Open Banking and API Security

Overview

Open Banking and directives like PSD2 define the standards for financial institutions to expose information and enable transactions with third parties. The core technology of Open Banking is the Application Programming Interface (API) which powers applications and enables the exchange of data while exposing the inner workings of applications and sensitive information. There are major benefits of Open Banking for consumers who gain more choices and better experiences. However, financial organizations are faced with securing these new APIs to protect sensitive customer data while complying with increasingly tight regulations around data protection, operational risk and cybersecurity. Unlike traditional applications, modern applications powered by APIs present new challenges and require new solutions for protection.

Challenges Securing APIs

APIs expose both the logic of an application and sensitive data such as Personally Identifiable Information (PII). As APIs have been increasingly adopted to power applications, they have also emerged as a prime target for attackers. The analyst firm Gartner predicted that "by 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise web applications." This prediction came true sooner than expected, with APIs becoming a top target by 2021. Other organizations such as the Cloud Security Alliance and the Open Web Application Security Project (OWASP) have also highlighted APIs as a top threat to modern applications.

A primary challenge is that APIs are unique to the application they power and the organization that develops them, meaning they not only have unique logic but also have unique vulnerabilities. This makes it impossible to secure an API with traditional solutions that depend on signatures to defend against known attack patterns. Many API attacks consist of subtly crafted API calls that are missed by traditional security solutions that don't understand the unique logic of the APIs they're employed to protect.

While direct attacks against API providers are a major concern, no less of a concern is the inherited risk of third parties accessing APIs. Protections may be in place to enforce authentication and authorization for an API but consider a breach of a partner can result in unauthorized access to and misuse of the API.

[1]How to Build an Effective API Security Strategy (Gartner 2017)

Risk to APIs

As APIs become more prevalent in modern applications, a successful attack can result in damage to the brand, loss of customers, liability of fraudulent transactions and, in some cases, significant fines due to non-compliance with existing regulations. When targeting **Open Banking APIs, attackers may look to accomplish the following:**

Account Takeover & Data Exfiltration

APIs expose user information including account numbers and other PII.
An attacker will look for ways to manipulate API logic and exfiltrate data at scale.

Fraudulent Transactions

One of the goals of Open Banking is to enable transactions like payments and transfers. Attackers will look for ways to use an API to execute fraudulent transactions.

Service Disruption

Unlike Distributed Denial of Service (DDoS) attacks that use volumes of traffic, attackers can use a single API call to overwhelm applications and cause outages.

How Salt Security Helps

The Salt Security API Protection platform can help organizations looking to extend their digital services and meet Open Banking requirements. The AI-powered solution is deployed in minutes, and it automatically and continuously discovers and learns the granular behavior of APIs to give you the context you need to secure them across the full API lifecycle. It requires no configuration or customization to help ensure API protection.

Salt Security solves the following Open Banking challenges for security teams:

Discovery – Visibility into APIs and Data Exposure

Find all known and unknown APIs in use across your environments automatically and continuously to help you eliminate blind spots, determine exposure of sensitive data, and protect your APIs, even as your environment evolves and changes.

Achieve Granular Visibility

Automatically discover and maintain a comprehensive catalog of all public or private APIs with granular details for each endpoint.

Discover Sensitive Data

Identify exposure of sensitive data like PII to assess risk, prioritize security efforts, and demonstrate compliance.

Track and Verify Changes

See APIs as they're deployed, stay up to date as changes are made, and verify that all APIs meet security requirements.

Runtime Protection – Preventing API Attacks

Pinpoint threats to your APIs in real time and stop attackers from advancing by using big data and patented learning algorithms instead of relying on signatures or manual configuration.

Behavioral Protection

Detect malicious activities that fall outside of the normal baseline of activity to stop attackers in reconnaissance before a successful attack.

Pinpoint the Source of Attacks

Identify attackers even as they mask their activity. Alerts combine attempts for each attacker to reduce generated alerts and eliminate false positives.

Expedite Attack Investigation

Quickly see and understand exactly what happened across attacks, reducing investigation times and allowing security teams to focus blocking efforts.

Proactive Security – Eliminating API Vulnerabilities

Bridge the gap between security and development teams for efficient identification and elimination of vulnerabilities at their source in the API.

API Design Analysis

Upload your Swagger or OAS files and gain immediate insights into security gaps in your APIs, before you release them into production.

API Security Testing

Send attack simulation traffic to your APIs to identify business logic gaps that bad actors could exploit for API attacks such as account takeover or data exfiltration.

Runtime Insights for Developers

Share detailed learnings from attackers actual behaviors in runtime so you can focus remediation efforts on real threats to have the most impact.

Contact us now to get the context you need to secure your APIs.
contact@salt.security | https://salt.security

SALT

SB-07182022