

Les API - la cible principale dans les environnements applicatifs d'aujourd'hui

Les API sont au cœur des applications modernes d'aujourd'hui, permettant aux entreprises de se connecter avec leurs clients et partenaires, de générer des revenus et d'innover par le biais d'initiatives de transformation numérique. Les API sont également devenues la principale cible des cybercriminels au niveau applicatif, comme le démontrent les innombrables attaques retentissantes. Gartner prévoit que « d'ici 2022, les abus liés aux API passeront du statut de vecteur d'attaque occasionnel à celui de vecteur d'attaque le plus fréquent, et aboutiront à des violations de données pour les applications Web d'entreprise. » Les solutions traditionnelles, notamment les WAF et les passerelles API, sont incapables de protéger vos API contre les attaques modernes.

Que se passe-t-il quand les cybercriminels ciblent des API?

- Exfiltration de données
- Perte de données
- Prise de contrôle de comptes
- Utilisation abusive du compte
- Perturbation des services
- Pannes de service
- Fraude



Présentation de Salt Security

La plateforme de protection des API Salt Security sécurise vos API tout au long de leur cycle de vie. La plateforme Salt récupère une copie du trafic des API sur l'ensemble de votre paysage applicatif et utilise le big data, l'apprentissage automatique (ML) et l'intelligence artificielle (IA) pour découvrir toutes vos API et leurs données exposées, stopper les attaques et éliminer les vulnérabilités à la racine. La plateforme Salt:

- **Découvre toutes les API et les données exposées** – Faites automatiquement l'inventaire de toutes vos API, y compris les API fantômes et zombies, et mettez en évidence tous les cas où vos API exposent des données sensibles. La découverte continue garantit que vos API restent protégées même si votre environnement évolue grâce aux pratiques agiles du DevOps.
- **Stoppe les attaques d'API** – Repérez et stoppez les menaces ciblant vos API en identifiant les cybercriminels à un stade précoce, durant leur phase de reconnaissance, et en les empêchant de progresser. La plateforme Salt établit une corrélation entre des activités et une entité seule, envoie une alerte consolidée pour éviter la multiplication des alertes et bloque l'attaquant plutôt que les opérations.
- **Améliore la sécurité de vos API** – Salt identifie de manière proactive les vulnérabilités de vos API avant même qu'elles ne traitent le trafic de production. La plateforme utilise également les cyberattaquants comme testeurs de pénétration, en détectant leur tentatives / leurs avancées pour fournir des informations aux équipes de développement tout en bloquant les malfaiteurs avant qu'ils n'atteignent leur objectif.

Qui utilise Salt?

- Des entreprises de toutes tailles, dans tous les secteurs d'activité, qui créent des API pour alimenter leurs applications internes et celles destinées à leurs clients et à leurs partenaires. Nous sommes particulièrement actifs dans les secteurs FinTech, FinServ, Tech SaaS et auprès d'entreprises pharmaceutiques.
- Les entreprises qui cherchent à prévenir les attaques d'API pour protéger leurs applications stratégiques et les données de leurs clients.
- Les entreprises qui cherchent à comprendre les risques, à répondre aux exigences de conformité et à éliminer les vulnérabilités de leurs API.

Avantages de Salt

- Identifier et arrêter les cyberattaquants à un stade précoce, pendant leur phase de reconnaissance, avant qu'ils ne puissent progresser
- Éliminer les angles morts grâce à un catalogue continuellement mis à jour comportant toutes les API connues et inconnues dans l'ensemble des environnements
- Répondre aux exigences de conformité en identifiant les API qui exposent des données sensibles
- Améliorer la sécurité et les flux de travail de développement pour fournir plus rapidement des applications sécurisées
- Éliminer les vulnérabilités des API à l'aide d'informations hiérarchisées et exploitables par les développeurs

Salt en action

La plateforme Salt se déploie sans agent et sans modification du code. Nous recueillons simplement une copie de votre trafic API et envoyons les métadonnées vers la plateforme big data de Salt. Nous découvrons toutes vos API, et nos algorithmes de ML et d'IA identifient les failles de sécurité de vos API et établissent une base de référence des modèles normaux d'API afin de pouvoir détecter et arrêter les cyberattaquants.



- 1 Pas en ligne
- 2 Automatisé, continu
- 3 Indépendant de l'environnement



Communication API

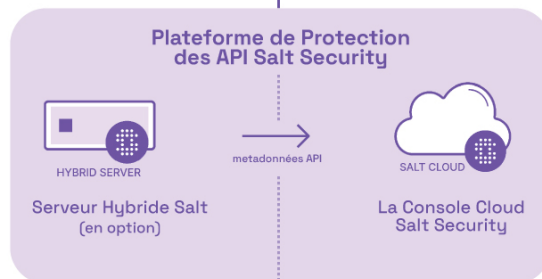


Blocage – manuel ou automatique

Mirroring du trafic API

Environnements clients

Cloud Salt



- Découverte automatique (APIs, fonctions, données sensibles)
- Baseline automatique du trafic normal
- Détection des comportements anormaux/attaques
- Blocage des attaquants

En quoi Salt contribue à vos bons résultats ?

La plateforme Salt permet à votre équipe d'économiser beaucoup de temps et d'efforts pour identifier et combler les lacunes en matière de sécurité des API.

33%

d'API non documentées en moins

20x

Un délai de résolution 20x plus rapide

96%

d'alertes en moins

3x

Remédiation 3x plus rapide des AP

75%

de gain de temps pour la conformité

Bénéficiez de la même tranquillité d'esprit que vos pairs

Nous sommes fiers des clients que nous avons pu protéger, en leur permettant de stimuler leur innovation métier via leurs API.



FINASTRA

Amway

AON

BerkshireBank

zoom

Baxter

CITY NATIONAL BANK
AN RBC COMPANY

MARKEL®

Salt Security protège les API qui sont au cœur de chaque application moderne. La plateforme de protection des API de la société est la première solution brevetée du secteur pour prévenir la prochaine génération d'attaques d'API, en s'appuyant sur la protection comportementale. Déployée en quelques minutes, la solution alimentée par l'IA découvre et apprend automatiquement et en continu le comportement granulaire des API d'une entreprise et ne nécessite aucune configuration ou personnalisation pour prévenir les attaques d'API.

SALT

Demandez une démo !
info@salt.security
www.salt.security