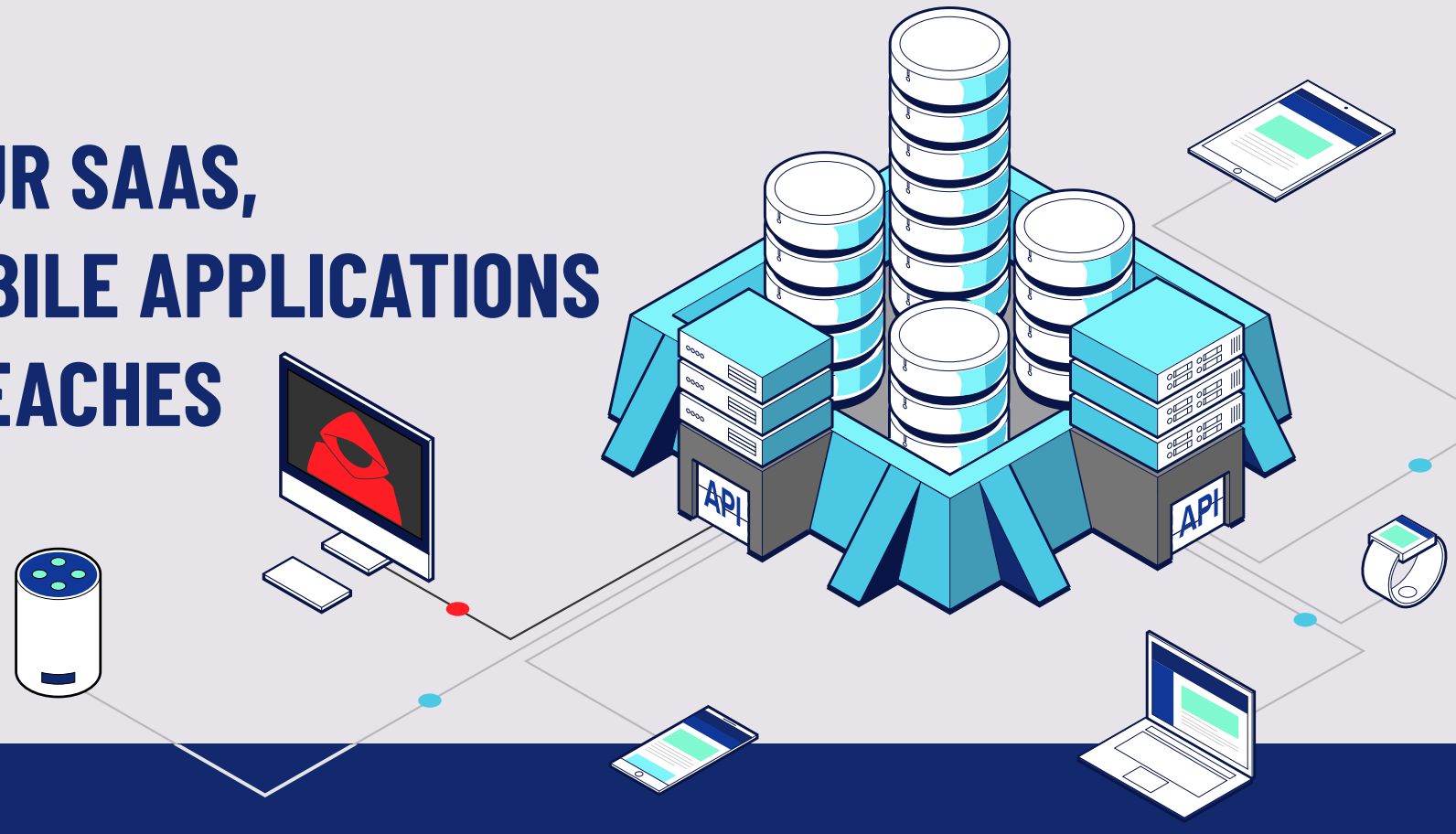
SALT

PROTECT YOUR SAAS, WEB AND MOBILE APPLICATIONS FROM API BREACHES



THINK YOU'RE PROTECTED? THINK AGAIN.

APIs are found at the core of every SaaS, web, mobile, microservices and IoT application and as API use has exploded the quantity and sensitivity of the data transmitted has increased. With this, API attacks have become more frequent and more complex, making them the number one threat for any company delivering applications. The market has already seen a huge increase in API attacks over the past few years, including breaches at Facebook, T-Mobile, Panera Bread, Verizon, and the latest vulnerability disclosures at the United States Postal Service (USPS) and Google+.

Gartner predicts "by 2022, API abuses will be the most frequent attack vector resulting in data breaches for enterprise web applications," and insecure APIs were ranked as the third most severe threat to cloud computing in 2018 by the Cloud Security Alliance. In addition, the Open Web Application Security Project (OWASP) recognized API security as a primary concern, with nine of the top 10 vulnerabilities in their current OWASP Top 10 report including an API component.

API Breaches Are The Number One Risk For Your Applications

APIs can be found everywhere exposed to employees, customers and partners behind your SaaS, web, mobile, microservices and IoT applications. Increasing complexity and sensitive data makes APIs a primary target for attackers and a growing risk for applications.

Developers Are Not Focused on Security

Developers are innovation driven, don't think like attackers and can unintentionally create vulnerabilities in APIs. Best practices like CI/CD mean developers are expected to deliver at an increasingly rapid rate which creates more risk in application environments.

Current Solutions Can't Protect Against Increasing API Attacks

APIs are a primary target for attackers who have evolved to target unique vulnerabilities of your unique APIs. It's impossible to detect and prevent today's API attacks with signature based Web Application Firewall (WAF) and Runtime Application Self Protection (RASP) solutions.

A new approach to API security is needed – one that is seamlessly integrated across your agile environment, and delivers visibility, prevention and remediation.

USE CASES

Data Exfiltration

Protect critical company and customer data from mass downloads and data exfiltration

Account Takeover

Prevent widespread account takeover vulnerabilities even for attacks that don't require user interaction

Service Disruption

Stop attackers from taking down your applications and services even with a single API call

Legacy Application Protection

Protect legacy applications without the need to understand or modify the existing code base

Cataloging APIs

Automatically and continuously discover all public, private or partner facing APIs and applications in your environment

API Vulnerabilities

Efficiently identify and eliminate API vulnerabilities with clear and actionable insights for developers

THE SOLUTION

Detect and prevent API attacks with the power of AI.
Deploys in minutes. No configuration required. Ever.

Catalog All Your APIs And Eliminate Blind Spots

Find all known and unknown APIs across your environments automatically and continuously for a complete inventory so you can eliminate blind spots, assess risk, determine sensitive data exposure (e.g. PII) and keep your APIs protected even as your environment evolves and changes.

Prevent API Attacks Missed By Other Security Solutions

Pinpoint and stop threats to your APIs with patented AI technology that baselines legitimate behavior and identifies attackers during reconnaissance to prevent them from advancing. With insights into legitimate behaviour, Salt detects targeted attack attempts to help security teams focus on and eliminate the root of the attack.

Eliminate API Vulnerabilities

Bridge the gap between security and development teams to efficiently eliminate vulnerabilities at their source in the API. Leverage each attacker as your personal pen-tester and gain detailed insights into how to remediate so development teams understand why a vulnerability exists and exactly where so they can quickly prioritize and eliminate vulnerabilities.

QUICK, NON-INTRUSIVE SETUP AND NO CONFIGURATION NEEDED

Unlike common, intrusive proxy deployments that add latency and can cause service disruption, Salt has a DevOps friendly setup. The Salt solution is not inline and has a variety of quick and easy setup options including agents, containers (Docker, Kubernetes, etc.) and support through port mirroring.

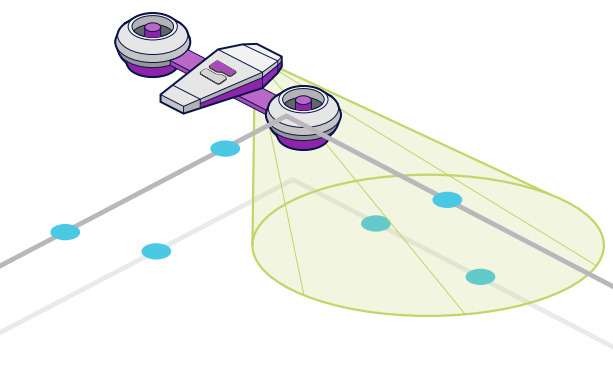
"With recent breaches affecting APIs, API security is more crucial than ever" Gartner

WHY NOW?

APIs are at the core of your SaaS, web, mobile, microservices and IoT applications and the quantity and sensitivity of the data transmitted across these environment has increased. With this, API attacks have become more frequent and more complex, making them the number one threat for any company delivering applications. API attacks fly under the radar and are missed by traditional security solutions. Don't wait until a breach occurs. Act now to discover what you don't know and stop attackers before they're successful.

WHY SALT?

Today's security solutions work based on signatures and detect only known attacks (e.g. SQL injection, XSS, etc.), produce heaps of false positives and require constant configuration. Current API attacks are inherently sophisticated, target unique application logic, and bypass the current solutions in your security stack. Today's solutions are 100% blind to modern API attacks. Salt leads, with its first to market patented solution that detects and prevents attacks in real time before attacks are successful.



SALT

Contact us now to start discovering what you don't know.

contact@salt.security

https://salt.security