Kiabi compte sur Forcepoint pour protéger son empire de la mode

L'enseigne française de mode à petits prix protège son réseau mondial de magasins et de bureaux avec le pare-feu nouvelle génération de Forcepoint.

Kiabi supervise plus de 450 magasins en pleine propriété ou franchisés dans le monde entier, ainsi que des bureaux, des entrepôts et des sites de vente en ligne comme kiabi.com. Connecter tous ces actifs de manière sécurisée est l'une des clés du succès de Kiabi, en particulier lorsqu'il s'agit de fournir un service client primé, dans ses boutiques comme en ligne. L'entreprise basée à Hem, en France, s'appuie sur la solution de pare-feu Forcepoint NGFW avec SD-WAN pour sécuriser son réseau informatique mondial et déployer des solutions de connectivité SD-WAN plus rapides et plus abordables pour la mise en ligne de nouveaux magasins.

Profil client
Kiabi est une société de distribution de prêt à porter qui propose des articles de mode de qualité à des prix abordables.

Secteur
Vente au détail

Pays
France

Produits
Forcepoint NGFW

Kiabi a contribué à révolutionner l'industrie de l'habillement grâce à son approche commerciale novatrice, visant à rendre abordable pour le consommateur moyen un prêt à porter inspiré des créateurs. Fondée en 1978 par Patrick Mulliez, Kiabi est restée une entreprise familiale, même si elle est passée d'un seul magasin situé à Roncq, en France, à plus de 450 points de vente en pleine propriété et en franchise dans le monde entier. L'entreprise a constamment adopté des mesures d'efficacité commerciale qui lui permettent de vendre la mode à des prix abordables.

Aujourd'hui, Kiabi doit ses performances à la technologie, et plus particulièrement grâce aux gains réalisés lors de la transformation numérique de ses activités commerciales. L'équipe informatique de l'enseigne est dirigée par son directeur technique, Anthony Pierson, depuis Lille, en France. L'équipe gère un réseau reliant les magasins, les bureaux et les entrepôts du monde entier. Le firewall nouvelle génération (NGFW) Forcepoint entre alors en jeu pour assurer la sécurité de ce réseau.

Gommer les différences dans un réseau informatique mondial avec SD-WAN

Kiabi entre maintenant dans les dernières étapes d'une transformation numérique majeure, afin de rester compétitif dans un contexte mondial concurrentiel pour la mode à petits prix. Le détaillant possède des centaines de magasins physiques en France et dans les territoires d'outre-mer, ainsi que des dizaines d'autres points de vente franchisés en Europe, en Afrique et au Moyen-Orient. Chacun de ces endroits est plus ou moins différent en termes de connectivité et de prix des télécommunications. Kiabi voulait une solution de sécurité réseau qui pouvait l'aider à gommer ces différences, offrir une performance réseau plus cohérente et qui pouvait réduire les coûts, a déclaré M. Pierson.

Le détaillant français avait aussi d'autres objectifs en matière de sécurité pour ses réseaux.

Kiabi voulait aussi :

- Une solution de sécurité réseau unifiée et à gestion centralisée
- S'assurer que son réseau résiste à l'épreuve du temps en anticipant des besoins croissants en sécurité
- La capacité de se conformer aux différentes réglementations en matière de protection des données selon les différents marchés

L'approche adoptée par Kiabi consistait à construire un réseau étendu à définition logicielle (SD-WAN) pour son activité mondiale de vente au détail. Le SD-WAN est une technologie réseau qui utilise des logiciels pour rendre les réseaux étendus plus rentables et plus flexibles que ceux reposant uniquement sur la commutation multi-protocole par étiquette (MPLS), en connectant différents sites géographiques directement à Internet, via les liaisons à large bande les plus appropriées et les plus fiables disponibles dans chaque lieu. Les configurations et les politiques d'accès des SD-WAN sont gérées de manière centralisée et sont facilement déployées sur tous les sites, ce qui évite d'avoir à administrer manuellement chaque appareil WAN régulièrement.

Au départ, le SD-WAN était une solution utilisée principalement par les petites et moyennes entreprises pour connecter des sites distants, en leur épargnant les coûts et les retards liés à la location de lignes MPLS vieillissantes. Mais au fil du temps, le SD-WAN a également été adopté par les grandes entreprises, notamment parce que la sécurisation de ces réseaux est devenue aussi robuste que les avantages qu'ils offrent en termes d'efficacité opérationnelle.

“Nous sommes une entreprise en pleine croissance et nous devons mettre en ligne de nouveaux magasins le plus rapidement et le plus économiquement possible. Le SD-WAN nous donne cette agilité - il est très utile pour établir rapidement une connexion entre nos datacenters, notre siège social et nos magasins. Il offre une meilleure latence et de meilleurs coûts dans l'ensemble”, a affirmé M. Pierson.

“Nous avons établi un partenariat de longue durée et productif avec Forcepoint et, grâce aux pare-feux NGFW, nous sommes en mesure de connecter nos nouveaux magasins très rapidement , tout en économisant de l'argent. Cette relation a permis un bon retour sur investissement, rien qu'en termes d'efficacité et d'économies sur les coûts de fonctionnement".

Défis

Sécuriser un réseau mondial SD-WAN reliant plus de 450 sites distants.

Maintenir un service réseau homogène dans les différentes zones géographiques.

Centraliser la gestion et le contrôle du réseau.

Approche

Déployer 1000 appliaces Forcepoint NGFW sur place dans les sites éloignés de Kiabi.

Forcepoint NGFW est exactement ce qu'il fallait pour le réseau

La sécurisation d'un SD-WAN à l'échelle du réseau de Kiabi nécessitait une solution de sécurité réseau spécialement conçue à cet effet. Les produits de sécurité réseau Forcepoint combinent la toute dernière connectivité SD-WAN avec la sécurité NGFW la mieux notée du secteur, le tout géré à l'échelle de l'entreprise depuis une seule console à fonctionnement basé sur des politiques. Ils sont utilisés par des entreprises de toutes tailles dans les secteurs du commerce de détail, de l'hôtellerie et des services financiers dans le monde entier.

Kiabi a déployé 1 000 appliances Forcepoint NGFW dans ses sites mondiaux, en tirant parti des principales fonctionnalités de "clustering", ou regroupement, des NGFW et des capacités SD-WAN. Ainsi, l'entreprise a pu créer une solution de sécurité réseau unifiée et gérable de manière centralisée, réduire les factures de télécommunications, surmonter les problèmes de connectivité et obtenir une solution plus rapide et plus rentable pour mettre en ligne de nouveaux sites.

M. Pierson a déclaré que les capacités de gestion centrale de Forcepoint NGFW et l'efficacité de son clustering facilitent le déploiement des mises à jour et la création et l'adaptation de règles, par rapport aux produits concurrents.

Forcepoint NGFW a également aidé Kiabi à améliorer la disponibilité et la résilience de son réseau, à protéger ses sites distants contre le phishing et les attaques de logiciels malveillants sur Internet, et à accélérer les performances de ses applications cloud.

À long terme, Kiabi prévoit d'assumer de nouvelles responsabilités en étendant le périmètre de sécurité de son réseau, pour y inclure les magasins franchisés qui gèrent actuellement leurs propres opérations de sécurité des données. La société comptera sur Forcepoint pour l'assister lorsque cela se produira.

"Actuellement, nous ne partageons pas toutes les données relatives à nos clients avec nos franchisés. Mais dans les années à venir, nous prévoyons d'étendre notre programme de fidélité à un plus grand nombre de ces magasins franchisés, ce qui signifie que nous devrons nous associer avec eux en matière de sécurité et de conformité. Nous pensons que Forcepoint NGFW nous a aidés à rendre viable ce scénario du côté du réseau", a déclaré M. Pierson.

S'attaquer aux nouvelles exigences de conformité en Russie

La récente expansion de Kiabi en Russie, où la société exploite désormais plusieurs magasins physiques, a posé un défi à l'équipe de Pierson, pour la gestion de nouvelles réglementations sur la protection des données. L'aide de Forcepoint était nécessaire pour rester en conformité avec ces réglementations. La loi fédérale russe exige que tous les opérateurs qui traitent des données personnelles de citoyens russes, qu'elles soient collectées en ligne ou hors ligne, traitent ces données personnelles dans des bases de données situées sur le territoire de la Fédération de Russie.

Cela signifie que Kiabi doit se conformer à la loi en effectuant localement toutes les opérations informatiques impliquant des données de clients russes, ce que la société fait par le biais d'un accord d'infrastructure en tant que service avec la société Internet russe Yandex. Le compte Yandex de Kiabi héberge également le logiciel Forcepoint NGFW, qui agit comme une passerelle reliant les données des clients russes hébergées dans le cloud avec les datacenters du détaillant en France.

"Nous devons nous conformer à la loi russe concernant les données personnelles, c'est pourquoi nous avons déployé cette infrastructure en tant que service dans le cloud russe, à l'aide du logiciel de Forcepoint. Mais nous devons également nous conformer aux réglementations du secteur, comme la norme PCI-DSS, dans chaque magasin. Et nous avons aussi des préoccupations principales en sécurité, comme le maintien d'une barrière entre le WiFi des invités et le WiFi des entreprises ", a déclaré M. Pierson.

"Nous utilisons les clusters de Forcepoint NGFW dans tous nos magasins; et ils remplissent bien leur rôle. Nous avons une relation très forte avec Forcepoint, et nous avons une confiance totale dans leurs produits et leur équipe".

Forcepoint NGFW a coché toutes les cases que Kiabi espérait pour sa solution de sécurité réseau, donnant au détaillant pionnier la liberté de faire ce qu'il fait de mieux : proposer à ses clients une mode de qualité et tendance à des prix accessibles à tous.

Résultats

Configuration et surveillance intégrées du SD-WAN.

La gestion centralisée avec une visibilité en temps réel et une configuration par glisser-déposer facilitent les changements de politique et les mises à niveau.

Amélioration de la disponibilité et de la résilience du réseau.

Priorisation du trafic basée sur les applications "qui marchent vraiment".

Forte protection anti-intrusions.

Intégration des contrôles de la qualité de service (QoS) dans les politiques de sécurité.

FORCEPOINT

[Kiabi-Customer Story-FR-FR-010619] 300199.010720

Contact : forcepoint.com/contact