LIVRE BLANC

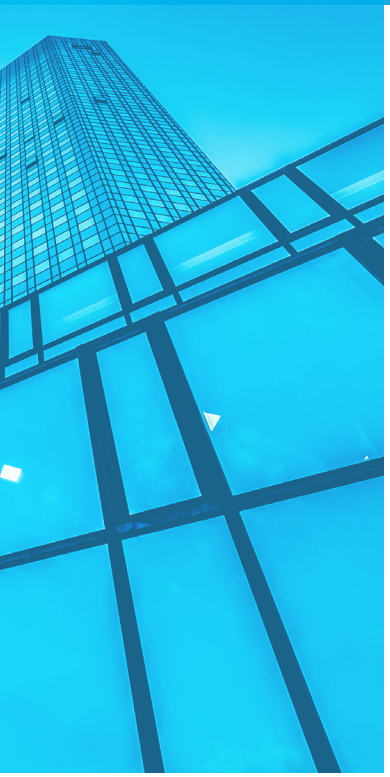
La sécurité à l'ère du télétravail

S'appuyer sur son infrastructure réseau

Avertissement

Les publications et les études Infoblox sont distribuées uniquement à des fins d'information générale. Les informations contenues dans la présente publication sont fournies en l'état. Infoblox n'endosse aucune responsabilité quant à l'utilisation de ces données. Tout développement ou toute recherche postérieurs à cette publication ne seront pas inclus dans le présent rapport.

Sommaire



« Le plus inquiétant, au cœur de cette crise sanitaire, est que la situation est encore aggravée par un nombre croissant d'escroqueries et de menaces de logiciels malveillants spécifiquement ciblés sur le COVID-19. Les attaques de phishing et les sites web liés au COVID-19 constituent des vecteurs d'attaque de plus en plus appréciés des cyberpirates qui profitent de la situation. Les recherches en Threat Intelligence ont définitivement montré que le courrier électronique portant des logiciels malveillants est l'un des vecteurs les plus utilisés pour lancer ces attaques ».

Anthony James, *vice-président marketing produit, Infoblox, Inc.*

Résumé

Suite à la pandémie de coronavirus, entreprises privées et publiques sont confrontées à des défis sans précédent. Nombre d'entre elles ont rapidement commencé à anticiper afin de permettre le télétravail de leurs collaborateurs.

Une enquête récente révèle qu'environ 44 % des consommateurs travaillant à plein temps ont déjà ressenti l'impact du coronavirus sur leur activité professionnelle, environ 55 % ont déjà annulé leurs projets de voyage et environ 40 % réduisent le nombre de réunions en face à face et augmentent l'utilisation des outils de vidéoconférence.[1]

Les télétravailleurs cherchent à accéder aux ressources de l'entreprise à partir de divers terminaux, qu'ils soient personnels ou fournis par l'entreprise, ainsi que de divers appareils mobiles. Bien entendu, le problème est que de nombreuses procédures de cybersécurité utilisées dans les entreprises ne fonctionneront pas à distance sans changement, sans préparation et sans planification d'envergure. Malheureusement, en raison de la brutalité de cette pandémie, les entreprises ont eu très peu de temps pour préparer et planifier les mesures de cybersécurité destinées à soutenir leurs effectifs, à distance et à grande échelle.

Tandis que les entreprises s'efforcent de répondre aux besoins de leurs nombreux collaborateurs, il est important de prendre en compte les risques liés aux connexions Wi-Fi grand public, aux partages de documents dans les dossiers cloud et aux navigateurs personnels configurés avec des plug-ins et des applications qui peuvent introduire un risque important. Les routeurs domestiques ne sont généralement pas sécurisés et ne présentent pas le niveau de correction préconisé par les fabricants. À la maison, les télétravailleurs ont tendance à consulter plus souvent qu'au bureau leur courrier électronique personnel et d'autres sites Web

1. Forbes.com. Remote Work Advocates Warn Companies About COVID-19 Work-From-Home Strategies (Les défenseurs du télétravail alertent les entreprises sur les stratégies dans le contexte du COVID-19). 5 mars 2020. https://www.forbes.com/sites/laurelfarrer/2020/03/05/ironically-remote-work-advocates-warn-companies-about-covid-19-work-from-home-strategies/#744aaae22051

non professionnels. Ces opérations ne font qu'augmenter la probabilité de rencontrer des « malvertisements » (publicités comportant des logiciels malveillants) qui risquent de porter préjudice à l'appareil d'un collaborateur et au final à l'entreprise. Par ailleurs, les pirates profitent de la soif générale d'information due à la gravité de la situation. Les collaborateurs peuvent facilement être victimes de liens comportant des logiciels malveillants dans les forums en ligne, sur les réseaux sociaux et via de petites publications issues de sites Web compromis. Ces problématiques resteront une menace constante, en particulier pour les utilisateurs distants.

Ce livre blanc aborde ces problématiques et propose des solutions permettant de renforcer rapidement la sécurité via des services réseau de base afin de répondre aux besoins de votre entreprise et de ses effectifs distants de plus en plus nombreux.

Les défis de sécurité liés au télétravail

En raison des récents risques sanitaires liés au coronavirus, les entreprises se sont mises à multiplier les environnements de travail à distance, sans réellement analyser ni évaluer les cybermenaces possibles dans le monde du télétravail. Aujourd'hui, les solutions de sécurité des entreprises sont surtout conçues pour protéger les données, les appareils, les ressources et les utilisateurs dans leur environnement de bureau ; elles ne sont pas optimisées pour fournir une protection identique aux télétravailleurs. Au vu des quarantaines à domicile imposées par le gouvernement, il est à présent évident que les entreprises ont aujourd'hui besoin d'une architecture de sécurité cohérente, conçue, déployée, gérée et appliquée de la même manière sur tous les segments du réseau.

La plupart des applications d'entreprise se trouvent dans le cloud et la plupart des utilisateurs n'ont plus besoin du VPN pour accéder aux applications et au courrier électronique de l'entreprise. Mais ces télétravailleurs continuent d'accéder aux données de l'entreprise et de les stocker sur leurs appareils ; ils doivent donc sécuriser leur activité Internet.

Les environnements de télétravail viennent également modifier le cadre de travail des équipes et ce changement répercuté sur le comportement peut entraîner divers problèmes, notamment des difficultés de communication, une baisse de productivité et l'exposition à de nombreux nouveaux risques de sécurité. Le télétravail expose également à une surface d'attaque beaucoup plus large puisque les travailleurs utilisent à la maison leurs propres appareils (BYOD) et des appareils mobiles qui partagent les réseaux Wi-Fi domestiques et publics, souvent avec une palette d'appareils IoT (Internet of Things) beaucoup plus vaste que celle de l'environnement de travail. Les réseaux Wi-Fi publics sont plus susceptibles d'être victimes d'un problème accidentel d'authentification et d'identifiants. Ces utilisateurs se trouvent largement hors de la portée des contrôles de périmètre et risquent encore davantage d'être compromis par des attaques de logiciels malveillants.

Bien entendu, les télétravailleurs ne disposent souvent pas du même niveau de sophistication qu'au bureau pour se protéger, par exemple les pare-feux nouvelle génération, la détection des intrusions, la technologie de tromperie et les contrôles de sécurité basés sur l'apprentissage automatique.

Des renseignements sur des menaces ciblées

Les cyberattaques sur le thème du coronavirus profitent déjà des bouleversements qui touchent l'environnement de travail. Le COVID-19 est devenu la grande tendance chez les cybercriminels qui cherchent à tirer profit des télétravailleurs loin de l'entreprise, lesquels sont déjà passablement inquiets.

Au cours de la première semaine de mars, notre équipe de Threat Intelligence a constaté que LokiBot Infostealer avait rejoint la liste des campagnes de logiciels malveillants diffusée par les cybercriminels exploitant la peur et la préoccupation liées à la propagation du coronavirus.2 Du 3 au 6 mars, nous avons observé deux campagnes e-mail de spam malveillant propageant LokiBot sous couvert de fournir des informations sur l'impact du coronavirus sur les chaînes logistiques.

LokiBot est devenu populaire auprès des cybercriminels en tant que renifleur d'informations cherchant à recueillir des identifiants et des jetons de sécurité sur les machines infectées. LokiBot cible de nombreuses applications, notamment, entre autres, Mozilla Firefox, Google Chrome, Thunderbird et FTP.

Les e-mails de la campagne principale avaient deux objets, dont l'un était censé être une mise à jour de la chaîne logistique dans le contexte du coronavirus (COVID-19). L'autre objet portait sur le thème plus classique du virement bancaire. Les deux séries de messages contenaient des fichiers joints portant le même nom que celui du code malveillant.

Protéger les télétravailleurs avec BloxOne™ Threat Defense

BloxOne Threat Defense protège les utilisateurs, les appareils et les systèmes des entreprises, où qu'ils se trouvent, en renforçant et en optimisant votre stratégie de sécurité dès le début. Notre architecture hybride unique permet d'étendre la protection à l'ensemble de vos locaux, de vos sites distants et de votre environnement de télétravail. Elle détecte et bloque le phishing, les exploits, les demandes de rançon et autres logiciels malveillants modernes, et elle empêche vos télétravailleurs d'accéder à des contenus répréhensibles exclus des règles de sécurité. Sa technologie brevetée unique empêche l'exfiltration des données DNS, ce qui permet de préserver la sécurité des données protégées, de surveiller les menaces avancées (notamment les Lookalike Domains) et d'automatiser la réponse aux incidents afin que votre écosystème de sécurité puisse rapidement réagir. Où que vous soyez et quoi que vous fassiez, les contrôles Infoblox appliquent les règles que vous avez définies et protègent vos utilisateurs en télétravail.

Grâce à l'utilisation du DNS comme point de contrôle essentiel, chaque requête Internet est inspectée afin de déterminer si elle est malveillante, tel qu'identifié par nos services intégrés de renseignements sur les menaces, d'analyse et d'apprentissage automatique. Le DNS vous permet également d'adapter le filtrage du Web et des contenus ainsi que de réduire les coûts généraux liés à la protection contre les menaces.

2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--62

Figure 1 : Vue d'ensemble de BloxOne Threat Defense et de ses composants de sécurité de base

Grâce au déploiement de BloxOne Threat Defense et aux capacités offertes par le cloud, les entreprises peuvent facilement étendre les avantages de cette protection à tous les utilisateurs, dans le monde entier, sans avoir à recourir aux VPN ou à d'autres techniques d'orientation du trafic. Le client BloxOne Threat Defense est à la fois léger et facile à déployer. Contrairement aux autres technologies client, BloxOne Threat Defense envoie uniquement des requêtes DNS pour inspection. Autrement dit, le trafic client va directement à l'application sans aucune latence supplémentaire. Les destinations malveillantes identifiées par les services de renseignements sur les menaces dans le cloud BloxOne Threat Defense sont immédiatement bloquées, ce qui permet d'éviter tout recours à d'autres logiciels de sécurité.

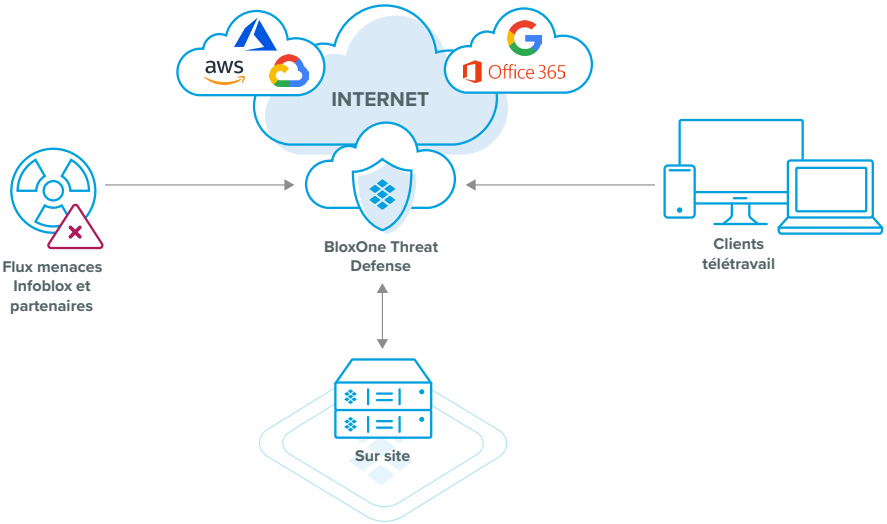


Figure 2 : BloxOne Threat Defense étend la protection aux télétravailleurs.

BloxOne Threat Defense fournit un point de contrôle et de visibilité architecturalement efficace et centralisé pour tout le trafic nécessitant une résolution des services DNS. Vous protégez votre marque en verrouillant vos réseaux et bénéficiez de la sécurité requise pour mettre en œuvre les composants stratégiques de la transformation numérique, tels que le cloud, le SD-WAN, les plateformes mobiles et une gigantesque toile d'appareils IoT. BloxOne permet également une intégration complète avec les solutions d'orchestration de la sécurité, d'automatisation et de réponse (SOAR), et réduit le temps nécessaire pour enquêter sur les menaces et y apporter une solution. BloxOne Threat Defense améliore les performances de tout votre écosystème de sécurité et réduit le coût total de possession consacré à la protection contre les menaces dans l'entreprise.

Aspects techniques importants

BloxOne Threat Defense est une solution de sécurité qui résout de manière unique un certain nombre de problèmes complexes pour tous les environnements, notamment la gestion des nombreux effectifs à distance. Elle offre une solution intégrée très économique permettant de protéger les utilisateurs, les applications et les données en utilisant le DNS comme première ligne de défense.

Lorsque BloxOne Threat Defense détecte les menaces de sécurité, et les fonctionnalités d'intégration permettent aux administrateurs de déclencher des actions supplémentaires, en toute transparence, à partir d'outils externes, afin de résoudre les problèmes affectant les systèmes des utilisateurs. Les API intégrées peuvent rapidement envoyer les données d'événements à ces outils de l'écosystème. Ces intégrations permettent d'automatiser les actions suivantes:

- analyse de vulnérabilité à distance
- analyse antivirus à distance
- protection contre les menaces récemment détectées pour tous les utilisateurs distants et les intégrations d'écosystèmes

Pour protéger des nouvelles menaces et des menaces en évolution, BloxOne Threat Defense utilise des analyses basées sur l'IA/ML sur DNS pour détecter des menaces qui ne peuvent pas l'être par d'autres moyens. Il s'agit notamment des Lookalike Domains, du tunneling DNS zero-day, des algorithmes de génération de domaines (DGA) et du Fast Flux. En outre, les nouvelles tendances en matière de protection de la vie privée, comme le DNS via TLS (DoT) et via HTTPS (DoH), ont des effets indésirables sur la sécurité. Le filtrage du contenu au point de contrôle DNS peut être une solution rentable, à faible latence, permettant d'empêcher les télétravailleurs d'accéder à des types spécifiques de contenus Web. Ces types de contenus sont présentés ci-dessous.

Lookalike Domains

Les cybercriminels qui souhaitent se faire passer pour l'entreprise ou la marque visée utilisent des Lookalike Domains qui dupent les victimes. Les sites de phishing proposent souvent des domaines qui imitent la véritable marque. Ces domaines sont créés de manière à ressembler à celui de la vraie marque.[3]

La substitution de caractères est une technique populaire employée par les cybercriminels. L'objectif est de manipuler les utilisateurs afin qu'ils révèlent leur numéro de carte de crédit, leur mot de passe et d'autres données sensibles. Les caractères comme le « 1 » peuvent être remplacés par un « l » (i majuscule). Il est possible de détecter de nombreuses substitutions mais nous avons tendance à voir ce que nous nous attendons à voir. Le seul fait de remplacer astucieusement un ou deux caractères dans votre URL permet de réaliser un grand nombre de tromperies. La substitution de plusieurs caractères permet également de détourner votre marque : par exemple, de nombreux clients se laisseront duper si la lettre « m » est remplacée par « rn ».

3. Info Security. Boom in Lookalike Retail Domains (Recrudescence des Lookalike Domains pour les marques de vente au détail). 14 novembre 2019. https://www.infosecurity-magazine.com/news/boom-in-lookalike-retail-domains/

« YAHOO » n'est pas la même chose que « YAHOO »

Mais plus de 136 000 caractères Unicode sont utilisés pour représenter les lettres et les symboles des noms de domaine courants, dans 139 écritures modernes et anciennes, comme le latin, le cyrillique, le grec, l'ukrainien et même le cherokee. Beaucoup de substitutions de caractères ont pu être détectées grâce à des analyses approfondies. Comme pour les illusions d'optique et les spectacles de magie, l'œil humain a toutefois tendance à voir ce que l'esprit attend. En naviguant sur le Web, peu d'utilisateurs remarqueront que « YAHOO » n'est pas la même chose que « YAHOO ».

Des chercheurs ont également constaté que les cybercriminels utilisent des certificats TLS (Transport Layer Security) valides pour tenter de faire ressembler les Lookalike Domains aux véritables domaines.

Fin 2019, ces chercheurs ont constaté que plus de 100 000 Lookalike Domains étaient travestis pour ressembler aux revendeurs légitimes. Le secteur de la vente au détail est dans la ligne de mire des agresseurs et subit de nombreuses attaques lorsque les cybercriminels tentent de dérober les données de carte de crédit des acheteurs. Des centaines de Lookalike Domains utilisés dans le cadre d'attaques de phishing ont également été récemment découverts dans le secteur bancaire canadien.[4]

Les attaques par Lookalike Domains se caractérisent par trois couches d'ingénierie sociale. Ces couches comprennent souvent les éléments suivants:

- **Contenu du site:** Le contenu d'un site peut être une copie modifiée d'un site Web légitime existant. Les cybercriminels mettront fréquemment à jour ce contenu au fil du temps afin d'améliorer l'efficacité de l'attaque
- **Chemin d'accès URL:** Pour que l'escroquerie paraisse solide, les attaquants doivent proposer un chemin d'accès crédible. Il peut ressembler à l'URL réelle ou être dissimulé d'une manière ou d'une autre.
- **Nom de domaine:** En général, les cybercriminels utilisent un nom de domaine créé pour paraître légitime en cas d'inspection rapide. Dans certains cas, des mots ou des caractères supplémentaires sont ajoutés. Dans d'autres, des caractères différents sont substitués, d'une autre langue ou d'une autre police ; ils peuvent quasi correspondre au caractère correct et sont difficiles à repérer si la lecture est rapide.

BloxOne Threat Defense Custom Lookalike Domain Monitoring vous permet de stopper de manière proactive les attaques d'ingénierie sociale par imitation. Vous pouvez soumettre à l'Infoblox Cyber Intelligence Unit (CIU) votre propre domaine ou des domaines fréquemment utilisés par votre entreprise. L'unité CIU analyse et identifie les Lookalike Domains suspectés et nécessitant une surveillance. Si ces Lookalike Domains génèrent une activité suspecte, votre entreprise reçoit rapidement une alerte pour toute activité susceptible de porter atteinte à la marque.

4. Bank Info Security. Phishing Scams Target Canadian Bank Customers (Les escroqueries par phishing ciblent les clients des banques canadiennes). 24 décembre 2019.
https://www.bankinfosecurity.com/phishing-scams-target-canadian-bank-customers-a-13551

Les télétravailleurs sont probablement actifs sur une combinaison d'appareils mobiles, de réseaux domestiques et de réseaux Wi-Fi publics et sont très probablement confrontés à des menaces d'imitation. Sans un contrôle de sécurité comme l'outil Custom Lookalike Domain Monitoring, il sera plus facile de cibler ces télétravailleurs, plus vulnérables face à ces attaques.

Algorithmes de génération de noms de domaine

Divers types de logiciels malveillants utilisent des algorithmes de génération de domaines (DGA) afin de générer méthodiquement des noms de domaines, ensuite utilisés pour faciliter la communication avec les serveurs de commande et de contrôle des cybercriminels. Les cybercriminels intègrent également les DGA directement dans les logiciels malveillants afin de générer la liste des domaines qu'ils peuvent utiliser pour la commande et le contrôle. Les DGA permettent aux attaquants de changer rapidement les domaines utilisés pour transporter les logiciels malveillants. Pendant que les systèmes de défense identifient et bloquent les domaines malveillants, les DGA permettent aux cybercriminels d'agir rapidement afin de bloquer ces actions.

L'apprentissage automatique fournit une nouvelle fonctionnalité permettant d'identifier et de bloquer les communications basées sur les DGA et présentant des risques pour votre entreprise. Infoblox Threat Insight utilise l'analyse de comportement pour classer les domaines DGA et les distinguer des domaines normaux. Grâce à des techniques telles que l'analyse de l'entropie, n-gramme, lexique et taille, Threat Insight permet d'identifier et de bloquer les DGA. Comme les DGA ne se résolvent généralement pas en adresses IP (Internet Protocol), ce comportement est également utilisé pour former les modèles mathématiques d'apprentissage automatique.

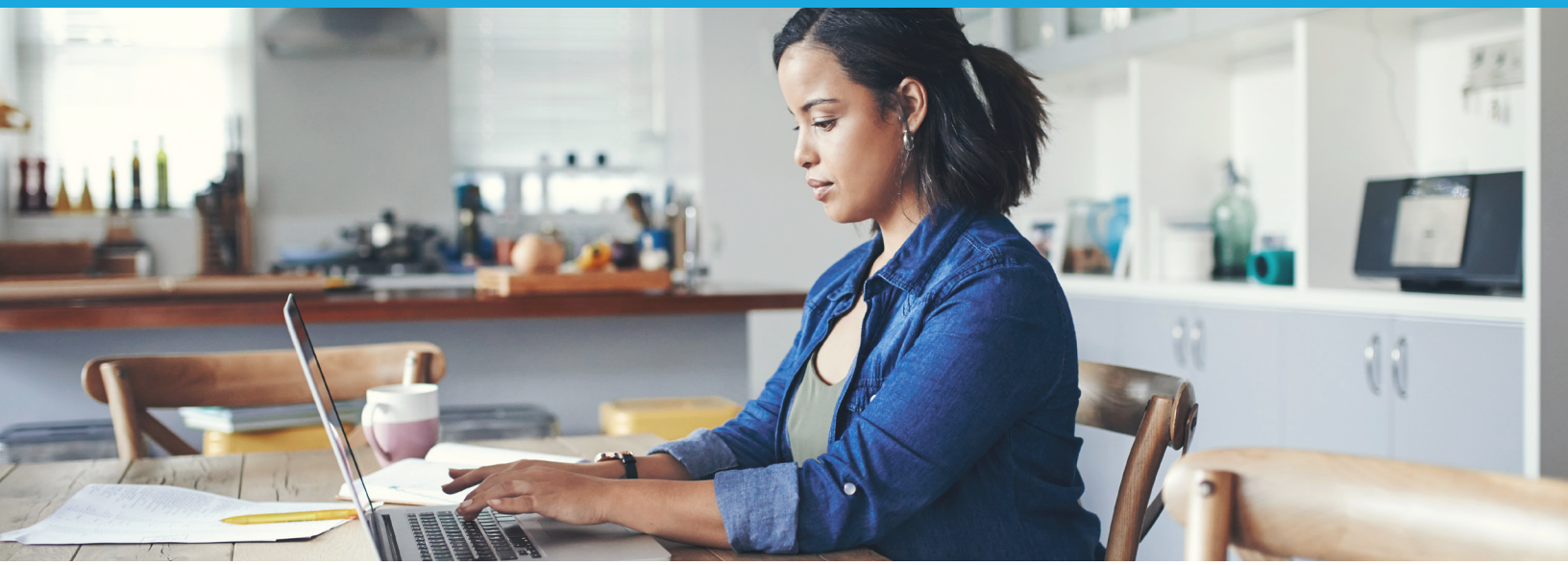
Fast Flux

Le Fast Flux est une technique DNS que les cybercriminels utilisent pour dissimuler les sites de phishing et de logiciels malveillants derrière un réseau changeant de forme, constitué d'hôtes compromis qui agissent comme des proxys. Grâce à cette technique, les botnets peuvent basculer d'une adresse IP à une autre, ce qui permet aux cybercriminels d'échapper à toute détection.

Les solutions de sécurité reposant uniquement sur la Threat Intelligence risquent de passer à côté ce type de technique déployée par des attaquants sophistiqués. Infoblox Threat Insight combine l'apprentissage automatique et l'analyse de comportement, personnalisés avec DNS pour distinguer les domaines Fast Flux des domaines normaux, afin de protéger les utilisateurs finaux et les collaborateurs distants de ces attaques. Threat Insight est intégré à la solution BloxOne Threat Defense.

Tunneling DNS

L'attaque via tunnels DNS est une technique qui utilise des logiciels malveillants pour recueillir des données sensibles sur le système infecté. Les données sont rassemblées en petits paquets intégrés dans une chaîne de requêtes DNS. Ces requêtes suivent le standard DNS et contournent toutes les solutions de sécurité. Les requêtes DNS portant les paquets sont livrées à un serveur DNS hébergé par l'attaquant, qui dépouille les requêtes DNS entrantes et



réassemble les données dérobées. BloxOne Threat Defense Threat Insight utilise l'analyse de comportement associée à l'apprentissage automatique pour effectuer une analyse en temps réel des requêtes DNS entrantes, notamment entropie, n-gramme, lexique, taille et fréquence pour détecter les tunnels DNS. Threat Insight réduit également le nombre de faux positifs en détectant toute utilisation bénigne des tunnels DNS.

Le tunneling DNS peut être détecté via deux méthodes principales : la Threat Intelligence pour trouver les tunnels connus (par exemple, IP et domaines malveillants connus) ou des analyses de comportement pour détecter des méthodes connues ou précédemment inconnues du tunneling DNS. La solution Infoblox utilise les deux méthodes et nos algorithmes de détection brevetés pour découvrir des attaques précédemment inconnues. Les autres solutions utilisent rarement plus d'une méthode de Threat Intelligence, ce qui limite leur capacité à détecter de nouvelles attaques et à protéger les télétravailleurs.

Filtrage de contenu

Pour protéger des effectifs distants et nombreux, l'échelle et la rentabilité deviennent des aspects fondamentaux. Si vos collaborateurs travaillent à domicile ou sur d'autres sites que leur site habituel, il est essentiel de veiller à ce que les contenus auxquels ils accèdent depuis les appareils de l'entreprise restent conformes aux règles définies. Mais le problème avec une mise en œuvre à si grande échelle, c'est qu'elle peut nécessiter des dizaines ou des centaines de passerelles Web sécurisées pour filtrer les contenus, ce qui augmenterait les coûts et la latence si tout le trafic devait être transporté via ces systèmes.

Intégré à chaque connexion, le DNS est un élément architectural essentiel de l'infrastructure qui permet de filtrer un nombre maximal de requêtes avec une efficacité optimale. Cela permet de bloquer l'accès aux contenus non conformes. Cela permet également de réduire la charge de travail liée aux solutions de sécurité plus onéreuses tout en mobilisant beaucoup moins de ressources et de temps pour la gestion.

BloxOne Threat Defense vous permet de filtrer les contenus au niveau du DNS, ce qui garantit qu'aucune connexion à un site Web ne peut avoir lieu si elle n'est pas conforme à la politique de l'entreprise. Cette solution permet également aux administrateurs d'examiner l'activité des contenus.

DoH

Le DNS via HTTPS (DoH) est une nouvelle fonctionnalité de plus en plus présente dans les principaux navigateurs Internet, comme Firefox. Malheureusement, le DoH contrevient ce faisant aux bonnes pratiques de sécurité des entreprises et autorise le trafic DNS chiffré. En utilisant le DoH, les appareils envoient tout leur trafic DNS à un résolveur DNS tiers externe, contournant ainsi l'infrastructure DNS interne de l'entreprise et tous les contrôles de sécurité DNS en place. Par conséquent, des menaces telles que l'exfiltration de données et les rappels C&C passent inaperçues.

Pour atténuer ces risques, les entreprises doivent utiliser l'infrastructure DNS interne et appliquer des règles de sécurité à l'aide du DNS en bloquant l'utilisation des résolveurs DoH publics tiers. BloxOne Threat Defense et la Threat Intelligence d'Infoblox incluent un flux spécial appelé « DoH Public IPs and Hostnames » permettant de détecter les tentatives d'accès à des résolveurs DNS via HTTPS non gérés et de les bloquer, ce qui oblige les navigateurs à basculer en douceur vers le DNS géré par l'entreprise, sans interrompre l'activité des utilisateurs. Cette fonction garantit qu'un collaborateur travaillant à domicile, ou sur un site distant, éventuellement dans FireFox ou d'autres applications qui utilisent par défaut des résolveurs DoH, sera toujours protégé contre l'exfiltration de données et les communications de logiciels malveillants.

Architecture hybride

La plupart des entreprises ont besoin d'analyses et de Threat Intelligence, associés à l'évolutivité du cloud, pour faire appliquer les règles et et résoudre les problèmes. Les solutions basées uniquement sur le cloud peuvent fournir des solutions d'échelle mais n'offrent pas les moyens de résoudre les problèmes de clients compromis ni d'obtenir une visibilité totale sur les menaces internes.

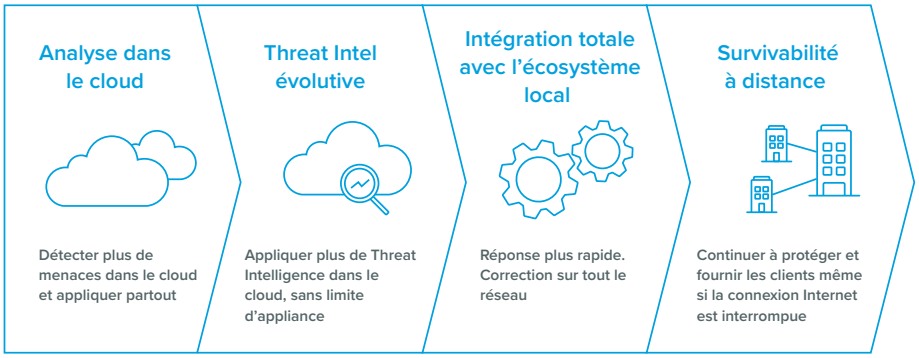


Figure 3 : L'architecture hybride offre des avantages par rapport à l'architecture cloud uniquement ou autonome locale.

L'architecture hybride d'Infoblox offre les avantages suivants:

- **Analyse évolutive dans le cloud:** Le modèle hybride d'Infoblox permet la détection par analyse d'un large éventail de menaces. Il peut s'agir d'algorithmes de génération de domaines, d'attaques Fast Flux, de logiciels malveillants sans fichier et de DGA avec dictionnaire. Une menace détectée chez un télétravailleur itinérant peut être automatiquement appliquée de manière universelle à tous les autres utilisateurs, appareils, ressources et applications.

- **Threat Intelligence évolutive:** Le modèle hybride d'Infoblox permet de disposer de renseignements hautement évolutifs avec support cloud. Infoblox partage uniquement les menaces actives afin de s'adapter aux limites d'échelle de vos appareils locaux.
- **Intégration de l'écosystème de sécurité:** Le modèle hybride d'Infoblox permet une intégration complète avec vos ressources technologiques locales. Cette intégration permet à votre équipe de rassembler des informations importantes sur le contexte réseau ainsi que de fournir une réponse plus rapide et plus précise aux incidents, avec ordre de priorité, ainsi que des mesures de correction pour l'ensemble du réseau.
- **Survivabilité et résilience:** La disruption d'Internet permet à vos solutions Infoblox locales de continuer à sécuriser votre réseau.
- **Point d'administration unique simplifié pour l'entreprise:** Vous disposez désormais d'un point unique pour la plupart de vos tâches d'administration, de contrôle et de visibilité, tant sur site que dans vos clouds. Cela simplifie et réduit le coût de l'administration et réduit les erreurs.

Recommandations

Étant donné la situation actuelle de la pandémie de coronavirus, les politiques locales et nationales exigent que les collaborateurs des entreprises travaillent à domicile et collaborent à distance avec les clients. Les entreprises ont annoncé la mise en place de nouvelles règles permettant aux collaborateurs de travailler à domicile ou sont sur le point de le faire.

Il est essentiel de déployer une stratégie de bonnes pratiques qui prenne en charge à la fois votre infrastructure locale et vos effectifs distants. Une visibilité complète sur votre activité à distance est également essentielle. L'utilisation de BloxOne Threat Defense et de nos services DNS, DHCP et de gestion des adresses IP (DDI) vous permet de mieux sécuriser les télétravailleurs, de protéger votre infrastructure stratégique et de sécuriser votre propriété intellectuelle.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com