Une entreprise internationale du BTP élargit sa cybersécurité

Une entreprise du BTP améliore la protection de ses endpoints, réduit le temps consacré au chiffrement et à l'application des correctifs et simplifie la gestion de sa sécurité.

LE DÉFI

La détection des infections est un élément primordial d'une solution de cybersécurité complète. Le blocage de ces infections et la désinfection des endpoints sont également essentiels. À l'époque où cette grande entreprise du BTP basée en France utilisait Trend Micro, son équipe informatique recevait quotidiennement des alertes signalant des infections. Résultat, les informaticiens devaient désinfecter manuellement les endpoints et les utilisateurs étaient interrompus dans leur travail.

L'équipe informatique a donc décidé de lancer une évaluation complète de plusieurs solutions de sécurité proposées par différents éditeurs : Bitdefender, F-Secure, Kaspersky, Malwarebytes, Sophos et Trend Micro. La solution Bitdefender GravityZone Elite s'est clairement démarquée.

D'après le responsable de la sécurité des systèmes d'information de cette grande entreprise internationale du BTP, « parmi toutes les solutions évaluées, Bitdefender GravityZone s'est distinguée par sa simplicité d'utilisation et son interface épurée. » Il ajoute : « Lors de notre proof of concept, GravityZone s'est déployée très facilement après avoir automatiquement désinstallé la solution Trend Micro. Elle a aussi été particulièrement efficace pour détecter et bloquer les infections, avant de désinfecter les endpoints lorsque c'était nécessaire. »

LA SOLUTION

L'entreprise utilise désormais Bitdefender GravityZone Elite pour protéger les endpoints de manière intégrée et gérer les risques sur 6 500 appareils : postes de travail macOS, Linux et Windows ; serveurs virtuels Microsoft Hyper-V et VMware ESXi ; machines virtuelles VMware vSphere ; smartphones et tablettes Android.

En outre, elle s'appuie sur le module GravityZone Full-Disk Encryption pour automatiser la gestion des clés de chiffrement BitLocker, ainsi que sur le module Patch Management pour automatiser l'application des correctifs des systèmes d'exploitation et des applications.

Cette grande entreprise internationale du BTP fournit aux entreprises et aux autorités gouvernementales des services d'ingénierie électrique, de communication et de sécurité, ainsi que des systèmes industriels. Basée en France, elle compte plus d'une centaine d'implantations en Europe et en Afrique.

Secteur
Construction

Siège
France

Employés
Plus de 10 000 (service informatique : 50)

Résultats

- Diminution de 80 % du temps passé à gérer les tickets concernant la protection des endpoints
- Amélioration significative du blocage des infections
- Amélioration de la sécurité des données et de la conformité grâce à l'automatisation du chiffrement
- Console facile à utiliser, formation plus rapide

L'entreprise utilise la fonctionnalité Sandbox Analyzer de GravityZone Elite, une sandbox intégrée aux endpoints qui analyse les fichiers suspects, exécute les charges utiles et signale aux administrateurs les actions malveillantes.

GravityZone protège les applications que l'entreprise utilise, parmi lesquelles Autodesk et Microsoft Active Directory.

LES RÉSULTATS

La console GravityZone, dont le design a plu à l'équipe informatique dès le processus de sélection, a montré bien d'autres avantages.

« Grâce à la console GravityZone, il est très facile pour notre équipe de déployer des endpoints, de gérer les stratégies et d'effectuer les tâches quotidiennes de gestion de la sécurité. Par conséquent, notre personnel a moins besoin d'être formé », explique le responsable de la sécurité des systèmes d'information.

Selon les estimations de ce dernier, l'équipe informatique a réduit de 80 % le temps passé à gérer les tickets concernant la protection des endpoints. Ce gain de temps témoigne de l'efficacité de la protection assurée par GravityZone, mais il montre également que les utilisateurs créent moins de tickets pour signaler des problèmes.

GravityZone protège cette grande entreprise du BTP contre les violations de sécurité depuis quatre ans et a généré seulement un faux positif ayant entraîné la mise en quarantaine d'un fichier non infecté. Il a suffi que l'équipe informatique réajuste les stratégies pour que le fichier quitte la zone de mise en quarantaine.

L'équipe informatique est chargée de veiller à ce que chacun des 6 500 endpoints qui composent l'infrastructure soit correctement chiffré et équipé des derniers correctifs. Les modules Full-Disk Encryption et Patch Management de GravityZone ont grandement simplifié la réalisation de ces tâches essentielles.

« Auparavant, nous devions gérer manuellement des milliers de clés de chiffrement, à l'aide de Windows, pour couvrir l'ensemble de notre environnement », précise le responsable de la sécurité des systèmes d'information. « Aujourd'hui, le module GravityZone Full-Disk Encryption nous permet d'enregistrer automatiquement ces clés de chiffrement et de les récupérer en cas de besoin. L'efficacité de ce chiffrement a également renforcé la sécurité de nos données, et nos processus sont désormais plus conformes aux dispositions réglementaires. »

Depuis que l'entreprise a abandonné une solution tierce de gestion des correctifs au profit du module Patch Management, le taux d'application des correctifs est passé de 5% à 80%. Depuis que GravityZone effectue les analyses et applique automatiquement les derniers correctifs, l'équipe informatique consacre également moins de temps à cette tâche.

Le responsable de la sécurité des systèmes d'information de l'entreprise apprécie également sa collaboration étroite avec Bitdefender.

Il déclare : « À chaque fois que nous avons une question ou que nous rencontrons un problème, Bitdefender nous apporte une réponse rapide et précise. Quand plusieurs milliers de nos employés ont dû télétravailler en raison de la pandémie de COVID-19, Bitdefender nous a guidé pour que nous puissions rapidement leur permettre d'accéder à nos ressources professionnelles depuis leurs ordinateurs personnels, grâce à un réseau sécurisé. Puisque Bitdefender investit en permanence dans le développement de technologies de pointe, nous sommes sûrs que les solutions de sécurité proposées évolueront au rythme de nos besoins. Nous envisageons d'ailleurs d'ajouter le service EDR à notre protection, les discussions sont en cours avec Bitdefender. »

« Grâce à la console GravityZone, il est très facile pour notre équipe de déployer des endpoints, de gérer les stratégies et d'effectuer les tâches quotidiennes de gestion de la sécurité. Par conséquent, notre personnel a moins besoin d'être formé. »

Responsable de la sécurité des systèmes d'information, Grande entreprise internationale du BTP

Solutions Bitdefender
- GravityZone Elite
- GravityZone Full-Disk Encryption
- GravityZone Patch Management

Environnement informatique
- Android
- Autodesk
- Microsoft Active Directory
- Microsoft Hyper-V
- VMware ESXi
- VMware vSphere

Systèmes d'exploitation
- Linux
- macOS
- Microsoft Windows

03112020-Bitdefender-Business-CaseStudy-ACF-creat4815-A4-fr_FR