SASE : un remède salutaire pour cet acteur de la santé

Cas d'usage

Le SASE (Secure Access Service Edge) aide un grand nom de la santé à optimiser ses opérations de sécurité

Protéger une grande marque

Dans le secteur de la santé, les entreprises ont la double mission d'améliorer le service client tout en garantissant la confidentialité des données patients. Or, plus la structure est grande, plus cette mission vire au casse-tête. À chaque création d'une nouvelle business unit, il devient de plus en plus difficile d'assurer une sécurité homogène sur l'ensemble de l'entreprise.

C'est cette problématique qui a poussé un grand groupe du secteur de la santé à se tourner vers Verizon en 2020, dans le cadre d'un vaste plan pluriannuel de renforcement de sa cybersécurité. À l'échelle mondiale, l'entreprise compte des dizaines de milliers d'employés répartis dans plusieurs business units, avec chacune ses propres ressources en termes de sécurité (équipes, technologies et méthodes). Il en résultait un vaste amalgame de solutions de sécurité, avec chacune ses propres processus et des impacts divers au niveau organisationnel, ce qui affaiblissait la cyber-résilience de l'entreprise. Celle-ci s'est alors fixé trois grands objectifs : 1) améliorer l'expérience collaborateur, 2) maximiser ses investissements technologiques et 3) exceller dans la gestion de sa sécurité.

Pour ce faire, il lui fallait une nouvelle méthode pour renforcer sa sécurité tout en harmonisant ses processus et ses outils.

Partir sur de bonnes bases

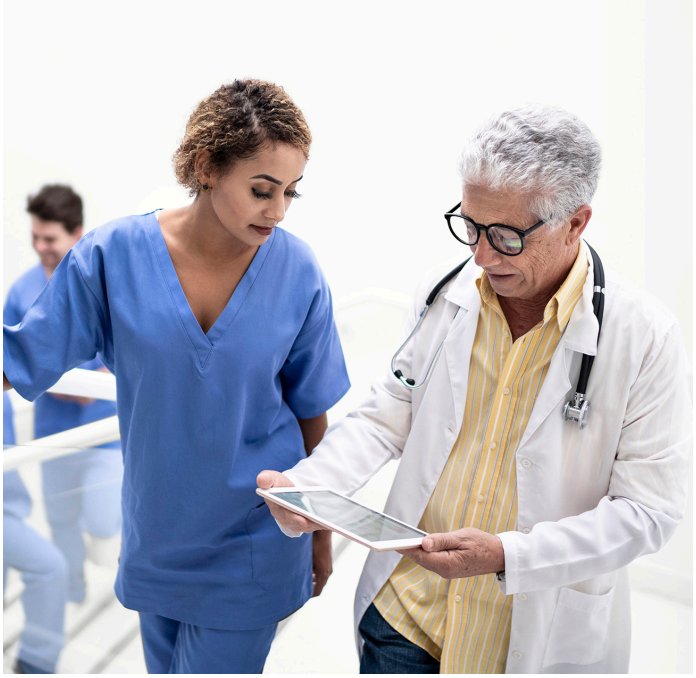
En partenariat avec Verizon, l'entreprise a opté pour une résolution progressive du problème, en commençant par un projet pilote dans une de ses business units. L'idée derrière cette démarche était de retenir les fonctionnalités de sécurité ayant fait leurs preuves dans le pilote, puis de les intégrer une à une à l'ensemble de la plateforme de sécurité.

L'entreprise avait pour principal objectif d'offrir à ses 30 000 utilisateurs répartis sur des centaines de sites un accès sécurisé à Internet et aux applications métiers. Elle a fait appel à Verizon en raison de la puissance de son réseau mondial et de la supériorité de ses compétences en matière de conception, d'implémentation et de gestion d'architectures réseau et sécurité intégrées. Son approche consultative, son solide écosystème de partenaires et sa capacité d'intégration multifournisseur ont également fait pencher la balance en sa faveur. Car le client souhaitait faire appel à un partenaire expérimenté à même de les guider, afin d'éviter les pièges courants et d'adopter les bons réflexes face à l'imprévu.

Pour Verizon, la première étape consistait à dresser un bilan initial de l'écosystème IT existant du client. En collaboration avec les équipes IT et de sécurité de ce dernier, nous avons d'abord défini les impératifs technologiques et métiers, puis mis au jour les limites et les problèmes d'implémentation posés par les solutions en place.

Collaboration et co-innovation

La phase suivante consistait à mettre en place les bases de la nouvelle solution. Le choix s'est porté sur le Network-as-a-Service (NaaS) de Verizon côté réseau, accompagné du SASE (Secure Access Service Edge) pour permettre aux collaborateurs de se connecter aux applications métiers, aux bureaux et aux sites de production en toute sécurité, où qu'ils se trouvent.



verizon business

Une solution homogène

Grâce à cette double infrastructure combinant réseau et sécurité au sein d'une solution parfaitement intégrée, la business unit pilote a pu instaurer le travail hybride en toute confiance. Résultat : sur les 200 sites que compte le groupe, les utilisateurs disposent d'un accès sécurisé à Internet et aux applications métiers depuis leurs appareils mobiles. Ils peuvent accéder aux ressources IT hébergées sur des serveurs on-prem et cloud depuis l'ensemble des bureaux et sites de production.

Autre avantage, la DSI ne jongle plus avec d'innombrables fournisseurs et outils. Elle compte désormais une seule stack technologique, avec un seul service support comme interlocuteur. De plus, l'entreprise a confié à Verizon la gestion quotidienne de la sécurité, comme l'onboarding de nouveaux utilisateurs et la relation avec les fournisseurs de sécurité pour le traitement des tickets de support. Les équipes IT et de sécurité internes du client peuvent ainsi se recentrer sur des missions plus stratégiques et porteuses de valeur.

Qui dit simplicité, dit visibilité et contrôle. La business unit cerne désormais mieux l'utilisation de ses ressources et ses dépenses, ce qui a permis aux équipes IT et de sécurité de réduire leurs coûts. Ainsi, les systèmes et outils performants ont été conservés et optimisés pour maximiser le retour sur investissement, tandis que les solutions redondantes ont été décommissionnées.

Enfin et surtout, les business units ne dépendent plus d'une infrastructure partagée qui les rendait plus vulnérables aux compromissions. Ainsi, elles peuvent mieux aligner leurs politiques de sécurité sur celles mises en place à l'échelle du groupe.

Perspectives d'avenir

Ayant optimisé ses opérations avec l'aide de Verizon, l'entreprise entame désormais une nouvelle phase de transformation de sa sécurité. Là encore, Verizon tiendra un rôle central pour continuer à améliorer non seulement les opérations de sécurité (SecOps), mais également l'intégralité de la plateforme. Verizon procèdera ainsi à l'ajout progressif de fonctionnalités de sécurité qui, intégrées à la solution SASE, permettront d'adopter une approche de services managés de détection et de réponse (MDR), XDR et EDR compris.

Plus d'informations :

Pour découvrir tous les avantages d'une solution SASE, contactez votre responsable de compte ou rendez-vous sur verizon.com/business/fr-fr/resources/lp/secure-access-service-edge.

verizon business