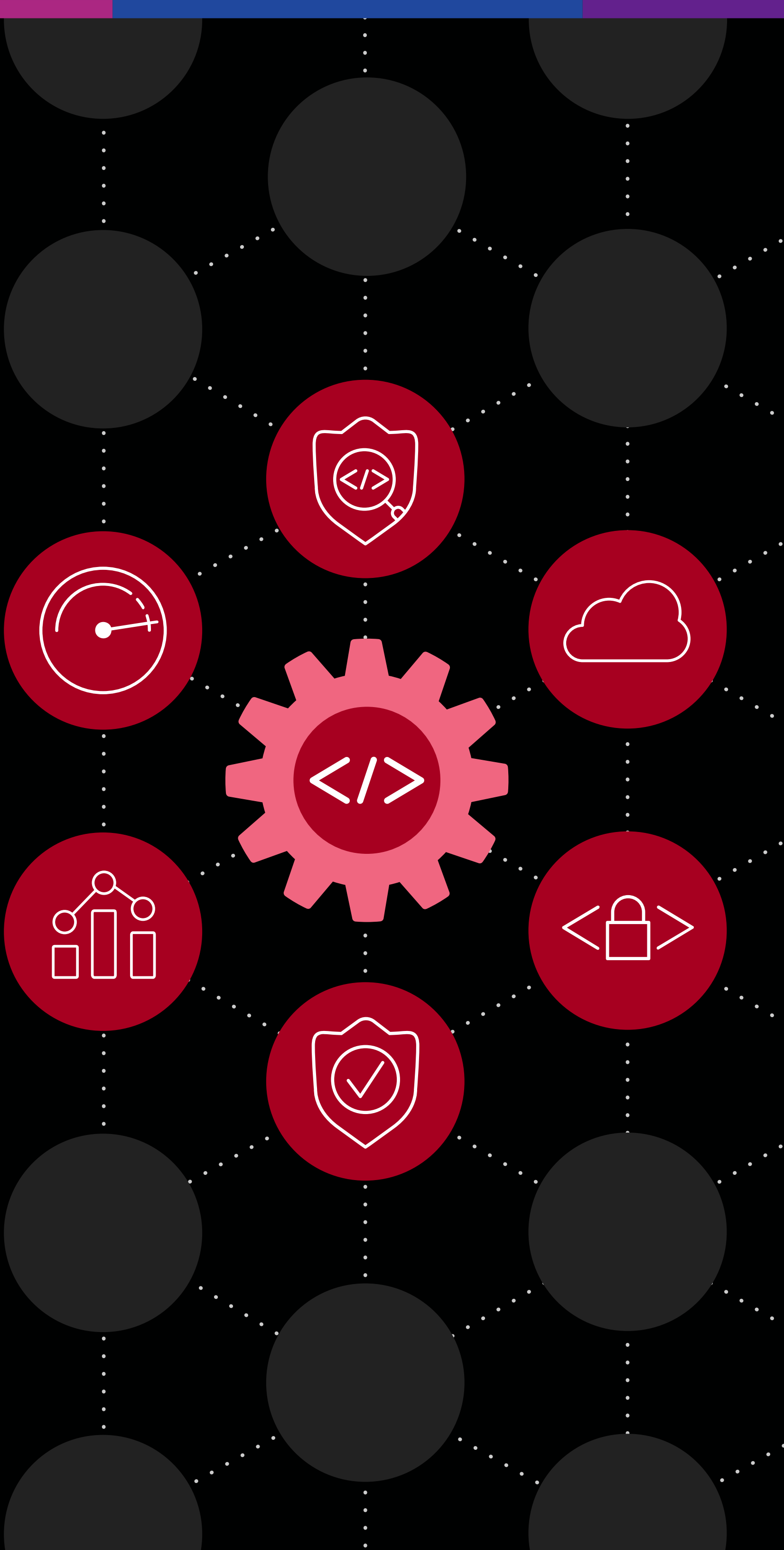
2024

State of Application Strategy Report: API Security

The Secret Life of APIs



Contents

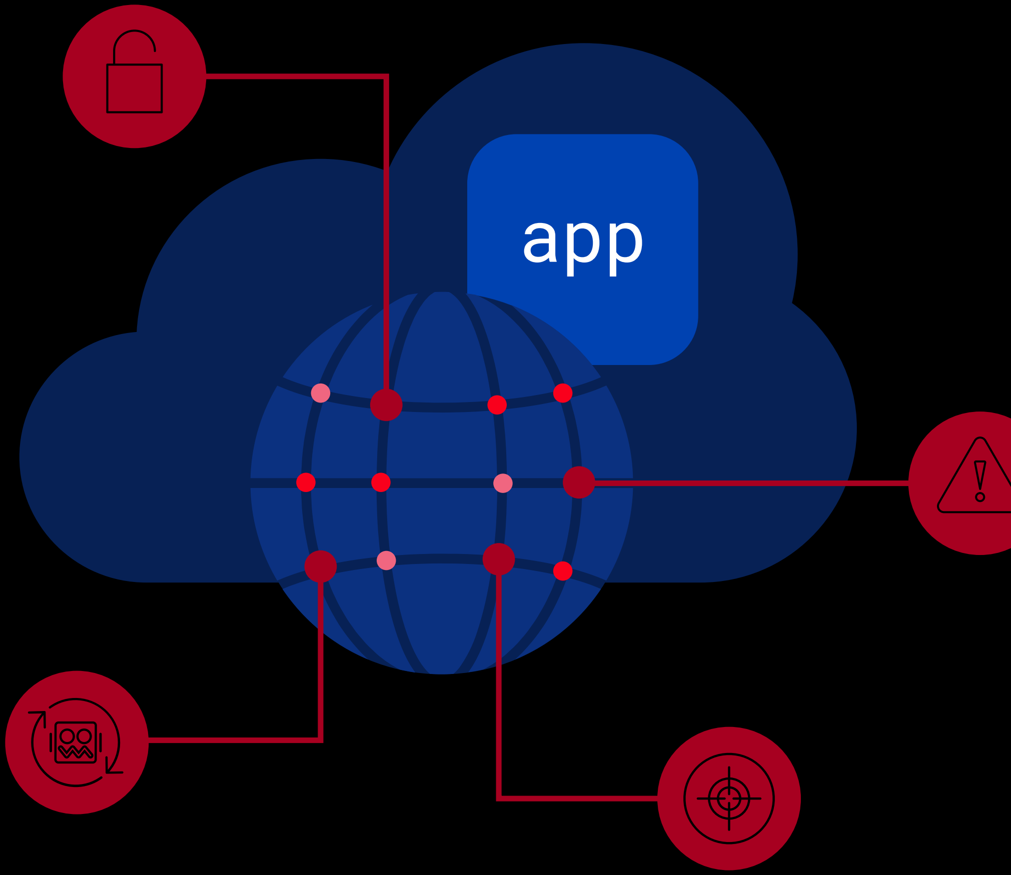
Scary Truths about APIs

Do you know where your APIs go at night—and how to make sure they're home safe in the morning?

We can start to answer these questions by considering a parallel in the natural history of computing. The HTTPS Everywhere project launched in 2010 as a collaboration between the Electronic Frontier Foundation (EFF) and the Tor Project. The initiative aimed to make the web more secure by encouraging and facilitating the use of HTTPS (Hypertext Transfer Protocol Secure) across websites. Fourteen years later, EFF estimates 90% of web pages are accessed via HTTPS—a happy ending, at least for web apps.

APIs (application programming interfaces), on the other hand, may be headed for tragedy. Despite typically leveraging HTTP as their communication protocol, the scary truth is that more than 30% of customer-facing (that is, public) APIs remain unprotected by HTTPS today. That may seem like a low percentage, but it translates into many thousands of APIs at risk. Without an intervention, APIs may become the Internet's single most targeted threat surface. That's concerning, since most organizations anticipate their API estates will grow by at least 10% in the next two to three years.

This is just one of the worrisome facts revealed in our recent survey of API security decision makers across industries, which supplemented our 2024 State of Application Strategy research. The results represent the views of respondents who are responsible for making decisions about APIs. Their answers to our questions about their API use, the security used to protect those APIs, and the security capabilities respondents consider important provide a glimpse into the secret lives of APIs. The implications can help you prevent potential heartbreak and keep your APIs safe.



Where Do APIs Hang Out?

The average organization manages 421 different APIs spread across infrastructure environments, applications, and architectures. API endpoints expose business logic so external systems can seamlessly exchange data with the business to expand service offerings and innovations. They're used for just about every enterprise purpose you can imagine, from CRM data access and payment processing to tracking social media engagement. As a result, a single API may have thousands of endpoints, adding significantly to the complexity of managing them.

Most APIs today are hosted in a public cloud. The majority (52%) exchange data using JSON, although the long-lived XML format is still a force, with 27% of APIs relying on it. The GraphQL language, now used by 13% of APIs, is also gaining ground.

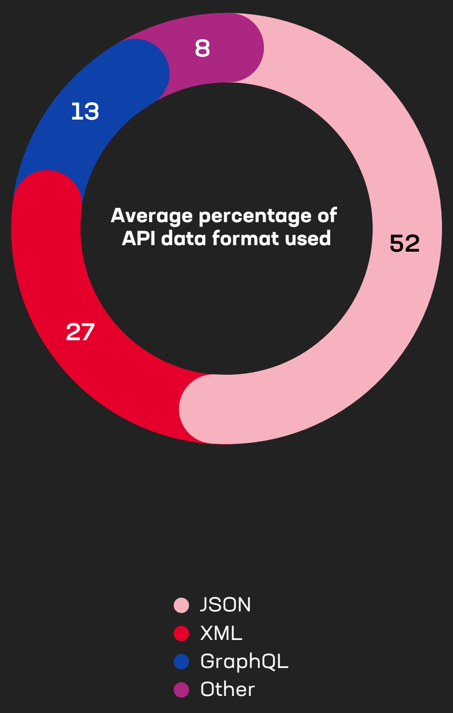
When we read about APIs, the writers typically are referring to customer-facing or public APIs used by web and mobile applications. These are the APIs vulnerable to the attacks that make headlines, from DDoS (distributed denial-of-service) attacks and account takeovers to emerging threats such as prompt injection and token stuffing.

In reality, these public APIs account for only a fraction of the total in most enterprise estates. A large number of other APIs stay busy, too, serving a variety of purposes but without the benefit of security services. That's just the first alarming finding from our survey.

Data Formats Used by APIs Today

We asked:
What percentages of your APIs are in the following data formats/protocols?

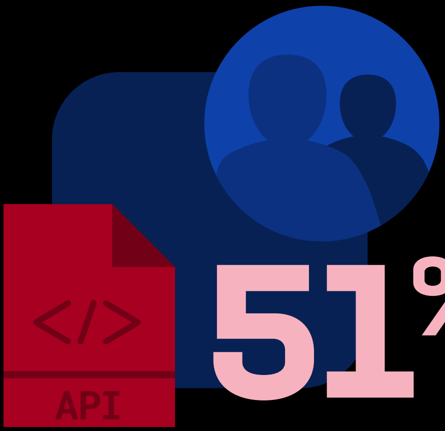
We learned:
The JSON format dominates, but GraphQL is gaining ground.



What Do APIs Do?

From deep inside applications, APIs assist with integration and invocation of diverse services relied upon by enterprise employees, customers, and partners. They drive operational workflows and connect microservices within modern application architectures.

Increasingly, APIs connect to AI inferencing services like OpenAI, Google Gemini, and IBM Watson. These connections, which are outbound API calls, pose a unique security challenge. Until now, organizations have primarily architected security for inbound API calls and the related use cases. The security models they're using need to expand to also address the risks incurred by outbound API traffic. APIs called by modern apps can be buried deep inside code, putting them off the radar of security teams not specifically focused on both inbound and outbound API security.



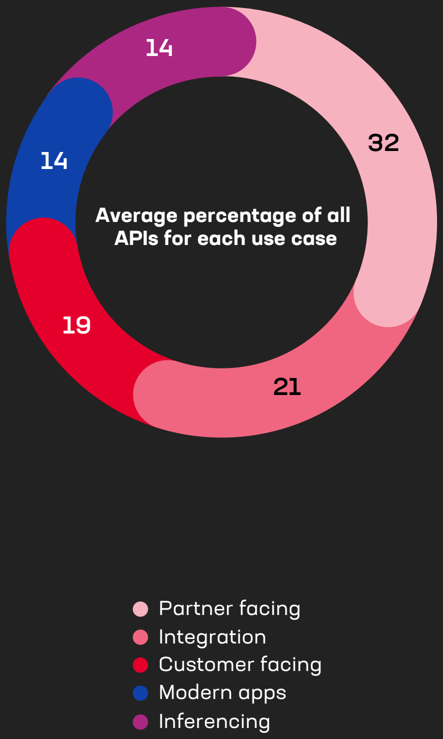
51%

of APIs face customers or partners

API Uses

We asked:
Please estimate the percentage of all your APIs that are currently used for each of these purposes.

We learned:
Half of APIs face customers or partners.



F5 Insight

Adapting to a security model that must consider both inbound and outbound API traffic will be a challenge for many organizations. The difficulty will only grow as the API estates of most organizations expand by an expected 10% or more over the next two to three years. This estimate may actually be conservative, since many organizations are busy implementing AI apps, which largely rely on even more APIs. In addition, as use of GraphQL grows, securing it will become an important capability of API security in general.

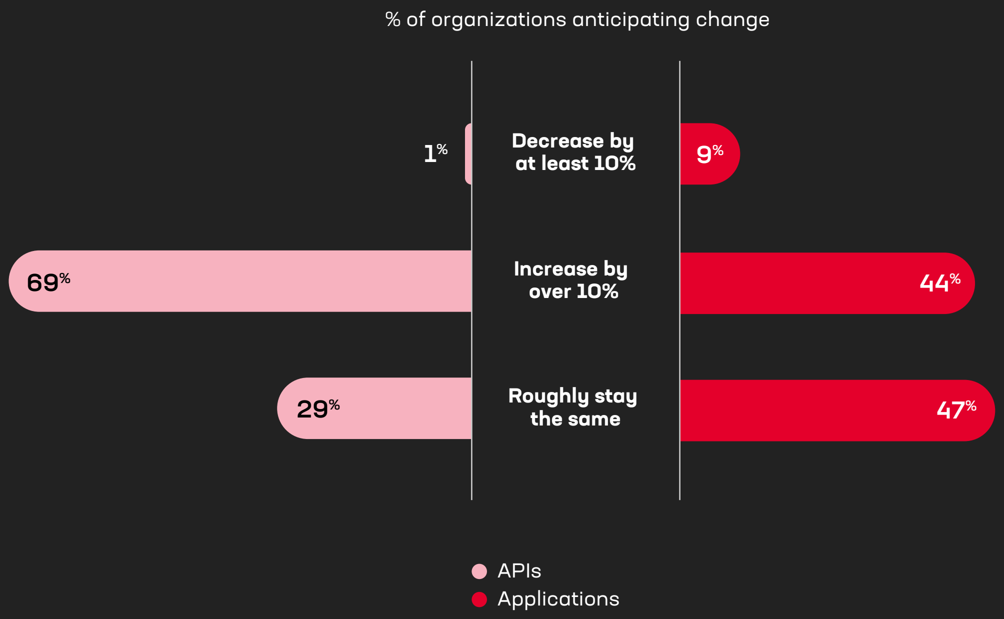
2/3

of respondents expect API numbers to grow

Expected Two-Year API and Application Growth

We asked:
Please select how you expect the number of applications and APIs deployed by your organization to change in the next two years.

We learned:
API numbers are expected to grow more than app numbers, and very few expect either to decrease.



Who Keeps APIs Safe?

When it comes to where the responsibility for API safety falls, a small majority of organizations (53%) place that security in the same domain as application security. But nearly one-third (31%) park it squarely with API management and integration platforms.

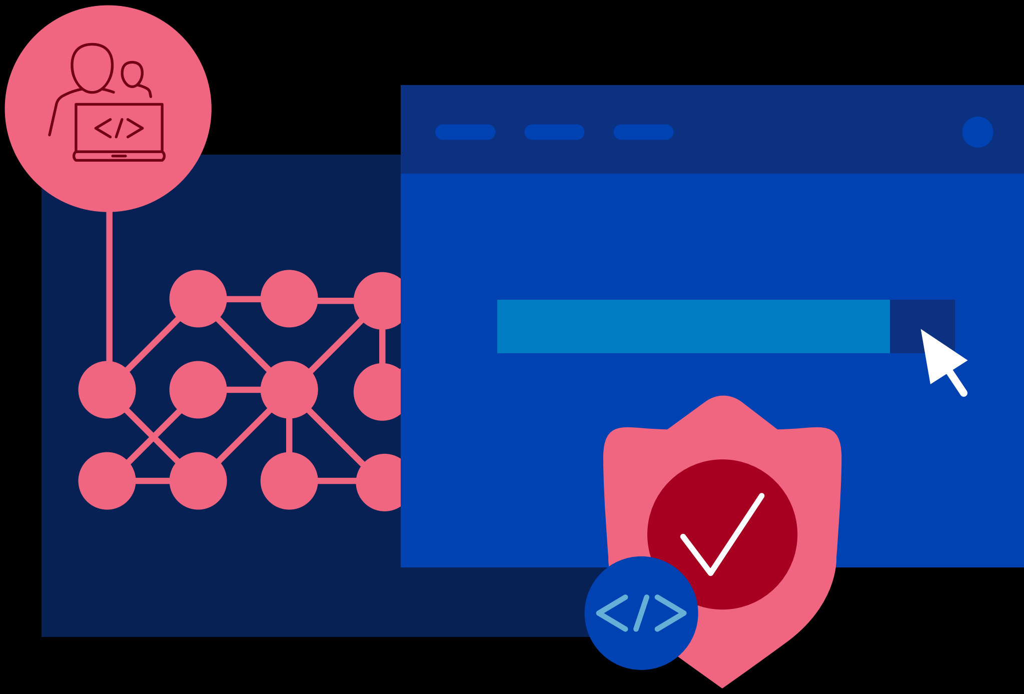
This division reflects the current marketplace for API security, which is divided between the two domains. Historical treatment of previous API protocols—such as the Simple Object Access Protocol (SOAP)—suggests this division will not continue indefinitely. We predict that API management tasks will diverge, with cataloging, billing, and other business-related API management concerns remaining under that umbrella while the security and traffic handling duties will merge with API gateways into an API delivery and security domain.

Nearly one-third of respondents stretch API security responsibilities across functions

This prediction is backed by current organizational responsibility for API security strategies. The largest segment of organizations (33%) relegates that responsibility to security teams, with 28% assigning it specifically to the CISO. Another 27% appear to be in transition, saying they consider API security a cross-organizational responsibility.

F5 Insight

Given both an increasing attack surface and today's AI-driven threats, API security is too important to allow it to fall between organizational cracks. Specific accountability will help ensure security is addressed, and the most effective solutions for doing so will leave the functionality of API management platforms to align with API gateways instead.

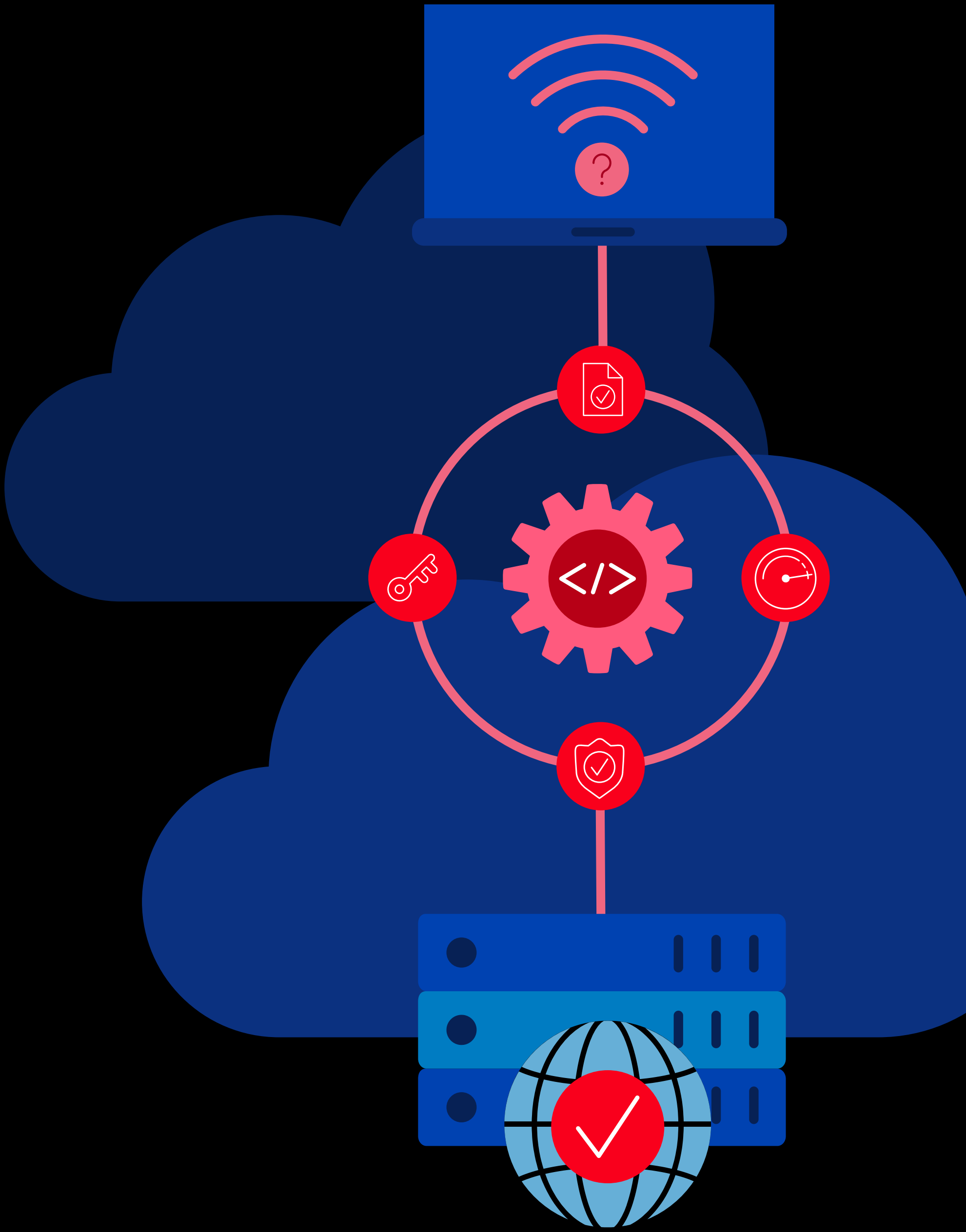


When and How Are APIs Secured?

“Secure by design” is a great marketing mantra, if not always one backed by action. We’re encouraged, however, to learn that 80% of organizations begin API security in the API design phase. In addition, 59% say they incorporate security at every stage of the API lifecycle. That aligns well with a 2024 State of Application Strategy survey finding that 87% of organizations have adopted or plan to adopt secure development lifecycle (SDLC) practices, which emphasize addressing security at every stage of the cycle.

Given the diversity of API purposes and data formats, we weren’t surprised to find a robust set of security offerings in use. Most organizations leverage multiple solutions and services. Three-quarters (76%) take advantage of API management and integration platforms. More than half (57%) use services from a platform that also offers adjacent security services such as web application firewall (WAF) and DDoS protection. A slightly smaller majority (53%) also leverage an application delivery controller (ADC) to provide the security, access, and delivery services needed.

Two-thirds of organizations leave operational workflow APIs unsecured



This confusing array of options makes sense when viewed through the lens of the API lifecycle. Organizations often use Security as a Service (SECaaS) platforms for operational security early in the lifecycle. Later, they incorporate delivery services as well as API management and integration platforms for visibility, rate limiting, and billing.

The research finding that makes less sense is a lackluster attention to securing APIs that drive operational workflows such as deploying a new security policy, making a change to an existing configuration or policy, or rotating certificates. Barely one-third of organizations use any service to protect those APIs, with HTTPS (SSL) in use the most. This finding leaves us speechless (if just for a moment).

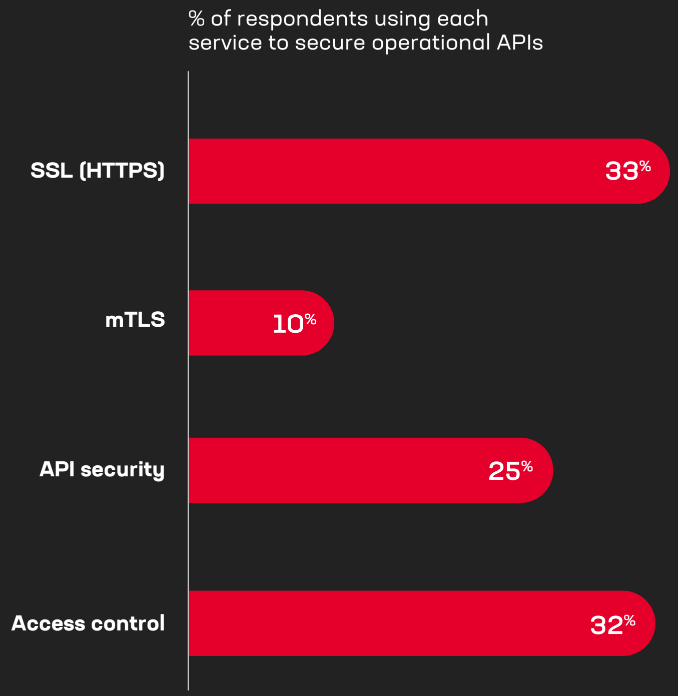
F5 Insight

With operational APIs playing increasingly important roles in automating workflows that impact app (or product!) availability, reliability, access, and even security, it's folly to leave them unprotected. Operational APIs are as vulnerable to attack—particularly lateral attacks from inside the network—as any other API. They need equivalent security services.

Services Used to Secure Operational APIs

We asked:
Please indicate the application services you use today to secure various API use cases.

We learned:
SSL provides the most likely protection for operational APIs, but overall rates of security for the operational use case are alarmingly low.



Which Services Protect APIs?

Some APIs live within a bubble of security services, from mTLS within microservices architectures to access control, DDoS and bot defenses, and API-specific security measures. As a result, those APIs are fairly well protected, in general.

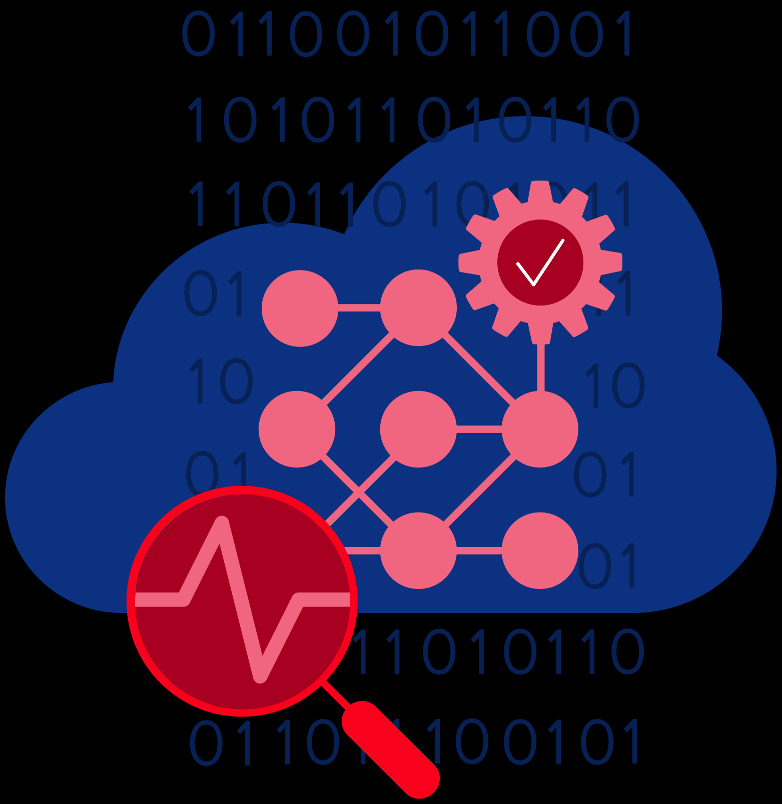
But a small percentage—under 10%—are left completely unprotected. That might not be concerning given the breadth of API use within most organizations. When we looked closer, however, we found an alarming percentage of customer-facing APIs (more than 30%, nearly one-third) protected by absolutely nothing. As noted in the introduction, even HTTPS and SSL protection for APIs fails to reach parity with web app protection.

Interestingly, specific security measures are applied most often to APIs in integration use cases, rather than those in customer- or partner-facing apps. And although 46% of respondents to our 2024 State of Application Strategy survey say they've adopted zero trust security models and another 45% plan to do so, the middling use of access control services across all types of APIs suggests that implementation of zero trust as it applies to APIs is much further behind.

Zero trust security hasn't fully reached APIs

F5 Insight

Leaving any APIs unprotected, whether in apps accessed by the public and partners or in operational integrations, is unwise. Organizations embracing zero trust security models need to extend their thinking beyond their apps to also ensure every API request, regardless of its source, is authenticated, authorized, and validated. They also need to enforce the same kinds of access privileges to reduce the risks of compromise.



What Security Capabilities Do APIs Really Need?

It may be that security services offered by the market today simply do not deliver the capabilities organizations really want. Repeatedly over the past three years and again in this targeted survey, we've asked which security capabilities are most valuable. The answers remain consistent: authentication and authorization, behavioral anomaly detection, and scanning for malicious data, in that order.

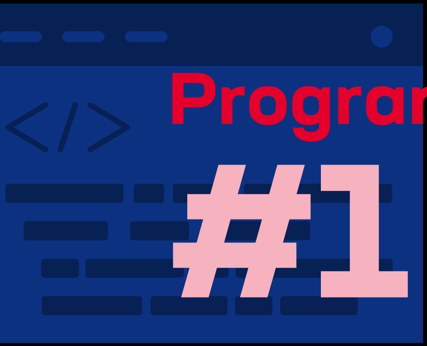
To better understand what organizations want from their API security offerings in the AI era, we asked respondents to rank the individual capabilities or features available in API security offerings by allotting a total of 100 points across various options. Unsurprisingly, a natural language interface and fine-grained access control ranked as relatively unimportant. The top honor went to programmability (24.2 points), which affords the ability to inspect and act on real-time API traffic and data. Programmable services enable organizations to address bespoke security (and delivery) needs while assisting in the immediate mitigation of zero-day threats. Those capabilities are appealing in a world where novel, AI-powered attacks target APIs at overwhelming rates and with alarming frequency.

Most Valuable API Security Capabilities

1
Authentication and authorization

2
Behavioral anomaly detection

3
Scanning for malicious data



Programmability is the #1 API security feature

Importantly, API security needs to be delivered in the right form factors for the infrastructure environments in which the relevant app is deployed. For on-premises apps and those in colocation environments—which afford greater control over infrastructure—organizations prefer appliances or software for their API security services. In the public cloud, equal weight is given to SECaaS and cloud provider API security services. There's logic behind these preferences, but the use of multiple options doesn't make comprehensive, real-time API security easier.

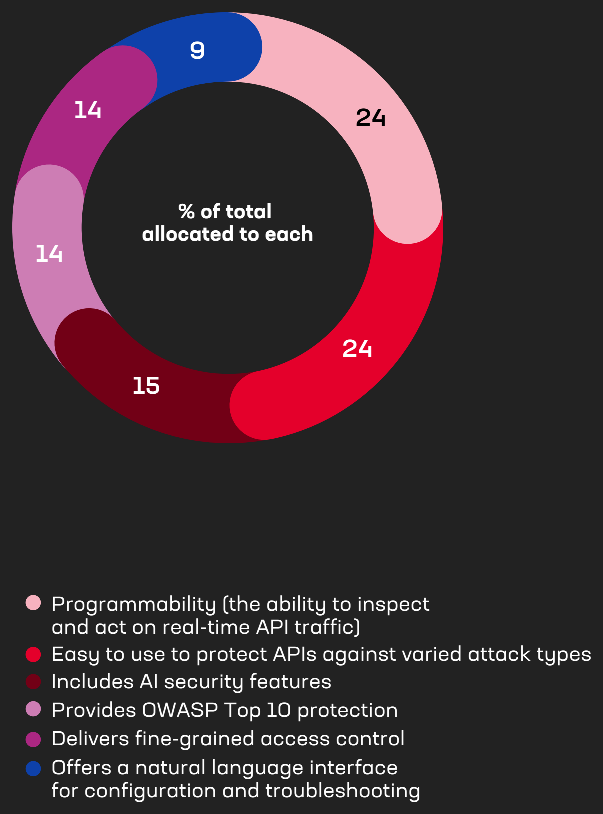
F5 Insight

Deploying apps, and therefore APIs, across multiple environments won't go away—there are too many benefits to being able to choose how and where to deploy. But the resulting complexity is exacerbated by the need for API security, since relatively few providers can deliver API security services in three distinct form factors or apply them comprehensively across different environments. Organizations can streamline management and gain an edge by consolidating on a single vendor or comprehensive solution suite of real-time API security and management capabilities.

Most Valuable Aspects of API Security Offerings

We asked:
From the following list of capabilities or features, please assign 100 points to indicate how you weight the importance of each for API security offerings.

We learned:
Programmability ranked as the most valuable feature, beating ease of use by six-tenths of a percent. (Chart values are rounded.)



APIs Exposed

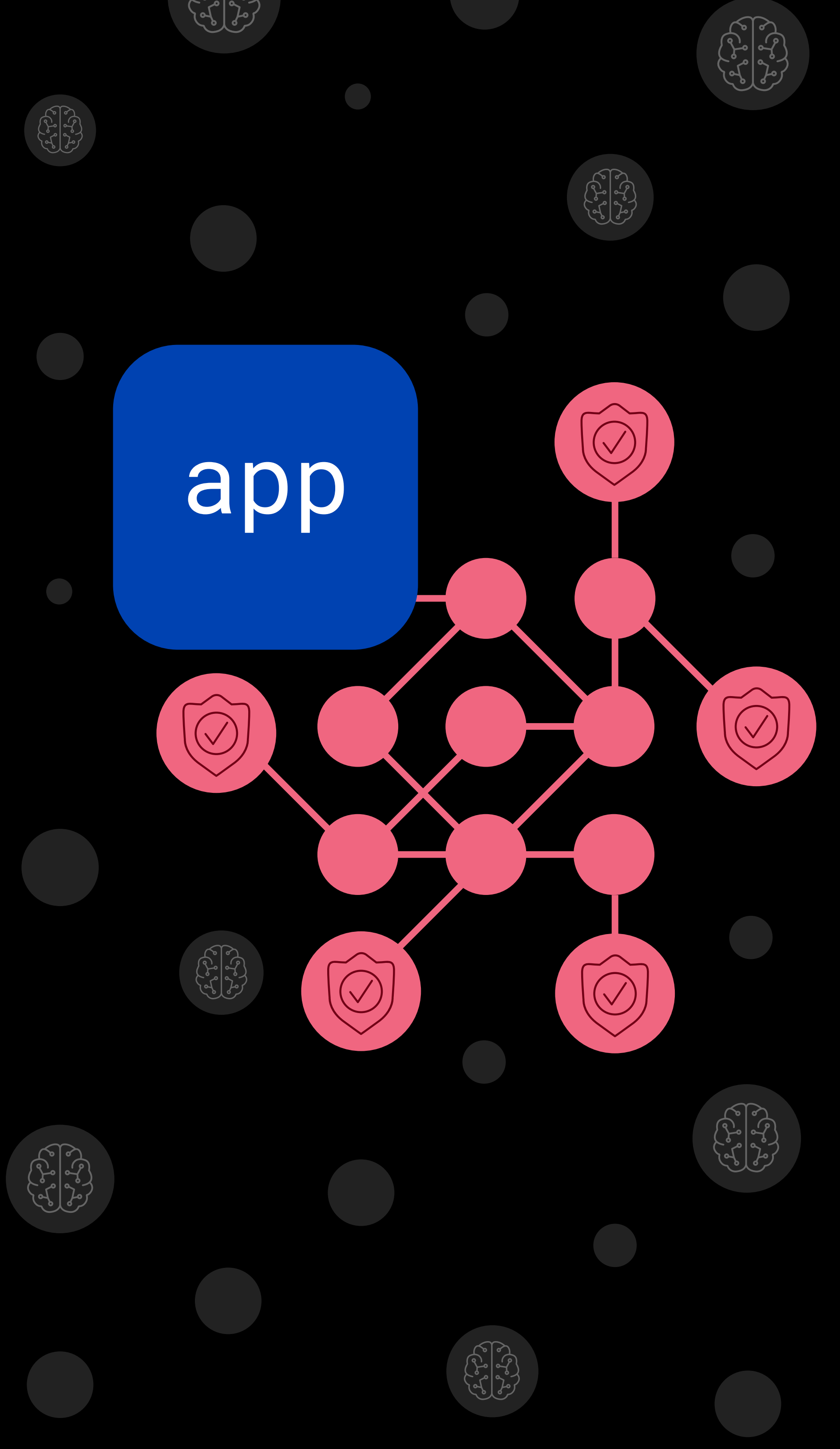
Together, gentle reader, we've glimpsed both the previously secret world of APIs and the insufficient security that exposes many of them to dangerous threats.

While our survey results indicate the attention most organizations shower upon all kinds of APIs, we remain concerned for the significant percentage that lack comprehensive security measures. Today's AI era is enabled by APIs. Without proper API security, AI can never truly be secure, either.

It's time to gather your APIs close, whether they're public or serving unheralded operational use cases, and get serious about API security.

About this report

The data presented in this report reflects results from both the annual F5 State of Application Strategy survey and targeted follow-up research with additional API decision makers—more than two-thirds of them in C-level roles. Respondents represented global organizations of all sizes and across industries, from technology, manufacturing, finance, and retail to organizations in healthcare and education.



ABOUT F5

F5 is a multicloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure every app and API—on premises, in the cloud, or at the edge. F5 enables organizations to continuously stay ahead of threats while providing exceptional, secure digital experiences for their customers.

For more information, go to f5.com. (NASDAQ: FFIV).