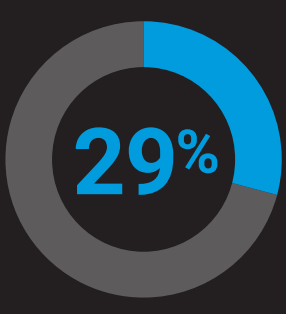
10 YEARS OF SECURITY INSIGHT

Lurking in the Shadows

Attack Trends Shine Light on API Threats

The widespread adoption of APIs has sparked innovation and efficiency across the modern enterprise. However, it has left security teams struggling to understand the scale and complexity of the risks that these APIs have introduced. Most organizations can't even account for all their undocumented or shadow APIs, creating points of entry in their perimeter. In our latest research report, we shed some light on the latest API attack trends.

A spotlight on API challenges



of all web attacks targeted APIs in 2023

Top 3 API attack vectors

44%
HTTP attack

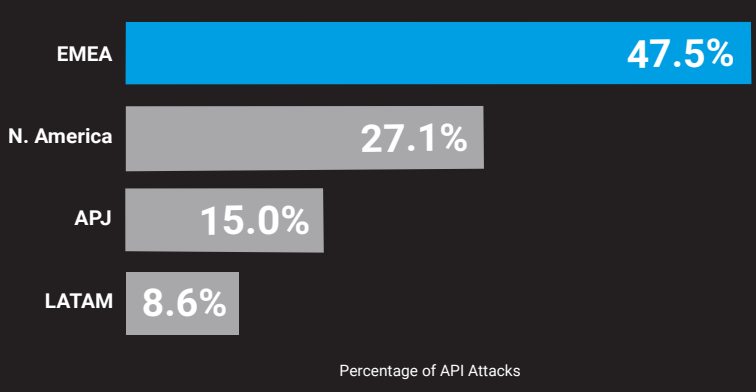
25%
Active Session

14%
Structured Query Language injection

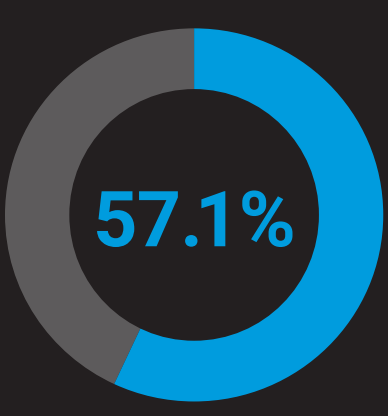
API landscape by the numbers

API Attacks by Region

January 1, 2023 – December 31, 2023



The Europe, Middle East, and Africa (EMEA) region has the highest percentage of API-targeted attacks on a global basis, at 47.5%.



of respondents estimated the accuracy of their API inventory was between 25% and 75%

Based on the 2023 SANS Survey on API Security

Top 3 verticals for API attacks

- Commerce
- Business services
- Other digital media

3 questions for organizations

API abuse and exploitation can extend beyond the vulnerabilities outlined by the OWASP API Security Top 10. Check the boxes to ensure you have a comprehensive security strategy:

- ☐ **Vulnerabilities**: Are you following best practices for development with your APIs?
- ☐ **Visibility**: Do you have process and technical controls to ensure your program is protecting all your APIs?
- ☐ **Business logic abuse**: Do you have a baseline of what the normal API traffic is, to identify suspicious activity?

Why visibility matters

API vulnerabilities are entry points to your environment. You need to discover them before attackers do.

Defending the API universe

How to safeguard your APIs

- ✔ Ensure all APIs are documented and incorporated into your API security controls to enhance visibility
- ✔ Address misconfiguration issues in your APIs and implement processes to prevent future vulnerabilities from emerging
- ✔ Establish API monitoring and threat hunting discipline to close security gaps before attackers can use them against you
- ✔ Choose a solution that can mitigate a whole range of threats, from the OWASP API Security Top 10 risks to traditional web attacks
- ✔ Leverage the OWASP guidance on coding practices to prevent the most common attacks
- ✔ Use security solutions that offer behavioral analytics to detect business logic abuse and other anomalies

Compliance is coming to an API near you

PCI DSS v4.0 includes new standards for how APIs are used in the development and maintenance of systems and software to reduce the risk of data compromise.

Shift left to prevent attacks

Coding best practices include testing your APIs before they go into production and reinforcing security throughout the API lifecycle.

The full report sheds more light on API attack trends and remedies. Read it now.

Download the report

| Published 03/24