Plans de service Radware Cloud Application Protection

Le service de protection des applications cloud de Radware offre des capacités de sécurité intelligentes alimentées par l'IA, ainsi qu'une automatisation avancée et des services de sécurité de pointe fournis par l'ERT (Emergency Response Team) de Radware, réputé dans le secteur.

Le service est proposé en trois plans. Chaque plan est conçu pour répondre à des besoins différents en matière de cybersécurité et d'exposition aux risques, ainsi qu'à différents niveaux de services gérés.

Protection des applications en nuage

Plan standard

Le plan Standard de Radware offre le niveau de protection de référence de l'industrie avec des fonctions et des capacités uniques supplémentaires. Il inclut le Cloud WAF de Radware, la protection des API, la protection contre les attaques du jour zéro, la protection de base contre les bots et une protection DDoS réseau de 1 Gbps, ainsi que l'accord de niveau de service exceptionnel de Radware.

Protection des applications en nuage

Plan avancé

Le plan Advanced de Radware fait passer la sécurité des applications au niveau supérieur en offrant des capacités de protection avancées pour ceux qui veulent s'assurer qu'ils sont bien protégés contre les attaques plus sophistiquées et inconnues. Ce plan inclut, en plus du plan standard, le WAF avancé de Radware avec son moteur de protection d'accès au chemin qui protège contre les attaques inconnues et zero-day plus sophistiquées, le moteur de corrélation basé sur l'IA (blocage de la source), une protection DDoS réseau de 10 Gbps, ainsi que la cartographie, la surveillance et la détection des attaques de la chaîne d'approvisionnement JS pour la protection côté client. Elle inclut également le flux de renseignements de Radware - ERT Active Attackers Feed (EAAF), ainsi qu'une assistance supplémentaire pour l'intégration et la révision des politiques.

Protection des applications en nuage

Plan complet

Le plan complet de Radware offre une couverture de sécurité pour l'ensemble de votre environnement applicatif. Du côté client au côté serveur et tout ce qui se trouve entre les deux. Ce plan comprend tout ce que le plan Advanced a à offrir, avec en plus Radware's Bot Manager et sa détection et son atténuation multicouches basées sur le comportement, la découverte automatisée d'API et la génération de politiques de sécurité API, la protection en temps réel contre les attaques API Business Logic et la mise en œuvre de la protection côté client.

	Radware Cloud Application Protection Service		
	 Standard	 Avancé	 Compléter
WAF	✓	✓	✓
Protection de l'API	✓	✓	✓
Protection de base contre les bots	✓	✓	✓
Règles avancées	✓	✓	✓
Limite du taux	✓	✓	✓
Contrôle d'accès et règles géographiques IP	✓	✓	✓
Rapports et analyses	✓	✓	✓
Demandes de renseignements sur les menaces (par mois)	50	50	50
Protection contre les attaques DDoS	1Gbps	10Gbps	10Gbps
Soutien standard	✓	✓	✓
Soutien avancé	✗	✓	✓
WAF avancé (Path Access Protection & AI-based Correlation)	✗	✓	✓
EAAF	✗	✓	✓
Protection côté client - Détection	✗	✓	✓
Protection côté client - Atténuation	✗	✗	✓
Découverte de l'API	✗	✗	✓
Protection contre les attaques de logique commerciale (BLA) de l'API	✗	✗	✓
Gestionnaire de robots	✗	✗	✓
Équilibreur de charge en tant que service*	Basculement	De base	Avancé
Protection contre les attaques DDoS sur le web	Complément d'information	Complément d'information	Complément d'information
Extension de la conformité PCI DSS 4	✗	Complément d'information	Complément d'information
DNS en tant que service	Complément d'information	Complément d'information	Complément d'information
Service de renseignement sur les menaces	Complément d'information	Complément d'information	Complément d'information
Conservation des données	30 jours	60 jours	90 jours
DDoS illimité	Complément d'information	Complément d'information	Complément d'information
CDN	Complément d'information	Complément d'information	Complément d'information
Soutien Premium	Complément d'information	Complément d'information	Complément d'information

Compléments

Protection contre les attaques DDoS sur le web

Protection de pointe de la couche applicative (L7) contre les attaques DDoS, basée sur la détection comportementale unique de Radware, fondée sur l'apprentissage automatique, qui distingue le trafic légitime du trafic malveillant et génère automatiquement des signatures granulaires en temps réel pour protéger contre les attaques de type " zero-day ". Avec des options uniques de déploiement de services DDoS en nuage hybrides, toujours actifs et à la demande, le service Cloud Web DDoS Protection de Radware offre une sécurité de premier ordre contre une grande variété de menaces, notamment les inondations HTTP, les bombes HTTP, les assauts faibles et lents, les attaques par force brute et les tsunamis DDoS en ligne perturbateurs.

ERT Premium Managed Service

Pour les organisations qui ne disposent pas de l'expertise en matière de cybersécurité en interne ou qui souhaitent simplement réduire davantage leurs frais de sécurité, Radware propose le service géré ERT Premium, d'une valeur inestimable :

- Accord de niveau de service SLA) pour une réponse dans les 10 minutes grâce à l'accès à la ligne directe
- Réponse d'urgence à la demande Atténuation des attaques
- Responsable de la réussite des clients
- Analyse médico-légale post-attaque et recommandations
- Rapports périodiques sur l'état de la sécurité
- Traitement des cas de service prioritaire
- Optimisation des politiques et aperçu de la sécurité des applications
- Journaux d'accès
- NoKey - Service de stockage des clés privées des certificats SSL/TLS grâce à l'intégration du HSM

CDN

Pour les entreprises qui souhaitent combiner la diffusion de sites Web avec la sécurité de leurs applications Web, Radware propose une solution de réseau de diffusion de contenu (CDN) intégrée directement dans le portail de protection des applications de Radware. solution CDN de Radware est basée sur Amazon CloudFront CDN pour une empreinte massive et mondialement distribuée, des performances améliorées et une convivialité DevOps.

Protection DDoS illimitée

Pour les entreprises qui subissent des attaques DDoS à haut volume et dont la capacité d'atténuation de 1G ou 10G ne suffit pas, Radware offre une protection illimitée grâce à sa solution de protection DDoS la mieux notée du secteur. Défendez votre entreprise contre les attaques DDoS les plus avancées, quelle que soit leur fréquence ou leur volume.

Contactez un conseiller Radware Cyber Security pour savoir quel plan correspond le mieux aux besoins de sécurité de votre entreprise.

Conformité PCI DSS 4

En plus du WAF et de la protection de l'API contre les attaques de logique commerciale, qui sont nécessaires pour la conformité à PCI DSS 4 et inclus dans les plans de service de Radware Cloud Application Protection, le module complémentaire Radware PCI DSS 4 offre aux clients des contrôles de protection étendus et spécifiques côté client, comme l'exigent les sections 6.4.3 et 11.6.1 de PCI DSS 4 :

- Il offre une visibilité complète de tous les scripts tiers exécutés du côté client de votre application, ainsi qu'un inventaire détaillé de tous les scripts. Cet outil comprend des alertes de suivi de l'activité en temps réel et des évaluations du niveau de menace, ainsi que des informations sur le script, s'il est autorisé ou non, et pourquoi, ainsi que des informations sur la source du script et le domaine de destination.
- Il vous informe de toute tentative de manipulation des en-têtes HTTP, des pages de formulaire et de paiement, et de toute tentative de DOM XSS.

Service de renseignement sur les menaces

Les services Radware Threat Intelligence permettent de comprendre pourquoi certaines IP sont signalées, en fournissant en temps réel des informations et un contexte inestimables. Ces informations exploitables vous permettront d'évaluer les menaces en toute confiance, de prendre des décisions éclairées et de vous défendre de manière proactive contre les menaces avant qu'elles ne s'aggravent. Qu'il s'agisse de bloquer une IP suspecte, d'affiner vos défenses ou d'identifier les systèmes compromis, nous sommes là pour vous aider. Les principales caractéristiques des services de renseignement sur les menaces sont les suivantes

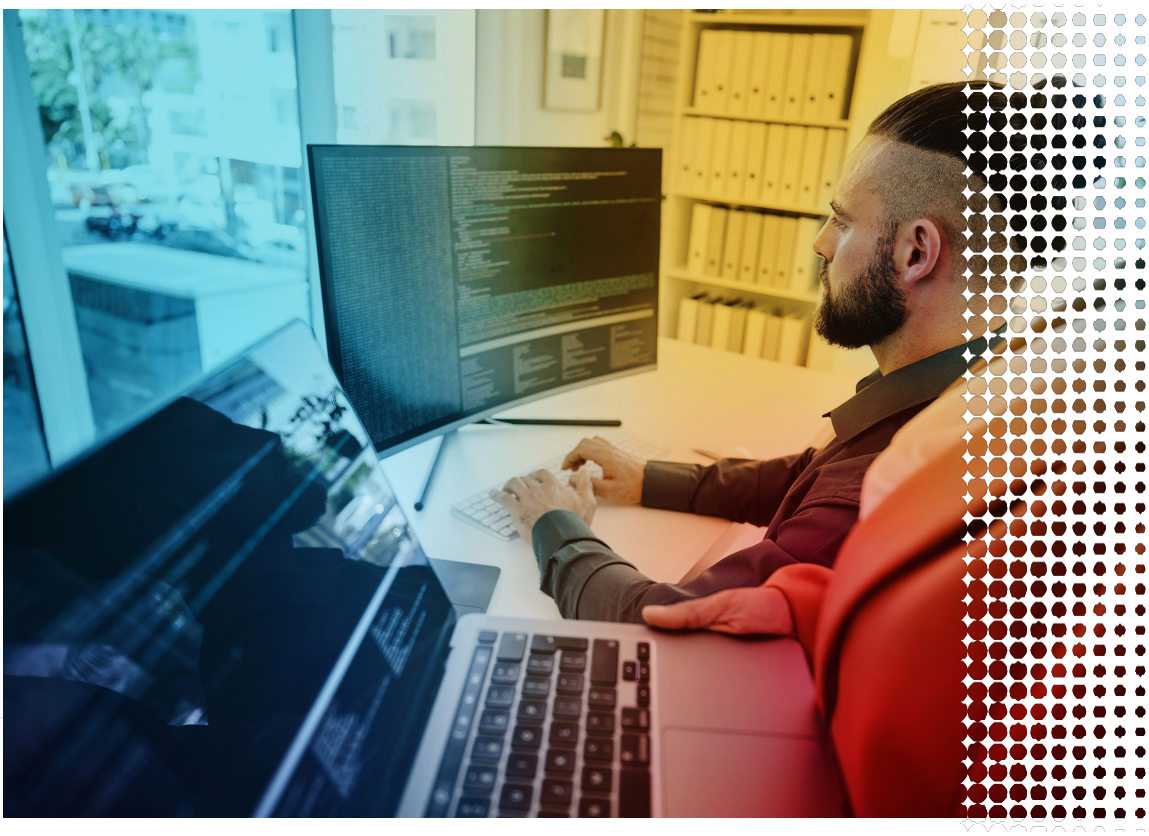
- Données exploitables issues de cyberattaques réelles
- Recherche de toute adresse IP suspecte avec IP insights, Open Proxys et Malware Data
- Alerte à la réputation pour garantir la sécurité et l'intégrité du réseau en informant de manière proactive des cyber-attaques potentielles provenant du réseau de l'organisation.
- Intégration transparente de l'API REST à tout environnement, aux flux de travail et aux systèmes de sécurité existants

DNS en tant que service

Radware DNSaaS offre une gestion complète du système de noms de domaine (DNS), qui est essentielle au fonctionnement transparent de toute application en ligne. L'investissement dans DNSaaS ne se limite pas à la gestion des noms de domaine ; s'agit de protéger la présence numérique de votre entreprise et de garantir à vos utilisateurs finaux une expérience transparente. Radware DNSaaS comprend :

- Une console de gestion centralisée avec une interface facile à utiliser pour gérer tous les hôtes DNS, les enregistrements et les configurations de contrôle de santé en un seul endroit.
- Contrôles de santé personnalisables pour une surveillance continue de l'état des sources de l'application.
- Options flexibles d'acheminement des enregistrements pour une haute disponibilité basée sur les politiques Geo et Failover.
- Contrôle de la distribution du trafic vers des ressources ou des points d'extrémité spécifiques afin que les utilisateurs finaux puissent être servis à partir du centre de données le plus proche ou le plus approprié, ce qui permet d'améliorer la qualité du service.
  la latence et l'expérience de l'utilisateur.
- Analyse en temps réel du nombre de requêtes par zone hébergée.

Le service DNS-as-a-Service est proposé en trois formules distinctes, dont le prix dépend du nombre de zones hébergées, du volume de requêtes DNS mensuelles et de la quantité d'objets de contrôle de santé.



Équilibreur de charge en tant que service

Radware Load Balancer as a Service (LBaaS) complète les services de protection des applications en nuage en améliorant le SLA et l'évolutivité tout en maintenant une haute disponibilité et en protégeant tous les sites d'origine. Il assure l'équilibrage actif/actif du trafic et de la charge utilisateur entre les sites d'origine.

	Basculement	De base	Avancé
Basculement (actif-secondaire)	✓	✓	✓
Nombre de serveurs réels actifs (origines)	1	8	8
Support multiport	✗	✓	✓
Équilibrage de charge actif-actif - Round Robin	✗	✓	✓
Persistance basée sur l'IP	✗	✓	✓
Équilibrage de la charge basé sur l'URL	✗	✗	✓
Équilibrage actif-actif de la charge - Connexion la plus faible	✗	✗	✓
Persistance basée sur les cookies	✗	✗	✓

Niveaux de soutien des services gérés

	Priorité basée sur le risque et l'impact	Soutien standard	Soutien avancé	ERT Premium Service (Add-On)
Réponse SLA	P1 (téléphone)	40 Min	30 minutes	10 Min
	P1 (Billet)	3 heures	2 heures	60 Min
	P2	6 heures	4 heures	2 heures
	P3	16 heures	12 heures	4 heures
	P4	24 heures	24 heures	12 heures
Mise à jour des billets	P1	48 heures	48 heures	24 heures
	P2	96 heures	72 heures	48 heures
	P3	120 heures	96 heures	72 heures
	P4	144 heures	120 heures	96 heures
Services gérés	Gestion des certificats et notifications	✗	✓	✓
	Onboarding et révision de la politique	✗	✓	✓
	Analyse post-attaque	✗	✓	✓
	Assistance par chat	✗	✓	✓
	Journaux d'accès	✗	✗	✓
	Rapport trimestriel sur la sécurité des primes	✗	✗	✓
	Préparation des événements spéciaux annuels	✗	✗	✓
	Test d'attaque annuel (DDoS L3-7)	✗	✗	✓
	Recommandations proactives en matière de sécurité	✗	✗	✓
	Examen de la configuration de la sécurité	✗	6 mois	3 mois
	Surveillance prolongée	✗	Contrôle externe sur les 5 principales applications	Surveillance externe de toutes les applications
	NoKey - Intégration HSM	✗	✗	✓ Disponibilité limitée