

LTE Group optimise sa cybersécurité

LTE, société de service en formation, réduit les menaces à néant, améliore la performance de ses bureaux virtuels et diminue de 80% le temps consacré à la gestion de la sécurité



LE DÉFI

L'entreprise britannique LTE Group, spécialisée dans l'apprentissage professionnel et la formation, se doutait bien que le remplacement de son vieux commutateur PBX par un système VoIP sur Skype allait changer la vie de ses 8 000 employés qui disposaient d'un téléphone. Mais elle ne s'attendait pas à ce que le déploiement de Skype soit interrompu par une infection qui est parvenue à contourner la solution McAfee installée à l'époque pour protéger les endpoints. L'infection entraînait des déconnexions et impactait la qualité des appels Skype sur lesquels les employés comptent notamment pour assurer des formations vidéo à distance.

Et ce n'est pas tout. Une violation de sécurité a obligé environ 1 000 employés et plusieurs milliers d'étudiants à travailler par intermittence pendant deux semaines, pour que le service informatique puisse déconnecter chacune des machines et les désinfecter. Même stoppé, le système de partage en peer-to-peer des fichiers de signature de McAfee causait des perturbations sur le réseau. Le service informatique a découvert que cela était dû à un problème au niveau de la capture des paquets. McAfee l'a reconnu mais n'a pas été en mesure de résoudre ce problème.

Déçue par cette violation de sécurité et par le grand nombre de menaces ayant échappé à la vigilance de la solution McAfee, l'équipe IT s'est mise à la recherche d'un autre prestataire et a évalué les solutions proposées par Sophos, Cylance, Microsoft Windows Defender et Bitdefender. Bitdefender GravityZone est arrivé en tête du classement réalisé.

Comme l'explique Jamie Marshall, Directeur informatique de LTE Group : « La solution Bitdefender était tout simplement la meilleure. Notre infrastructure est complexe, diversifiée et très virtualisée. Pendant notre phase de test, la solution GravityZone a automatiquement tout retiré et a immédiatement commencé à bloquer des menaces. Elle a relevé tous les défis que nous lui avons lancés. »



LTE Group est un organisme de formation réputé qui fournit à ses clients des opportunités d'apprentissage et d'emploi à travers tout le Royaume-Uni. Les 5 000 collaborateurs de l'entreprise accompagnent plus de 100 000 personnes dans leur formation professionnelle et leur recherche d'emploi en proposant des formations continues, des apprentissages et des stages pratiques.

Secteur

Formation professionnelle

Siège

Manchester, Angleterre, Royaume-Uni

Employés

5 000 (équipe informatique : 48)

Résultats

- Aucun incident de sécurité à déplorer depuis le déploiement il y a 18 mois
- Analyse complète en 20–30 minutes seulement, contre une heure ou plus auparavant
- Délais de connexion et de réponse des bureaux virtuels réduits de 30%
- Réduction du temps consacré à la gestion de la sécurité : une heure par semaine, contre trois à huit heures auparavant

LA SOLUTION

Bitdefender GravityZone protège désormais 6 000 postes de travail Windows et macOS chez LTE Group, et il est prévu de déployer cette solution sur 4 000 postes supplémentaires. Bitdefender sécurise également 600 serveurs virtuels, 1 750 bureaux virtuels VMware Horizon View, 70 serveurs Windows et Linux et 7 000 boîtes de messagerie Microsoft Exchange.

Parmi les autres applications protégées par Bitdefender dans l'infrastructure de LTE Group, citons Microsoft SQL Server, Skype, le gestionnaire de fichiers et le Learning management system EBS.

Le déploiement de Bitdefender a été remarquablement fluide, précise Jamie Marshall : « Je n' avais jamais assisté à une implémentation aussi simple que celle de GravityZone. La désinstallation de la solution McAfee s'est faite automatiquement dès l'installation de GravityZone, qui n'a pas perdu de temps avant de détecter des menaces. Et tout cela sans que les utilisateurs se rendent compte de quoi que ce soit ! Habituellement, ces déploiements mobilisent beaucoup de ressources, mais pour GravityZone nous n'avons presque rien eu à faire. »

LES RÉSULTATS

Maintenant que GravityZone empêche les malwares et autres menaces de pénétrer l'infrastructure vaste et diversifiée de LTE Group, l'équipe informatique est beaucoup plus disponible. James Coppock, Enterprise Architect chez LTE Group, affirme : « Nous n'avons subi aucune violation de données depuis que nous avons installé GravityZone il y a 18 mois. La solution bloque des centaines de menaces chaque jour. »

Auparavant, le principal point d'entrée des malwares au sein de l'infrastructure était les périphériques USB connectés aux endpoints par le personnel et les étudiants. « Le module de contrôle des appareils de GravityZone nous permet de bloquer des périphériques USB sur des endpoints Windows et macOS », ajoute James Coppock. « Les exceptions automatisées et le filtrage des contenus sont très efficaces. Tous ces garde-fous nous font gagner du temps car nous n'avons plus de problèmes de sécurité à traiter ou de systèmes à désinfecter manuellement. Le temps de travail hebdomadaire consacré à la gestion de la sécurité a diminué de plus de 80%. « Avant, nous passions entre trois et huit heures par semaine à vérifier les mises à jour de McAfee et à traiter les endpoints laissés de côté », se rappelle Jamie Marshall. « Sans compter le temps passé à résoudre les problèmes de sécurité. Avec Bitdefender, une simple vérification quotidienne sur la console suffit et cela représente une heure par semaine au maximum. Et nous ne perdons plus de temps à traiter les infections, puisqu'il n'y en a pas. » En outre, depuis l'adoption de la solution Bitdefender le nombre d'appels concernant la sécurité informatique est passé d'environ 150 à moins de 50 en moyenne par mois. James Coppock le reconnaît : « Les petites équipes informatiques comme la nôtre ont besoin de solutions autonomes. Bitdefender a vraiment tapé dans le mille car GravityZone est à la fois très simple à utiliser et extrêmement puissant. » Autre amélioration majeure : la performance des endpoints. Lorsque l'équipe informatique, craignant une infection, exécutait une analyse de grande ampleur avec McAfee, l'infrastructure était quasiment paralysée. Selon Jamie Marshall, « Bitdefender n'a en revanche aucun effet sur le fonctionnement des endpoints pendant les analyses. Les analyses complètes sont aussi beaucoup plus rapides : 20 à 30 minutes, alors qu'elles duraient une heure ou plus avec McAfee. » L'intégration fluide de GravityZone dans l'environnement VMware NSX de l'entreprise permet aussi d'expliquer ces performances optimales. Cette intégration rend possible la mise en place d'une sécurité sans agent. Il n'est donc plus nécessaire d'installer et d'exécuter un agent sur les endpoints virtuels. Résultat : les serveurs et les bureaux virtuels sont plus performants. Les tâches de sécurité qui mobilisent d'importantes ressources, comme les analyses antimalwares et les mises à jour des bases de données sur les cybermenaces, se font sur un serveur de sécurité dédié et non pas sur chacune des machines virtuelles. « Depuis que nous avons installé GravityZone, les utilisateurs de nos bureaux virtuels ont vu les délais de connexion et de réponse baisser d'environ 30% », précise Jamie Marshall.

« Les petites équipes informatiques comme la nôtre ont besoin de solutions autonomes. » Bitdefender a vraiment tapé dans le mille car GravityZone est à la fois très simple à utiliser et extrêmement puissant. »

James Coppock, Enterprise Architect,
LTE group

Solutions Bitdefender

- GravityZone Advanced Business Security

Environnements

- VMware ESXi
- VMware Horizon View
- VMware NSX

Systèmes d'exploitation

- Apple macOS
- Linux
- Microsoft Windows