L'entreprise de services publics irlandaise ESB consolide sa transformation numérique avec Forcepoint

La compagnie nationale d'électricité irlandaise protège sa stratégie technologique axée sur le cloud avec l'aide de Forcepoint Edge Advantage.

Electricity Supply Board s'appuie sur Internet et le cloud, qu'elle considère comme outils essentiels pour la fourniture de ses services d'infrastructures critiques à plus d'un million de clients. Après avoir longtemps dépendu de Forcepoint Web Security pour sécuriser son utilisation d'Internet, ESB est passé à Forcepoint Edge Advantage comme fondement de sa cybersécurité et pour la prochaine phase de sa transformation numérique protégée par SASE.

PROFIL CLIENT :
Service public fournissant de l'électricité via la production, le transport et la distribution d'énergie

SECTEUR :
Énergie

PAYS D'ORIGINE :
Irlande

PRODUIT :
Forcepoint Edge Advantage

Electricity Supply Board (ESB) est un service public diversifié et verticalement intégré, qui fournit de l'électricité à environ 1,4 million de clients et exploite des réseaux électriques en Irlande et en Irlande du Nord. ESB est un service public qui opère sur l'ensemble du marché de l'électricité, depuis la production jusqu'à la transmission et la distribution. L'entreprise détient également des participations plus modestes dans la distribution de gaz naturel, les réseaux et les télécommunications, ainsi que dans les infrastructures publiques de recharge des véhicules électriques.

ESB est un client de longue date de Forcepoint, qui a fait confiance à Forcepoint Web Security pour protéger ses employés et les données avec lesquelles ils travaillent afin de maintenir l'infrastructure critique, de fournir de l'énergie et d'offrir des services à leur clientèle. Cette entreprise du service public exploite plusieurs centrales électriques en Irlande et au Royaume-Uni, ainsi que le réseau électrique d'Irlande du Nord. Cette infrastructure critique doit être protégée contre la menace croissante de cyberattaques malveillantes.

Une protection efficace contre ces menaces exige des solutions souples qui peuvent être adaptées à des contextes et des défis industriels uniques, tout en étant suffisamment puissantes pour tenir à l'écart les adversaires les plus tenaces ou les plus sophistiqués. Dans le cadre de sa transformation numérique ces dernières années, ESB a cherché la bonne approche en matière de cybersécurité pour accompagner sa transformation numérique vers des solutions natives du cloud et basées sur le SaaS pour toutes ses couches informatiques, a déclaré Chris Madden, responsable de l'ingénierie de la cybersécurité chez ESB.

Au moment de renouveler son contrat avec Forcepoint, ESB a décidé de faire migrer sa sécurité vers le cloud pour mieux s'adapter à son utilisation accrue des applications et des plateformes cloud telles que Microsoft Office 365, Salesforce et SAP HANA.

« Il y a quelques années, il est devenu de plus en plus évident que notre infrastructure de sécurité n'était pas assez développée pour arriver là où ESB voulait se positionner en tant qu'opérateur de services essentiels.

« Ce que nous voulions, c'était un prestataire de services proxy leader sur le marché, à haute disponibilité et très évolutif, qui puisse répondre à nos besoins techniques et tarifaires, et qui nous donnait la possibilité d'activer des fonctionnalités supplémentaires en fonction de nos besoins, conformément à notre stratégie numérique », a déclaré M. Madden.

ESB et Forcepoint ont élaboré une stratégie de cybersécurité qui commencerait par la migration vers un déploiement dans le cloud de Secure Web Gateway (SWG), et qui se développerait au fil du temps vers un cadre SASE complet et convergent pour sécuriser la périphérie du réseau et l'accès au cloud.

Mise en place progressive des solutions de sécurité SASE avec le bon prestataire

« En choisissant un partenaire de cybersécurité à long terme pour un programme aussi ambitieux, ESB voulait un fournisseur capable de l'aider à atteindre plusieurs objectifs informatiques stratégiques clés », a déclaré M. Madden.
Cela incluait :

- → Réduire la complexité des technologies de l'information et de la cybersécurité et améliorer l'efficacité opérationnelle.
- → Augmenter les capacités pour prendre en charge et assurer la sécurité des travailleurs distants.
- → Établir une relation solide à long terme avec un partenaire stratégique dans le domaine de la sécurité, disposant d'un vaste portefeuille de solutions SaaS et SASE.
- → Adopter une approche progressive pour le déploiement des technologies de transformation dans le cadre d'un plan quinquennal de croissance et d'expansion.
- → Tirer parti des partenaires technologiques stratégiques existants comme Microsoft.

Défis

Réduire la complexité des technologies de l'information et de la cybersécurité et améliorer l'efficacité opérationnelle.

Augmenter les capacités pour prendre en charge et assurer la sécurité des travailleurs distants.

Sécuriser l'utilisation accrue des applications et des services dans le cloud

Fournir une feuille de route pour une stratégie technologique et de cybersécurité basée sur le SASE.

Approche

Déployer le SWWG et le CASB de Forcepoint Edge Advantage dans le cadre de la première partie du déploiement progressif des solutions de cybersécurité SASE.

En plus de cette liste d'objectifs stratégiques, ESB est extrêmement sélectif quant aux fournisseurs avec lesquels nous travaillons, a déclaré M. Madden.

« Une chose en particulier qui est très importante pour ESB est la relation client-fournisseur. Nous avons toujours eu une très bonne relation avec Forcepoint, et nous avons toujours eu le sentiment que Forcepoint nous traitait comme un client de valeur. Lors de toutes nos interactions, notre directeur national et les consultants seniors de Forcepoint ont vraiment bien travaillé ensemble. Ils s'efforcent toujours de répondre aux exigences d'ESB et d'adapter leurs solutions à nos besoins », a-t-il déclaré.

Pour la phase suivante du partenariat, ESB a opté pour une licence Forcepoint Edge Advantage, à la fois pour répondre à ses besoins immédiats et pour se positionner en vue de l'introduction progressive, sur plusieurs années, de protections supplémentaires en matière de cybersécurité dans un cadre stratégique SASE. Forcepoint Edge Advantage propose des licences pour le SWG, le Cloud Access Security Broker (CASB), la sécurité dans le cloud, les systèmes de prévention des intrusions (IPS) et le Firewall nouvelle génération (NGFW) avec SD-WAN, plus l'isolation du navigateur à distance et la détection avancée des malwares en tant que modules complémentaires optionnels. Plus tard, ESB aura la possibilité, au besoin, d'ajouter les solutions Forcepoint de protection des données et des utilisateurs, grâce à une licence complète Forcepoint Advantage.

« Cela nous convenait, car la première chose que nous voulions faire était de passer de la sécurité cloud vers une solution évolutive. Une fois que nous avions eu cela, notre attention s'est tournée vers ce qui arrive ensuite – et c'est évidemment plus de cloud. ESB a une approche « cloud avant tout », et il est très probable qu'il y aura encore des transitions cloud qui seront effectuées sur des facettes de notre activité qui ne sont toujours pas dans le cloud. Notre consommation de services cloud ne fera qu'augmenter au fil du temps », a déclaré M. Madden.

Le modèle de licence Forcepoint Edge Advantage signifie également qu'ESB bénéficiera de nouvelles fonctionnalités dès leur sortie – sans frais supplémentaires – et aura la possibilité d'ajouter un nombre illimité d'utilisateurs pendant la durée du contrat, réduisant ainsi le coût total de possession.

Forcepoint CASB donne à ESB un accès toujours plus important au cloud, en toute sécurité

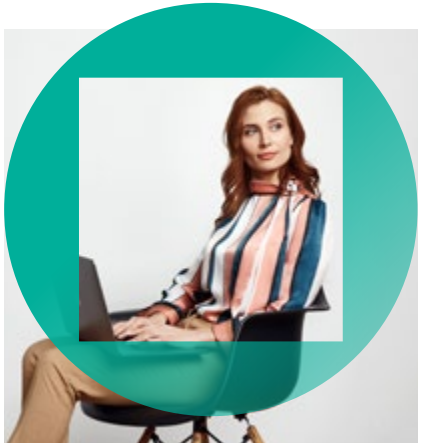
Après avoir déployé la passerelle d'accès sécurisé au web (SWG), ESB a commencé à déployer Forcepoint CASB pour avoir plus de visibilité et de contrôle sur les applications cloud utilisées par ses employés, tout en permettant à son personnel d'accéder de manière sécurisée aux outils dont il a besoin pour faire son travail.

Forcepoint CASB protège les applications cloud autorisées par ESB contre la perte de données et accélère l'utilisation des systèmes CRM modernes, comme Salesforce, grâce à une meilleure sécurité des données et des utilisateurs. La combinaison de CASB et de SWG garantit également que même les applications cloud non autorisées, ou « Shadow IT », peuvent être sécurisées sans être nécessairement bloquées.

« L'intégration entre Forcepoint SWG et Forcepoint CASB a été d'un grand avantage pour ESB. Comme les deux systèmes sont reliés et gérés par une interface commune, ESB obtient toutes les informations dont il a besoin en un seul endroit, avec une visibilité globale », a déclaré Brian Barry, directeur national de Forcepoint.

En fin de compte, le déploiement de Forcepoint CASB par ESB a permis à ses employés d'utiliser davantage le cloud avec moins de risques – ce qui signifie que les employés sont habilités à expérimenter de nouvelles applications cloud de manière sécurisée, en accédant en toute sécurité à de nouveaux outils qui peuvent apporter des gains de productivité et améliorer l'activité.

La prochaine étape de la transformation d'ESB en matière de cybersécurité consistera à déployer davantage de technologies Forcepoint Edge Advantage, comme les NGFW avec SD-WAN, a déclaré M. Barry. La plateforme de solution complète est maintenant disponible pour ESB, et elle peut être activée selon les besoins pour soutenir des initiatives telles que la mise en réseau plus rapide de nouveaux bureaux distants, la sécurisation des travailleurs à distance et l'introduction prévue d'une nouvelle base de données principale sur le cloud.



À l'avenir, ESB envisagera également d'utiliser les solutions Forcepoint pour ses besoins en sécurité pour ses technologies opérationnelles, en plus de sa sécurité informatique. L'un des principaux défis auxquels sont confrontés les organismes chargés des infrastructures critiques est de maintenir une visibilité unifiée dans l'ensemble de la couche informatique (couche IT) et la couche opérationnelle (couche OT). Forcepoint est l'un des rares prestataires en cybersécurité ayant la capacité éprouvée et le portefeuille de produits nécessaires pour combler cette lacune – par exemple, en déployant Forcepoint NGFW et Forcepoint Data Guard pour sécuriser le flux de trafic au-dessus et en dessous de la zone industrielle, en permettant une visibilité à travers la couche IT/OT complète, en permettant le mouvement sécurisé des données entre des systèmes IT et OT physiquement séparés, et en réduisant considérablement le risque de compromission de part et d'autre.

Un nouveau modèle de sécurité pour une nouvelle façon de travailler

ESB a constaté des avantages concrets de son partenariat avec Forcepoint et en attend d'autres, a déclaré M. Madden.

« Dans le contexte de ce que nous faisons – la production, le transport et la distribution d'électricité – l'utilisation d'Internet dans le travail quotidien de nos employés est un service essentiel pour nous et pour nos clients. Lorsque nous nous sommes engagés pour la première fois avec Forcepoint, nous voulions un système hautement disponible, car la solution proxy précédente connaissait des pannes environ dix fois par an », a-t-il déclaré.

« Nous n'avons pas eu une seule panne spécifiquement liée au proxy lui-même depuis que nous sommes passés à une solution plus robuste en 2016. »

« Nous n'avons pas eu une seule panne spécifiquement liée au proxy lui-même depuis que nous sommes passés à une solution plus robuste en 2016. »

CHRIS MADDEN, RESPONSABLE DE L'INGÉNIERIE EN CYBERSÉCURITÉ CHEZ ESB

Madden pense que Forcepoint et ESB sont fortement alignés sur la stratégie de cybersécurité qui va se poursuivre. Cette synergie, ainsi que la feuille de route technologique et les services d'entreprise de Forcepoint, continuera à inspirer la planification à long terme d'ESB, a-t-il déclaré.

« Les solutions de Forcepoint sont très importantes pour notre planification », a déclaré M. Madden. « Nous voulons bénéficier de tous les avantages qui découlent de la mobilité, de la collaboration et du cloud, ce qui signifie que nous devons envisager un modèle de sécurité différent pour la manière dont nous fournissons l'accès à Internet et au cloud et dont nous sécurisons le réseau. L'approche traditionnelle "château, douve et pont-levis" en matière de sécurité est obsolète.

Aujourd'hui, le périmètre est l'endroit où vos gens accèdent depuis le monde entier, et c'est là que se trouve la sécurité. La sécurité est dans votre identité, la sécurité est dans votre appareil, la sécurité est dans les données elles-mêmes. Nous voulons faire appliquer cette approche dans toute notre entreprise. »

Résultats

- Réduction à zéro des interruptions de service mensuelles d'accès à Internet
- Apport de contrôle et de visibilité sur l'utilisation du cloud par les employés.
- Mise en place d'une fondation pour le déploiement du réseau SASE, de solutions de sécurité des données dans le cloud, pour suivre un calendrier quinquennal de transformation numérique.

Forcepoint