infoblox

ÉTUDE DE CAS

Stupp Bros. renforce sa sécurité avec Infoblox Threat Defense™

VUE D'ENSEMBLE

Basé à Saint-Louis, Missouri, Stupp Bros. est un fournisseur de premier plan de matériaux et de services indispensables à la construction d'infrastructures critiques aux États-Unis.

L'entreprise fabrique des charpentes métalliques utilisées dans la construction de ponts, gratte-ciel, hôpitaux, centres de congrès, stades sportifs et lieux de divertissement à travers le pays. En plus de son activité principale, Stupp Bros. propose une gamme de services, notamment des services bancaires régionaux, la capture de données permettant aux secteurs à forte charge opérationnelle de rester conformes, ainsi que des services haut débit pour les particuliers comme pour les entreprises.

> *"Threat Defense est le fossé qui entoure notre château. Il faudra le franchir avant de pouvoir causer le moindre dommage aux murs extérieurs."*
>
> **John Roosa,**
> **Directeur des systèmes d'information, Stupp Bros.**

LA SITUATION

Adopter une stratégie de défense en profondeur

Fondée il y a plus de 165 ans, Stupp Bros. s'est principalement concentré sur l'amélioration des méthodes de fabrication et l'expansion des marchés pour ses matériaux de construction de haute qualité. Cependant, avec la numérisation croissante de ses activités ces dernières décennies, la cybersécurité figure désormais parmi ses principales priorités.

Au milieu des années 1990, John Roosa, alors consultant, aidait l'entreprise à optimiser son réseau à l'aube d'Internet lorsque le virus Melissa a frappé. « Ça a été mon signal d'alarme », dit-il. Cet incident de 1997 lui a montré à quel point l'environnement de la sécurité avait radicalement changé et à quel point les réseaux informatiques n'étaient pas préparés à cette nouvelle réalité.

Depuis, M. Roosa est devenu un ardent défenseur d'une approche holistique de la cybersécurité. En tant que DSI chez Stupp Bros. depuis 18 ans, il a supervisé la mise en place d'une stratégie de défense en profondeur visant à protéger l'entreprise et ses plus de 350 employés contre les menaces actuelles.

STUPP BROS., INC.
ESTABLISHED 1856 | ST. LOUIS, MISSOURI

Pour atteindre ces objectifs, M. Roosa et ses collègues ont déployé une architecture de sécurité intégrant des pare-feux nouvelle génération (NGFW) et d'autres solutions de protection des endpoints, soutenue par Microsoft Sentinel, la plateforme de gestion des événements et des informations de sécurité (SIEM) de Microsoft, ainsi que par des outils complémentaires.

Bien que ces déploiements aient été globalement efficaces, ils n'ont pas permis de résoudre adéquatement un problème de sécurité majeur : les employés adoptant involontairement des comportements risqués en ligne.

LE DÉFI

Là où vont les internautes, les menaces suivent

Selon M. Roosa, les défis liés au comportement des utilisateurs ont fortement évolué depuis qu'il est devenu DSI en 2007. « C'était bien plus simple à l'époque. Les risques n'étaient pas aussi complexes. » À l'époque, les utilisateurs disposaient de moins d'appareils, les applications professionnelles s'exécutaient principalement sur des ordinateurs de bureau, et la technologie cloud venait à peine de naître. Même si le risque lié aux employés existait déjà, « il était alors plus facile à atténuer du point de vue des technologies de l'information qu'aujourd'hui », souligne M. Roosa.

Aujourd'hui, tous les employés de Stupp Bros. disposent de smartphones ou d'autres appareils qui leur offrent un accès internet instantané où qu'ils aillent. De plus en plus, une grande partie du travail consacré à la fabrication moderne de l'acier, à la construction et aux services haut débit par fibre optique dépend des e-mails, des SMS, ainsi que de l'accès aux applications et ressources cloud.

Cependant, avec autant de moyens de se connecter, il est devenu de plus en plus difficile pour M. Roosa et son équipe de contrôler où vont les employés en ligne et ce qu'ils y font. Contrairement aux grandes entreprises, Stupp Bros. ne dispose pas des ressources nécessaires pour fournir à chaque employé des appareils verrouillés ou des postes de travail entièrement gérés. Par conséquent, certains employés cliquaient parfois sur des liens de phishing ou visitaient des sites contenant des bannières publicitaires douteuses, les redirigeant vers des destinations malveillantes sur Internet, voire déclenchant le téléchargement de malwares.

Pour John, la formation des employés était cruciale pour atténuer ces risques. Dans l'ensemble, ces efforts se sont révélés très efficaces, mais pas toujours suffisamment réactifs. Par exemple, les alertes de sécurité ont augmenté lorsque Stupp Bros. a acquis une nouvelle unité commerciale avant que ses employés n'aient reçu la formation de sécurité adéquate.

Il était déterminé à prévenir ces situations à l'avenir. Mais même les utilisateurs les plus avertis peuvent être victimes de contenus en ligne malveillants astucieusement déguisés en contenus légitimes. Inévitablement, les alertes de notification de virus ont atteint les NGFW et autres outils de sécurité des terminaux chez Stupp Bros., incitant les équipes de sécurité à passer des heures à enquêter et à y remédier.

Pour relever ce défi, Stupp Bros. avait besoin d'une solution complète qui réduirait les risques associés aux activités en ligne non sécurisées tout en renforçant sa posture de sécurité avec un impact minimal sur les employés et le personnel de sécurité.

LA SOLUTION

Exploiter le pouvoir proactif du DNS pour renforcer la sécurité

Roosa a reconnu que le meilleur moyen d'empêcher les employés de cliquer sur des liens dangereux était de les en empêcher dès le départ. En conséquence, Stupp Bros. a déployé une série de produits de filtrage du web, qui ont tous débouché sur des résultats insatisfaisants. « C'était des produits classiques, du type : "autoriser tel sujet, interdire tel autre" » , explique M. Roosa.

Client : ***Stupp Bros.***
Secteur : ***Construction***
Lieu : ***Saint-Louis, MO***

LES OBJECTIFS :

- Atténuer les risques associés aux comportements en ligne non sécurisés
- Optimiser la gestion du filtrage web pour réduire les efforts manuels
- Réduire le volume des alertes de virus et le temps nécessaire pour les résoudre

LES RÉSULTATS :

- Déploiement en 15 minutes de la solution de sécurité DNS basée sur le cloud
- Blocage proactif des interactions numériques malveillantes sur l'ensemble du réseau
- Élimination quasi totale des alertes de virus, réduisant considérablement le bruit lié aux alertes
- Réduction de 50 % du temps moyen pour enquêter sur les menaces

LE PRODUIT :

- Infoblox Threat Defense™

Ces solutions obligeaient également John et son équipe à identifier manuellement les sujets et destinations web à bloquer, une tâche chronophage qui demandait des recherches approfondies et une configuration permanente. Cependant, le plus grand inconvénient était le défaut de conception fondamental au cœur de ces outils de sélection. « Je n'aime vraiment pas travailler dans le domaine de la protection des internautes, car je sais comment fonctionne l'internet et combien il est facile de contourner un grand nombre de ces 'filtres' », explique John.

M. Roosa a découvert Infoblox alors qu'il recherchait des options de gestion DHCP pour la division Internet fibre optique de son entreprise. Au cours de ses recherches, il a découvert Infoblox Threat Defense™ et son approche innovante de la sécurité basée sur le DNS. « Infoblox a été une véritable révélation pour moi », explique-t-il. « Tout commence par le DNS. »

Avec Threat Defense, John s'est rendu compte qu'il pouvait « faire d'une pierre deux coups ». Tout d'abord, il a résolu le problème de la définition des destinations web malveillantes. Ensuite, parce qu'il opère au niveau du plan de contrôle DNS, il empêche complètement les utilisateurs d'accéder à ces sites, éliminant ainsi les solutions de contournement associées à d'autres options de filtrage. « C'est finalement devenu évident pour moi », poursuit M. Roosa. « Si je peux contrôler le DNS dans les recherches de noms, alors je peux arrêter une grande partie des activités malveillantes avant même qu'elle ne commencent. »

John et ses équipes ont facilement déployé la solution basée sur le cloud en seulement 15 minutes. La mise en œuvre a été fluide, transparente pour les utilisateurs finaux, et fonctionne sur toutes les infrastructures : sur site, hybrides et dans les environnements multicloud. Threat Defense protège tous les employés de Stupp Bros. sur le réseau, quel que soit leur emplacement ou leur appareil. Cela empêche de manière proactive les utilisateurs de communiquer avec des domaines web associés à des risques potentiels, notamment le téléchargement automatisé de malware et de virus, le vol d'informations d'identification et l'exfiltration de données, entre autres.

Les fonctionnalités avancées de filtrage Web au sein de Threat Defense sont hautement personnalisables. De plus, elles sont constamment mises à jour avec les derniers domaines affectés découverts par Infoblox Threat Intel, le groupe de recherche le plus important du secteur, qui se concentre sur les menaces émergentes basées sur le DNS. Ces renseignements sont complétés par des algorithmes basés sur l'IA pour exposer les indicateurs de menace dans les domaines que les autres méthodes de sécurité ne peuvent pas détecter.

Chez Stupp Bros, Threat Defense fonctionne parallèlement à d'autres déploiements de sécurité, notamment Microsoft Sentinel et des outils connexes, qui gèrent les dispositifs compromis et la remédiation. Alors que ces déploiements sont principalement de nature réactive, déclenchant des réponses uniquement après que les outils de sécurité des endpoints ont détecté une menace, Threat Defense empêche de manière proactive les menaces d'atteindre le réseau. Il s'agit d'une capacité essentielle que le DSI apprécie grandement. « Threat Defense est notre première ligne de défense pour tout », note John.

LES RÉSULTATS

Renforcer la posture de sécurité

Avec Threat Defense, Stupp Bros. a trouvé une solution efficace au problème de la protection des employés contre les menaces qui exploitent les interactions numériques modernes. En empêchant l'accès à des destinations web malveillantes sur le réseau, cette solution limite les comportements en ligne à risque. « Si Infoblox déclare qu'il ne s'agit pas d'un bon site, vous n'y allez pas », explique M. Roosa.

Les capacités de filtrage de la solution ne nécessitent aucune intervention de la part des employés. Cela rend également la tâche beaucoup plus simple pour John et son équipe lorsqu'il s'agit de déterminer quelles destinations constituent une menace, un avantage qu'il considère comme un argument de vente majeur. « Maintenant, je n'ai plus à m'inquiéter de ce que nous devrions bloquer. Threat Defense s'en charge. »

Comme Threat Defense arrête les menaces au niveau du plan de contrôle DNS, il a considérablement réduit la charge qui pesait sur les défenses périmétriques de Stupp Bros. Comme l'explique M. Roosa, « nous éliminons la majorité du trafic indésirable avant même qu'il ne nous atteigne. Cela génère beaucoup moins de bruit sur notre plateforme d'analyse. »

Cette réduction du bruit, combinée à un taux de faux positifs extrêmement faible de seulement 0,0002 %, permet aux équipes de sécurité de gérer un volume d'alertes nettement inférieur. Par exemple, depuis le déploiement de Threat Defense, les notifications de virus qui étaient autrefois courantes ont pratiquement disparu. Selon John, grâce à la réduction du volume d'alertes permise par Infoblox, ses équipes de sécurité ont réduit de moitié le temps consacré à l'analyse des menaces, leur permettant ainsi de se focaliser sur des initiatives stratégiques renforçant la posture globale de sécurité de l'organisation.

Threat Defense a également permis à John de gagner un temps précieux. Il est convaincu que les interactions risquées que la plateforme arrête sont basées sur les renseignements les plus récents du secteur concernant les menaces basées sur le DNS, qui évoluent rapidement. « C'est l'aspect le plus intéressant de ce produit », déclare-t-il. « Je peux honnêtement vous dire que je n'ai pas perdu de temps à le gérer, à m'en occuper, ou quoi que ce soit. »

En plus de tirer parti des capacités avancées de filtrage Web de Threat Defense, Stupp Bros. activera prochainement des fonctionnalités supplémentaires, à commencer par l'intégration des données Infoblox dans son écosystème de sécurité Microsoft. John prévoit que la télémétrie en temps réel des activités de menace liées au DNS de la solution améliorera considérablement les efforts de triage et de remédiation de l'organisation. « Nous serons en mesure de détecter beaucoup plus de choses avec la défense contre les menaces », ajoute-t-il.

De manière plus générale, John ne mâche pas ses mots pour résumer la valeur de son déploiement Infoblox : « Threat Defense est le fossé qui entoure notre château. Il faudra le franchir avant de pouvoir causer le moindre dommage aux murs extérieurs. Nous allons vous arrêter avant même que vous ne vous approchiez. »

infoblox.

Infoblox unifie réseau et sécurité pour offrir des performances et une protection inégalées. Reconnu par les entreprises listées au classement Fortune 100 et par des innovateurs émergents, nous assurons une visibilité et un contrôle en temps réel sur les utilisateurs et les appareils connectés au réseau, accélérant ainsi les opérations et neutralisant les menaces plus rapidement.

Siège social
2390 Mission College Boulevard,
Ste. 501 Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com/fr

Version : 20250620v1