L'entreprise en communication britannique Communisis s'appuie sur Forcepoint pour protéger les données à caractère personnel pour le compte de ses clients des secteurs de la finance, des assurances, des services et du gouvernement

Cette agence de marketing et de communication a fait confiance à Forcepoint pour sécuriser sa transformation numérique tout en offrant une sécurité flexible, afin de maintenir la productivité et la sécurité des communications entre son équipe créative et ses clients finaux.

Communisis fournit des services de communication et de gestion d'impression à certaines des plus grandes agences gouvernementales, sociétés de services financiers et compagnies d'assurance du Royaume-Uni, ainsi que des services de création et de marketing sur point de vente pour de grandes marques mondiales.Ces missions exigent les meilleures solutions de cybersécurité pour garder en sécurité les données, le Web, le courrier électronique et le cloud. Depuis des années, Communisis fait confiance à Forcepoint Web Security, Email Security et DLP pour préserver la sécurité de ses collaborateurs et ses données. Récemment, la société a décidé de rehausser d'un cran son dispositif de sécurité avec Forcepoint Dynamic Data Protection, pour adapter les systèmes de défense des données aux risques encourus, et d'utiliser un CASB pour gagner en visibilité sur l'utilisation du cloud – pour mieux aligner sa stratégie de sécurité sur son parcours de transformation numérique.

PROFIL CLIENT :
Marketing et communication transactionnelle d'entreprise, agence de création et déploiement sur le point de vente.

SECTEUR :
Marketing & Communication

SIÈGE SOCIAL :
Royaume-Uni

PRODUITS :
- Forcepoint Web Security
- Forcepoint Email Security
- Forcepoint DLP
- Forcepoint DDP
- Forcepoint CASB

Les relevés bancaires, les documents d'assurance, les factures de cartes de crédit et les déclarations d'impôts sont un élément de base de notre vie financière quotidienne. Ces documents sont essentiels pour la communication entre les services financiers et les organismes gouvernementaux avec leurs clients respectifs. Autrefois, ces documents papier faisaient partie du courrier quotidien, mais aujourd'hui, même les organisations les plus traditionnelles communiquent avec leurs clients par le canal qui correspond le mieux à leurs besoins, qu'il s'agisse d'une enveloppe livrée dans une boîte aux lettres à domicile ou d'une communication numérique par courrier électronique, ou via un portail en ligne. L'agence britannique de marketing et de communication Communisis aide les plus grandes banques, compagnies d'assurance et services publics britanniques, tels que British Gas, à fournir ces communications individuelles de manière efficace et sécurisée.

Faisant partie du groupe américain OSG et ayant son siège à Londres, Communisis regroupe environ 1 500 employés, au service de clients répartis dans toute l'Europe. Une partie de ses activités se concentre sur la conception, la création et la fourniture de ces communications essentielles aux clients par le biais de multiples canaux. Une deuxième partie crée et diffuse des communications de marque individuelles couvrant tous les secteurs, tous les canaux et toutes les zones géographiques pour de grandes marques mondiales. Les deux parties de l'entreprise ont besoin de la cybersécurité la plus efficace qui soit pour sécuriser à la fois les Informations d'Identification Personnelles des clients finaux et leurs propriétés intellectuelles, mais les deux parties diffèrent considérablement, de sorte qu'une sécurité souple et basée sur le risque est essentielle.

« Le travail que nous faisons pour nos clients signifie qu'un très grand nombre de données personnelles circulent sur notre réseau. Nous devons nous assurer que ces informations sont sécurisées. Nous devons également protéger, par exemple, un document marketing exclusif qu'une grande marque est sur le point de publier », a déclaré Michelle Griffey, Chief Risk Officer de Communisis. « Au cours des dix dernières années, Communisis a renforcé son expertise et la confiance de ses clients dans la sécurité de leurs informations. C'est essentiel pour notre activité. »

Passer au cloud nécessite un certain sens de l'équilibre, mais présente aussi de grands avantages, tant pour les clients que pour les consommateurs finaux

Récemment, Communisis a commencé à franchir le pas de la transformation numérique en migrant une partie de ses activités et de ses données dans le cloud, où cela peut se faire en toute sécurité.

« C'est un équilibre délicat, car nous avons des exigences contractuelles avec un client qui peut lui-même aller dans le cloud, mais qui peut être un peu plus réticent à permettre à un fournisseur de le faire, car il y a un élément de risque en termes de contrôle », a déclaré Michelle Griffey. « Cela signifie simplement que nous devons être prudents et prendre cette décision en restant vigilants, tant en ce qui concerne les exigences de nos clients que sur nos propres besoins et notre propre sécurité."

Ces clients et leurs clients finaux sont également les moteurs de cette évolution. « Historiquement, les relevés bancaires ou les relevés de cartes de crédit ont été livrés sous forme imprimée, mais beaucoup de ces entreprises souhaiteraient idéalement que leurs clients examinent les documents en ligne pour un certain nombre de raisons », a expliqué Michelle Griffey.

« Avoir un partenaire qui peut produire des communications par n'importe quel canal souhaité par le client final est d'une importance capitale pour nos clients. Si une personne appelle sa compagnie d'assurance pour modifier sa police, elle peut demander une confirmation par le canal qu'elle préfère : papier, courrier électronique, etc. Nous pouvons l'envoyer par courriel, et si le courriel nous est renvoyé pour une raison quelconque, nous en serons informés et nous lancerons un envoi par courrier imprimé traditionnel. Cela permet de s'assurer que nos clients respectent leurs exigences réglementaires. »

La COVID-19 a accéléré ce passage à l'offre de services plus innovants pour Communisis. Comme les clients peuvent ne pas être en mesure de produire des documents à partir de plusieurs bureaux répartis sur plusieurs sites, étant donné que de plus en plus d'employés travaillent à domicile en raison des fermetures, la société a récemment commencé à offrir un service de courrier hybride. Il est ainsi possible de regrouper tous les documents de plusieurs employés sous une même désignation, de les regrouper et de les envoyer soit à des centres d'impression, soit par courrier électronique, ce qui évite à un employé de devoir aller les chercher sur une imprimante de bureau.

Défis

Fournir une cybersécurité souple pour protéger les deux facettes de l'entreprise.

Veiller à ce que les données personnelles sensibles du client final soient en sécurité afin de conserver sa confiance.

Prendre en charge la transformation numérique et le passage au cloud.

Approche

Ajouter Forcepoint DDP et CASB à l'infrastructure de sécurité existante.

Résultats

Permettre la productivité créative d'un côté de l'entreprise tout en protégeant les données personnelles sensibles de l'autre.

Construire un partenariat solide pour relever les défis de la cybersécurité.

Le CASB et la protection dynamique des données offrent plus de visibilité et de flexibilité pour faire fonctionner ensemble les deux parties de l'entreprise

Depuis plusieurs années, l'agence s'appuie sur Forcepoint Web, Email et DLP pour sécuriser le trafic Web, les communications par courriel, ainsi qu'assurer la visibilité et le contrôle des données. Mais le passage à des services davantage basés sur le cloud a donné une nouvelle orientation à la stratégie de sécurité de Communisis. La société a décidé d'étendre sa relation avec Forcepoint en ajoutant Forcepoint Cloud Access Security Broker (CASB) et Dynamic Data Protection (DDP) à sa sécurité.

« Il est essentiel pour nous que le CASB commence à travailler stratégiquement sur la manière dont nous pouvons protéger ce futur monde dominé par le cloud, qui est notre destination commune », a déclaré Michelle Griffey. Et Forcepoint DDP a la capacité de fournir une posture de sécurité plus flexible, ce qui est très utile lorsque les deux parties de l'entreprise exigent deux approches très différentes de la sécurité des données.

« C'est presque comme s'il y avait une échelle variable des besoins en matière de sécurité », a déclaré Michelle Griffey. « La création d'une nouvelle publicité ou d'une campagne marketing est tout aussi importante pour ce client que les cent mille dossiers personnels individuels appartenant à une banque. Mais ces documents nécessitent un niveau de protection différent, car les détails que vous pourriez trouver dans un relevé bancaire, et qui concernent votre salaire, votre prêt immobilier, vos habitudes de dépenses, vos coordonnées bancaires et l'endroit où vous vivez, peuvent être vraiment très dangereux s'ils se retrouvent entre de mauvaises mains. Ainsi, la protection de ces données doit naturellement se placer plus haut sur cette échelle variable. »

« Je trouve DDP incroyablement séduisant, en raison du fait que nous pouvons désormais commencer à cibler beaucoup plus précisément notre sécurité. »

MICHELLE GRIFFEY, CHIEF RISK OFFICER, COMMUNISIS

« Je trouve DDP incroyablement séduisant, en raison du fait que nous pouvons désormais commencer à cibler beaucoup plus précisément notre sécurité, plutôt que de dresser un mur et dire : « Nous n'allons laisser personne faire quoi que ce soit » », a déclaré Michelle Griffey. « Nous pouvons faire la différence entre le côté communication individuelle, qui exige un niveau de sécurité plus élevé, et le côté marketing individuel, où nos salariés qui travaillent de manière créative ont besoin de plus de liberté pour collaborer. Et je pense que cela va nous permettre de faire mieux travailler nos équipes, à leur propre rythme, avec leur propre style. »

Gagner la même guerre dans le monde cybernétique – où les gens sont le plus en danger, et où ils sont la plus grande opportunité

Forcepoint et Communisis ont travaillé en étroite collaboration pour surmonter tous les obstacles et les difficultés, au point que Communisis envisageait d'ajouter un CASB et d'étudier les possibilités offertes par DDP. La collaboration établie avec Forcepoint leur a donné la confiance nécessaire pour passer à ces solutions et, en même temps, mettre à niveau leur dispositif de soutien.

« Au cours des derniers mois, nous avons eu une réelle opportunité de travailler directement avec Forcepoint pour aplanir les difficultés de notre environnement, et pour discuter de la manière dont nous pouvons apporter des améliorations continues », a déclaré David Perkins, responsable Information Assurance chez Communisis. « D'après l'ensemble des équipes chargées de la sécurité de l'information et des technologies de l'information, nous pensons avoir trouvé nos meilleures solutions. »

« Je vois cela comme un partenariat », a déclaré Michelle Griffey. « Je pense que nous pouvons travailler ensemble lorsque nous avons un défi de mise en œuvre unique à relever pour trouver une solution. Et ensuite, nous pouvons transmettre ces informations à Forcepoint pour qu'ils les partagent avec leurs autres clients. Je peux parier que si nous avons ce problème, d'autres clients l'ont probablement aussi. En fin de compte, on en profite et d'autres clients de Forcepoint en profiteront également. »

« C'est pourquoi il est important que nous travaillions en partenariat avec des sociétés de sécurité comme Forcepoint. En fait, nous menons tous un même combat dans le cyber espace », a déclaré Michelle Griffey. « Et l'approche de la cybersécurité de Forcepoint, centrée sur le facteur humain, est essentielle, car en fin de compte, ce sont les personnes qui vont potentiellement poser les plus grands risques, mais elles sont aussi notre plus grande chance pour nous protéger. »

« Ce sont les personnes qui vont potentiellement poser les plus grands risques, mais elles sont aussi notre plus grande chance pour nous protéger. »

MICHELLE GRIFFEY
CHIEF RISK OFFICER, COMMUNISIS