API Security for LGPD

The changing API landscape

Companies across Brazil and those who do business in Brazil must comply with the data protection requirements of Lei Geral de Proteção de Dados (LGPD) - Law n° 13.709/2018. Modern applications depend on APIs to enable services and exchange personal data and this creates challenges under this recent law:

- Increased use of APIs, growing the attack surface
- Greater and often unknown exposure of sensitive data
- More frequent API changes thanks to agile development
- Designing privacy into APIs and applications

Attacks targeting APIs are on the rise

Attackers have realized that APIs make an attractive target. The industry has seen a steep rise in the volume and sophistication of API attacks, typically motivated by these common goals:

- Data exfiltration
- Fraudulent transactions
- Service disruption

Companies in Brazil and across the globe have employed multiple layers of security solutions and practices but have still been unable to detect or prevent API attacks, because traditional application security tools miss the vast majority of attacks targeting APIs.

> ***By 2022, API abuses will move from infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications."***
>
> Gartner

Business impact of an API attack

LGPD Fines

Organizations can face fines of up to R$50 million in the event of an attack where data loss occurs. Organizations may also face daily penalties until meeting compliance requirements.

Intellectual Property Theft

Attackers can use APIs to access intellectual property (IP), including unreleased financial results, strategic plans, and product details. Exposure of IP can impact company valuation and competitive advantages.

Revenue and Brand Impact

A data loss event will have even greater visibility with the LGPD and can damage a brand reputation, resulting in loss of customer confidence and impact on revenue.

What's needed to protect APIs and data for LGPD

Discovering APIs

Shadow APIs, and the sensitive data they expose, put organizations at risk. All organizations need ways to continuously discover APIs and sensitive data exposure.

Stopping API Attacks

Preventing API attacks requires deep understanding of API logic and unique API behavior, both of which depend on the use of big data, machine learning (ML), and artificial intelligence (AI).

Eliminating Vulnerabilities

Efficient remediation relies on DevOps teams getting clear, prioritized, and actionable insights about how attackers have successfully probed APIs.

The Salt Security API Protection Platform

Discovery

Inventory all your APIs and eliminate blind spots

- Dynamically inventory existing, new, and changed APIs
- Identify shadow APIs
- Catalog exposed sensitive data such as PII and IP to protect data and meet LGPD and other compliance requirements

Prevention

Stop attackers early during reconnaissance

- Correlate anomalous activity to identify attackers
- Pinpoint attackers early, during reconnaissance, and shut down the attack
- Cut incident response from hours to minutes with a comprehensive attack timeline view

Remediation

Eliminate API vulnerabilities at their source

- Share remediation details with DevOps to eliminate vulnerabilities in APIs
- Continuously harden APIs during development to ensure security doesn't slow application rollout

> ***"APIs underlie all our financial platforms, and Salt Security helps us protect the data and services connecting our partners by immediately identifying and stopping fraudulent or malicious activity. It also provides the remediation details we need to constantly increase our API security posture."***

Nir Valtman,
head of product and data security

FINASTRA

Salt Security customers include:

BV
xp investimentos
FINASTRA
CITY NATIONAL BANK AN RBC COMPANY
celsius network
Payoneer

Salt Security protects the APIs that are at the core of every modern application. The company's API Protection Platform is the industry's first patented solution to prevent the next generation of API attacks, using behavioral protection. Deployed in minutes, the AI-powered solution automatically and continuously discovers and learns the granular behavior of a company's APIs and requires no configuration or customization to prevent API attacks.

Request a demo today!
info@salt.security
www.salt.security

SALT

SB-06092021