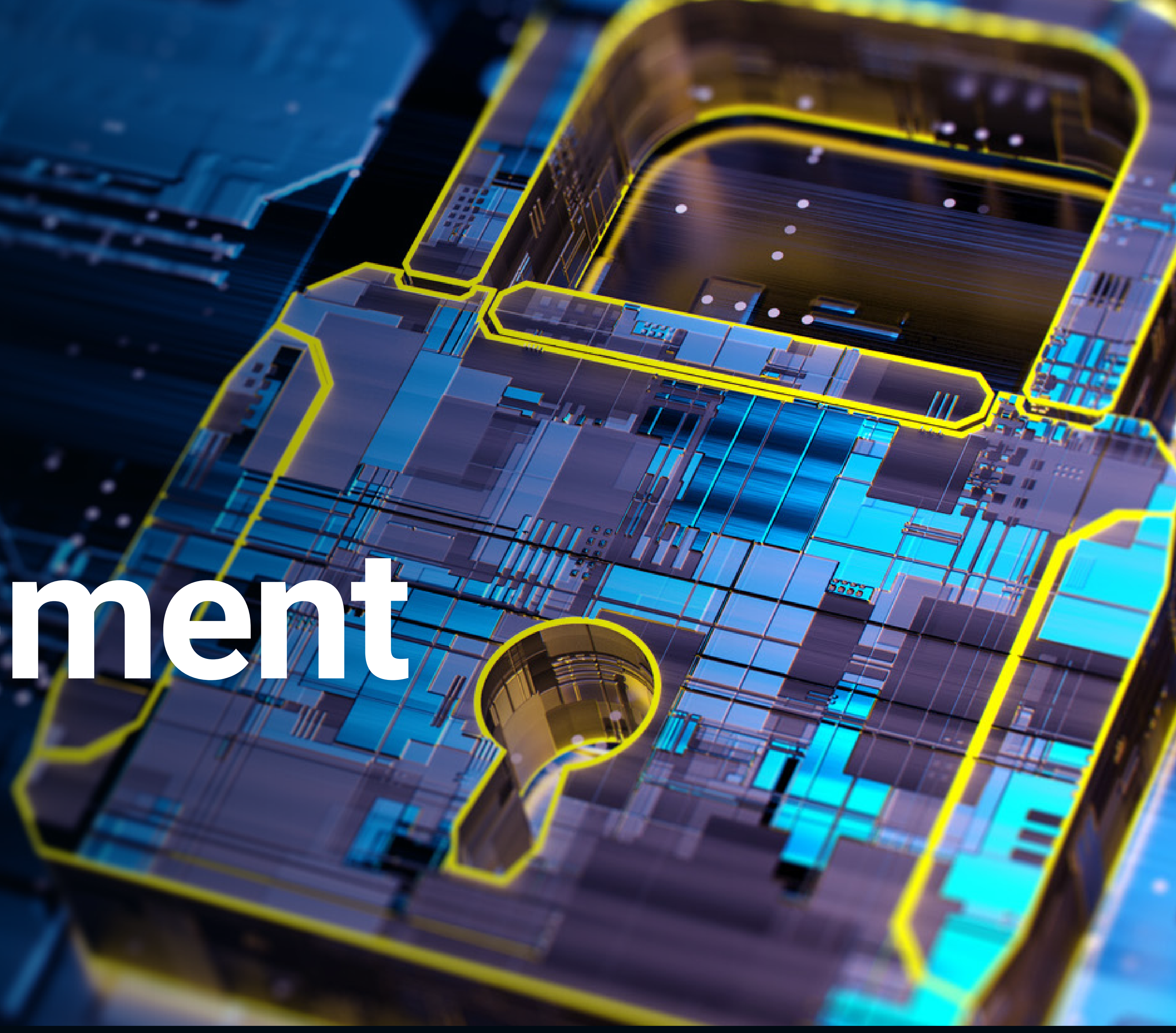
Enterprise Strategy Group™
by TechTarget

API Security From Development to Runtime



Every API is a potential attack vector, and adversaries have a variety of avenues to compromise endpoints at their disposal. Attacks on availability, exploitation of weak authentication, and the abuse of shadow APIs are all common and can easily lead to sensitive data loss. Success requires security operations and tools spanning the software development process, from development to runtime, to help teams discover, manage, configure, monitor, and protect APIs. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity professionals to gain insights into these trends.

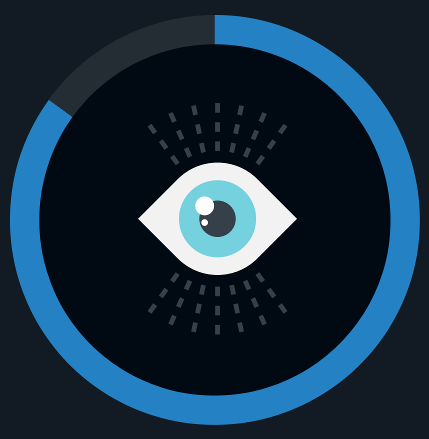
Notable findings from this study include:

64%

of organizations **have faced an API attack or security incident** in the last 12 months.

87%

of organizations say they are concerned with data governance and/or data exposure issues due to insecure APIs.

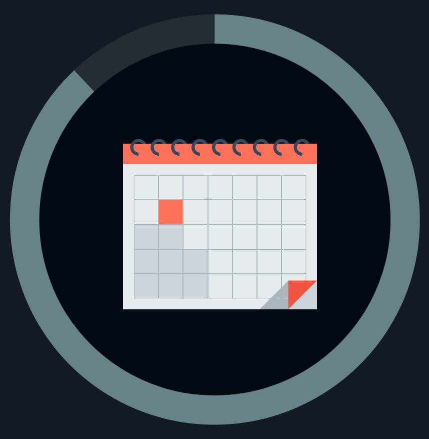


85%

of organizations say APIs used to connect to LLMs for AI are a concern.

79%

of organizations say specialized API security tools are completely or mostly effective.



88%

of organizations say it takes one day or longer to remediate an API vulnerability.

55%

of organizations say **ensuring the security and availability of applications** is their *top* cybersecurity priority.

For more from this Enterprise Strategy Group study, read the full research report, ***API Security From Development to Runtime.***

LEARN MORE

Source: Enterprise Strategy Group Research Report, *API Security From Development to Runtime*, January 2025.