétiser leur vision, ajoute-t-il. McAfee propose continuellement des solutions qui répondent à nos exigences métier, par exemple pour nous aider à réduire le délai entre la détection et la correction ou pour accompagner notre transformation numérique. »

Mise en place de défenses unifiées reposant sur OpenDXL

Prashanth MJ salue également McAfee pour le développement d'OpenDXL. Cette initiative du secteur des technologies vise à créer des systèmes adaptatifs de solutions interconnectées qui communiquent et partagent des informations afin d'améliorer la prise de décisions en temps réel en matière de sécurité. Grâce à OpenDXL, Sutherland Global Services travaille actuellement à intégrer sa solution SIEM d'un éditeur tiers avec la solution de protection des terminaux de McAfee. L'intégration avec la passerelle web et le pare-feu de l'entreprise figurent également sur la feuille de route OpenDXL de Sutherland Global Services.

« Le potentiel d'OpenDXL est énorme, affirme Prashanth MJ. Nous disposons de plusieurs produits de sécurité proposés par différents éditeurs, chacun s'exécutant dans un environnement isolé. Pour créer une défense unifiée contre les cyberattaques, il est primordial que les données de cyberveille d'un système puissent être utilisées par tous les autres. »

Défis

- Assurer une disponibilité 24 h/24 et 7 j/7 aux utilisateurs professionnels du monde entier
- Intégrer des solutions de sécurité pour une cyberdéfense unifiée
- Respecter les réglementations, en particulier dans les secteurs des soins de santé et des services financiers

Solutions McAfee

- McAfee® Advanced Threat Defense
- McAfee® DLP Endpoint
- McAfee® Endpoint Encryption
- McAfee® Endpoint Security
- McAfee® Endpoint Threat Defense and Response
- McAfee® ePolicy Orchestrator®
- McAfee® File Integrity Monitoring
- Services professionnels McAfee®
- McAfee® Threat Intelligence Exchange

La consolidation de la protection des terminaux permet de réduire les coûts et d'augmenter le potentiel de génération de revenus

Pour protéger ses terminaux dans le monde entier, Sutherland Global Services s'appuie dans une large mesure sur la console de gestion centralisée McAfee ePolicy Orchestrator (McAfee ePO™). Le logiciel McAfee ePO permet aux administrateurs de gérer et de surveiller plusieurs produits et fonctionnalités de sécurité McAfee (antivirus, prévention des fuites de données sur l'hôte, prévention des intrusions sur l'hôte, chiffrement des terminaux, surveillance de l'intégrité des fichiers, etc.) à partir d'une console unique.

« [Le logiciel] McAfee ePO nous permet de gérer notre entreprise internationale de façon simple et efficace, assure Prashanth MJ. En outre, il est tellement facile à utiliser que je n'ai pas à faire appel à des ingénieurs en sécurité de niveau 2 ou 3, ce qui me reviendrait cher. »

Au cours des deux dernières années, dans le cadre d'une mise à niveau et d'une transformation complètes de la protection de ses terminaux, l'entreprise a consolidé sept serveurs hébergeant McAfee ePO, disséminés partout dans le monde, en un seul serveur. Aujourd'hui, la protection de ses quelque 50 000 terminaux est gérée par le biais d'une seule console centralisée McAfee ePO au sein de son SOC.

« Lorsque nous avons décommissionné les six autres serveurs hébergeant McAfee ePO, nous avons immédiatement réalisé des économies, se remémore Prashanth MJ. En plus de réduire les coûts matériels et logiciels, la consommation d'énergie des centres de données et le temps consacré à la maintenance et à la charge administrative ont fortement diminué. Nous avons également ajouté de nouvelles fonctionnalités sans augmenter nos effectifs et avons permis au personnel de se consacrer à des tâches à plus forte valeur ajoutée. »

« Par ailleurs, la refonte de la protection des terminaux a amélioré la disponibilité des systèmes à l'échelle de l'entreprise, ajoute-t-il. Cette disponibilité accrue a augmenté notre potentiel de génération de revenus supplémentaires. »

Plus simple et plus rapide, la génération de rapports de conformité permet d'obtenir des niveaux de conformité supérieurs à 95 %

La consolidation en une seule console centralisée s'est traduite par un gain de temps considérable en matière de conformité, en particulier dans les secteurs des soins de santé et des services financiers. « Avec une seule console centralisée, la génération de rapports de conformité est désormais beaucoup plus efficace, explique Prashanth MJ. Nous sommes en mesure de fournir rapidement et facilement des tableaux de bord personnalisés et contextualisés aux responsables de sécurité de différents secteurs, clients et régions géographiques. Par conséquent, il est bien plus simple de produire les rapports nécessaires, et notre niveau de conformité est désormais supérieur à 95 % ».

Résultats

- Réduction de la charge administrative et des coûts matériels et logiciels
- Disponibilité accrue des systèmes
- Meilleur potentiel de génération de revenus supplémentaires
- Gestion simplifiée de la protection des terminaux, permettant aux administrateurs du monde entier de se consacrer à des tâches plus importantes
- Protection multiniveau renforcée contre les malwares, notamment les menaces « jour zéro »
- Génération plus efficace de rapports de conformité dans le monde entier
- Obtention de niveaux de conformité supérieurs à 95 %
- Accélération de la détection et de la réponse aux menaces

Une protection multiniveau basée sur le partage de cyberveille renforce les défenses contre les menaces « jour zéro »

La migration de McAfee® VirusScan® Enterprise vers McAfee Endpoint Security a également joué un rôle déterminant dans la transformation du dispositif de protection des terminaux. « Nous savions qu'il était temps d'adopter une solution antimalware de nouvelle génération, offrant des couches de protection supplémentaires. Heureusement, McAfee proposait exactement ce dont nous avions besoin, explique Prashanth MJ. Nous étions particulièrement intéressés par le confinement d'application dynamique, pour mettre en quarantaine les fichiers inconnus, ainsi que par la fonctionnalité d'apprentissage automatique de Real Protect pour analyser les fichiers suspects à la volée. »

L'entreprise a également migré vers McAfee Endpoint Security pour bénéficier de McAfee Threat Intelligence Exchange, qui stocke des données de cyberveille locales et mondiales constamment mises à jour, puis les partage de manière bidirectionnelle avec tous les systèmes connectés à Data Exchange Layer (DXL). McAfee Endpoint Security se connecte à DXL sans configuration nécessaire. « Ainsi, lorsque l'un de nos terminaux rencontre un fichier malveillant, ou quand un centre de recherche mondiale détecte une nouvelle menace "jour zéro", plutôt que d'avoir à attendre que des signatures soient disponibles et distribuées par un administrateur, tous nos terminaux en ont immédiatement connaissance », explique Prashanth MJ.

Sutherland Global Services a fait appel aux Services professionnels McAfee pour effectuer une migration fluide en plusieurs phases vers McAfee Endpoint Security, sans impact sur la disponibilité des systèmes pour ses utilisateurs professionnels aux quatre coins du monde. La migration de tous les terminaux vers McAfee Endpoint Security comprenait le module Advanced Threat Protection de la solution, qui intègre les technologies Real Protect et de confinement d'application dynamique. L'entreprise a également déployé la structure DXL et McAfee Threat Intelligence Exchange à l'échelle de son réseau.

Accélération de la réponse aux incidents

Dans le cadre de la transformation de la protection de ses terminaux, Sutherland Global Services a également implémenté une appliance McAfee Advanced Threat Defense à des fins d'analyse dynamique et statique en environnement sandbox. « McAfee Advanced Threat Defense nous aide de deux façons, précise Prashanth MJ. Premièrement, lorsque l'un de nos terminaux rencontre un fichier inconnu et le met en quarantaine, le fichier est directement envoyé à l'appliance McAfee pour une analyse approfondie. Une fois l'analyse terminée, les résultats sont partagés [via McAfee Threat Intelligence Exchange] à l'échelle de l'entreprise. Nous avons ainsi pu bloquer un certain nombre de fichiers malveillants et protéger l'ensemble de nos terminaux de manière proactive. »

> « Nos services innovent au carrefour de l'entreprise et des technologies, en transformant les processus de nos clients afin de concrétiser leur vision. McAfee propose continuellement des solutions qui répondent à nos exigences métier, par exemple pour nous aider à réduire le délai entre la détection et la correction ou pour accompagner notre transformation numérique. »
>
> — Prashanth MJ, Vice-Président Directeur, Responsable mondial de l'infrastructure technologique, Sutherland Global Services

« Deuxièmement, McAfee Advanced Threat Defense accélère notre processus d'investigation des indicateurs de compromission, poursuit-il. Auparavant, pour chaque indicateur de compromission inconnu, nous devions envoyer un échantillon de hachage au support technique McAfee et attendre son retour pour savoir s'il était malveillant. Grâce à McAfee Advanced Threat Defense, nous pouvons désormais analyser nous-mêmes l'indicateur de compromission et déterminer plus rapidement l'action à mettre en œuvre. »

En outre, l'entreprise est en passe d'ajouter McAfee Endpoint Threat Defense and Response afin de renforcer sa capacité à traquer proactivement les menaces. « Nous voulons passer à l'offensive, sans plus nous contenter d'une approche défensive, explique Prashanth MJ. Je pense que McAfee Endpoint Threat Defense and Response sera l'un des outils les plus importants de notre arsenal pour nous protéger contre les menaces latentes qui pourraient se trouver dans notre environnement, dans l'attente de déclencheurs... Il est essentiel de pouvoir réagir rapidement. Sans cela, même les actions les plus efficaces seront inutiles. »

Pour se préparer à l'avenir, les produits de sécurité ne sont pas suffisants

« Notre partenariat avec McAfee s'est avéré extrêmement fructueux. Il m'a donné l'assurance que nos systèmes sont protégés et prêts à faire face à l'avenir », déclare Doug Gilbert, DSI et Directeur de la transformation numérique de Sutherland Global Services. « Vos partenariats ne doivent pas se résumer à un ou plusieurs produits, mais tenir compte de tout l'écosystème. Avec McAfee, nous nous sentons entourés : l'objectif n'est pas seulement de nous vendre des produits, mais aussi de nous aider à les concevoir, à les déployer, à en assurer la maintenance et à les optimiser. »

Au fur et à mesure de la migration de Sutherland Global Services vers le cloud et de sa transformation numérique déjà en route, McAfee va continuer à jouer un rôle déterminant. Prashanth MJ cite les nouveaux produits McAfee® MVISION comme un exemple d'innovation supplémentaire qui permettra à son entreprise de prospérer : « Compte tenu de la complexité du paysage des menaces, il est essentiel d'avancer main dans la main. McAfee se charge de nous fournir des technologies adaptées. Nous apportons notre connaissance du secteur. Pour faire face à l'avenir, la collaboration est indispensable : nous adhérons pleinement au slogan "Together is Power". »

« Notre partenariat avec McAfee s'est avéré extrêmement fructueux. Il m'a donné l'assurance que nos systèmes sont protégés. Vos partenariats ne doivent pas se résumer à un ou plusieurs produits, mais tenir compte de tout l'écosystème. Avec McAfee, nous nous sentons entourés : l'objectif n'est pas seulement de nous vendre des produits, mais aussi de nous aider à les concevoir, à les déployer, à en assurer la maintenance et à les optimiser. »

— Doug Gilbert, DSI et Directeur de la transformation numérique, Sutherland Global Services

McAfee
Together is power.

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