Pare-feu applicatif Web : une protection incontournable pour toute entreprise moderne

Découvrez ce que les solutions de sécurité réseau traditionnelles ne peuvent pas faire et pourquoi votre entreprise a besoin d'un pare-feu applicatif Web comme pierre angulaire de sa stratégie de sécurité

CITRIX®

Protéger efficacement les sites Web omniprésents dans toute entreprise moderne implique une compréhension approfondie des fonctionnalités, mais aussi des limites, des différentes technologies de sécurité disponibles. Par exemple, si les pare-feu réseau et les systèmes de prévention des intrusions traditionnels sont efficaces pour éliminer un volume important de menaces ciblant les couches inférieures, ils s'avèrent nettement moins adaptés à la protection contre les menaces de plus en plus ciblées et spécialisées qui affectent désormais les applications des entreprises. Malgré une granularité significativement améliorée en matière de contrôle d'accès aux ressources réseau, même les pare-feu de nouvelle génération souffrent d'insuffisances majeures dans le domaine critique de la protection des propriétés Web.

Ce livre blanc souligne les difficultés liées à la protection adéquate des sites Web modernes contre les cybermenaces et examine les rôles que les différentes technologies de sécurité peuvent et, ce qui est peut-être encore plus important, ne peuvent pas jouer dans ce domaine. Il explique également pourquoi le pare-feu applicatif Web constitue un composant essentiel de toute stratégie d'entreprise de protection Web et pourquoi NetScaler AppFirewall (grâce à sa combinaison unique de fonctionnalités de sécurisation des applications et d'optimisation des performances applicatives) est incontestablement la solution idéale pour répondre à ce besoin.

Protection des applications Web : la problématique

Les propriétés Web de l'entreprise constituent aujourd'hui un risque significatif pour de nombreuses raisons. Les principaux problèmes trouvent leur origine dans l'omniprésence de ces propriétés, dans le fait qu'elles sont devenues la cible de prédilection de la nouvelle communauté du piratage et du fait de la protection inadéquate assurée par les soi-disantes solutions de sécurité de la « couche applicative ».

Les propriétés Web sont omniprésentes

De nos jours, les entreprises conçoivent et achètent massivement des applications Web. C'est déjà le cas pour les applications stratégiques ou orientées clients, et de plus en plus fréquent pour les applications mobiles ou destinées à délivrer des fonctionnalités et services d'arrière-plan. Bien que les applications générant directement du revenu drainent encore la plus grande attention, il serait vraiment imprudent de sous-estimer la criticalité de ces autres types d'applications (notamment celles liées à la gestion de la chaîne d'approvisionnement, aux flux financiers, aux ressources humaines, à la recherche et au développement de produits).

Qu'est-ce que cela signifie pour les équipes en charge de la sécurité informatique ? En premier lieu, les applications Web étant de plus en plus présentes au sein de l'entreprise et employées aussi bien par des utilisateurs internes que par des utilisateurs externes, les protections correspondantes ne doivent plus se contenter de couvrir le simple périmètre du réseau.

Un autre impact significatif découle directement de l'énorme diversité d'applications Web déployées en entreprise. Avec un nombre incalculable de combinaisons d'applications Web commercialisées ou développées sur mesure, on ne peut évidemment pas s'attendre à ce que des technologies de sécurité s'appuyant exclusivement sur des règles et des mécanismes à large spectre (comme par exemple la détection d'anomalies de protocole sur la couche réseau) puisse toutes les protéger de façon efficace et complète. Les équipes en charge de la sécurité ont également besoin d'outils offrant une plus grande flexibilité, une granularité d'inspection et de contrôle bien plus poussée et, dans l'idéal, une capacité d'apprentissage et d'adaptation automatique aux nouvelles applications.

Les sites Web constituent la « cible de choix » des pirates informatiques

Leur omniprésence n'est pas la seule chose qui attire les pirates : la vulnérabilité notoire des sites Web est également une source d'attrait. Cette situation est due à plusieurs facteurs :

- Le haut degré de complexité de nombreux sites Web
- L'utilisation régulière de bibliothèques tierces intégrées
- L'incorporation fréquente de fonctionnalités, technologies et de protocoles d'avant-garde (c'est-à-dire en réalité pas encore éprouvés)
- Les développeurs et responsables commerciaux qui favorisent les fonctionnalités et la rapidité de mise sur le marché au détriment de l'amélioration de la qualité du code et de la réduction des vulnérabilités

Ce qui accroît encore la valeur de la cible, c'est que bon nombre d'applications Web servent également de canaux directs vers des données sensibles ou précieuses, de type données de commande ou de paiement, spécifications de produits propriétaires, dossiers médicaux ainsi que la multitude de données d'identification personnelles. Une fois qu'un pirate parvient à pénétrer la porte d'entrée généralement très conviviale d'une application Web orientée client, il lui suffit de récupérer un ou plusieurs chemins configurés menant aux bases de données d'arrière-plan associées.

Dans ces circonstances, il n'est pas étonnant de découvrir régulièrement des violations Web massives aboutissant à la compromission de millions de dossiers, ou de tomber sur des statistiques telles que celles publiées dans le rapport Verizon 2014 sur les violations de données (2014 Verizon Data Breach Investigations Report), qui indique que 35 % des violations de données confirmées analysées en 2013 étaient attribuées à des attaques ciblant les applications Web. Il est également important de bien comprendre que les attaques Web connues du public ne constituent que la partie émergée de l'iceberg. La situation réelle est bien pire que ce qu'imaginent la plupart des responsables d'entreprise, l'immense majorité des attaques Web ne faisant pas la une des journaux ou n'étant tout simplement pas signalées par les entreprises affectées.

Protéger les services de la couche applicative ne suffit pas

Il ne faut pas négliger non plus la confusion potentielle introduite par la terminologie et les infrastructures de networking traditionnelles. Notamment, bien qu'appelée la « couche applicative », la couche 7 du célèbre modèle de référence OSI ne concerne (au même titre que toutes les autres couches de ce modèle) que les communications réseau. Techniquement, elle renvoie au recueil des protocoles et services que les applications utilisent pour identifier des partenaires de communication, déterminer la disponibilité des ressources et synchroniser la communication entre deux parties utilisant la même application. Parmi les protocoles de la couche applicative, citons HTTP (pour le Web), FTP (pour les transferts de fichiers) et SMTP (pour les messageries).

La confusion résulte du grand nombre de technologies de sécurité commercialisées comme étant capables de fournir une protection de la « couche applicative ». Bien que ces prétentions puissent être techniquement exactes (par exemple, lorsqu'un système de prévention des intrusions vérifie la conformité RFC pour HTTP) elles peuvent malheureusement également s'avérer quelque peu trompeuses. Le problème est que la protection fournie par ces solutions est très loin d'assurer une couverture complète des « applications », puisqu'elles se contentent de contribuer indirectement à sécuriser les applications infrastructurelles des « couches de niveau supérieur » (par exemple les serveurs Web et les systèmes de gestion des bases de données), les applications commerciales (comme Salesforce.com) et des données qui sont également invariablement présentes (voir Figure 1).

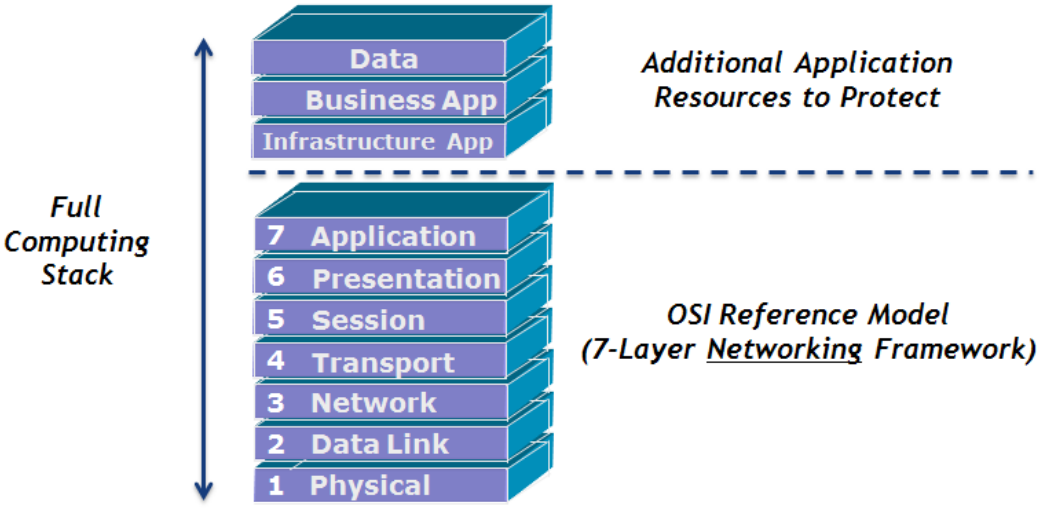

Figure 1 : Le modèle complet de pile informatique

Pour protéger efficacement leurs sites Web, les entreprises ont besoin de technologies de sécurité offrant de façon réellement complète :

- Une couverture physique : protection pour tous les scénarios d'utilisation, à la fois internes et externes au périmètre
- Une couverture fonctionnelle : non seulement application des stratégies sous la forme d'un contrôle d'accès granulaire, mais également détection et prévention explicites des menaces
- Une couverture logique : protection de toutes les couches de la pile informatique, depuis les protocoles et services des couches réseau et application jusqu'aux applications infrastructurelles, aux applications commerciales personnalisées et même aux données

Établir une couverture complète de ce type exige d'investir bien plus que dans de simples pare-feu réseau et systèmes de prévention des intrusions ordinaires.

Les technologies de sécurité réseau existantes

Les technologies de sécurité réseau couramment déployées ont clairement un rôle à jouer dans la défense des propriétés Web stratégiques de l'entreprise. Il est cependant primordial de bien comprendre qu'elles ont des limites et ne suffisent pas à elles seules à fournir un degré adéquat de protection.

Pare-feu réseau

La principale fonction d'un pare-feu réseau courant est le contrôle d'accès : déterminer quel trafic applicatif est autorisé à pénétrer les limites du réseau au sein duquel il est déployé. Les pare-feu à état (ou dynamiques) permettent d'effectuer les vérifications de façon dynamique et d'autoriser le trafic de retour correspondant aux sessions sortantes autorisées (et vice versa). Toutefois :

- Uniquement basée sur des attributs de la couche réseau (port, protocole, adresses IP source ou de destination, etc.), la fonctionnalité de contrôle d'accès des pare-feu classiques manque de granularité. De fait, le pare-feu ne peut pas toujours distinguer (et par conséquent contrôler) les différentes applications utilisant un protocole ou un port donné (par exemple, la multitude d'applications Web HTTP qui utilisent le port TCP 80).
- Les pare-feu réseau classiques ne sont pas équipés pour détecter et prévenir explicitement les menaces. La seule protection qu'ils assurent contre les malwares, les attaques et toutes les autres activités non autorisées est un sous-produit des stratégies de contrôle d'accès qu'ils sont chargés d'appliquer. Par exemple, si une menace exploite un chemin de communication qui n'est pas « ouvert », celle-ci sera, par défaut, repoussée (sans même avoir été détectée).

En conclusion, les pare-feu réseau classiques ne fournissent qu'une protection relativement limitée aux propriétés Web de l'entreprise.

Les systèmes de prévention des intrusions réseau (IPS)

N'offrant en général que très peu en termes de fonctionnalités de contrôle d'accès, la technologie IPS se concentre à la place sur la détection des menaces. Les mécanismes à large spectre sur lesquels cette technologie s'appuie comprennent notamment les signatures de menaces et vulnérabilités connues, ainsi que la détection des anomalies de comportement ou de protocole pour les soupçons d'activités malveillantes et les menaces inconnues. La couverture est en général assurée jusqu'à la couche des services applicatifs (incluse) et intègre tous les protocoles Internet courants : HTTP(s), DNS, SMTP, SSH, Telnet et FTP.

Une couverture sporadique est également assurée pour des couches plus élevées de la pile informatique, car il est fréquent d'inclure des signatures de menaces et de vulnérabilités connues associées aux applications commerciales et infrastructurelles les plus couramment utilisées au sein des entreprises modernes. Bien qu'il s'agisse là d'un pas dans la bonne direction, cette extension de couverture ne suffit tout simplement pas et laisse la technologie IPS coincée entre deux feux, sujette à la fois :

- A des faux-négatifs : le manque de visibilité et de compréhension approfondies des applications la maintenant totalement aveugle face aux menaces ciblant les couches les plus élevées (par exemple celles qui travaillent en manipulant la logique du processus applicatif), et
- A des faux-positifs : tenter d'écrire des signatures applicables à un large spectre, correspondant à un large éventail de menaces des couches supérieures ciblant à la fois des applications Web standards et personnalisées menant inéluctablement à d'innombrables fausses alertes

Bien que fournir une détection et une prévention explicites des menaces fasse de la technologie IPS un précieux complément aux pare-feu réseau classiques, la couverture intermittente au dessus de la couche des services applicatifs ne génère qu'un gain relatif de protection pour les propriétés Web de l'entreprise.

Les pare-feu de nouvelle génération

Les pare-feu de nouvelle génération (NGFW) associent les fonctionnalités IPS et de pare-feu réseau au sein d'une solution unique. Outre ces fonctionnalités, la technologie NGFW offre en général la capacité à utiliser l'identité de l'utilisateur et de l'application comme attributs pour le contrôle d'accès à/ou depuis un réseau. Pour les scénarios d'utilisation impliquant des exigences de débit très élevées (c'est-à-dire supérieur à plusieurs Gb/s), cette technologie offre une solution bien consolidée avec toutes les fonctionnalités nécessaires. Cependant, en matière de protection des propriétés Web, une lacune significative demeure : la reconnaissance applicative. La capacité à identifier de façon fiable des applications indépendamment du port et du protocole utilisés, fonctionnalité également appelée reconnaissance applicative, est une fonctionnalité différente de la fluidité applicative.

Grâce à la reconnaissance applicative, des techniques comme le décodage de protocole applicatif ou la signature d'application identifient l'infrastructure et les applications à l'origine de tout le trafic réseau. En clair, la reconnaissance applicative autorise un contrôle d'accès d'une grande précision, permettant désormais de définir des stratégies distinctes lorsque plusieurs applications et services sont utilisés sur les mêmes ports et protocoles. Par exemple, le trafic Web peut être découpé en plusieurs morceaux pour permettre l'accès à quelques applications Web stratégiques ou utiles, tout en restreignant de façon sélective ou en bloquant totalement l'accès à d'autres applications Web moins souhaitables (messageries Web, services de partage de fichiers, jeux Facebook, etc.).

Prérequis nécessaire pour la détection explicite des menaces des couches supérieures, la fluidité applicative implique une compréhension encore plus poussée des applications protégées, intégrant la connaissance des entrées et des séquences de navigation valides et de la façon dont l'application est censée se comporter (et ne pas se comporter).

En fin de compte, bien que les pare-feu de nouvelle génération (NGFW) permettent un contrôle d'accès accru et offrent l'opportunité de supprimer de nombreuses appliances monotechnologie, les entreprises ne disposent toujours que des fonctionnalités basiques de détection et de prévention explicites d'un système IPS ordinaire. L'ampleur et l'exhaustivité de la couverture ne sont tout simplement pas suffisantes pour protéger la plupart des sites Web (et notamment les sites Web personnalisés) contre les attaques de plus en plus ciblées et sophistiquées qui constituent désormais une part significative du paysage de la menace.

Le pare-feu applicatif Web : le maître du domaine applicatif

Le pare-feu applicatif Web (WAF) complète les failles des autres technologies, offrant une protection efficace contre les menaces ciblant les plus hauts niveaux de la pile informatique. Des routines d'apprentissage automatisées complétées par des stratégies configurées manuellement garantissent une « compréhension » haute fidélité du fonctionnement de chaque application Web protégée, notamment de sa couche logique et de ses fonctionnalités personnalisées. Toute déviation détectée constitue un soupçon de trafic malveillant et donne lieu à un traitement automatique (blocage, autorisation soumise à restrictions, enregistrement dans un journal, etc.) en fonction de stratégies définies préalablement par l'administrateur.

Si on les compare aux technologies de sécurité présentées précédemment, les WAF offrent une capacité unique à :

- Valider les entrées, et donc stopper les dangereuses attaques par injection SQL, cross-site scripting ou directory traversal
- Détecter les attaques par modification de cookie, de session ou de paramètre
- Bloquer les attaques exploitant les vulnérabilités des sites Web personnalisés
- Stopper l'exfiltration des données sensibles via l'identification et le blocage au niveau des objets

- Inspecter complètement le trafic chiffré SSL pour tous les types de menaces intégrées
- Prévenir les menaces qui opèrent en exploitant les failles logiques au sein des applications d'entreprise personnalisées
- Assurer une protection efficace contre les attaques par déni de service distribué (DDoS) et les attaques par déni ciblant la couche applicative
- Masquer de façon dynamique les données de réponse des serveurs, potentiellement utiles aux pirates
- Assurer une protection XML complète, comprenant la validation de schéma pour les messages SOAP et des défenses contre l'injection XPath, et identifier et bloquer les pièces jointes XML hébergeant un contenu malveillant
- Garantir la conformité à l'exigence 6.6 de la norme PCI DSS (Payment Card Industry Data Security Standard)

En complément de toutes ces protections orientées applications, les solutions WAF leaders du marché (telles que NetScaler AppFirewall) intègrent également la prise en charge de règles de contrôle d'accès pour la couche réseau et un composant basé sur la signature destiné à la détection des menaces connues. Les équipes de sécurité doivent cependant réaliser que les mécanismes de protection des pare-feu applicatifs Web, de par leur nature, sont essentiellement axées vers les protocoles Web (HTTP, HTTPS, XML et SOAP).

Un tour d'horizon des technologies de sécurité

Le tableau 1 fournit une comparaison des différentes technologies de sécurité présentées précédemment. Quelques éléments clés :

- Bien qu'elles soient utiles pour éliminer un volume important de menaces ciblant les couches basses, les technologies de sécurité les plus couramment déployées (pare-feu réseau et systèmes de prévention des intrusions) assurent une couverture très imparfaite en matière de protection des applications Web
- Bien qu'aucune technologie de sécurité ne garantisse aux applications Web une protection véritablement complète, les pare-feu applicatifs Web s'en approchent fortement
- Associer des pare-feu de nouvelle génération à des pare-feu applicatifs Web constitue un moyen efficace de défense puissante et à large spectre contre les menaces ciblant toutes les propriétés Web importantes de l'entreprise

Comparaison des différentes technologies de sécurité utilisées pour la protection des propriétés Web

	Pare-feu réseau	Système de prévention des intrusions	Pare-feu de nouvelle génération	Pare-feu applicatif Web
Fonctionne aux	Couches 3 à 4	Couches 3 à 7	Couches 3 à 7	Couches 3 à 7 et plus
Architecture de déploiement type	Passerelle de la couche 3	Mode transparent	Passerelle de la couche 3	Proxy inversé
Granularité du contrôle d'accès	Port, protocole, adresse IP	S/O	Port, protocole, adresse IP, utilisateur, application	Port, protocole, adresse IP
Détection des menaces/ techniques de prévention	S/O	Signatures, reconnaissance de formes, détection des anomalies de comportement et de protocole	Signatures, reconnaissance de formes, détection des anomalies de comportement et de protocole	Signatures, détection des anomalies de protocole, détection des anomalies propres à chaque application
Couverture de protocole	Tous	Tous	Tous	Orienté Web : HTTP(s), XML, SOAP, SPDY
Inspection du trafic chiffré/SSL	S/O	S/O	Oui	Oui
Protection contre le déni de service distribué	Couche réseau (basique)	Couche réseau	Couche réseau	Couche applicative
Protection des applications Web	Minimale	Menaces/vulnérabilités connues/inconnues principalement pour les couches réseau et des services applicatifs	Menaces/vulnérabilités connues/inconnues principalement pour les couches réseau et des services applicatifs	Etendue, comprenant une couverture complète de la couche applicative

NetScaler AppFirewall

Ses fonctionnalités uniques de protection Web font du pare-feu applicatif un composant essentiel de l'architecture de sécurité de l'entreprise et accentuent l'importance du choix d'une solution véritablement complète.

NetScaler AppFirewall est une solution de sécurité Web complète, certifiée ICSA, qui garantit le blocage de toutes les attaques connues et inconnues visant les applications et les services Web. Basé sur un modèle de sécurité hybride et sur l'analyse de l'ensemble du trafic bidirectionnel (y compris des communications chiffrées en SSL), AppFirewall permet de contrer un large éventail de menaces sans qu'il ne soit nécessaire d'apporter la moindre modification aux applications.

Quelques fonctionnalités clés de NetScaler AppFirewall :

Un modèle de sécurité hybride. 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. En complément, un moteur basé sur un modèle négatif s'appuie sur les signatures d'attaques pour assurer une protection efficace contre les menaces applicatives connues.

Sécurité XML. NetScaler AppFirewall ne se contente pas de bloquer les attaques courantes pouvant être modifiées pour cibler les applications XML (cross-site scripting, injection de commande, etc.), il intègre également un ensemble très complet de mesures de sécurité spécifiques à XML, comprenant une validation complète des schémas et la capacité à contrer les attaques de type déni de service (récursion excessive, par exemple).

Protection avancée des éléments dynamiques. De multiples protections de type « sensibles à la session » protègent les éléments applicatifs dynamiques, comme les cookies, les champs de formulaires et les adresses URL spécifiques à chaque session, contrant ainsi efficacement les attaques ciblant la relation de confiance établie entre le client et le serveur (comme, par exemple, la contrefaçon de requêtes cross-site).

Des stratégies de sécurité sur mesure. Un moteur d'apprentissage avancé détermine automatiquement le comportement attendu des applications Web d'entreprise et génère des recommandations stratégiques interprétables par l'utilisateur. Les administrateurs peuvent alors personnaliser la stratégie de sécurité en fonction des exigences propres à chaque application, et ainsi éviter les faux-positifs éventuels.

Une conformité garantie. NetScaler AppFirewall permet aux entreprises d'assurer leur conformité aux normes de sécurisation des données comme PCI-DSS, qui encourage explicitement l'utilisation de pare-feu applicatifs Web pour toutes les applications destinées au public et traitant des informations liées aux cartes de crédit. Des comptes-rendus détaillés peuvent être générés afin de documenter toutes les mesures de protection adoptées dans la stratégie de pare-feu pour se conformer aux obligations PCI.

Des performances sans compromis. La solution de sécurisation des applications Web la plus performante du marché délivre plus de 12 Gb/s de protection complète sans aucune dégradation des temps de réponse applicatifs.

Autre élément différenciateur de NetScaler AppFirewall : sa capacité inégalée à être déployée sous la forme d'un composant à part entière de la plateforme complète de mise à disposition d'applications NetScaler. Cette approche offre de nombreux avantages : gains significatifs de performance des applications Web (grâce aux fonctionnalités d'accélération avancée et de délestage des serveurs) et de fiabilité (grâce aux fonctionnalités de répartition de la charge serveur, de suivi de l'état des serveurs et de reprise au niveau du site). C'est en fin de compte une solution idéale, qui garantit une protection Web inégalée doublée d'une expérience applicative haute définition aux utilisateurs modernes extrêmement exigeants.

Conclusion

Par le passé, les pare-feu réseau classiques et les systèmes de prévention des intrusions suffisaient à fournir une protection appropriée à la poignée d'applications Web que les entreprises estimaient importantes. Désormais, du fait de la dépendance fortement accrue des entreprises vis-à-vis de leurs propriétés Web et de la dramatique évolution des attaques qui ciblent de plus en plus les applications, ce n'est plus le cas. Même les pare-feu de nouvelle génération ne suffisent pas, les améliorations qu'ils offrent se situant principalement dans la consolidation des infrastructures et la granularité accrue de définition et d'application des stratégies de contrôle d'accès.

Pour assurer une protection complète des nombreuses propriétés Web externes et internes de l'entreprise, les équipes en charge de la sécurité doivent compléter ces contremesures (qui demeurent utiles pour filtrer de gros volumes de menaces ciblant les couches inférieures) par un pare-feu applicatif Web. En maintenant une compréhension approfondie du fonctionnement normal de chaque application protégée et en recherchant toute anomalie de donnée ou de comportement au-delà de la couche protocole/services applicatifs, les pare-feu applicatifs Web complets comme NetScaler AppFirewall garantissent un degré élevé de protection qu'aucune autre technologie de sécurité courante, ancienne ou récente, n'est capable de fournir.

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

CITRIX®

À propos de Citrix
Citrix (NASDAQ : CTXS) est à la pointe de la transition vers le bureau logiciel. En combinant virtualisation, gestion de la mobilité, solutions networking et SaaS, Citrix offre aux entreprises et aux utilisateurs de nouveaux moyens pour mieux travailler. Les solutions Citrix favorisent la mobilité professionnelle grâce à des espaces de travail mobiles 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. Le chiffre d'affaires annuel de l'entreprise a atteint 3,14 milliards de dollars en 2014. 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