Protégez les serveurs Web contre les menaces modernes avec Citrix NetScaler.

Protéger les serveurs Web de votre entreprise s'avère aujourd'hui plus difficile que jamais. Par le passé, les équipes informatiques en charge de la sécurité avaient juste une poignée d'applications Web d'entreprise à défendre. Désormais, elles doivent protéger des infrastructures Web hébergeant d'innombrables applications mobiles, SaaS et d'autres solutions basées sur le cloud.

Dans le même temps, le nombre et la diversité des menaces s'accroissent. Par exemple, les défenses modernes ne doivent plus se contenter de ne prendre en compte que la partie la plus visible de l'environnement des menaces, à savoir les malwares avancés. Beaucoup d'autres menaces ciblées exigent une grande attention : attaques spécifiques de la couche applicative, déni de service et déni de service distribué (DoS/DDoS), atteintes à la fonctionnalité des services liées à la sécurité, etc.

Ce livre blanc présente les défis associés à la protection des serveurs Web modernes contre les menaces modernes. Il explique comment le contrôleur de mise à disposition d'applications Citrix® NetScaler® complète efficacement les mécanismes de protection contre les malwares avancés et autres produits de sécurité importants pour former une solution de protection idéale contre les nouvelles menaces, capable de défendre un plus grand nombre de cibles. Les avantages offerts par l'utilisation de NetScaler à cet effet sont nombreux :

- Réduction des risques de sécurité grâce au blocage non seulement des malwares avancés, mais également des attaques par déni de service ou de la couche applicative.
- Réduction des risques commerciaux grâce au renforcement de l'utilisation par les clients et de la fidélisation grâce à l'automatisation de la sécurité et à l'augmentation des performances.
- Amélioration de l'agilité commerciale grâce à la capacité des directions informatiques à adopter pleinement les solutions mobiles, Web et cloud, fortement transformatrices, sans crainte de compromission ou autres défaillances liées aux infrastructures.

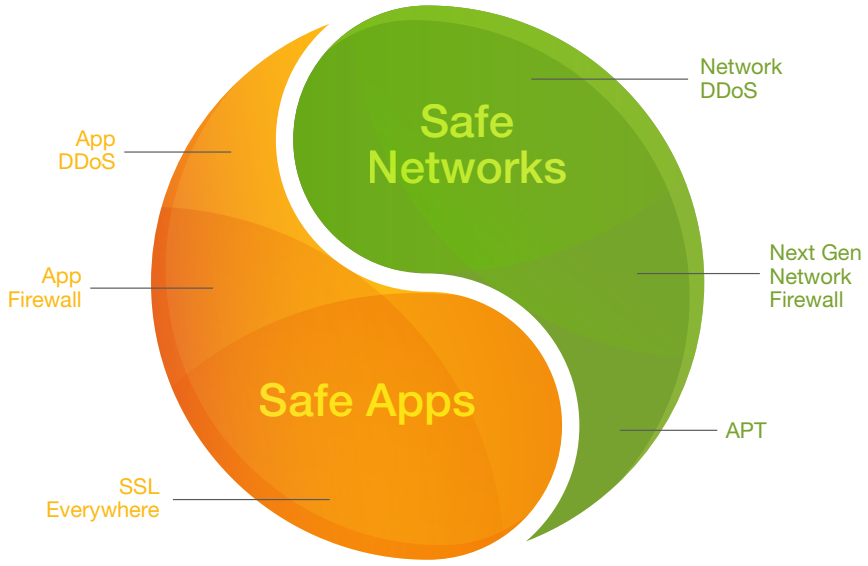

Figure 1 : Une solution complète de protection des serveurs Web

« Et les APT ? »
Bien que les fournisseurs de solutions de protection contre les malwares avancés les lient souvent, les menaces persistantes avancées (ou APT) et les malwares avancés sont deux choses bien différentes. En fait, lorsque l'on parle d'APT, on pense plus à l'auteur de la menace (bien organisé, amplement financé et constant dans sa démarche) qu'à une classe bien précise de menace employée. Les APT emploient en général dans la durée de multiples techniques et méthodes d'attaque, comprenant par exemple non seulement des malwares avancés, mais également des composants DoS et de la couche applicative, dans le but d'accéder aux données puis de créer une diversion pendant que ces données sont extraites.

Les sites Web modernes : bien plus que vos applications Web traditionnelles

Au début, les serveurs Web n'impliquaient guère plus qu'un navigateur (en général Internet Explorer) interagissant avec un site Web d'entreprise. Aujourd'hui, cependant, le moins que l'on puisse dire est que ces solutions Web ont considérablement évolué. Désormais, les serveurs Web d'entreprise impliquent un éventail très diversifié de composants :

- Nombreux navigateurs interagissant avec de nombreux sites et composants Web.
- Réseaux de mise à disposition de contenu et sites/applications Web hébergés sur le cloud.
- Autres solutions SaaS et cloud de mise à disposition, de type plateforme sous forme de service (PaaS) ou infrastructure sous forme de service (IaaS), pour lesquels la propriété et le contrôle passent progressivement de l'entreprise à un tiers.
- Mashups, pour lesquels le contenu est extrait de façon dynamique à partir de nombreux sites externes.
- Puissantes interfaces API permettant l'intégration de la chaîne d'approvisionnement et une automatisation accrue.
- Solutions mobiles impliquant une communication entre les micro-applications côté périphérique et les composants Web d'arrière-plan.

De fait, la protection des propriétés Web ne peut plus se limiter à la simple protection des applications Web d'entreprise. L'étendue des ressources exigeant une protection s'est considérablement développée, notamment pour inclure désormais des solutions cloud et mobiles.

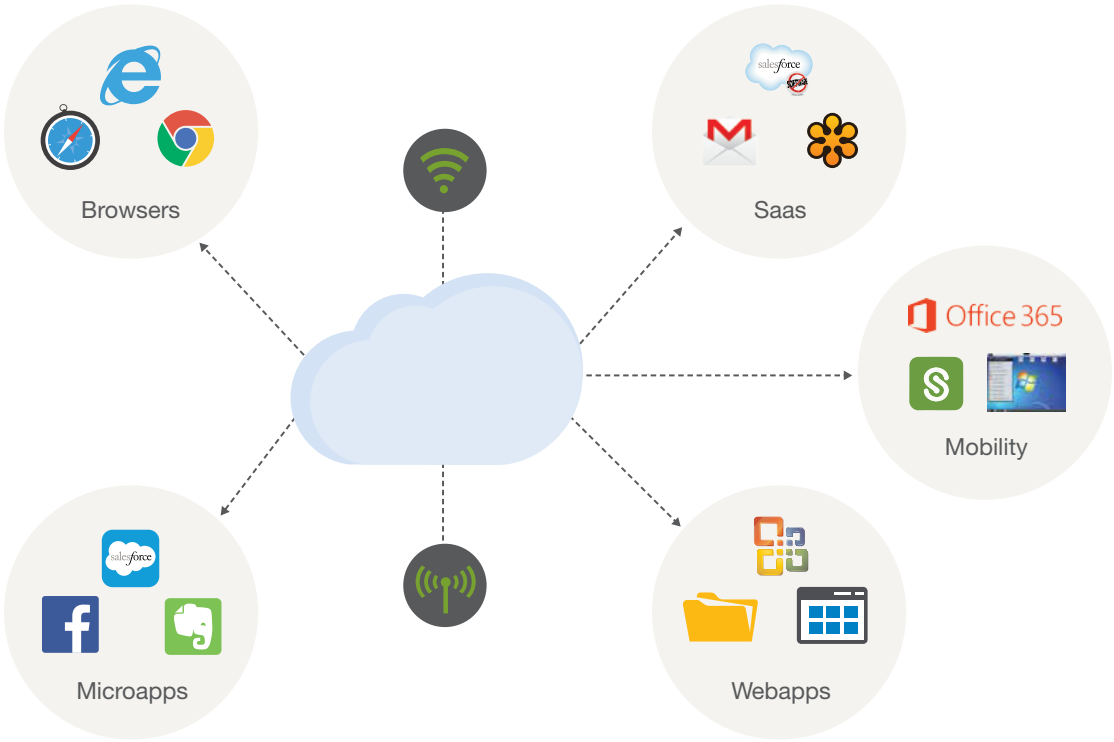

Figure 2 : Un monde complexe de propriétés Web

Les menaces modernes : les malwares sophistiqués ne sont que la partie émergée de l'iceberg

Les malwares avancés suscitent de nos jours beaucoup de craintes, et à juste titre. Les défenses basées sur des signatures les plus couramment déployées ne sont plus adaptées à la nouvelle génération de malware spécialement conçue pour les contourner (par exemple, en ciblant des vulnérabilités jusqu'alors non divulguées, en s'appuyant sur des authentifiants compromis ou en utilisant le polymorphisme et d'autres techniques pour modifier rapidement l'apparence ou les fonctionnalités du code malveillant).

Il en résulte pour les entreprises modernes une nécessité urgente d'investir dans des solutions de protection contre les malwares avancés qui ne soient plus dépendantes de mécanismes basés sur les signatures, uniquement capables de détecter les menaces déjà identifiées (également appelées menaces connues). Cependant, les malwares avancés ne constituent qu'une classe parmi toutes les menaces faisant peser des risques significatifs sur les sites Web de l'entreprise. Les attaques par déni de service (DoS), les attaques spécifiques à la couche applicative et les atteintes à la fonctionnalité des services exigent également l'adoption de mesures d'atténuation du risque.

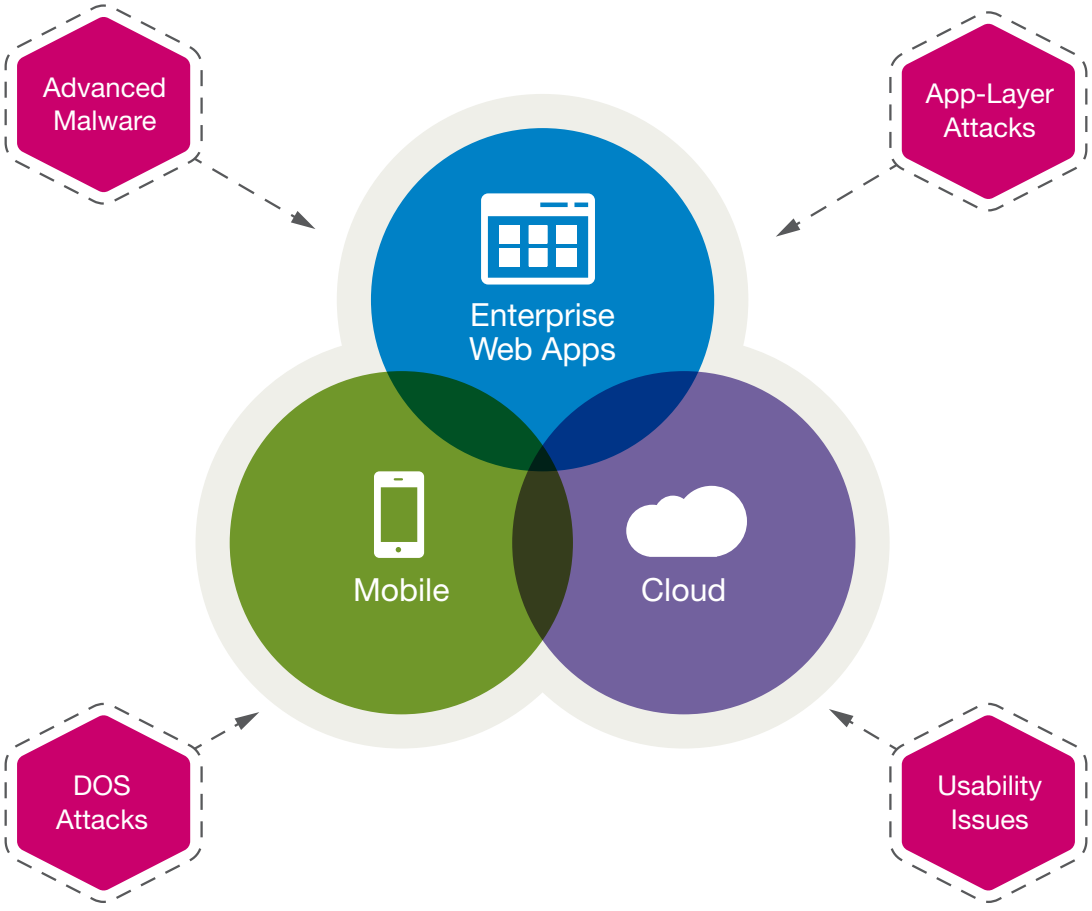

Figure 3 : Le paysage des menaces modernes

Attaques par déni de service (DoS) : ces deux dernières années ont été marquées par une forte recrudescence des attaques DoS, de même que par une évolution significative de la nature même de la menace. Les plus gros sites Internet ne sont plus les seuls à être ciblés. Désormais, du fait de la disponibilité étendue de boîtes à outils et de botnets peu coûteux (respectivement pour la création et la mise en œuvre d'attaques DoS), toute entreprise, quels que soient sa taille et son

secteur d'activité, court un risque. Parvenir à détecter ces attaques est également bien plus difficile qu'auparavant, des variantes de la couche applicative, furtives et à faible bande passante, dont l'objectif est de saturer les ressources d'arrière-plan, s'ajoutant désormais aux toujours fréquentes attaques à grande échelle destinées à inonder vos canaux Internet ou à rendre indisponibles les périphériques réseaux frontaux de type routeur, pare-feu ou ADC de base.

Attaques de la couche applicative, spécifiques au Web : dans ce cas, la menace n'est pas nouvelle, mais s'avère toujours significative. Confrontés à une multitude de mécanismes courants de défense opérant au niveau de la couche réseau, les pirates ont logiquement décidé de concentrer leurs efforts sur les couches supérieures de la pile informatique, dans le but d'obtenir de meilleurs résultats. On observe donc un pourcentage substantiel d'attaques ciblant des faiblesses découvertes au sein des technologies et des composants Web largement dispersés (tels que le protocole HTTP lui-même, Java ou des applications et des serveurs Web populaires) et les propres applications Web personnalisées de l'entreprise. Les menaces courantes qui entrent dans cette catégorie comprennent notamment le cross-site scripting, la falsification de requête cross-site, l'injection SQL et les attaques par saturation, pour n'en citer que quelques-unes.

Atteintes à la fonctionnalité des services : une fonctionnalité dégradée est trop souvent négligée ou insuffisamment prise en compte, car perçue d'un point de vue technique plus comme un problème de performance que comme une véritable menace pesant sur la sécurité. Ces atteintes sont cependant classées comme attaques par les solutions de sécurité et constituent une menace très réelle, tout au moins pour l'activité de l'entreprise. Des performances médiocres imputables à des procédures d'inspection gourmandes en ressources, une surcharge SSL, des processus de connexion alambiqués et des fonctionnalités d'accès incohérentes peuvent inciter les utilisateurs à adopter des solutions de rechange non sécurisées, générer une insatisfaction de la clientèle qui, en fin de compte, se détournera de vous au profit de vos concurrents. En outre, compenser ces conditions passe souvent pour l'entreprise par l'achat d'un matériel plus important ou de plus grande capacité qu'initialement prévu dans les budgets. C'est pourquoi les équipes en charge de la sécurité informatique doivent être bien conscientes que les solutions de sécurité elles-mêmes peuvent représenter une menace si leur architecture n'a pas été pensée afin d'éviter ou de compenser ces problèmes d'atteinte à la fonctionnalité.

En définitive, la conclusion est que la protection des propriétés Web modernes implique la prise en compte de toutes ces classes de menaces et non plus uniquement des malwares avancés. Ne pas le faire expose notamment à un risque accru de vol ou de divulgation des données, de perte de clients, d'augmentation du coût total de possession et de non-conformité légale.

Les défenses modernes : le rôle de NetScaler

NetScaler, le meilleur ADC pour la création de réseaux cloud d'entreprise, est également la solution idéale pour la protection des propriétés Web modernes. Déjà composant stratégique adopté au sein de plusieurs milliers de datacenters d'entreprise et de réseaux de fournisseurs de services cloud, NetScaler offre des fonctionnalités étendues de protection Web qui complètent parfaitement les solutions de protection contre les malwares avancés proposées par exemple par FireEye ou Palo Alto Networks. Grâce à NetScaler, les entreprises disposent de tout le nécessaire pour garantir la disponibilité, la sécurité, la fonctionnalité et l'agilité de leurs sites Web tout en bloquant efficacement les attaques de type déni de service et dirigées contre la couche applicative cherchant à interrompre l'activité et à extraire des données sensibles. En outre, toutes ces fonctionnalités indispensables sont réunies au sein d'une solution étroitement intégrée sur une plateforme unique et hautement évolutive. De fait, les entreprises n'ont plus besoin d'investir dans une multitude de produits ponctuels de sécurité et évitent de subir la complexité accrue générée par leur mise en œuvre.

Maintenir les lumières allumées

Les serveurs Web qui ne sont plus accessibles du fait d'interruptions multiples sont quasiment inutiles et peuvent même causer d'importants dommages à l'image de l'entreprise. C'est pourquoi les défenses de NetScaler destinées aux serveurs Web commencent par intégrer un large éventail de fonctionnalités de protection contre les menaces susceptibles d'interrompre votre activité et de rendre indisponibles vos services essentiels.

- **Haute disponibilité pour les composants critiques** : dans l'hypothèse où un serveur Web ou tout autre composant clé d'une propriété Web connaît une défaillance pour une quelconque raison, des algorithmes de répartition de charge dirigent de façon dynamique le trafic affecté vers des instances alternatives configurées dans le cadre d'un groupe de ressources géré par NetScaler. De cette façon, NetScaler garantit une disponibilité permanente durant les opérations de maintenance planifiées, les défaillances imprévues et les interruptions dues à des attaques.
- **Suivi de l'état pour une gestion proactive des défaillances** : les vérifications d'état de NetScaler contrôlent le statut des composants clés et mettent en œuvre des fonctionnalités de répartition de charge afin d'éviter tout problème de façon proactive. Contrairement à de nombreuses solutions concurrentes qui parviennent à peine à confirmer qu'une connexion réseau est disponible et que le serveur sous-jacent est en ligne, NetScaler effectue des vérifications de contenu étendues pour confirmer également que les services essentiels de niveau système et que chacune des procédures logicielles sont également en bon état de marche.
- **Répartition de la charge serveur globale pour la reprise après sinistre** : un large éventail de fonctionnalités de répartition de la charge globale garantit une reprise après sinistre transparente des serveurs Web modernes. Si un site entier devient indisponible pour une quelconque raison, le trafic affecté est automatiquement dirigé vers un datacenter de secours. Une expérience positive et cohérente est également assurée grâce à des stratégies et des contrôles intelligents permettant de diriger régulièrement les sessions vers le meilleur site en fonction de priorités choisies par l'administrateur (telles que la proximité, le niveau d'utilisation des ressources ou les performances générales).
- **Protection multicouche contre les attaques DoS** : grâce à NetScaler, les entreprises bénéficient d'une première ligne de défense puissante contre tous les types de menaces DoS. Une couverture est assurée non seulement contre les attaques volumétriques destinées à consommer toute votre bande passante Internet, mais également contre celles plus insidieuses cherchant à épuiser les tableaux d'état des périphériques, à utiliser frauduleusement les services de la couche infrastructurelle ou applicative (DNS, SSL, HTTP, etc.) ou à utiliser frauduleusement des fonctionnalités applicatives d'une manière qui dégrade significativement les performances (en émettant par exemple de façon répétée des requêtes générant des calculs complexes, des interrogations d'arrière-plan ou des opérations de recherche).

Difficulté de détection croissante

	Type d'attaque	Fonctionnalités NetScaler d'atténuation du risque
Application	Inondations POST et GET malveillantes ; attaques slowloris, POST lent et autres variantes à faible bande passante	Validation de protocole applicatif, protection contre les pics de charge, file d'attente, protection contre les inondations HTTP, protection contre les attaques HTTP à faible bande passante
Connexion et Session	Inondations des connexions, inondations SSL, inondations DNS (udp, requête, nxdomain)	Architecture full-proxy, conception haute performance, gestion intelligente de la mémoire, protections DNS étendues
Réseau	Syn, UDP, ICMP, inondations ACK et PUSH, attaques LAND, smurf et teardrop	Défenses intégrées, modèle de sécurité avec blocage par défaut, validation de protocole, limitation des taux

Figure 4 : « Citrix NetScaler : Une protection puissante contre les attaques de type déni de service »

Contrôle des pics d'utilisation en cas de surcharge imprévue : un pic soudain et important d'utilisation d'un serveur Web peut avoir les mêmes conséquences qu'une attaque DoS. NetScaler gère ce type de situation via la protection contre les pics d'utilisation, une fonctionnalité qui traite aisément les pics de trafic ponctuels en basant le taux de présentation des connexions aux serveurs d'arrière-plan sur leur capacité à les traiter. Facteur important, grâce à ce mécanisme, aucune connexion n'est abandonnée. NetScaler les met en cache et les met à disposition, dans leur ordre de réception, uniquement lorsque les serveurs d'arrière-plan sont prêts à les traiter.

Bloquer les menaces avancées

Quoique primordiale, la lutte contre les menaces ciblant la disponibilité ne constitue qu'un point de départ. Grâce à NetScaler, les entreprises bénéficient également d'une solution capable non seulement de bloquer directement les attaques ciblant la couche applicative, mais également de travailler en coopération avec les principaux produits tiers du marché afin de contrer la dernière génération de malwares sophistiqués.

Protection de protocole pour une défense à large spectre de la couche applicative : assurer la conformité aux normes RFC et aux meilleures pratiques d'utilisation de HTTP est une méthode hautement efficace utilisée par NetScaler pour éliminer un large éventail d'attaques basées sur des requêtes malformées ou le comportement illégal du protocole HTTP. Des mécanismes personnalisés de vérification peuvent être ajoutés à la stratégie de sécurité en s'appuyant sur les fonctionnalités de filtrage de contenu intégré, de réponse personnalisée et de réécriture HTTP bidirectionnelle. Le résultat obtenu est une protection à large spectre contre les malwares de reconnaissance (destinés par exemple à extraire des informations des réponses serveur afin de perpétrer ultérieurement une attaque), les malwares ciblant HTTP (Nimda, Code Red, etc.) et autres menaces ciblant la couche applicative.

NetScaler AppFirewall pour les menaces spécifiques à la couche applicative : les pare-feu réseau traditionnels n'offrent pas le niveau de visibilité et de contrôle indispensable à une protection efficace contre les plus de 70 % des attaques Internet qui ciblent directement les vulnérabilités de la couche applicative. Au contraire, NetScaler AppFirewall™ est une solution de sécurité certifiée ICSA qui analyse tout le trafic bidirectionnel, y compris les communications chiffrées en SSL, afin de contrer les menaces à la fois connues et inconnues ciblant la couche applicative sans nécessiter la moindre modification des serveurs Web de l'entreprise. Quelques fonctionnalités clés :

- **Protection contre les attaques** : une combinaison astucieuse de modèles de sécurité positive et négative assure la protection la plus complète contre tous les modes d'attaque. Afin de contrecarrer les nouveaux exploits encore inconnus, un moteur de stratégies à modèle positif comprend les interactions utilisateur/application admissibles et bloque automatiquement tout le trafic n'entrant pas dans ce cadre. Un moteur à modèle négatif s'appuie en parallèle sur les signatures des attaques pour contrer et signaler les menaces connues ciblant les applications.
- **Protection contre le vol de données** : les vérifications de données Safe Object assurent une protection efficace contre les fuites inattendues de données d'entreprise sensibles (propriété intellectuelle, numéro de carte de crédit, etc.), peu importe que l'événement à leur origine soit une attaque réelle, une utilisation abusive par un utilisateur autorisé ou un défaut dans la conception d'une application Web. Une combinaison d'expressions standards définies par l'administrateur et de plug-ins personnalisés indique au pare-feu applicatif NetScaler le format de ces données, tandis que des règles associées précisent les actions appropriées à effectuer (par exemple masquer le champ protégé, ou bien bloquer l'intégralité de la réponse provenant de l'application).
- **Maintien de la conformité** : NetScaler AppFirewall permet aux entreprises d'assurer leur conformité réglementaire aux normes PCI-DSS(Payment Card Industry Data Security Standard), qui encouragent explicitement l'utilisation de pare-feu applicatifs Web pour toutes les applications destinées au public et traitant des informations liées aux cartes de crédit. NetScaler

publie des rapports détaillés afin de documenter toutes les mesures de protection définies dans la stratégie de pare-feu et correspondant à des exigences des normes PCI-DSS ou de toute autre norme de conformité.

Figure 5 : NetScaler assure une protection efficace contre les pertes de données sensibles, peu importe le type de menace à l'origine de la fuite. (source : livre blanc « NetScaler pour la sécurité des datacenters »)

Solutions tierces certifiées Citrix Ready pour le blocage des malwares avancés : si NetScaler ne peut pas détecter directement toutes les formes de malwares avancés, son large éventail de fonctionnalités de sécurité n'en offre pas moins un rempart très efficace contre cette classe de menace en constante prolifération. NetScaler peut notamment diminuer l'impact des malwares en stoppant par exemple tout composant combiné s'appuyant sur les techniques d'attaque Web courantes, tout composant causant ou s'appuyant sur un comportement applicatif anormal et toute tentative d'extraction de données d'entreprise sensibles. Les données d'événements des couches réseau et application générées par NetScaler peuvent également être utilisées, généralement en association avec d'autres flux de données d'événements, afin de révéler dans un premier temps la présence d'un malware, puis d'aider à le localiser. En outre, des solutions tierces proposées par des partenaires Citrix Ready, spécifiquement conçues pour contrer les malwares avancés, fournissent aux entreprises fortement ciblées des mécanismes de protection propres aux différents types de menaces.

Garantir la fonctionnalité des services

Eviter l'indisponibilité des serveurs Web modernes est une nécessité incontournable. Les atteintes à la fonctionnalité (dégradation des performances, processus compliqués ou incohérents d'accès aux serveurs Web, etc.) sont moins spectaculaires, mais sans doute plus destructrices du fait de leur fréquence accrue. Contrairement à la plupart des solutions de sécurité, qui tendent à exacerber ces problèmes, NetScaler travaille activement à les résoudre via la combinaison de décisions de conception astucieuses et de nombreuses fonctionnalités spécifiquement destinées à l'amélioration des performances applicatives.

Garantie haute performance : les fonctionnalités de NetScaler qui aident l'entreprise à résoudre ses problèmes de performance dus à la sécurité, au réseau ou aux applications sont nombreuses :

- Les optimisations TCP intégrées (temporisation avancée, redimensionnement de fenêtre, contrôle de la congestion, etc.) renforcent les capacités des systèmes, réduisent le taux de perte des paquets et améliorent les temps de réponse grâce à l'utilisation plus efficace de la bande passante et des ressources serveur disponibles.
- La mise en mémoire cache des contenus à la fois statiques et dynamiques (NetScaler AppCache™), associée à des procédures agressives de compression des données (NetScaler AppCompress™), permet de réduire la congestion du réseau et des serveurs, tout en améliorant significativement les temps de réponse applicatifs.
- Grâce à l'intégration de matériel dédié d'accélération SSL et à la prise en charge de longues clés de chiffrement (2048 bits et plus), NetScaler offre des fonctionnalités de chiffrement stratégiques

permettant d'éviter d'avoir à assurer un compromis entre le renforcement de la sécurité et la qualité de l'expérience des utilisateurs.
- La mise en file d'attente fournit un mécanisme de qualité de service permettant de hiérarchiser les requêtes entrantes en fonction de l'importance relative des applications qui leur sont associées.
- Grâce à l'intégration d'une passerelle SPDY, NetScaler permet l'utilisation de ce protocole de plus en plus populaire qui optimise la façon dont les requêtes et les réponses HTTP sont transmises sur le réseau sans aucune modification des applications côté serveur.
- NetScaler ActionAnalytics permet un suivi et une réaction à la dégradation des performances totalement automatisés, tandis que NetScaler Insight Center™ fournit aux administrateurs une visibilité détaillée qui les aide à identifier et à résoudre les problèmes potentiels avant qu'ils n'aient eu le temps d'avoir un réel impact.

Accès transparent : NetScaler compte de nombreuses fonctionnalités qui contribuent à atténuer le risque d'atteinte à la fonctionnalité des services en renforçant l'expérience via d'autres méthodes non liées aux performances :

- **Single sign-on (SSO)** : les utilisateurs n'ont à s'authentifier qu'une seule fois, puis NetScaler les connecte de façon transparente à toutes les ressources d'un domaine donné.
- **Authentification et autorisation centralisées** : le même éventail étendu de services de contrôle d'accès peut être employé pour tous les sites Web de l'entreprise et tous les périphériques de chaque utilisateur. Cette fonctionnalité simplifie non seulement l'administration des serveurs Web et des utilisateurs mobiles, mais elle garantit en outre une expérience cohérente aux utilisateurs.

Garantir à la fois un faible coût et l'agilité

Une autre raison pour laquelle une solution de sécurité peut parfois représenter elle aussi une menace (au moins du point de vue commercial), c'est en coûtant trop cher ou en ne parvenant pas à répondre aux principaux besoins commerciaux. C'est pourquoi Citrix a également développé et commercialisé NetScaler pour répondre à cette problématique.

Consolidation inégalée : NetScaler est la seule solution de mise à disposition d'applications associant répartition de charge, répartition globale de la charge serveur, connectivité VPN SSL et bien d'autres choses encore au sein d'une unique plateforme intégrée et hautement évolutive. Les solutions concurrentes obligent les entreprises à acheter, mettre en œuvre et intégrer une multitude de produits et périphériques ponctuels pour pouvoir obtenir un éventail comparable de fonctionnalités capables de délivrer et de défendre efficacement les serveurs Web. Grâce à NetScaler SDX™, les directions informatiques peuvent également consolider leur infrastructure ADC en disposant de la possibilité de mettre en œuvre jusqu'à 80 instances NetScaler isolées sur une même plateforme.

Adaptation à la migration vers le cloud : le passage progressif aux réseaux cloud d'entreprise est grandement facilité par l'adoption des appliances virtuelles compatibles cloud NetScaler VPX™. Version complète et exclusivement logicielle de NetScaler App Delivery Controller™, cette solution permet de mettre en œuvre les fonctionnalités d'optimisation des performances et de protection de NetScaler à la demande, en tout point d'un quelconque datacenter d'entreprise ou datacenter cloud tiers. NetScaler VPX permet aux entreprises d'exécuter en toute sécurité leurs services et applications Web à l'endroit qui leur semble le plus adapté.

Prise en charge de la mobilité des utilisateurs : en matière de facilitation des initiatives de mobilité d'entreprise, NetScaler ne se contente pas de protéger et d'optimiser les serveurs Web associés. NetScaler fournit également les mêmes services au profit de l'infrastructure de gestion associée, notamment Citrix XenMobile®. Solution complète de gestion des périphériques, des applications et des données mobiles, XenMobile offre aux utilisateurs la liberté de travailler et de

vivre à leur manière. Tandis que les directions informatiques bénéficient d'un contrôle total et de la capacité à protéger l'intégralité de leur environnement mobile, les utilisateurs bénéficient de l'accès en un seul clic à toutes leurs applications Windows, Web, SaaS et mobiles à partir d'une librairie applicative d'entreprise unifiée. L'association de NetScaler et de XenMobile garantit :

- La haute disponibilité des composants clés de l'infrastructure de mobilité d'entreprise.
- Des couches supplémentaires de protection des périphériques, des applications et des données mobiles.
- La capacité à faire évoluer les opérations mobiles sans perturbation des employés ou lourde mise à niveau.

Conclusion

Protéger les actifs Web de votre entreprise implique bien plus que la simple protection d'une poignée d'applications Web d'entreprise contre le fléau des malwares avancés. Vos défenses doivent également prendre en compte les actifs Web d'arrière-plan en soutien des applications mobiles natives, des solutions SaaS et des autres services cloud. De plus, ces défenses doivent fournir une couverture pour d'autres classes toutes aussi redoutables de menaces, notamment les attaques de la couche applicative, les attaques DoS et les atteintes à la fonctionnalité des services imputables à un défaut de sécurité.

Citrix NetScaler constitue un complément idéal aux solutions modernes et haut de gamme de protection contre les malwares avancés. L'ADC NetScaler :

- Réduit les risques en atténuant les principales autres classes de menaces ciblant les propriétés Web (notamment les attaques DoS et de la couche applicative).
- Réduit le risque commercial en améliorant les performances et la fonctionnalité des serveurs Web afin de renforcer l'attraction et la fidélisation des utilisateurs.
- Réduit le coût total de possession en fournissant des opportunités étendues de consolidation des infrastructures et d'optimisation de l'utilisation des ressources.
- Renforce l'agilité informatique et commerciale en offrant aux entreprises les fonctionnalités stratégiques de sécurité dont elles ont besoin pour poursuivre en toute confiance leurs initiatives de mobilité des utilisateurs, de consumérisation informatique et de migration vers les réseaux cloud d'entreprise.

Pour en savoir plus sur la façon dont NetScaler peut aider votre entreprise à protéger ses propriétés Web stratégiques, consultez www.citrix.fr/netscaler.

Siège social
Fort Lauderdale, Floride, États-Unis

Siège Silicon Valley
Santa Clara, Californie, États-Unis

Siège Europe, Moyen-Orient, Afrique
Schaffhausen, Suisse

Centre de développement Inde
Bangalore, Inde

Siège Division en ligne
Santa Barbara, Californie, États-Unis

Siège Pacifique
Hong Kong, Chine

Siège Amérique latine
Coral Gables, Floride, États-Unis

Centre de développement Royaume-Uni
Chalfont, Royaume-Uni

À propos de Citrix

Citrix (NASDAQ:CTXS) est le leader en matière d'espaces de travail mobiles, combinant virtualisation, gestion de la mobilité, mise en réseau et services de cloud pour offrir de nouveaux modes de travail plus efficaces. Les solutions Citrix favorisent la mobilité professionnelle grâce à des espaces de travail personnels et sécurisés offrant aux utilisateurs un accès instantané aux applications, postes de travail, données et communications sur tout périphérique, tout réseau et dans le cloud. Cette année, Citrix célèbre 25 ans d'innovation qui rend aujourd'hui l'informatique plus accessible et les employés plus productifs. Le chiffre d'affaires annuel de l'entreprise a atteint 2,9 milliards de dollars en 2013. Les produits Citrix sont utilisés dans le monde entier par plus de 330 000 entreprises et plus de 100 millions d'utilisateurs. Pour en savoir plus www.citrix.fr.