corero [THE DDoS PROTECTION SPECIALISTS] blue.

BLUE

ÉTUDE DE CAS _

Blue assure un service et une disponibilité optimale grâce à Corero SmartWall One

A propos

Fondé en 2005, Blue (ex-Bretagne Télécom) est un fournisseur de services cloud qui propose une large gamme de solutions performantes: réseaux internet à très haut débit, réseaux privés, externalisation des systèmes d'information, cybersécurité, etc. L'entreprise est présente dans huit centres de données interconnectés en France ainsi que dans son propre centre de données certifié ISO 27001. Avec 5 000 serveurs cloud, Blue accompagne les directeurs des systèmes d'information de plus de 2 500 PME et grands groupes technologiques en France. https://www.bt-blue.com/

Le défi

Blue avait besoin de prévenir les attaques DDoS à la fois pour ses propres systèmes et pour les réseaux de ses clients. Bien que la société subisse moins de 10 attaques par semaine et que ces attaques ne durent généralement que quelques minutes, ne saturent pas les liens du réseau, elles provoquent parfois des problèmes de latence ou des interruptions de service pour leurs clients. Blue voulait s'assurer que ses clients bénéficient d´un niveau de service optimal à tout moment.

"Notre réseau est relativement propre car nous ne desservons que des entreprises et des services informatiques", explique Nicolas Turpault, directeur de l'infrastructure chez Blue. Pourtant, explique M. Turpault, lorsqu'une IP publique sur une connexion à bas débit était attaquée, elle devenait inutilisable. Cela entraînait des demandes d'assistance de la part des clients et du stress pour l'équipe de sécurité informatique.

Pourquoi ils ont choisi Corero

Blue souhaitait mettre en place une protection DDoS pour tous ses liens réseau, mais ne voulait pas dépendre de ses fournisseurs de transit pour la protection DDoS. L'entreprise souhaitait également une mise en œuvre simple, une assistance et une maintenance fiables afin de pouvoir se concentrer sur ses principaux objectifs commerciaux.

Blue a examiné plusieurs fournisseurs de solutions d'atténuation des attaques DDoS et a finalement choisi la plateforme Corero SmartWall One en raison de ses fortes capacités dans ces domaines.

> “Corero a gagné notre confiance parce que leur solution était simple à mettre en œuvre et que le contrat d'assistance et maintenance garantissait que presque tout était fait par Corero.”
>
> **- M. Turpault, Directeur de l'infrastructure, Blue.**

Le déploiement

Blue utilise la solution Corero SmartWall en mode de protection en ligne. Cela signifie que tout le trafic entrant du côté internet est inspecté par Corero.

Souvent considérée comme la méthode la plus simple de défense contre les attaques DDoS, la protection en ligne est rapide et automatique. Plus précisément, le déploiement de Corero positionne des dispositifs matériels directement sur le chemin entre l'Internet au sens large et les routeurs de Blue. Ces dispositifs de protection bloquent ensuite tout trafic DDoS avant qu'il n'atteigne Blue et ses clients, garantissant ainsi que seul le trafic légitime arrive sur leur réseau.

L'approche en ligne présente l'avantage d'offrir la détection et la correction les plus rapides et d'être très simple à mettre en œuvre. Toutefois, elle nécessite un dispositif sur chaque routeur périphérique. Par conséquent, à mesure que Blue poursuit sa croissance et que ses volumes de trafic continuent d'augmenter, elle prévoit de passer à un modèle d'épuration pour une meilleure évolution.

Heureusement, l'un des principaux avantages de la plateforme Corero SmartWall est la flexibilité qu'elle offre pour répondre aux besoins spécifiques des clients. Notre conception modulaire et flexible permet aux clients de choisir parmi de nombreuses options - y compris en ligne, datapath, edge et scrubbing - afin qu'ils puissent personnaliser leur protection DDoS en fonction de leur secteur d'activité et de leur environnement commercial.

Résultats

Protection efficace et tranquillité d'esprit

De nombreuses solutions DDoS sont exclusivement réactives, ce qui signifie qu'elles ne commencent à fonctionner que lorsqu'une attaque DDoS a déjà touché sa victime. Avec la solution SmartWall de Corero, les attaques sont prévenues de manière proactive avant qu'elles ne causent des dommages au réseau de Blue ou à ses clients en aval.

Avant que Blue ne mette en œuvre Corero, une IP publique sur une connexion à bas débit devenait inutilisable en cas d'attaque DDoS. Aujourd'hui, selon l'entreprise, tout fonctionne - un résultat qui a apporté à Blue une grande tranquillité d'esprit.

> “Aujourd'hui, nous n'avons plus de tickets de support client liés à des problèmes de DDoS, et nous pouvons plus facilement respecter nos accords de niveau de service (SLA)”
>
> **- M. Turpault, Directeur de l'infrastructure, Blue.**

Configuration simple

Blue recherchait une mise en œuvre facile avec une gestion minimale. La protection DDoS de Corero s'intègre à l'infrastructure réseau existante des clients et contient les informations les plus récentes sur les menaces DDoS pour une détection et une protection immédiates des attaques, de sorte que Blue n'a eu que très peu de configuration à effectuer.

M. Turpault confirme qu'il s'agit là d'un avantage pour l'entreprise: "Les règles par défaut intégrées dans Corero sont très pratiques et utiles, bloquant efficacement et facilement la majorité des attaques DDoS, sans configuration particulière."

Meilleure visibilité des attaques

Blue a noté que l'une des fonctions les plus utiles de Corero est son tableau de bord SmartWall personnalisable. Ce tableau de bord offre des preuves médico-légales avant, pendant et après les attaques, y compris des détails granulaires tels que les types d'attaques DDoS tentées et comment et quand elles sont bloquées. En obtenant une visibilité sur les dernières attaques et le trafic bloqué sur son réseau, Blue est en mesure de mieux comprendre les menaces DDoS auxquelles elle est confrontée et est bien préparée à se défendre contre les attaques futures.

Service à valeur ajoutée

Tous les clients de Blue sont automatiquement protégés par le SmartWall de Corero, puisque l'entreprise a choisi d'offrir la protection DDoS comme un service à valeur ajoutée afin de garantir une performance optimale et une disponibilité maximale. Le résultat est l'assurance de conditions opérationnelles pour l'ensemble de l'infrastructure de Blue.

Excellent service client

Un autre facteur clé pour Blue a été le service de support client personnel et réactif de Corero. Ce service combine l'expertise des analystes du centre d'opérations de sécurité (SOC) et des informations de pointe sur les menaces. Corero comprend l'importance de fournir des réponses rapides et utiles pendant et après les attaques. L´équipe du SOC se tient également en état de veille permanente, et est au fait des nouvelles menaces DDoS ce qui permet le blocage préventif des vecteurs d'attaque nouveaux et de type "zero-day" lorsque cela s'avère necessaire.

Points forts de la solution Corero SmartWall One

- Supprime automatiquement et chirurgicalement le trafic des attaques DDoS avant qu'il n'atteigne les systèmes critiques, éliminant ainsi les temps d'arrêt et garantissant des performances optimales et une disponibilité maximale.
- Atténue l'impact d'un large éventail d'attaques DDoS, des simples inondations volumétriques aux attaques sophistiquées d'épuisement de l'état, aux couches 3 à 7.
- Offre une protection contre les attaques DDoS en ligne, de 1 Gbps à 100 Gbps par unité de rack, dans une solution qui évolue vers des térabits par seconde de débit protégé.
- Fournit une analyse complète au niveau médico-légal avant, pendant et après les attaques.
- Il garantit que le trafic légitime n'est pas affecté par les faux positifs.
- Inspecte chaque en-tête de paquet entrant et les données utiles, éliminant chirurgicalement les paquets DDoS sans perturber l'acheminement du trafic réseau légitime.
- Répond rapidement aux attaques DDoS complexes et évolutives en ajustant et en déployant automatiquement des "règles intelligentes" en fonction des besoins.
- Détecte et atténue le trafic d'attaque en moins d'une seconde, au lieu des minutes ou des dizaines de minutes requises par les solutions traditionnelles de défense contre les attaques DDoS.

A propos de Corero Network Security

Corero Network Security est un fournisseur de premier plan de solutions de protection contre les attaques DDoS, spécialisé dans les solutions de détection et de protection automatiques avec visibilité du réseau, outils d'analyse et de reporting. La technologie de Corero protège contre les menaces DDoS externes et internes dans des environnements complexes de périphérie et d'abonnés, garantissant ainsi la disponibilité des services Internet. Avec des centres opérationnels à Marlborough (Massachusetts, États-Unis) et à Édimbourg (Royaume-Uni), Corero a son siège à Londres et est cotée sur le marché AIM de la Bourse de Londres (ticker: CNS). Visitez www.corero.com et suivez-nous sur LinkedIn et Twitter.