Le Forrester Wave ™: pare-feu applicatifs Web, T2 2018

Les 10 fournisseurs qui comptent le plus et comment ils se superposent

25 juin 2018

Par **Amy DeMartine** avec Christopher McClean , Kate Pesa , Trevor Lyness et Peggy Dostie

Pourquoi Lire Ce Rapport

Dans notre évaluation à 33 critères des fournisseurs de pare-feu applicatifs Web (WAF), nous avons identifié les 10 plus importants - Akamai Technologies, Amazon Web Services, Barracuda Networks, Cloudflare, F5 Networks, Fortinet, Imperva, Schwarz Cybersecurity - et les a recherchées, analysées et notées. Ce rapport montre comment chacun se mesure et aide les professionnels de la sécurité à faire le bon choix.

Points À Retenir

Akamai Technologies, F5 Networks et Imperva Incapsula mènent le pack

Les recherches de Forrester ont montré que sur le marché du pare-feu applicatif Web (WAF), Akamai Technologies, F5 Networks et Imperva Incapsula étaient en tête du peloton. Imperva SecureSphere, Radware, Barracuda Networks et Rohde & Schwarz Cybersecurity offrent des options compétitives. Cloudflare, Fortinet, Positive Technologies et Amazon Web Services sont à la traîne.

Les fournisseurs se démarquent en gardant le rythme grâce aux progrès des technologies et des attaques liées aux applications

Les attaquants malveillants cherchent constamment à violer les applications et les WAF constituent un élément clé d'une stratégie de prévention efficace et à plusieurs niveaux. Les professionnels de la sécurité ont besoin d'un WAF qui protège automatiquement les applications Web, garde une longueur d'avance sur les attaques du jour zéro et protège les nouveaux formats d'applications, tels que les API et les architectures sans serveur.

LES APPLICATIONS WEB SONT SANS DEFENSES

Les applications sont trop facilement violées. Quarante-deux pour cent des décideurs mondiaux de la sécurité des réseaux d'entreprise dont l'entreprise a subi une violation au cours des 12 derniers mois ont déclaré que les attaques étaient externes, les deux principales méthodes d'attaque externes étant les applications Web (injection SQL et scripts intersites). vulnérabilités logicielles. (voir note 1) Même dans un monde utopique, où les équipes de développement suppriment toutes les vulnérabilités et faiblesses connues du code source de leurs applications, les menaces continueront

d'exister sous la forme d'attaques «jour zéro». Les applications nécessitent une protection dans l'environnement de production.

Ne vous contentez pas d'utiliser des WAF pour être conforme; Les WAF devraient augmenter considérablement la protection

Les pare-feu d'applications Web ont été largement adoptés après 2006, lorsque la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) exigeait la protection des applications de l'environnement de production avec des fichiers WAF ou des outils similaires. (voir note 2) Les WAF ont évolué pour être plus utilisables, évolutifs et mieux adaptés aux menaces, ce qui les rend pertinents dans le monde des pirates intelligents et motivés et des applications hybrides qui vivent sur site et dans le cloud. Pour trouver un WAF allant au-delà de la conformité afin de réduire considérablement le risque de violation d'une application, recherchez les éléments suivants:

- **Les mises à jour continues devraient suivre l'évolution des technologies et des attaques des applications.** Le paysage que les professionnels de la sécurité doivent protéger évolue pour inclure de nouvelles options de déploiement d'applications et de nouveaux types d'applications, tels que les API et l'architecture sans serveur. En outre, les pirates utilisent une combinaison de méthodes manuelles et automatisées pour rechercher en permanence de nouvelles façons de violer les applications. Par conséquent, les WAF doivent utiliser des méthodes de détection d'attaques automatisées telles que l'évaluation des risques, la liste blanche dynamique et la prise d'empreintes digitales pour comprendre si et quand une attaque se produit. À leur tour, les professionnels de la sécurité doivent être convaincus que les capacités de détection et de prévention de leur WAF resteront à la hauteur des attaques de demain.

- **Les capacités de sécurité devraient inclure diverses techniques de prévention et de réponse.** Il n'y a pas si longtemps qui devait distinguer les utilisateurs réels des attaquants automatisés utilisant captcha (test entièrement automatisé du public Turing pour dire les ordinateurs et les humains à part) la façon la plus avancée pour contester une demande d'application Web. Cependant, les clients étaient rapidement frustrés par le captcha et les attaquants persistants ont trouvé des moyens de le contourner. (voir note 3) Désormais, les fichiers WAF doivent identifier et prévenir les attaques avec un large éventail de méthodes de sécurité, telles que la prévention des fuites de données, les pots de miel, les instructions erronées et l'application de correctifs virtuels.

- **Les données d'attaque doivent être facilement disponibles pour améliorer le développement et le déploiement.** Historiquement, les fichiers WAF étaient des îlots de données d'attaque que les clients exportaient peut-être dans un format brut et difficile à corréler vers un outil SIM. Aujourd'hui, les développeurs ont besoin de comprendre comment les attaquants ciblent les applications afin qu'ils puissent hiérarchiser les mesures correctives, les équipes de distribution d'applications ont besoin d'un moyen facile de mettre à jour les règles WAF pour couvrir les vulnérabilités ou faiblesses qui ne sont pas assainis avant la sortie, et les professionnels de la sécurité ont besoin des alertes consolidées et des capacités de prévention pour étouffer les attaquants persistants. Les attentes des acheteurs pour le WAF sont incroyablement élevées.

APERÇU DE L'ÉVALUATION DE LA WAF

Pour évaluer l'état du marché WAF et voir comment les fournisseurs s'accumulent, Forrester a évalué les forces et les faiblesses des principaux fournisseurs de WAF. Après avoir examiné les recherches passées, les évaluations des besoins des utilisateurs et les entretiens avec les fournisseurs et les experts, nous avons développé un ensemble complet de 33 critères, que nous avons regroupés en trois catégories:

- **Offre actuelle** La position de chaque fournisseur sur l'axe vertical du graphique Forrester Wave ™ indique la force de son offre actuelle. Les critères clés pour cette évaluation comprennent la détection des attaques; réponse à l'attaque; interface de gestion; protection contre les attaques de jour zéro; rapports et analyses; et des boucles de rétroaction avec les outils de développement, de SecOps et de numérisation préliminaire.

- **Stratégie.** Le positionnement sur l'axe horizontal indique la force de la stratégie de chaque fournisseur. Notre évaluation de la stratégie comprenait la stratégie de produit, l'approche du marché, la feuille de route de l'exécution et la formation.

- **Presence COMMERCIALE.** Représentés par la taille des marqueurs sur le graphique, nos scores de présence sur le marché reflètent la base d'installation, le taux de croissance et la rentabilité de chaque fournisseur.

Critères d'évaluation des fournisseurs et d'inclusion

Forrester incluait 10 fournisseurs dans l'évaluation: Akamai Technologies, Amazon Web Services (AWS), Barracuda Networks, Cloudflare, F5 Networks, Fortinet, Imperva, Positive Technologies, Radware et Rohde & Schwarz Cybersecurity (RSCS). Chacun de ces fournisseurs a (voir Figure 1):

- **Un outil WAF complet et professionnel.** Tous les fournisseurs de cette évaluation proposent une gamme de fonctionnalités WAF adaptées aux professionnels de la sécurité. Les fournisseurs participants devaient disposer de la plupart des fonctionnalités suivantes: détection des attaques pour les applications Web, y compris les API; capacité à bloquer les attaques, y compris les attaques du jour zéro; l'utilisation de l'apprentissage automatique pour modifier les règles; et la possibilité de signaler visuellement les données d'attaque.

- **10 millions de dollars ou plus en 2017 revenus WAF.** Tous les fournisseurs de cette évaluation ont généré des revenus globaux de 10 millions de dollars ou plus directement à partir des capacités WAF.

- **Intérêt des clients de Forrester ou pertinence pour eux.** Les clients de Forrester discutent souvent des fournisseurs et des produits participants pendant les enquêtes et les entretiens. Selon le jugement de Forrester, le fournisseur participant peut également être inclus en raison de ses capacités techniques et de sa présence sur le marché.

Figure 1: Fournisseurs évalués: informations sur les produits et critères d'inclusion

Vendor	Product evaluated	Product version evaluated
Akamai Technologies	Kona Site Defender	5
Amazon Web Services	AWS WAF AWS Firewall Manager	07/03/2018
Barracuda Networks	Barracuda Web Application Firewall	9.1
Cloudflare	Cloudflare WAF	07/03/2018
F5 Networks	F5 Silverline WAF F5 Silverline WAF Express F5 Advanced WAF F5 Application Security Manager	13.1.0
Fortinet	FortiWeb	5.8.5
Imperva	Incapsula	07/03/2018
Imperva	SecureSphere	13
Positive Technologies	PT Application Firewall	3.6.3
Radware	AppWall, Alteon, Cisco WAF, Cisco ACI, AppWall VA, Alteon VA, Cloud WAF	AppWall 7.5.7, Alteon 32.0.1, Cloud WAF 3.6
Rohde & Schwarz Cybersecurity	Web Application Firewall	WAF 6.4

Vendor inclusion criteria

A comprehensive, enterprise-class WAF tool. All vendors in this evaluation offer a range of WAF capabilities suitable for security pros. Participating vendors were required to have most of the following capabilities out of the box: attack detection for web applications, including APIs; ability to block attacks, including zero-day attacks; the use of machine learning to modify rules; and the ability to visually report attack data.

$10 million or more in 2017 WAF revenue. All vendors in this evaluation earned $10 million or more in global revenue directly from WAF capabilities.

Interest from Forrester clients or relevance to them. Forrester clients often discuss the participating vendors and products during inquiries and interviews. Alternatively, the participating vendor may, in Forrester's judgment, have warranted inclusion because of technical capabilities and market presence.

PROFILS DE VENDEURS

Cette évaluation du marché WAF se veut un point de départ uniquement. Nous encourageons les clients à consulter des évaluations détaillées des produits et à adapter les pondérations des critères en fonction de leurs besoins individuels via l'outil de

comparaison des fournisseurs basé sur Forrester Wave Excel (voir la figure 2 et la figure 3). Cliquez sur le lien au début de ce rapport sur Forrester.com pour télécharger l'outil.

Figure 2: Forrester Wave ™: Pare-feu d'applications Web, Q2 2018

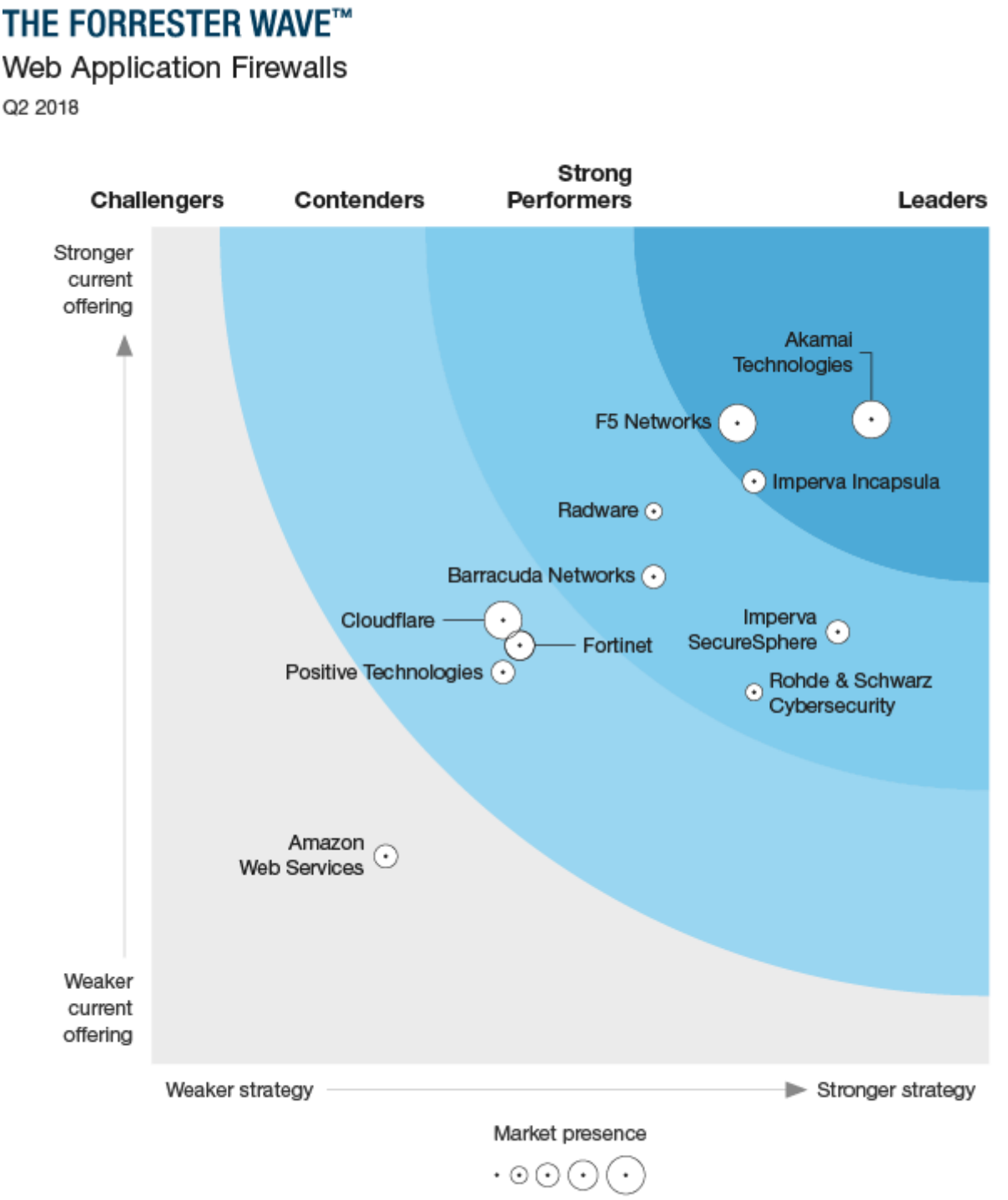

Figure 3: Forrester Wave ™: Tableau de bord des pare-feu applicatifs Web, deuxième trimestre de 2018

	Forrester's weighting	Akamai Technologies	Amazon Web Services	Barracuda Networks	Cloudflare	F5 Networks	Fortinet	Imperva Incapsula	Imperva SecureSphere	Positive Technologies	Radware	Rohde & Schwarz Cybersecurity
Current Offering	50%	3.85	1.24	2.91	2.65	3.83	2.50	3.48	2.58	2.34	3.30	2.22
Attack detection	25%	4.20	1.00	2.90	2.40	4.30	2.40	2.90	3.90	2.80	3.70	3.00
Attack response	30%	3.80	1.00	3.60	3.80	5.00	3.60	4.40	1.60	1.60	3.60	2.40
Management interface	10%	3.60	2.60	2.30	1.50	2.10	2.10	2.90	3.60	2.00	3.10	2.30
Zero-day attacks	20%	5.00	1.40	2.60	3.00	3.00	1.40	4.20	1.40	3.00	3.00	1.00
Reporting and analytics	10%	2.20	1.00	1.80	1.00	3.00	1.80	2.20	3.00	2.20	1.80	1.80
Feedback loops	5%	1.60	1.00	3.40	1.20	2.80	3.00	1.60	3.60	2.80	4.00	2.80
Strategy	50%	4.30	1.40	3.00	2.10	3.50	2.20	3.60	4.10	2.10	3.00	3.60
Product strategy	50%	3.80	1.80	3.00	2.20	3.40	2.20	3.40	4.20	3.00	2.20	3.40
Market approach	25%	5.00	1.00	3.00	3.00	3.00	3.00	5.00	5.00	1.00	5.00	5.00
Execution road map	20%	5.00	1.00	3.00	1.00	5.00	1.00	3.00	3.00	1.00	3.00	3.00
Training	5%	3.00	1.00	3.00	1.00	1.00	3.00	1.00	3.00	3.00	1.00	1.00
Market Presence	0%	4.46	2.60	2.80	4.42	4.48	3.12	2.94	2.62	2.90	1.50	1.32
Install base	60%	4.60	1.00	3.00	4.20	4.80	3.20	3.40	3.20	2.00	2.00	1.20
Growth rate	10%	2.00	5.00	1.00	4.00	1.00	3.00	3.00	1.00	5.00	3.00	0.00
Corporate profitability	30%	5.00	5.00	3.00	5.00	5.00	3.00	2.00	2.00	4.00	0.00	2.00

All scores are based on a scale of 0 (weak) to 5 (strong).

141629 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Dirigeants

- **Akamai Technologies renforce la valeur de son réseau de diffusion de contenu avec WAF.** L'offre WAF d'Akamai Technologies est Kona Site Defender. Ces dernières années, la société a ajouté davantage de fonctionnalités de libre-service au produit, notamment la possibilité pour ses clients de créer leurs propres règles personnalisées et a introduit Web Application Protector. Akamai offre une très forte couverture d'attaque de jour zéro et une forte détection des attaques, avec une réponse aux attaques sonores et une

interface utilisateur de gestion. Les clients de référence ont loué l'intégration entre les services WAF et CDN d'Akamai, ainsi que la stabilité et la fiabilité du WAF. Cependant, les clients ont exprimé leur frustration quant à leur capacité à gérer les nouveaux types d'attaques et à limiter les alertes en temps réel.

- **F5 Networks permet de contrôler les WAF déployés dans les déploiements de cloud hybride.** F5 Networks fournit des fonctionnalités WAF via son service géré par Silverline et son offre autogérée, ainsi que l'appliance WAF avancée et son dispositif traditionnel Application Security Manager, doté d'options de déploiement de dispositifs standard ou virtuels. Ces produits offrent une réponse aux attaques très forte et des capacités de détection d'attaques puissantes. Ils offrent une couverture, des rapports et des analyses d'attaques de jour zéro fiables. Les clients de référence de F5 Networks ont fait l'éloge du support qu'ils recevaient de la part de l'entreprise, tout en notant le besoin de connaissances techniques approfondies pour utiliser certaines fonctionnalités, telles que le script iRules.

- **Imperva Incapsula évalue toutes les attaques pour protéger tous les clients.**Incapsula est l'un des deux produits WAF du portefeuille d'Imperva, acquis via une acquisition en 2014. Outre les règles de sécurité natives du produit, l'équipe de sécurité d'Incapsula examine en permanence les données d'attaque, crée des règles pour bloquer les menaces et les déploie. atteindre tous les clients en moins d'une minute. Le produit Incapsula offre une forte réponse aux attaques et une couverture de jour zéro. Les clients de référence ont exprimé leur frustration à l'égard de l'interface utilisateur de gestion du produit, des supports de formation, de la détection des menaces, des rapports et des analyses, ainsi que des boucles de rétroaction. Imperva dispose d'une interface utilisateur sur sa feuille de route qui permettra aux clients de gérer à la fois ses produits Incapsula et SecureSphere WAF.

Des artistes performants

- **Imperva SecureSphere offre aux clients un contrôle granulaire et un aperçu de leur WAF.** L'un des deux produits WAF du portefeuille d'Imperva, SecureSphere offre une détection des attaques sonores, une interface utilisateur de gestion, des rapports et des analyses, ainsi que des boucles de rétroaction. Les clients peuvent payer un supplément pour s'abonner aux services ThreatRadar de la société afin d'améliorer les renseignements sur les menaces et la création automatique de règles, mais ces fonctionnalités ne sont pas incluses dans cette évaluation. (voir note 4) Les clients d'Imperva SecureSphere ont fait l'éloge du contrôle granulaire et de la perspicacité du produit. Imperva dispose

d'une interface utilisateur sur sa feuille de route qui permettra aux clients de gérer à la fois ses produits Incapsula et SecureSphere WAF.

- **Radware offre aux clients un large éventail d'options de déploiement.** Radware propose WAF en tant que service géré, appliance, machine virtuelle et module ADC au-dessus des plates-formes Alteon. Les produits intègrent des boucles de rétroaction et une détection des attaques sonores, une réponse aux attaques, une interface de gestion et une couverture d'attaques de jour zéro. Les clients de référence de Radware ont fait l'éloge de la flexibilité de déploiement et de la valeur des fonctionnalités pour le prix, mais ils ont exprimé leur frustration avec le matériel de formation de la société. Les clients de Radware peuvent obtenir une licence pour des fonctionnalités de reporting supplémentaires avec le produit distinct de la société, Vision, et le service d'abonnement de la société, Vision Reporter, dont aucun n'est pris en compte dans cette évaluation.

- **Barracuda Networks applique des règles à partir d'hôtes sécurisés et de scanners de vulnérabilité.** Barracuda WAF peut continuellement apprendre de nouvelles règles de liste blanche d'applications, avec la possibilité de limiter l'apprentissage aux seuls hôtes de confiance. En plus de prendre en charge une variété de scanners de vulnérabilité Web, Barracuda Networks propose également son propre scanner de service de correction de vulnérabilité. Les clients peuvent importer des résultats d'analyse dans le Barracuda WAF et appliquer de nouvelles règles basées sur ces derniers en tant que correctifs virtuels. Barracuda WAF offre une réponse aux attaques sonores et des boucles de rétroaction. La société n'a pas été en mesure de fournir des clients de référence.

- **RSCS a acquis DenyAll pour fournir WAF avec ses autres produits de sécurité.** En décembre 2016, RSCS a acquis DenyAll. RSCS WAF (anciennement DenyAll WAF) peut utiliser les résultats de RSCS Vulnerability Manager pour créer des correctifs virtuels pour des vulnérabilités d'applications spécifiques. DenyAll WAF offre de fortes capacités de détection d'attaque. RSCS n'a pu fournir qu'un seul client de référence, qui a loué la facilité d'utilisation du produit, mais souhaiterait disposer de fonctionnalités supplémentaires de reporting et d'analyse.

Les prétendants

- **Cloudflare inclut des fonctionnalités WAF pour tous les clients.** Cloudflare fournit quatre plans d'abonnement pour ses clients; le plan gratuit inclut les fonctionnalités de base de WAF et les plans payés incluent une fonctionnalité

WAF complète. Actuellement, les clients ne peuvent ajouter de nouvelles règles personnalisées qu'en fournissant des détails d'attaque à l'équipe de sécurité de Cloudflare, qui examine les demandes et crée de nouvelles règles à déployer dans les environnements clients. Cependant, avec la nouvelle fonctionnalité de Cloudflare Workers, les clients peuvent créer des validations API et spécifiques au client à l'aide de JavaScript sur la plate-forme Edge de Cloudflare. Cloudflare offre une réponse aux attaques sonores et une attaque par jour zéro. Les clients de Cloudflare apprécient la facilité de mise en œuvre du produit et les règles prêtes à l'emploi, mais demandent des alertes par e-mail et un plus grand libre-service via les API.

- **Fortinet FortiWeb renforce la sécurité avec des intégrations avec d'autres produits Fortinet.** Fortinet a récemment ajouté un WAF FortiWeb hébergé basé sur le cloud pour augmenter ses offres de cloud, de machines virtuelles et d'applications. Le produit FortiWeb WAF intègre une forte réponse aux attaques et des boucles de rétroaction. Les clients peuvent s'abonner aux services FortiGuard Web Application Security, qui mettent à jour les clients avec les dernières règles de sécurité, que ce soit toutes les deux semaines ou en cas d'urgence. Les clients de référence de Fortinet ont fait l'éloge du prix et de l'assistance de FortiWeb, mais souhaitaient un meilleur reporting et une déconnexion.

- **Positive Technologies utilise l'apprentissage automatique pour établir un trafic normal.** Le produit Positive Technologies Application Firewall (PT AF) utilise des techniques d'apprentissage automatique pour comprendre à quoi ressemble un trafic normal, puis alerte les utilisateurs et bloque le trafic en cas d'anomalies. PT AF a une intégration avec PT Application Inspector pour créer des patchs virtuels basés sur des analyses SAST, DAST et IAST. PT AF offre une couverture sonore de l'attaque zéro jour. Les clients de référence de la société ont fait l'éloge de la détection du produit et de l'application des correctifs virtuels, mais souhaitaient davantage de rapports et d'analyses.

Challengers

- **AWS WAF est l'un des 13 services de sécurité disponibles pour les déploiements dans le cloud.** Les clients peuvent choisir de déployer AWS WAF sur Amazon CloudFront, qui peut gérer une Amazon API Gateway ou un équilibreur de charge d'application. La nouvelle version de AWS Firewall Manager est une console unificatrice permettant de gérer plusieurs déploiements WAF sur des ressources de plusieurs comptes. Pour obtenir encore plus de visibilité et de contrôle, des services supplémentaires ne sont pas inclus dans cette évaluation. Par exemple, CloudTrail peut fournir une journalisation et des

rapports. Les modèles CloudFormation peuvent créer, mettre à jour et supprimer des ressources AWS WAF. et Kinesis Data Firehose peut transférer des données en continu dans des magasins de données et des outils d'analyse. Seuls les clients qui déploient uniquement sur AWS trouveront ces services utiles pour comprendre et gérer leur WAF. Les clients de référence de l'entreprise ont noté le produit '

MATÉRIEL SUPPLÉMENTAIRE

Ressource en ligne

La version en ligne de la figure 2 est un outil de comparaison de fournisseurs basé sur Excel qui fournit des évaluations détaillées des produits et des classements personnalisables. Cliquez sur le lien au début de ce rapport sur Forrester.com pour télécharger l'outil.

Sources de données utilisées dans cette vague Forrester

Forrester a utilisé une combinaison de trois sources de données pour évaluer les forces et les faiblesses de chaque solution. Nous avons évalué les fournisseurs participant à ce Forrester Wave, en partie, en utilisant les documents qu'ils nous ont fournis au plus tard le 7 mars 2018.

- **Enquêtes auprès des fournisseurs.** Forrester a interrogé les fournisseurs sur leurs capacités en fonction des critères d'évaluation. Une fois que nous avons analysé les enquêtes réalisées auprès des fournisseurs, nous avons effectué des appels aux fournisseurs, le cas échéant, afin de recueillir des informations sur les qualifications des fournisseurs.

- **Présentation de la stratégie produit et démos.** Nous avons demandé aux fournisseurs de faire des démonstrations des fonctionnalités de leurs produits. Nous avons utilisé les résultats de ces démonstrations de produits pour valider les détails des fonctionnalités de chaque fournisseur.

- **Enquêtes de référence client.** Pour valider les qualifications des produits et des fournisseurs, Forrester a également effectué des appels de référence avec trois des clients actuels de chaque fournisseur.

La méthodologie des vagues de Forrester

Nous effectuons des recherches primaires pour développer une liste de fournisseurs qui répondent à nos critères d'évaluation sur ce marché. À partir de ce groupe initial de

fournisseurs, nous réduisons notre liste finale. Nous choisissons ces fournisseurs en fonction des critères suivants: 1) ajustement du produit; 2) le succès client; et 3) la demande du client Forrester. Nous éliminons les fournisseurs qui ont des références clients limitées et des produits qui ne correspondent pas à la portée de notre évaluation. Les fournisseurs marqués comme participants incomplets répondaient à nos critères d'inclusion définis mais ont refusé de participer ou n'ont contribué que partiellement à l'évaluation.

Après avoir examiné les recherches antérieures, les évaluations des besoins des utilisateurs et les entretiens avec les fournisseurs et les experts, nous développons les critères d'évaluation initiaux. Pour évaluer les fournisseurs et leurs produits par rapport à notre ensemble de critères, nous collectons des informations sur les qualifications des produits en combinant des évaluations en laboratoire, des questionnaires, des démonstrations et / ou des discussions avec les références des clients. Nous envoyons des évaluations aux fournisseurs pour examen et nous ajustons les évaluations pour fournir une vue plus précise des offres et des stratégies des fournisseurs.

Nous définissons des pondérations par défaut afin de refléter notre analyse des besoins des grandes entreprises utilisatrices - et / ou d’autres scénarios, comme indiqué dans l’évaluation Forrester Wave - puis nous évaluons les fournisseurs selon une échelle clairement définie. Nous souhaitons que ces pondérations par défaut ne servent que de point de départ et encouragent les lecteurs à adapter les pondérations à leurs besoins individuels via l'outil Excel. Les notes finales génèrent la représentation graphique du marché en fonction de l'offre actuelle, de la stratégie et de la présence sur le marché. Forrester a l'intention de mettre à jour régulièrement les évaluations des fournisseurs au fur et à mesure de l'évolution des capacités des produits et des stratégies des fournisseurs. Pour plus d'informations sur la méthodologie suivie par Forrester Wave, veuillez consulter sur notre site Internet.

Politique d'intégrité

Nous effectuons toutes nos recherches, y compris les évaluations de Forrester Wave, conformément aux informations affichées sur notre site Web.