CEQUENCE SECURITY

The Future of API Security

More and more IT executives are seeing the importance of APIs in their digital transformation projects. Given its widespread adoption across many industries, it's natural for many organizations to think more deeply of how their API environments are secured.

But how mature are organizations when it comes to API security? And who calls the shots when making the most important security decisions? In this brief study in collaboration with Pulse, we asked 100 IT executives about what their biggest security concerns were as well as what strategies they're employing to stay ahead of the curve.

API SNAPSHOT

Stepping back to see the lie of the land, the landscape of the use of APIs clearly shows important trends within IT departments. The majority of companies use them for Public-facing Web Apps (63%) as well as 3rd party integrations (81%). These are usually within Servers (80%) or Containers (56%) with only 35% at this stage going Serverless. And when it comes to deployment environments, AWS (65%) beats Azure (49%) with Google much further behind at 13%.

APIs

How are APIs being used

- Partner/Ecosystem/3rd party integration — 81%
- Public facing web apps — 63%
- Mobile Apps — 41%
- Internal Apps — 34%

Environments

What environments are their API-based applications based in?

- 80% Servers
- 56% Containers
- 35% Serverless

Deployment

What are APIs deployed on?

- AWS 65%
- Google 49%
- Azure 13%

SECURITY CONCERNS

71% - Among common API security concerns, the leaking of data or loss of IP was the security lapse most worried about by IT executives.

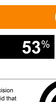
21% were concerned about business logic abuse and another 45% about their organization being susceptible to automated bot attacks.

API Security Approaches

46% - When asked when IT leaders were planning on implementing API security, said it would be within the year (6-12 months)

whereas only 18% said they had planned to do so immediately.

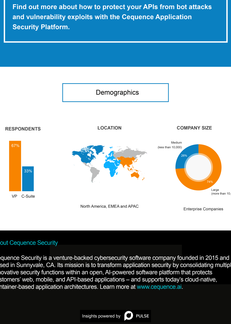
The remaining 36% either had no plans to implement API security or would do so well into the future.



The large majority of organizations were planning on using gateways to protect their APIs whereas half of all respondents (50%) will protect APIs via tighter Access Control.

48% were also looking to implement API security point products.

What are organizations' preferred API security deployment model?



Who calls the shots?

A number of groups can weigh in as the driver or owner of a project. This study found that groups related to Cyber or App Security (63%) and Network Security were the most likely to be the driver or owner of an API Security project.

Similarly when it comes to holding the purse strings, it was found that Cyber and App Security groups were most likely to be in charge of the budget. More than half of all respondents (53%) also said that Network and Infrastructure groups played an important part in budgeting decisions.

- Cyber or App Security — 63%
- Network and Infrastructure — 53%

Finally, when it comes to being the tech decision maker, more than half of all respondents said that once again Cyber/App Security, Infrastructure and Network Security groups were crucial to making key tech decisions at the organization.

GREATER API SECURITY

A majority of organizations now understand the importance of API security for their public-facing and mobile apps.

Why are organizations increasingly interested in SaaS-based enterprise class security solutions that protects APIs from outside attacks?

> *"It would be great if a solution like this can tackle most of these key issues without us getting involved in development."*
> **- VP in Professional Services**

> *"It will save us a lot of effort and cost."*
> **- VP in Consumer Goods**

> *Great to have this capability "baked-in"*
> **- CIO in Healthcare**

> *"SaaS is attractive as it helps me keep headcount and costs low."*
> **- CIO in Software**

> *"We can't afford to stay on top of this with internal resources."*
> **- VP in Manufacturing**

Find out more about how to protect your APIs from bot attacks and vulnerability exploits with the Cequence Application Security Platform.

Demographics

RESPONDENTS

LOCATION

North America, EMEA and APAC

COMPANY SIZE

Enterprise Companies