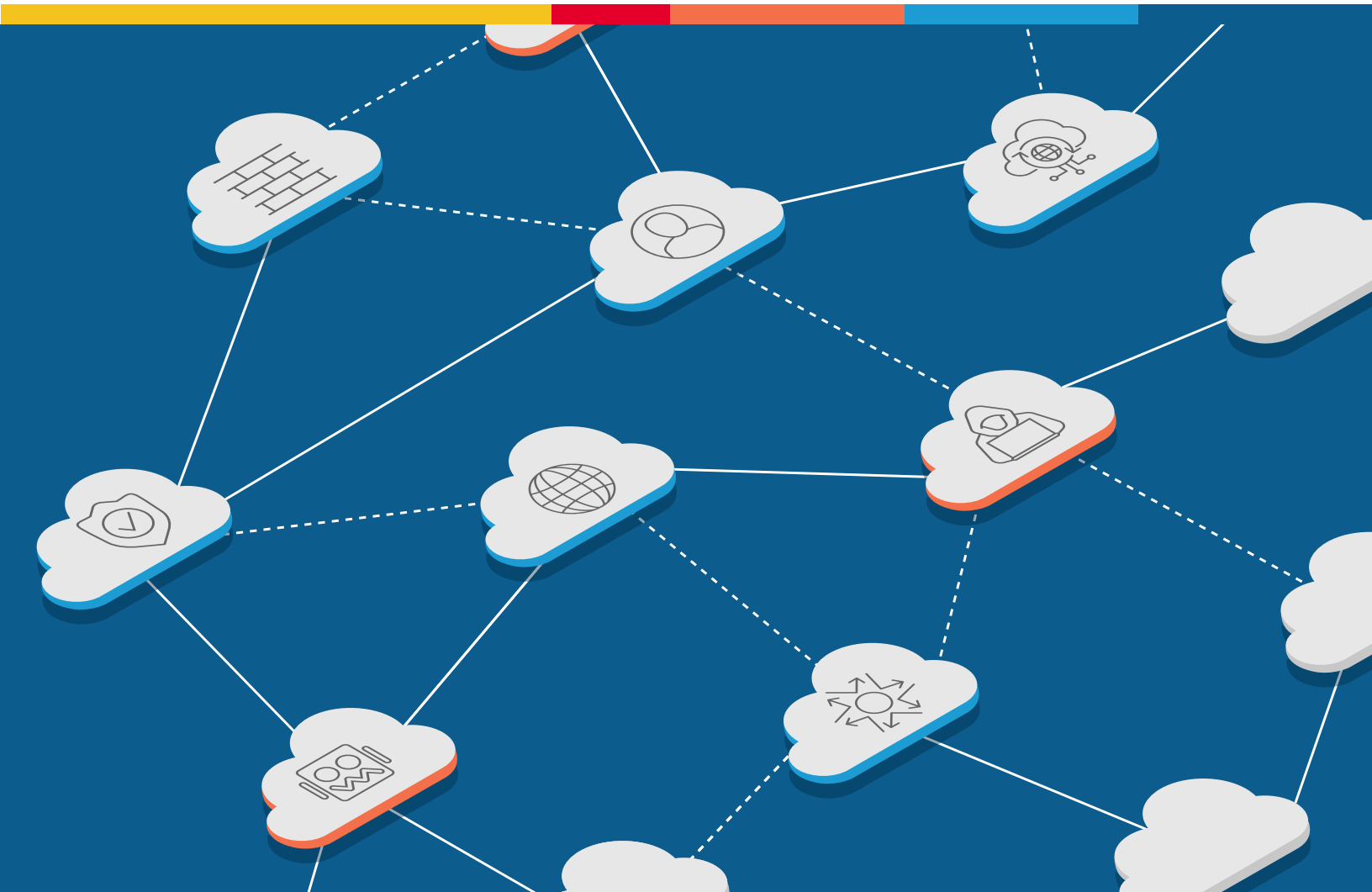
Discover APIs and Prevent Data Leakage

Combine the power of data analytics and deep insights from AI and machine learning to discover your app APIs and mitigate threats. F5 Distributed Cloud API Security blocks API attacks in real time and eliminates vulnerabilities at their source.



KEY BENEFITS

Faster onboarding
Rapid deployment with automated API discovery, leading to faster rollouts.

Global coverage
Global points of presence (PoPs) protect API endpoints from abuse and exploits.

Visibility and insights
Observe global API metrics from a single, centralized user interface.

APIs are a fundamental building block of modern application development, powering apps that impact lives. As modern applications have evolved, dependencies on APIs have increased. That's because by enabling disparate systems to work collectively, APIs can speed up time to market for application development and deliver improved user experiences.

The flipside is that the use of APIs has decentralized application structures. This makes securing them even tougher, which in turn makes them extremely attractive to attackers. API endpoints increase an application's attack surface area and introduce new risks and vulnerabilities that current security tools struggle to mitigate. Without proper management and security controls, APIs can pose a serious risk to organizations.

Threats and attacks that target APIs deployed or integrated into larger applications are hard to mitigate and even harder to remediate. Scanning and testing APIs in a runtime environment helps security teams uncover vulnerabilities in APIs before they're in production, where remediation is more costly and frustrating. Understanding how to secure APIs is a struggle for most security teams.

Similarly, organizations frequently have outdated APIs—often owned or third-party APIs that connect to applications they lose track of—that lead to security vulnerabilities. Automated API discovery can reveal those vulnerabilities and protect against cybercriminal abuses and attacks.

WITHOUT PROPER MANAGEMENT AND SECURITY CONTROLS, APIS CAN POSE A SERIOUS RISK TO ORGANIZATIONS.

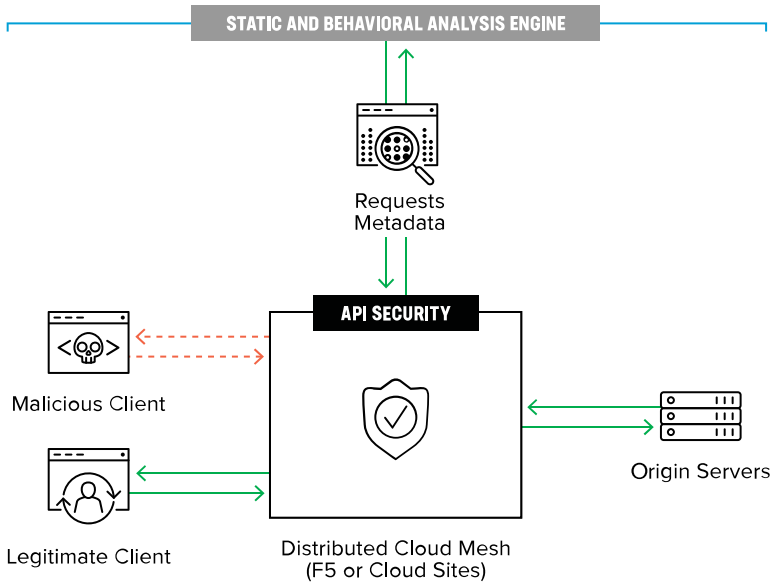


Figure 1: An architectural view of how F5 Distributed Cloud API Security works.

KEY FEATURES

Positive security model
You can automatically create and enforce a positive security model from your own Open API specifications.

Automatic API discovery
Detect APIs across your applications, including rogue and shadow APIs, with the generation of Swagger files.

Lifecycle security
Integrate security into the API lifecycle process via CI/CD tools or leading API management vendors.

ML-based traffic monitoring
Continuous machine learning monitors all traffic, allowing API security to predict and block suspicious activity.

Globally distributed
Distributed infrastructure across clouds and edge sites provides a consistent operational experience.

Automated policy generation
Automatically generate policies based on Swagger import and API patterns.

YOU GET DISCOVERY AND DEEP INSIGHTS, LEVERAGING AI AND MACHINE LEARNING.

Discover, Control, and Mitigate Threats to APIs Using Machine Learning

F5® Distributed Cloud API Security is a comprehensive solution to securely manage APIs across any data center or cloud using a simple, fast, and scalable architecture. It helps drive business velocity by enabling automated API deployments and management, while also protecting against API-specific threats.

Distributed Cloud API Security—part of the F5® Distributed Cloud Web App & API Protection (WAAP) solution—delivers advanced security controls in a SaaS-based solution, reducing tool sprawl and architectural complexity. Using advanced analytics on the data collected across users on its multi-tenant platform, Distributed Cloud API Security identifies behavioral anomalies and automatically updates to mitigate threats from users as well as internal apps.

You get discovery and deep insights, leveraging AI and machine learning (ML). Block API attacks in real time and eliminate vulnerabilities at their source. A SaaS-based portal will manage and provide threat analytics, forensics, and troubleshooting for your modern application. Detect and block Open Web Application Security Project (OWASP) API Top 10 attacks in real time by using automatic detection at the development and production layers.

Conclusion

Distributed Cloud API Security use cases include:

- **Hybrid security deployments:** Protect existing workloads in one or more clouds and/or in on-premises environments.
- **Workload management using a service mesh:** Mesh a Kubernetes controller and multi-layer security in and across clusters.
- **API endpoint identification:** Automatically discover API endpoints with Swagger import and export capabilities.

Organizations must maintain and evolve their traditional APIs, while simultaneously developing new ones using modern architectures. These can be delivered with on-premises servers, from the cloud, or in hybrid environments. APIs are difficult to categorize, as they're used to deliver a variety of user experiences, each one potentially requiring a different set of security and compliance controls. Distributed Cloud API Security can address multiple use cases or architectural patterns.

For more information, visit f5.com/waap or contact sales@f5.com to schedule a demo.

DC0222 | OV-838311885-XC-API Protection