UBIKA

le nouveau DenyAll

L'EXPERT SOUVERAIN EUROPÉEN DE LA SÉCURITÉ APPLICATIVE

SOMMAIRE

LES ASSISES

Nos temps forts de l'événement

ATELIER, jeudi 12 octobre, 15h

RETEX CNAM : relever le défi d'une sécurisation renforcée des APIs et dans un environnement SecNumCloud avec 3DS OUTSCALE

Avec Alexandre Fenyo, RSSI de Mon Espace Santé et du Dossier Médical Partagé, à la CNAM, nous verrons pourquoi les Applications Web et API sont vulnérables, comment elles sont exploitées et comment les protéger des attaques. Vous découvrirez son retour d'expérience sur la protection des applications Web et des API à l'aide d'un WAAP souverain.

Edouard CAMOIN, VP Résilience, croisera ce retour d'expérience en mettant en lumière les bénéfices des solutions hébergées dans le cloud d'hyper-confiance d'OUTSCALE.

- Retrouvez-nous sur le STAND 104, niveau Diaghilev, dans le village HEXATRUST.
- Participez à notre tirage au sort sur notre stand pour GAGNER une enceinte.

Vision marché

D'ici 2024, 70 % des entreprises mettant en œuvre des stratégies multicloud pour les applications web dans les environnements de production privilégieront les services de plateforme de protection des applications web et des API dans le cloud (WAAP) par rapport aux appliances WAAP et aux WAAP natifs IaaS.

D'ici 2026, 40 % des entreprises choisiront un fournisseur de WAAP sur la base de ses fonctions avancées de protection des API et de sécurité des applications web - contre moins de 15 % en 2022.

D'ici 2026, plus de 40 % des entreprises ayant des applications orientées vers le consommateur et qui ne comptaient initialement que sur un WAAP pour atténuer les attaques de robots chercheront à obtenir une technologie supplémentaire de détection d'anomalies auprès de fournisseurs spécialisés - contre moins de 10 % en 2022.

Source : Magic Quadrant for Cloud Web Application and API Protection

À PROPOS

UBIKA, le Nouveau DenyAll

Fondée en 2001 avec son siège social à Meudon en France et un centre de recherche à Montpellier, UBIKA, connu précédemment sous les étendards de BeeWare, DenyAll ou plus récemment Rohde & Schwarz Cybersecurity est un fournisseur européen en matière de cybersécurité. Sa mission est d'aider les organisations à sécuriser leur transformation digitale en protégeant les applications et les APIs contre les cyberattaques. La société fournit des solutions innovantes de protection des applications Web & des APIs contre les nouvelles menaces comme le DDOS volumétrique ou applicatif, les injections de code malveillant, les défacements et en général contre le TOP 10 de l'OWASP.

Notre technologie Web Application & API Protection (WAAP), omniprésente et agnostique vis-à-vis du cloud, peut être déployée sur site, dans le cloud, en mode SaaS ou comme conteneur, pour sécuriser à la fois les applications existantes et les applications cloud-native et prévenir les cyberattaques de manière proactive plutôt que réactive. Plus de 600 entreprises et institutions publiques dans 35 pays nous confient la sécurité de leurs applications et de leurs APIs.

2015 - 2023

Solutions labellisées Label France Cybersecurity depuis 2015.

2022

Reconnu par nos clients comme « Strong Performer » en 2022 pour les solutions de protection des applications web et des API.

Solutions distribuées en France et à l'international avec l'aide d'un réseau partenaires.

Font partie du CLUSIF

UBIKA est membre fondateur d'HEXATRUST, association de confiance dans le domaine du numérique de confiance et de la cybersécurité.

SOLUTIONS

Nous sécurisons vos applications partout, dans le cloud, on-premise, en mode SaaS.

UBIKA WAAP Gateway
On Prem Edition & Cloud Edition

- Sécurise les applications web, API et websockets
- Bloque les attaques sur la couche applicative y compris celles du Top 10 OWASP
- Surveille l'utilisation des applications web pour prévenir toute menace interne
- Intègre de multiples moteurs de sécurité et un workflow graphique et intuitif

UBIKA Cloud Protector

- Service SaaS souverain hébergé en France garantissant la confidentialité des données, la conformité RGPD
- Société et hébergeur de droit français non soumis au cloud Act
- Anti-DDOS volumétrique et applicatif pour des applications toujours disponibles
- Engagement de disponibilité de 99%

Nos modules

UBIKA Extended API Security

- Sécurise spécifiquement les API
- Permet de chiffrer/déchiffrer des messages webservices
- Permet d'obfusquer des données dans les flux API
- Permet de sécuriser les websockets, protocole de communication temps réel

UBIKA Web Access Manager

- Déploie un portail centralisé d'authentification pour un accès instantané à toutes les applications de l'entreprise (Web SSO)
- Renforce l'authentification des utilisateurs grâce à l'ajout d'un MFA
- Permet d'ajouter des mécanises modernes d'authentification SAML, OAuth ou OpenIdConnect

Management Console

- Plate-forme dédiée pour la configuration et la gestion centralisée de toutes les instances et applications
- Déploiement automatisé de la politique de sécurité des applications sur toutes les instances, y compris celles dans le cloud Surveillance des applications web en temps réel
- Accès basé sur les rôles pour les tâches de gestion distribuée

IP Reputation

- Ajout de renseignements sur les menaces à jour à la politique de sécurité
- Garantie l'optimisation des performances en filtrant les requêtes provenant de sources IP malveillantes
- Réduction du risque de faux positifs en ajustant la politique en fonction de l'origine de la requête Ignore les requêtes de robots indésirables

Avantages de nos solutions

SOUVERAINETÉ, CONFIANCE & CONFORMITÉ RGPD

AUTOMATISATION DE LA SÉCURITÉ DE VOS API, SERVICES CRITIQUES ET WEB

DÉFINITION DES POLITIQUES DE SÉCURITÉ GRÂCE À UN WORKFLOW GRAPHIQUE

PIONNIER DU WAF DANS LE MONDE DEPUIS 20 ANS, TOUJOURS À LA POINTE

SUPPORT & SERVICES MANAGÉS

EQUIPE SUPPORT TECHNIQUE EXPERTE BASÉE EN FRANCE

PORTAIL 24/7 POUR LA GESTION DES TICKETS DE SUPPORT POUR TOUS TYPES D'INCIDENTS

ASSISTANCE TÉLÉPHONIQUE 24/7 EN FRANÇAIS ET EN ANGLAIS

FORMATION À LA CERTIFICATION DES PRODUITS POUR LES PARTENAIRES ET ADMINISTRATEURS

TÉMOIGNAGES CLIENTS

Franck Calcavecchia, Information Security Officer,
Hôpitaux universitaires de Genève

« Etant donné la multitude de sites à protéger, il nous faut pouvoir prendre en compte différents facteurs et pouvoir adapter la couche sécuritaire en fonction du besoin de chacun. Par exemple, pour les sites qui sont accessibles depuis un device personnel, le protocole à mettre en place est différent que s'il s'agit « simplement » de l'intranet de l'hôpital »

Jérôme POGGI, RSSI, Ville de Marseille

« Nous nous servons de Cloud Protector pour bloquer toutes les attaques du Top10 de l'OWASP. Nous savons que nous allons en avoir encore plus car nous faisons partie des quelques villes qui ont une grosse exposition avec les JO 2024, en particulier avec l'arrivée de la flamme olympique. Nous avons choisi Cloud Protector pour sa facilité et son service managé qui nous permet de déployer très facilement. »

Pierre Louis Dessuges, Architecte Technique des Infrastructures, Grenoble Alpes Métropole.

« L'aspect graphique de l'outil et la facilité d'exploitation des workflows nous apporte un confort et une centralisation qui sont très importants. C'est mieux que d'avoir 10 à 20 serveurs exposés, pour lesquels il faudrait gérer des briques de sécurité à chaque fois. »

Eric Detoisien, Responsable Sécurité, Ingenico

« Les équipes d'UBIKA ont été très réactives. Nous avions une exigence de temps qui a été respectée de bout en bout. Le déploiement s'est très bien déroulé, sans contrainte, ni retard. »

CAS CLIENT GIP MDS

Recours au cloud pour bloquer un grand nombre de requêtes liées à des demandes d'authentification envoyées par erreur

Contexte

Le Groupement d'Intérêt Public de Modernisation des Déclarations Sociales (GIP MDS) a été créé en 2000 dans le but de mutualiser les moyens et les expertises des organismes de protection sociale en termes de dématérialisation, et surtout de faciliter aux entreprises et à leurs représentants l'accès aux déclarations dématérialisées.

Le GIP MDS c'est :

- Un objectif commun, la simplification au service de la Protection Sociale
- Une expertise éprouvée sur des projets d'envergure : Déclaration Sociale Nominative, Prélèvement à la source…
- Net-entreprises.fr, un portail unique pour toute la sphère sociale
- 70 procédures remplacées un flux unique, la DSN

L'accès aux applications publiées par le GIP-MDS sur son portail nécessite une authentification de l'utilisateur. Ce service d'authentification est donc vital et doit être protégé.

Enjeux

- L'objectif est de bloquer temporairement les utilisateurs qui émettent beaucoup de requêtes d'authentification (souvent à cause d'une mauvaise configuration de leur logiciel) conduisant ainsi à la saturation de l'infrastructure d'authentification, voir à son blocage.
- Si un acteur malveillant essaye de faire du brute force sur un compte, le compte sera bloqué au bout de 5 tentatives et l'utilisateur légitime ne pourra plus avoir accès à l'application
- Il faut donc implémenter un mécanisme se basant sur l'adresse IP
- La première approche a donc consisté à bloquer temporairement les IP au bout de 5 tentatives infructueuses
- Le problème de cette approche et que nous avons des concentrateurs qui déclarent pour plusieurs utilisateurs donc s'il y a un problème sur un compte utilisateur vu que l'IP du concentrateur est bloquée il ne peut plus déclarer pour ses autres utilisateurs

CAS CLIENT GIP MDS

Solution retenue

Le GIP MDS a fait le choix de la solution UBIKA WAAP CLOUD.
Approche retenue :

- La solution retenue a consisté à bloquer temporairement les requêtes des utilisateurs sur la base d'éléments transmis dans la requête d'authentification (format XML) et spécifiques à chaque utilisateur.

- Pour cela une "clé de session" a été construite à partir de ces éléments qui est unique pour chaque utilisateur. Cette clé est utilisée pour identifier chaque utilisateur dans le WAF et, en fonction de la configuration d'un compteur des requêtes émises par l'utilisateur, de bloquer temporairement, pour une durée configurable, ce dernier. Une fois le délai de blocage écoulé les requêtes de l'utilisateur sont de nouveau acceptées.

- L'infrastructure d'authentification recevant beaucoup moins de requêtes est ainsi protégée contre le risque de saturation et de blocage.

- Les requêtes étant identifiées par une "clé de session" spécifique à chaque utilisateur, il n'y a plus de risque de bloquer l'ensemble des utilisateurs déclarés via un concentrateur.

UBIKA WAAP CLOUD, solution WAF développée par UBIKA, protège les applications déployées dans le Cloud et les API contre les cybermenaces avancées grâce à de puissants workflow personnalisés.

Bénéfices

1) Dépollution du WAF : Le WAF permet de bloquer un grand nombre de requêtes liées à des demandes d'authentification envoyées par erreur. Le client dépollue les flux sur son backend et allège fortement le trafic en aval du WAF grâce à une méthode de filtrage avancée.

2) Le client dégage un ROI :
- Allégement de la consommation de ressource sur les backends
- Amélioration des temps de réponse et réduction des risques de saturation
- En venant palier des lacunes de l'applicatif, le WAF permet d'éviter des travaux couteux d'évolution (économie de TMA)

3) Personnalisation des enjeux métier

4) Souplesse dans les workflows

5) Optimisation trafic

ACTUALITÉS 2023

Premier opérateur cloud de confiance accessible en tant que service, OUTSCALE met à disposition des entreprises un Cloud automatisé et évolutif, qui accompagne les projets informatiques les plus complexes, tout en maîtrisant leurs aspects opérationnels. Il offre une réactivité optimum des infrastructures IT en répondant aux demandes en quelques secondes.

Qualifié SecNumCloud, le plus haut niveau de sécurité délivré par l'ANSSI, l'environnement SecNumCloud d'OUTSCALE répond aujourd'hui aux enjeux les plus exigeants en matière de sécurité, de confidentialité et de souveraineté numérique des acteurs publics, parapublics et Opérateurs d'Importance Vitale (OIV).

Nous sommes présents sur la Marketplace d'OUTSCALE.

Le programme Open Trusted Cloud a pour vocation de cocréer un écosystème de solutions SaaS dans le cloud avec tous les acteurs du numérique. Ce programme est une plateforme de solutions hébergées dans un cloud ouvert, réversible et de confiance d'OVHcloud. Avec 4 engagements :

Souveraineté
- Indépendance vis-à-vis des lois extraterritoriales
- Respect des réglementations locales (RGPD, SNC, CISPE) sur la protection des données

Innovation
- Co-construction de solutions transparentes, réversibles et interopérables
- Accès en avant-première aux dernières technologies OVHcloud

Fiabilité
- Accompagnement privilégié par les équipes OVHcloud (24/7)
- Certifications et formations OVHcloud

Durabilité : engagement et actions en faveur du développement durable

COMMUNIQUÉS DE PRESSE

UBIKA lance la nouvelle génération de son service Cloud Protector pour renforcer la sécurité des applications Web

UBIKA, éditeur de la technologie WAAP (Web Application & API Protection) annonce le lancement de la nouvelle génération de sa solution SaaS souveraine, “Cloud Protector”.
Le service vise à augmenter le niveau de sécurité des applications en fournissant une solution complète et ergonomique pour protéger les services numériques exposés sur Internet, qu’ils soient basés sur des applications Web traditionnelles ou des interfaces de programmation d’applications (API). Il permet aux entreprises de protéger efficacement leurs actifs numériques tout en réduisant le coût total de possession (TCO).

"La nouvelle génération de Cloud Protector est un grand pas en avant, a déclaré Stéphane de Saint Albin, PDG d’UBIKA. Elle protège désormais les API, offre un contrôle plus granulaire, facilite l’agilité DevOps et améliore la délégation dans les environnements de gouvernance distribués. À une époque où les API sont tentaculaires et où les applications web sont de plus en plus critiques pour les entreprises, Cloud Protector s’impose comme une solution moderne, simplifiée et digne de confiance."

Lors de son lancement en 2014, Cloud Protector était le premier WAF-As-a-Service souverain en France et en Europe, un logiciel basé sur le cloud qui rationalise la protection des services web numériques pour les entreprises et les organisations publiques de toutes tailles. Le produit a évolué au fil des années pour fournir un ensemble complet de fonctionnalités, combinant une protection DDoS au niveau du réseau, une technologie WAAP de pointe et une interface utilisateur intuitive, ce qui le rend facile à utiliser quel que soit le niveau de compétence technique.

UBIKA a travaillé en étroite collaboration avec ses clients des secteurs public et privé afin de répondre à leurs besoins et de créer une solution qui réponde à leurs nouvelles exigences. Les fonctionnalités de “Cloud Protector” comprennent la protection des API, la protection active du trafic Websocket et la gestion fine des faux positifs.

Pour répondre au besoin croissant de délégation totale, la société a également créé une offre de services managés qui s'adresse aux organisations ayant besoin d'une protection mais ne disposant pas nécessairement de la bande passante ou ayant des compétences minimales pour s'en charger elles-mêmes.
Cloud Protector est désormais disponible sous forme d'abonnement.

COMMUNIQUÉS DE PRESSE

Stéphane de Saint Albin, UBIKA : Notre approche de la sécurité intégrée au cœur de toutes les applications est notre marque de fabrique

A l'occasion de l'édition 2022 du FIC, Rohde & Schwarz Cybersecurity France a annoncé son changement d'identité : UBIKA. De ce fait, elle a renommé l'ensemble de sa gamme de produits et a annoncé sa nouvelle stratégie. Cette approche permet d'intégrer la sécurité dès la phase de conception des applications cloud natives et des APIs ce qui permet d'obtenir une meilleure couverture des risques quel que soit l'environnement. Stéphane de Saint Albin, Directeur Général d'UBIKA considère que cette approche de la sécurité intégrée au cœur de toutes les applications est la marque de fabrique de son organisation.

Global Security Mag : Comment s'est déroulé pour vous l'édition 2022 du Forum International de la Cybersécurité ?
Stéphane de Saint Albin : A l'occasion du FIC 2022, Rohde & Schwarz Cybersecurity France a annoncé son changement d'identité : UBIKA. De plus elle a présenté sa stratégie suite à son rachat par Total Specific Solutions en avril dernier.

Global Security Mag : Qu'avez-vous présenté à cette occasion ?
Stéphane de Saint Albin : L'équipe UBIKA a présenté sa vision stratégique de la sécurité qui est centrale pour toutes les entreprises ou organisations en pleine transition numérique. En effet, UBIKA fait référence au don d'ubiquité et positionne la sécurité au cœur de tous les process pour favoriser la croissance des entreprises. Ses équipes accompagnent aussi bien les DSI et RSSI que les DevOps grâce à une approche DevSecOps, en apportant la sécurité, la simplicité et la visibilité. Cette approche permet d'intégrer la sécurité dès la phase de conception des applications cloud natives et des APIs ce qui permet d'obtenir une meilleure couverture des risques quel que soit l'environnement.

Cette approche à 360 degrés s'accompagne de l'automatisation qui garantit une simplicité d'usage car les solutions s'adaptent à tous les contextes, environnements et croissances. UBIKA facilite la vie des développeurs et des équipes de sécurité.
Le FIC a été également l'occasion d'annoncer les nouveaux noms de l'ensemble de ses produits :

• UBIKA WAAP Gateway WAF déployé on-premises,
• UBIKA WAAP Cloud, WAF dans le cloud ou en mode hybride,
• UBIKA Cloud Protector pour le WAF en mode SaaS,
• UBIKA WAAP Container pour la protection de vos applications cloud native

Les autres modules optionnels restent inchangés : Web Access Manager, Extended API Security, Management Console, IP Reputation.

Global Security Mag : Quels sont les points forts de ces solutions ?
Stéphane de Saint Albin : UBIKA propose des solutions éprouvées qui permettent de protéger toutes les entreprises et organisations. Ses différentes solutions s'intègrent facilement et rapidement à l'infrastructure existante des entreprises en toute transparence. L'approche innovante d'UBIKA offre une vision à 360 et permet aux équipes de dev et de sécurité de travailler de concert pour plus de protection.

Global Security Mag : Quel est votre message à nos lecteurs ?
Stéphane de Saint Albin : Cette nouvelle identité de marque renforce notre volonté de nous recentrer sur notre expertise et de poursuivre notre collaboration étroite avec nos clients, actuels et futurs, pour cocréer les solutions de demain. « Notre approche de la sécurité intégrée au cœur de toutes les applications est notre marque de fabrique », conclut Stéphane de Saint Albin, Directeur Général d'UBIKA.

COMMUNIQUÉS DE PRESSE

Protéger vos sites web et API avec Cloud Protector Nouvelle Generation

UBIKA présente son produit nommé Cloud Protector, qui vient répondre à la prolifération des API. Ce WAAP as-a-Service souverain est hébergé par OVH. Nejib Jemli, Directeur des Produits UBIKA explique sa stratégie.

Global Security Mag : Quelle sera votre actualité lors du Forum International de la Cybersécurité 2023 ?

Nejib Jemli : Nous sommes honorés aujourd'hui de vous annoncer le lancement de la nouvelle génération de notre solution SaaS souveraine, "Cloud Protector". Le service vise à augmenter le niveau de sécurité des applications en fournissant une solution complète et ergonomique pour protéger les services numériques exposés sur Internet, qu'ils soient basés sur des applications Web traditionnelles ou des interfaces de programmation d'applications (API). Après une collaboration avec nos 70+ clients utilisant déjà Cloud Protector, nous sommes heureux de pouvoir lancer la nouvelle génération et le présenter lors d'un événement important.

Global Security Mag : Quels sont les points forts des solutions que vous allez présenter à cette occasion ?

Nejib Jemli : Ce produit est une véritable pépite, car en plus d'avoir une protection efficace contre les attaques Web et la sécurisation des API, la solution se déploie en quelques clics avec un minimum d'administration en phase d'exploitation. La protection est conçue pour traiter les attaques en déni de service (DDoS) au niveau applicatif et réseau, la limitation du débit, la géolocalisation et la réputation des adresses IP. Et puis, c'est un produit français, qui respecte la confidentialité des données, conforme RGPD et non soumis aux lois extraterritoriales étrangères telles que le Cloud Act.

En résumé, avec le développement tentaculaire des API et où les applications web sont de plus en plus critiques, "Cloud Protector" s'impose comme une solution moderne, simplifiée et digne de confiance, qui protège efficacement les actifs numériques tout en réduisant le coût total de possession (TCO).

En résumé, avec le développement tentaculaire des API et où les applications web sont de plus en plus critiques, "Cloud Protector" s'impose comme une solution moderne, simplifiée et digne de confiance, qui protège efficacement les actifs numériques tout en réduisant le coût total de possession (TCO).

Global Security Mag : Comment les technologies doivent-elles évoluer pour conter ces menaces ?
Nejib Jemli : Aujourd'hui, les entreprises doivent agir rapidement pour contrôler la prolifération des API. Une prolifération non contrôlée des API peut entraîner des problèmes de cohérence et de sécurité des données sensibles qu'elles permettent souvent de manipuler et d'exposer aux membres de son écosystème. Les API qu'une organisation publie et consomme peuvent utiliser des formats différents, ce qui rend potentiellement difficile la normalisation, l'agrégation et la comparaison de données provenant de sources diverses.
Sans un contrôle adéquat, il peut être difficile de gérer la qualité et l'intégrité de ces flux de données. En plus de cela, ce problème peut engendrer des coûts de développement, de maintenance et de gestion importants. En l'absence d'un suivi approprié, il peut être difficile de déterminer les coûts associés à chaque API.

Global Security Mag : Quel message souhaitez-vous transmettre aux RSSI ?
Nejib Jemli : "Cloud Protector" est une solution éprouvée et souveraine avec une mise sous protection immédiate des applications Web et des API, avec une grande simplicité d'administration, s'adaptant aux évolutions du parc client. C'est une excellente alternative aux solutions étrangères soumises aux lois américaines. Créée par une société française (DenyAll devenue UBIKA en Juin 2022), pionnière du WAF en France et en Europe depuis la fin des années 90, "Cloud Protector" est hébergé en France par OVH, une autre société française non sujette au Cloud Act. La solution existe et protège efficacement plus de 70 entreprises et établissements publics dans de nombreux secteurs d'activité, dont la santé, depuis 2014. L'expérience dans ce domaine c'est clé !

CONTACT DIRECTION

Stéphane DE SAINT ALBIN
stephane.desaintalbin@ubikasec.com
06 22 56 01 50

CONTACT COMMERCIAL

Christine AMORY, VP Sales & Marketing
christine.amory@ubikasec.com
06 07 24 76 00

CONTACT PRESSE

Paloma Siggini, Chargée marketing
paloma.siggini@ubikasec.com
06 75 78 75 80