

Une université néerlandaise élève ses standards de cybersécurité

Bitdefender bloque tous les malwares et les infections sans fichier, améliore les performances et la durée d'activité des systèmes et simplifie les tâches de gestion de la sécurité



LE DÉFI

Maintenir une solution de sécurité à jour dans une entreprise devrait être simple. Le principal défi est souvent de repousser les cyberattaques en constante évolution. Pour l'université HAN de sciences appliquées, la protection contre les attaques avancées, l'administration de la sécurité et les performances posaient problème avec leur ancienne solution de sécurité McAfee.

Non seulement McAfee manquait des infections, mais lors des mises à jour, les milliers de postes de travail et serveurs de HAN étaient souvent paralysés, ou les mises à jour n'étaient tout simplement pas appliquées sur certains systèmes, ce qui les empêchait d'obtenir le niveau désiré de protection. Lors du téléchargement et de l'application des mises à jour, ou de l'exécution des analyses antimalwares, les performances des postes de travail et des serveurs ralentissaient à l'extrême, entraînant souvent des heures d'indisponibilité pour le personnel, la faculté et les étudiants.

Cherchant à résoudre ces difficultés, HAN a évalué les solutions proposées par Bitdefender et Trend Micro. Elle a finalement choisi Bitdefender GravityZone pour protéger ses environnements physiques et virtuels. Plus récemment, l'université a évalué et testé Fortinet, Palo Alto Networks et Bitdefender GravityZone Elite. Encore une fois, Bitdefender est arrivé en tête.

Johan Vorsterman van Oijen, Technical Project Lead pour HAN, explique pourquoi : « Nous avons été très impressionnés par le Machine Learning et l'analyse en sandbox, deux des atouts qui permettent de détecter et de neutraliser les menaces avancées comme les attaques sans fichier et les attaques Zero-day. Parmi toutes les solutions de sécurité que nous avons testées, GravityZone est celle qui a donné le meilleur taux de détection des malwares : 100%. Nous avons également apprécié la possibilité de déporter les analyses pour qu'elles ne limitent pas les performances de nos serveurs. En outre, l'intégration de GravityZone avec VMware vCenter Server nous a permis de simplifier la gestion de la sécurité en automatisant un grand nombre de tâches. »

LA SOLUTION

Aujourd'hui, HAN peut compter sur GravityZone Elite pour protéger son infrastructure qui regroupe 1 900 ordinateurs portables sous Windows, ainsi qu'un déploiement sous VMware englobant 1 350 bureaux virtuels et des serveurs virtuels Windows et Linux. HAN prévoit aussi d'étendre la



Hogeschool van Arnhem en Nijmegen (HAN) est l'une des cinq grandes universités de sciences appliquées aux Pays-Bas. Sur ses campus à Arnhem et à Nimègue, HAN dispense des formations appliquées de grande qualité à plus de 30 000 étudiants.

Secteur

Enseignement supérieur

Siège

Arnhem et Nimègue, Pays-Bas

Employés

3 600 (équipe informatique : 90)

Résultats

- Amélioration de la détection et du blocage des malwares et autres menaces (100% au lieu de 90%)
- Amélioration des performances des postes de travail et des bureaux virtuels, entraînant une réduction des coûts et une meilleure réactivité des applications
- Élimination presque totale des signalements de problèmes liés à la sécurité
- Réduction du temps hebdomadaire moyen consacré à la gestion de la sécurité (quelques minutes au lieu de plusieurs heures)
- Ajout de nouveaux postes de travail et de nouveaux serveurs en quelques minutes seulement

protection Bitdefender aux applications fonctionnant dans le cloud Microsoft Azure en cours de développement. On parle de près de 450 applications, parmi lesquelles SolidWorks, Autodesk et Office 365.

LES RÉSULTATS

Avec Bitdefender aux commandes, HAN détecte et élimine 100% des menaces qui tentent de pénétrer son environnement. L'ancienne solution de sécurité utilisée par l'université enregistrait un taux de détection de 90% environ.

Johan Vorsterman van Oijen apprécie tout particulièrement les multiples couches de technologies avancées Next-Gen intégrées à la solution GravityZone Elite. Il cite notamment Sandbox Analyzer, une sandbox intégrée aux endpoints qui analyse les fichiers douteux, exécute les charges utiles et signale aux administrateurs les actions malveillantes ; ou encore HyperDetect qui s'appuie sur du Machine Learning paramétrable, l'analyse comportementale avancée et plusieurs techniques de lutte contre les exploits.

« GravityZone Elite est un véritable atout pour nous », déclare Johan Vorsterman van Oijen. « Dès que nous avons affaire à un fichier douteux, nous l'envoyons à Sandbox Analyzer qui nous dit très rapidement si ce fichier peut être mis sur liste blanche. »

Les performances des postes de travail et des bureaux virtuels ont aussi été considérablement améliorées depuis le déploiement de GravityZone. Auparavant, l'équipe informatique recevait chaque mois une dizaine de demandes d'utilisateurs relatives à des problèmes de performance liés à la sécurité. Aujourd'hui, elle ne reçoit plus aucune demande de ce type.

« Les analyses et les mises à jour des bases de données de sécurité mobilisent une grande partie des ressources des systèmes. Leur délocalisation sur un serveur dédié est un moyen d'éviter un ralentissement des performances lorsque GravityZone effectue des mises à jour ou des analyses. Nos utilisateurs sont donc plus productifs et plus satisfaits », explique Johan Vorsterman van Oijen.

La gestion de la sécurité a aussi été simplifiée grâce à GravityZone car les administrateurs de HAN peuvent désormais effectuer toutes les tâches de sécurité pour les machines virtuelles et physiques depuis une seule et même console.

En outre, l'intégration native de la gestion de VMware vCenter Server dans GravityZone permet d'automatiser l'utilisation d'outils de sécurité, l'application des politiques de sécurité à l'échelle de l'entreprise et la récupération des licences de sécurité des bureaux virtuels désactivés. L'ajout de nouveaux postes de travail ou de nouveaux serveurs se déroule aujourd'hui en quelques minutes, alors que cela prenait plusieurs heures avec l'ancienne solution. Le même constat peut être fait au sujet de l'application des mises à jour.

Autre preuve de la facilité de la gestion avec GravityZone, l'équipe informatique de HAN consacre désormais deux heures par semaine seulement à la gestion de la sécurité.

« En ce qui concerne la sécurité, tout est plus facile à administrer et mieux protégé avec GravityZone », déclare Johan Vorsterman van Oijen. « Nous sommes protégés contre les malwares et ne souffrons plus des temps morts et des problèmes de performance liés à la sécurité. Pour l'université, ce projet a vraiment été un succès. »

« En ce qui concerne la sécurité, tout est plus facile à administrer et mieux protégé avec GravityZone. Nous sommes protégés contre les malwares et nous ne souffrons plus des temps morts et des problèmes de performance liés à la sécurité. Pour l'université, ce projet a vraiment été un succès. »

- Johan Vorsterman van Oijen, Technical Project Lead, HAN

Solutions Bitdefender

- GravityZone Elite Security
- Console de gestion GravityZone On-Premises

Environnement informatique

- Autodesk
- Linux
- Microsoft Azure
- Microsoft Windows
- SolidWorks 3D CAD
- VMware