GlobalDots

A CISO's Essential Guide to API Security

A CISO's Essential Guide to API Security

Executive Summary

CISOs have to maintain a delicate balancing act. They must protect the business from an ever-changing landscape of security risks while still enabling the business to achieve the required speed-to-market for key initiatives. No CISO can afford to get in the way of or slow down vital programs.

Assessing risk has gotten ever more complicated. As the pace of development has increased, CISOs must assess risk faster while still taking care to keep the business safe. CISOs must determine the value of a particular initiative, the risk that initiative poses, and how to prioritize security investments based on those calculations.

Today's digital transformation initiatives provide a compelling example of the CISO's balancing act. Digital transformation delivers competitive advantages, increases business efficiencies, and provides new avenues for growth. The APIs that enable digital transformation, however, introduce a critical new attack surface and a high-risk point of potential data exposure.

In a global Statista survey, 94.5% of security leaders cited securing their digital transformation initiatives as their top post-pandemic priority. CISOs must be proactive with security processes to keep digital transformation moving forward and satisfy regulators to avoid costly fines. To do so demands that they focus on API security.

In its State of Cybersecurity Resilience 2021, Accenture says CISO cyber champions have the ability to «strike a balance between cyber resilience and business objectives, with strong alignment to business strategy that is best at protecting an organization's key assets.»

Why APIs present CISOs with the biggest risk

APIs have been built specifically for services that share critical data with your customer, partners, and employees. Mobile applications run on APIs. Research shows that more than 80% of Internet traffic is APIs. Companies now have thousands of APIs, and they're changing regularly. In its 2021 State of the API Report, Postman found over half of developers deploy new APIs to production once per day, once per week, or once per month.

In addition, APIs are used across both external partner and customer channels, enabling new and transformative mobile and online services. But in doing so, they also facilitate connectivity for usage of highly sensitive data, such as personally identifiable information (PII), financial data, and medical records. Becouse APIs hold the key to a treasure trove of data, they've become an attaractive target for attackers, as reflected in a growing number of cyber threats targeting company APIs.

Many enterprise companies, including Parler, Experian, Facebook, and Peloton, have experienced API breaches. API attacks can decrease customer trust, cause loss of revenue, and irrevocably damage a company's reputation. In the case of crypto exchange platform Coinbase, had its API vulnerability not been detected, it could have bankrupted the business.

Despite all of these risks, APIs remain poorly protected today. According to Salt Security's latest research, more than a third of organizations lack any API security strategy.

Existing solutions can't keep up with API security needs. API attacks operate based on a string of related events, but traditional solutions, such as WAFs, only view transactions one at a time. They're built for 'known' paths, whereas APIs are unique and require detection of slower reconnaissance activities. To identify and defend against threats, security leaders must have the ability to see all activity.

Moreover, even using APIs as they were meant to be used can result in exploitation. Salt Security empirical research data_You can't merely rely on authentication to protect APIs.

Excessive data exposure, as outlined in the OWASP API Security Top 10, can also unwittingly provide access to more data than actually required for a specific request. In the aforementioned examples of Experian and Peloton, the APIs were targeted for data expfiltration simply by using them as designed, that is, in response to legitimate queries.

> "A WAF in front of an API falls down. It doesn't protect against these threats. It doesn't provide the visibility you need – not to mention that if you don't know all your APIs out there, or that they even exist, it's really hard to protect them."
>
> – Tyler Warren, Deputy Information Security Officer, Prologis

The 3 pillars of API security

The way you could protect a handful of APIs in the past doesn't work when organizations are building 10s and 100s of APIs in weeks and, in some cases, even days. With such a rapid development cadence, the API attack surface is constantly growing.
To effectively protect this evolving landscape, CISOs require an API solution that can deliver the following three capabilities:

- ***Automatic visibility into all API traffic***
- ***Continuous analysis in runtime***
- ***Remediation insights for proactive security***

Complete visibility into API traffic

A company's API footprint is constantly expanding. Systems, applications, and APIs and the data they interact with span multiple environments. If you don't have visibility into all of your APIs, you can't protect them. You also need to understand which APIs might be exposing sensitive data.

With an accurate baseline inventory of their APIs that can be easily and instantly dynamically updated, CISOs can eliminate blind spots. Without it, CISOs cannot understand their full business exposure or prioritize risk management.

Continuous and dynamic analysis in runtime

You need a baseline of normal API traffic to identify abuse or attacks. Because APIs are not just straight code where you can look for code flaws in development and testing but instead instantiations of business logic, you need to see your APIs in action to spot flaws in that logic. Seeing patterns in runtime, as APIs are exercised, provides organizations with the most context when it comes to API security to identify malicious activity.can eliminate blind spots. Without it, CISOs cannot understand their full business exposure or prioritize risk management.

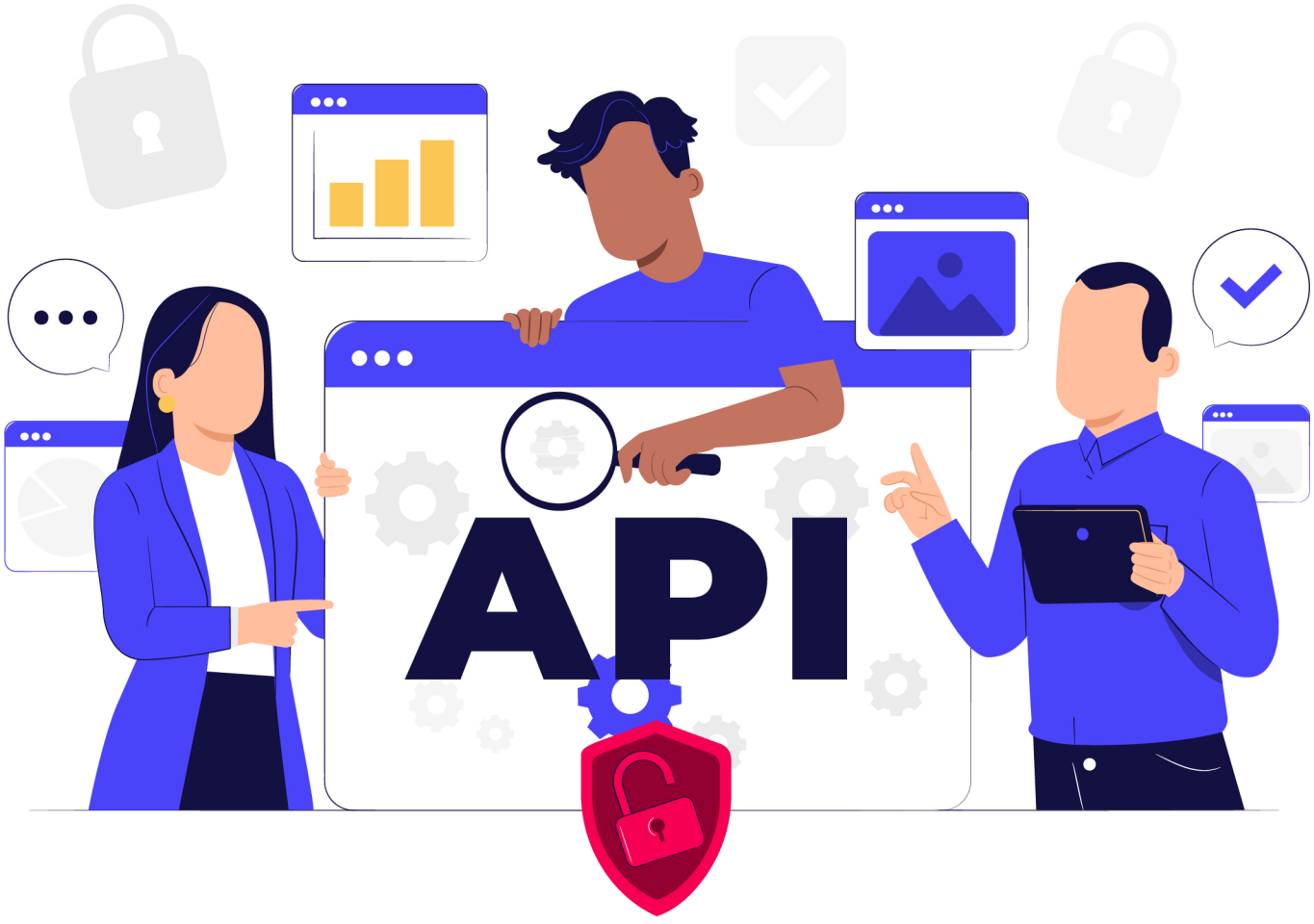
Remediation insights for proactive security

It's important to share what you're learning about your APIs – and their potential vulnerabilities – back to your R&D and DevOps teams. Remediation insights help bring your API security findings back into developer training and development to give them the broadest insights for hardening their APIs. With remediation details, you support shift left practices to get ongoing value for your APIs – allowing you to identify risks before they become exploited. These insights help your developers to write better APIs, even as they continue to build new ones. You also want to tap runtime learnings for additional remediation insights.

Ensuring successful implementation

In a CISO panel at the recent API Security Summit, the verdict was unanimous. A CISO's success starts with establishing the right security culture. This need is particularly acute with APIs. APIs touch almost all parts of the organization, requiring a cross-functional mindset that acknowledges and understands the importance of API security in reducing business risk.

In addition, organizations need dedicated API security; it must be its own program. By establishing API security as its own essential category in securing platform services in 2021, Gartner validated this requirement.



Leveraging automation, big data, and intelligence

To support exponential API growth, CISOs also need solutions that can be integrated into existing DevOps and SecOps workflows. API discovery, anomaly detection, and sharing remediation insights must be tied into CI/CD and Incident Response systems, and they must all be automated.

To gain the context needed to accurately identify API attacks, API security solutions must apply cloud-scale big data and AI and ML to the problem. API attacks take place over days, weeks or months, as bad actors must painstakingly investigate how your APIs work to find business logic flaws. API security solutions need the ability to process large amounts of data over a long time to develop the context needed to distinguish attack traffic from normal traffic. You can't get this level of rich context with on-prem, VM-based solution - only cloud-scale big data, combined with artificial intelligence (AI) and machine learning (ML), provides the ability to track millions of users in parallel over days, weeks, or months.

Don't let gaps in API security inhibit business innovation

At a time when cybersecurity has become the crucial issue, APIs have become the weakest link in IT systems. Without API security, CISOs cannot maximize the value of digital and IT modernization initiatives. Even worse, API weaknesses place potential business profits at risk. To be a CISO cyber champion, you need to be threat-aware, business aligned, and proactive. By implementing a dedicated API security program, CISOs can help the organization accelerate digital innovation, build a more security-centric culture, and generate business growth.

To learn how GlobalDots' API Protection services prevent API attacks, book a custom demo