How to secure modern apps F5 Distributed Cloud Web App and API Protection (WAAP)

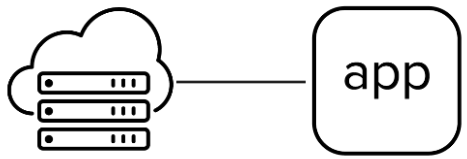
Bogdan ION

F5 Networks System Engineer – Alef Romania

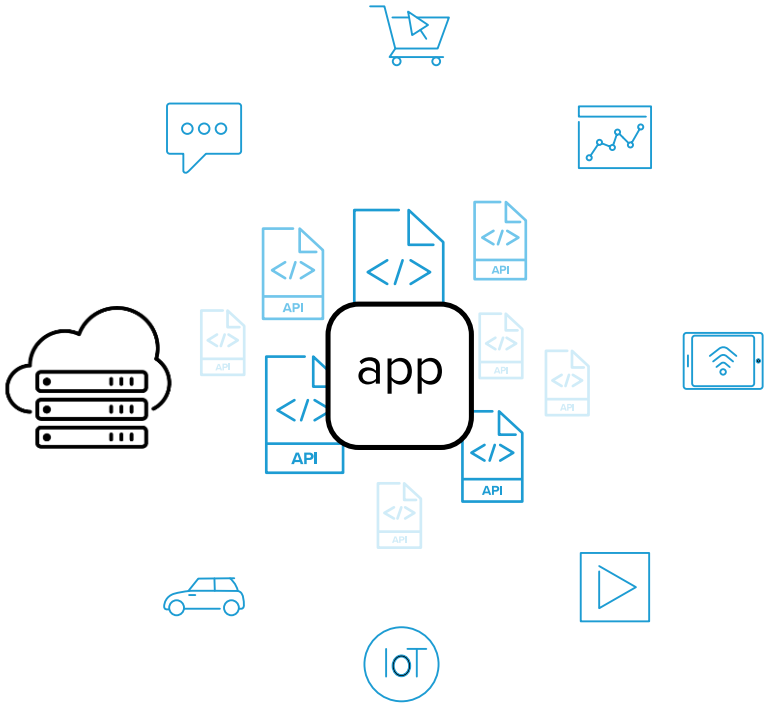
24 Oct 2024

Apps are evolving and becoming increasingly complex

API first architectures for apps are not table stakes

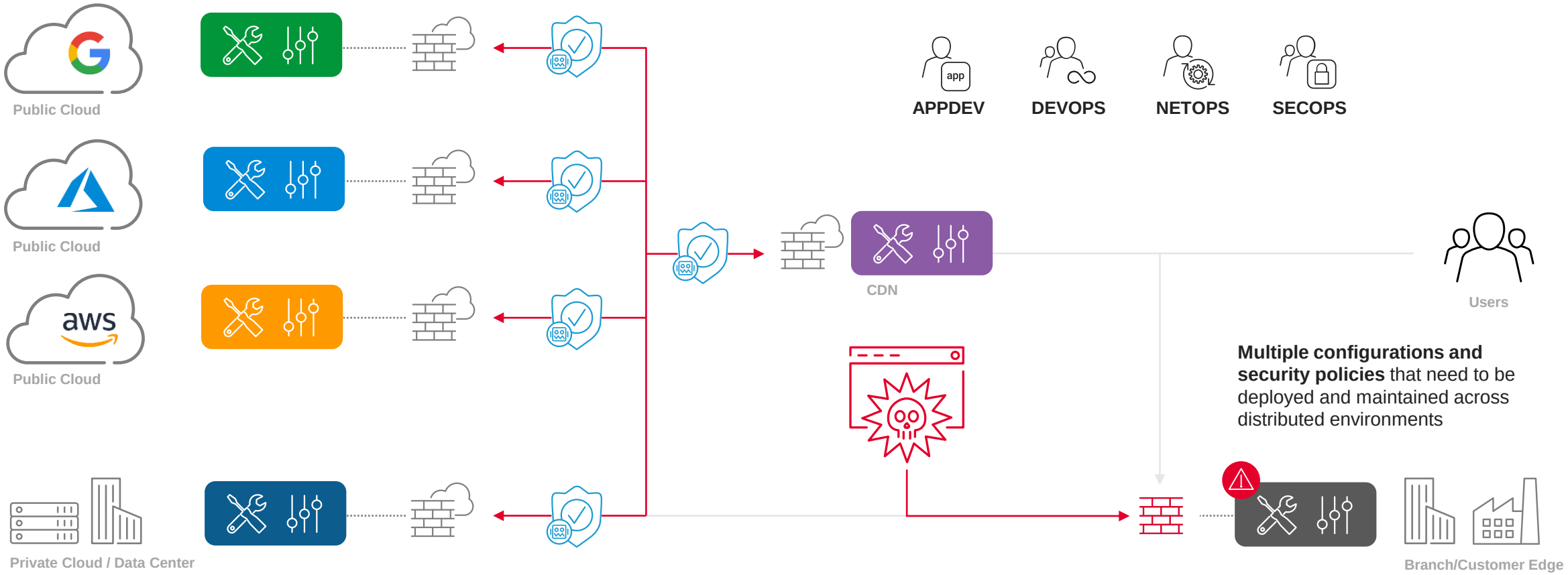


Simple application with back-end server



Increased back-end API services and connectivity

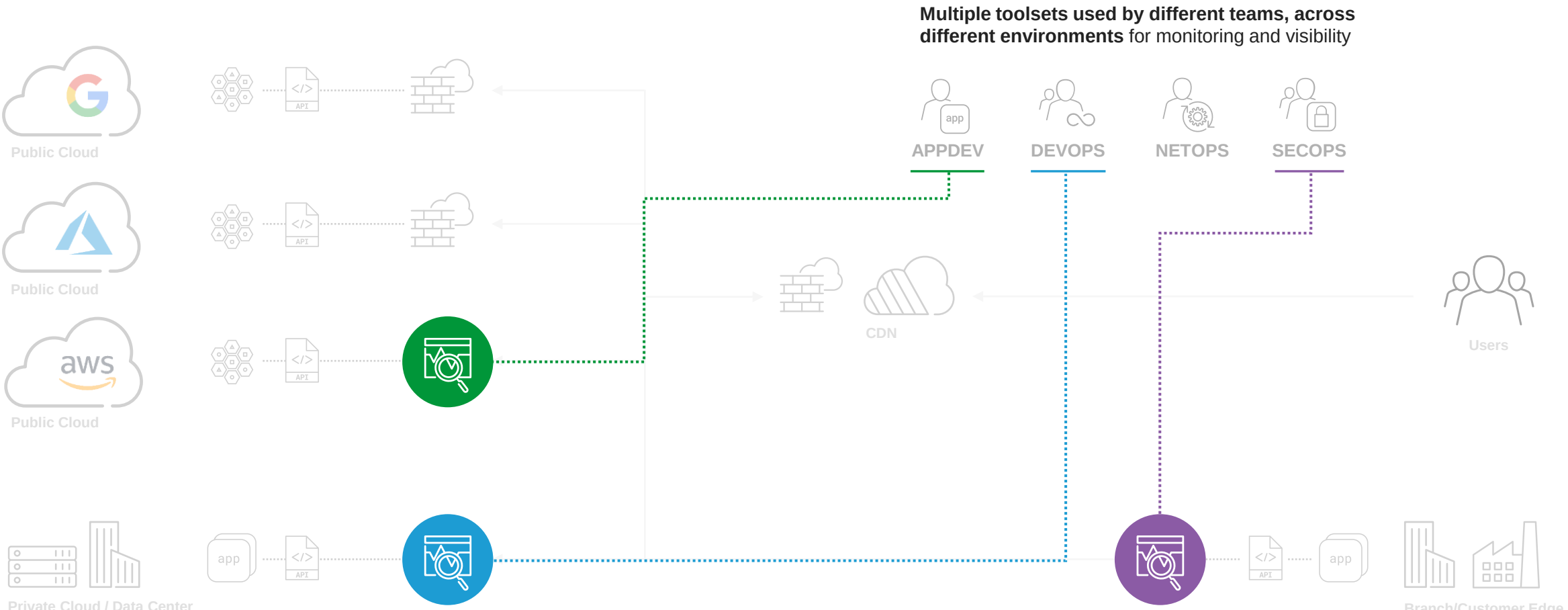
Increasing complexity and risk



Multiple configurations and security policies that need to be deployed and maintained across distributed environments

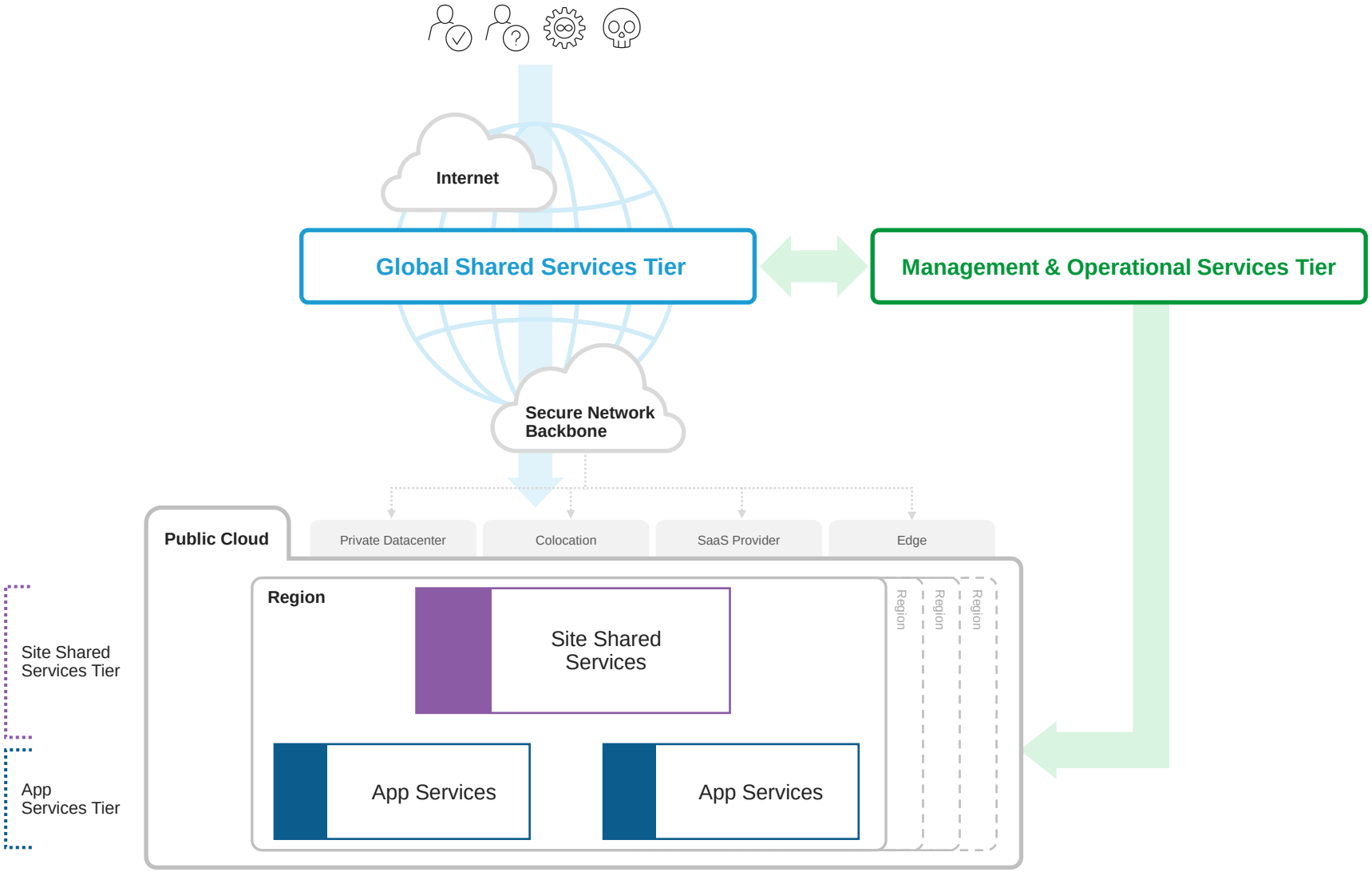
Increased vulnerabilities due to misconfigurations and inconsistent policies

Lack of end-to-end visibility



Simplifying App Services – Generic Architecture

A framework for organizing and optimizing critical app services



Management & Ops Tier

- System Source of Truth
- Integration and Testing
- Automated Delivery
- Operational Observability and Insights
- Business Workflow Management

Global Service Tier

- Scalable App Delivery
- Anti-Abuse
- Global Connectivity Services
- Global App Health
- Global App Protection

Site Shared Service Tier

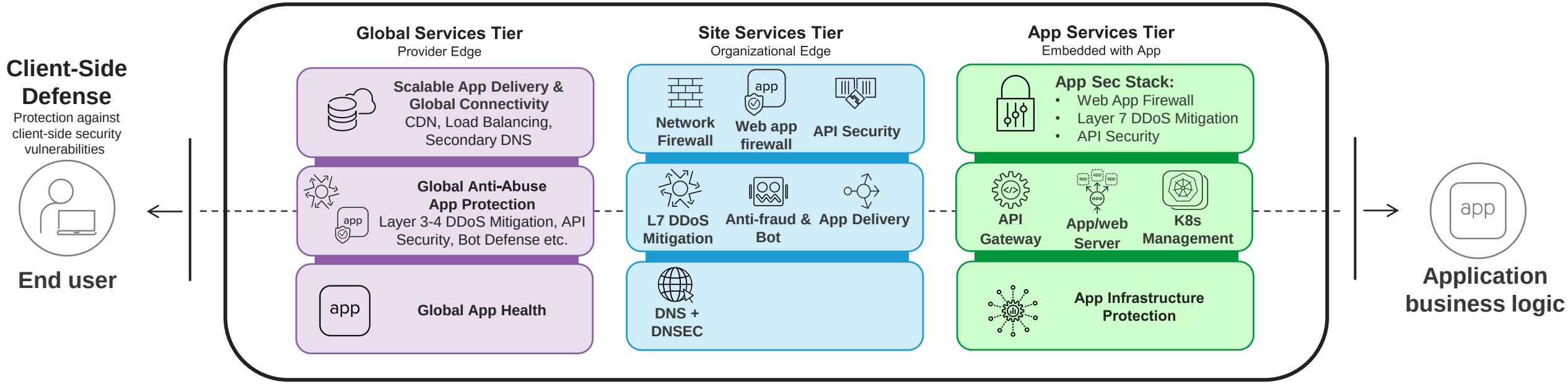
- Scalable App Delivery
- Site Security
- Site Connectivity
- Site App Health

App Service Tier

- Scalable App Delivery
- Instance Security
- Instance Connectivity
- Instance App Health

The F5 portfolio of best-in-class application services

Application security and delivery



ACROSS ANY INFRASTRUCTURE

MULTI-CLOUD

Physical systems | Virtual machines | Containers | Public cloud | Software-as-a-Service | Managed services

Multi-Level Application Security

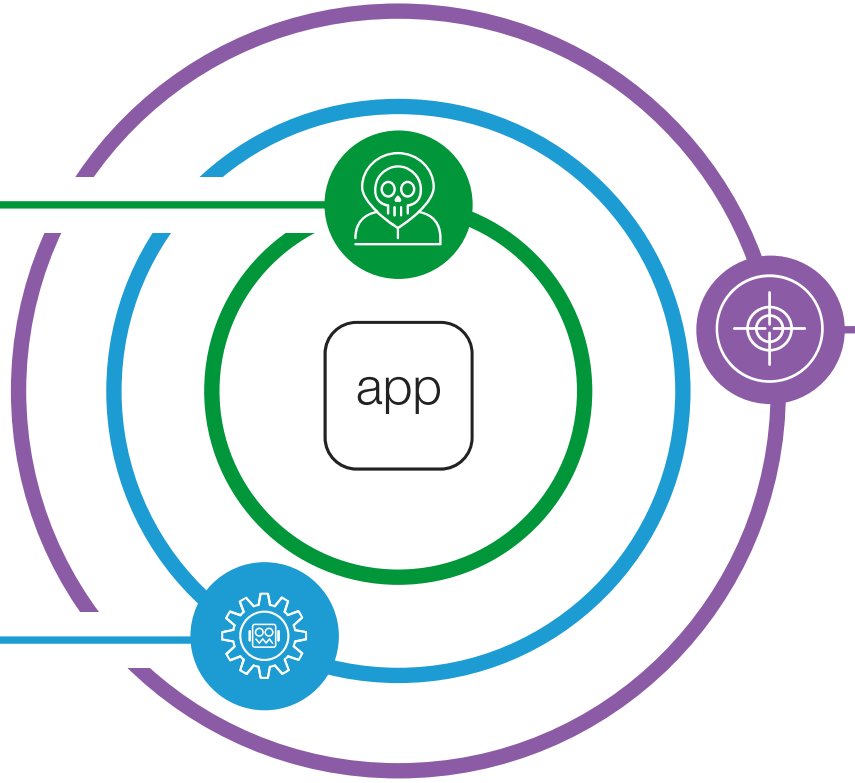
Enforce critical app security policy and implement controls at the appropriate level

App Services Tier

- Closest to the application
- Integrated security controls and policy into automation and CI/CD pipelines (agile with apps)
- Workload specific security policy definitions and enforcement across containers/microservices
- Application and cloud infrastructure security

Site Services Tier

- Localized, site level security policy, definition and enforcement with more specific, granular controls



Global Services Tier

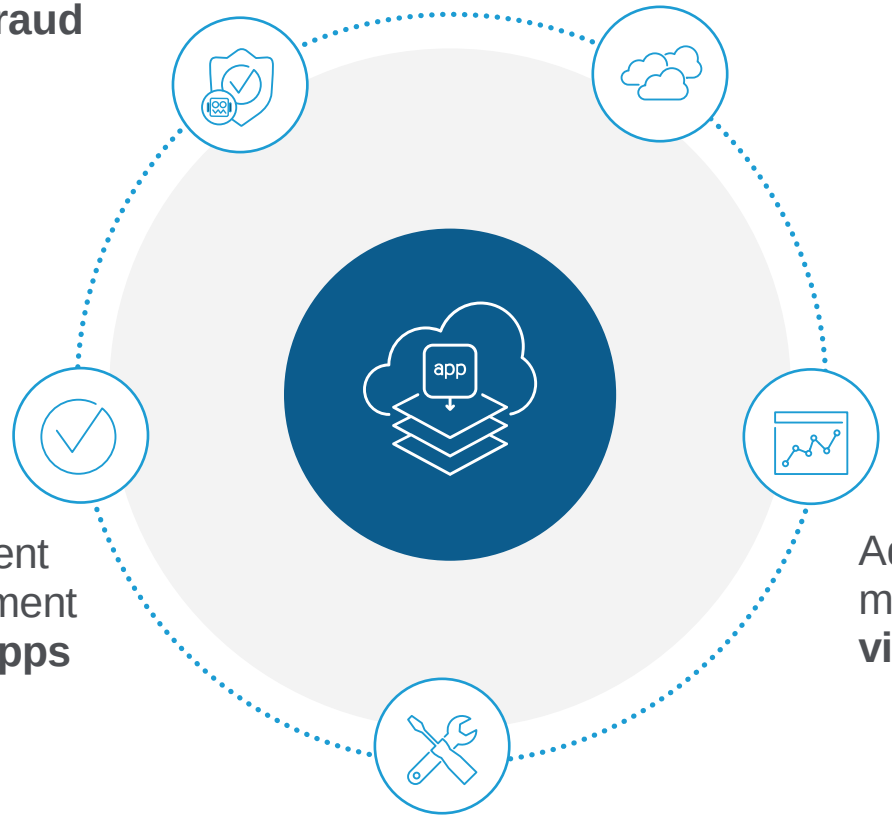
- Keep unwanted traffic off your infrastructure
- Broad spectrum volumetric DDoS volumetric mitigation (layers 3-4)
- Anti-abuse including bot/fraud detection and mitigation at scale
- Standard company app security policy/policies used by all apps

SaaS-delivered Application Security

A differentiated approach to application and API security

More than just WAF, protect apps and APIs against **bots, automation** and **fraud**

Easily scale and **deploy in any cloud**



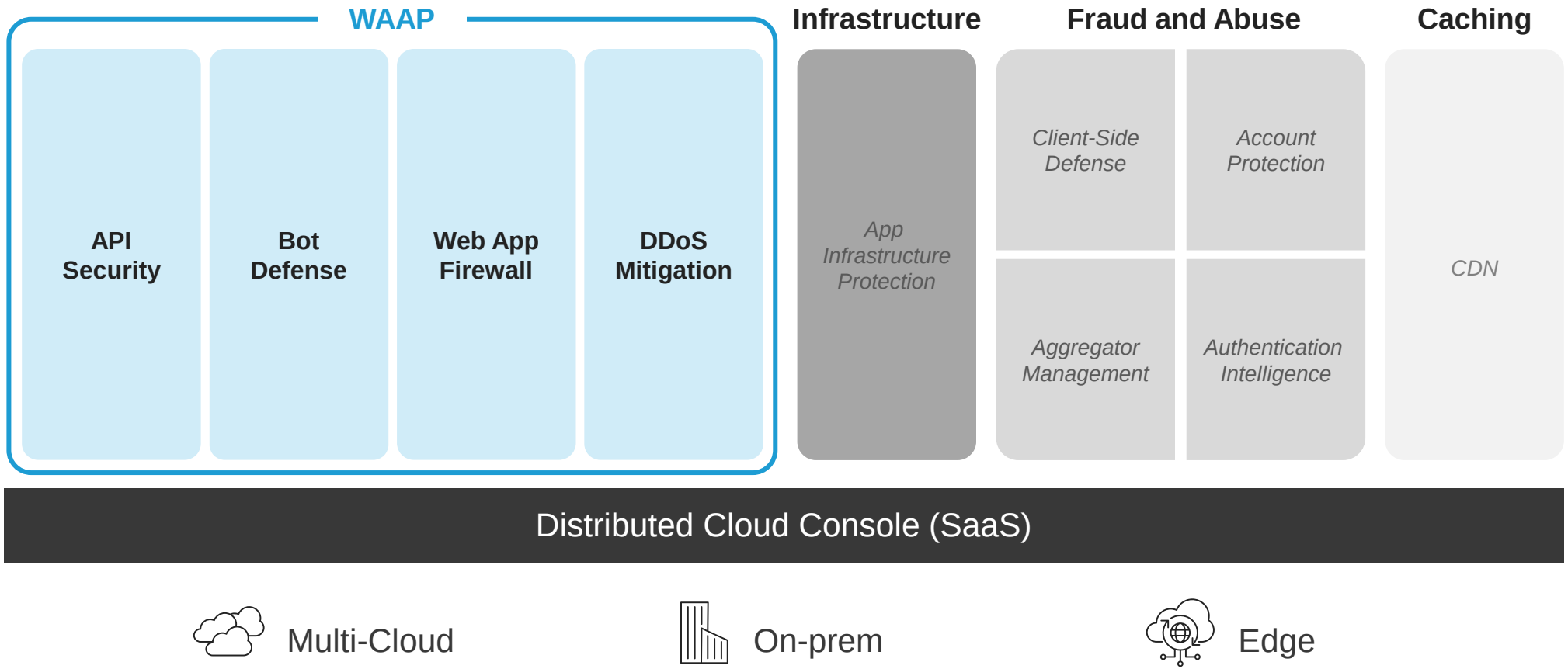
Simplify management and policy enforcement – **deploy secure apps faster**

Advanced monitoring and **visualization**

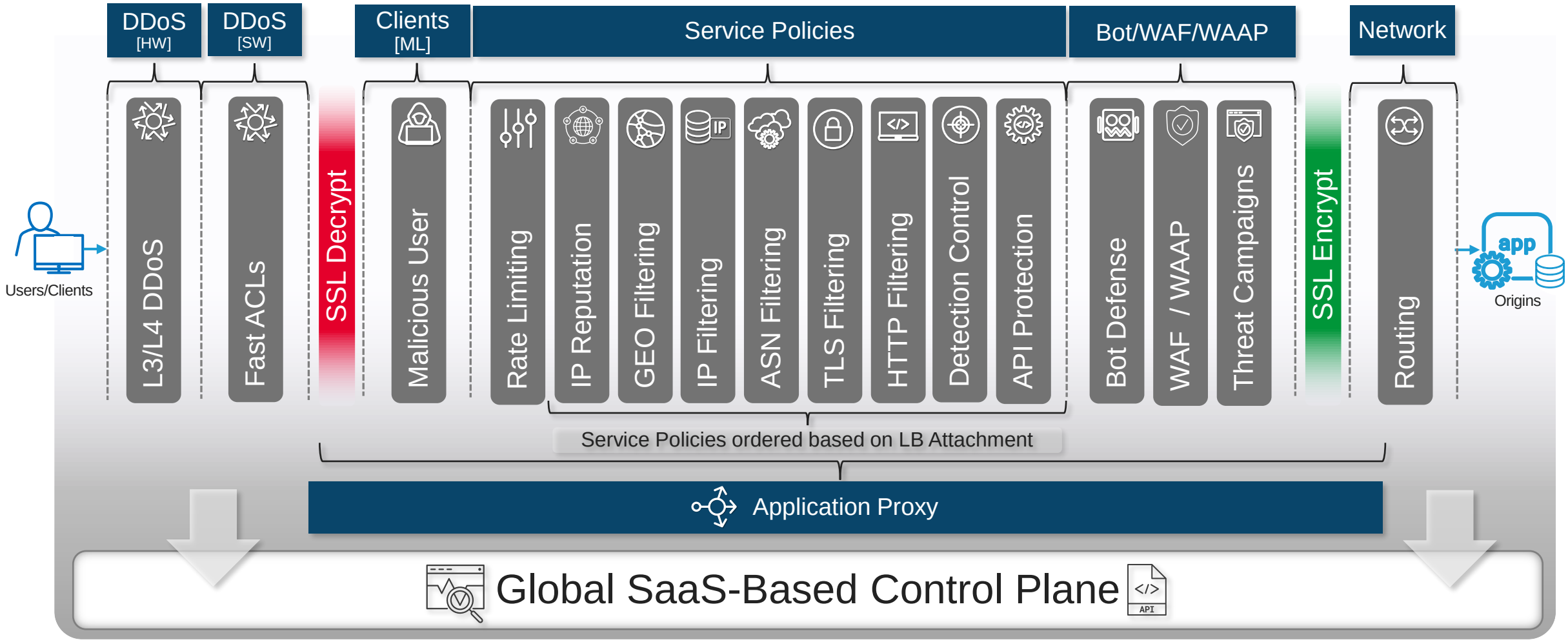
Securely and efficiently **handle increasing request traffic**

F5 App Security-as-a-Service

Multi-layered, highly effective modern app security bringing together the best of F5 application security



It’s much more than just WAAP

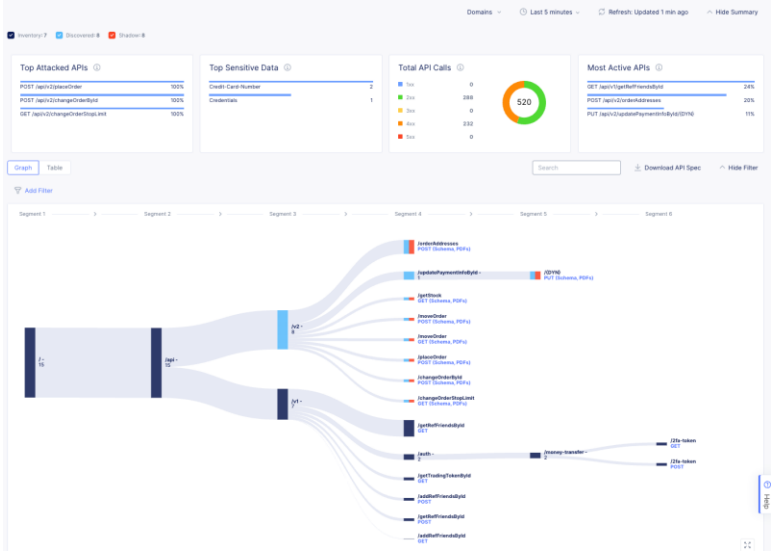


Note: All aspects of flow not represented

API Security

Continuous API discovery, enforcement and observability

API Security	*Bot Defense*	*Web App Firewall*	*DDoS Mitigation*



Discover – detection of API endpoints and request/response schemas, sensitive data, authentication state

Monitor – traffic inspection, analysis, ML-based anomaly detection and risk scoring

Secure – enforcement of schemas, rate limiting, and blocking of undesirable and malicious traffic

Our API Security breaks new ground for operational simplification with automated discovery & policy management

OWASP API Coverage

Broad and expanding coverage for the OWASP API Top 10 vulnerability exploits that updates automatically as new exploits are identified.

Importing Swagger and OpenAPI Spec Enforcement

Allows for positive security, enabling users to allowlist endpoints based on valid schema characteristics such as parameters, methods, authentication types and payloads, tightening security against abuse.

Response Analysis

The WAAP will analyze how the server responds to queries, identifying persistent outliers that receive bad response codes, but persist in sending bad requests.

Risk Scoring and Insights

API endpoints are tagged with a comprehensive risk score and operators can track the activity history and vulnerabilities of all endpoints.

Automated Discovery and Inventory

APIs change frequently. As APIs are used, the system determines normal behavior, usage, methods, sensitive data and detects outliers helping you detect shadow APIs, shadow parameters and Zombie APIs.

Monitoring and Anomaly Detection

Analyzes what endpoints are used, in what order and the frequency, identifying bad actors not obeying normal behavior.

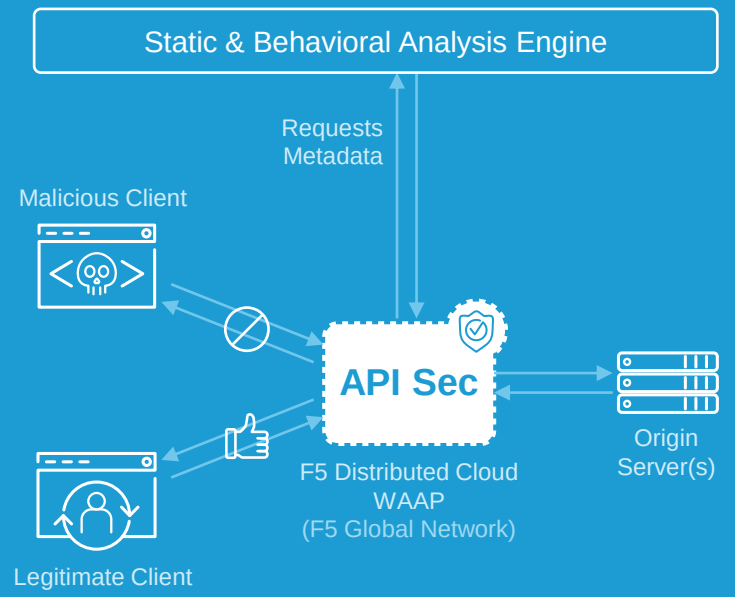
Visualize API Usage

Identify usage patterns for APIs and show the most used and attacked APIs, plus correlate good and bad actor activity to optimize APIs for a better client experience.

Determine the Response

Allow, rate limit or **deny** a client using the API based on the threat level that it poses. Delivered via in-depth forensics on suspicious and malicious traffic.

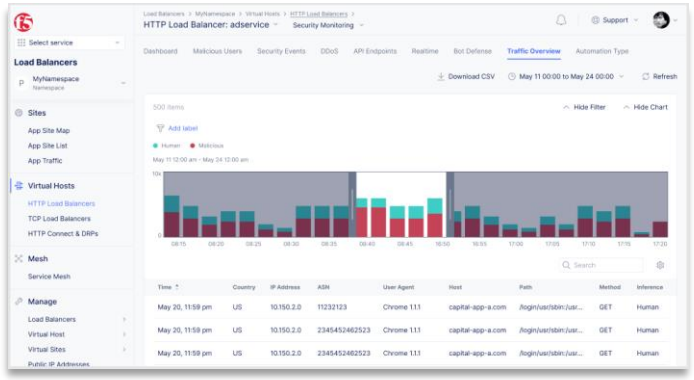
Automated API Protection



F5 Distributed Cloud Bot Defense

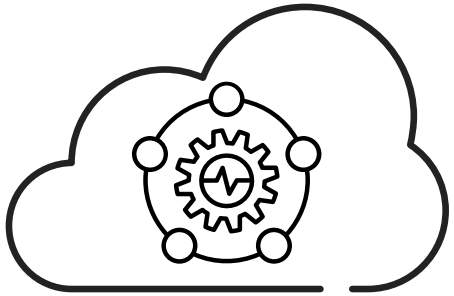
Enhanced AI/ML driven bot detection and mitigation

API Security	**Bot Defense**	*Web App Firewall*	*DDoS Mitigation*



Mitigate malicious automation that impairs the user experience, imposes high financial costs, and impacts the user experience:

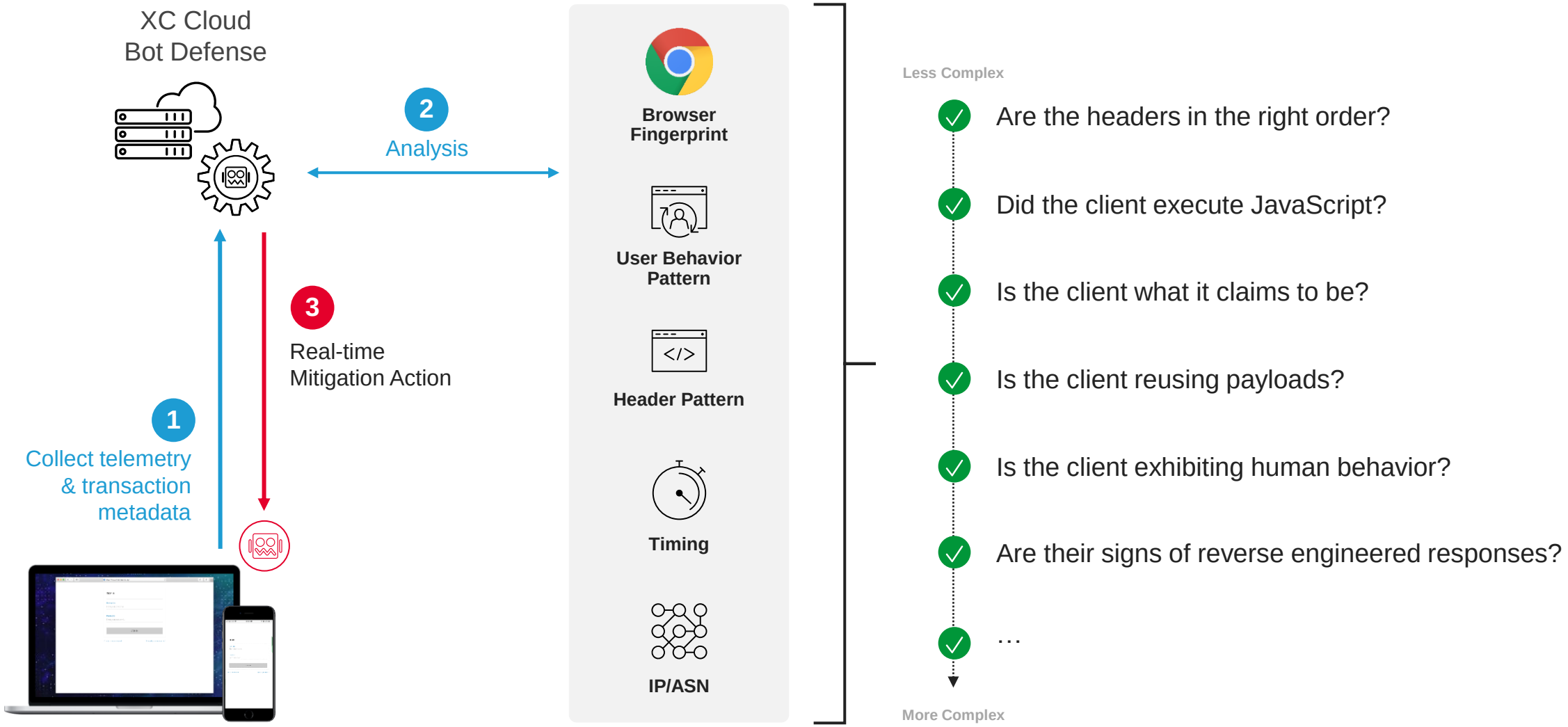
- Credential stuffing bots lead to account takeover
- Loyalty point bots steal value from customers
- Carding bots that validate stolen credit card data result in charge backs and fees
- Scraping bots slow performance, increase infrastructure costs, and can bring down sites
- Scalping bots that take advantage of limited time offers frustrate loyal customers
- Inventory hoarding bots prevent customers from buying goods and services available in inventory



Bot Defense mitigates malicious automation to prevent sophisticated, human-emulating attacks–bringing together unified telemetry, network intelligence, and AI/ML with human analysis to identify and defend against automated threats.

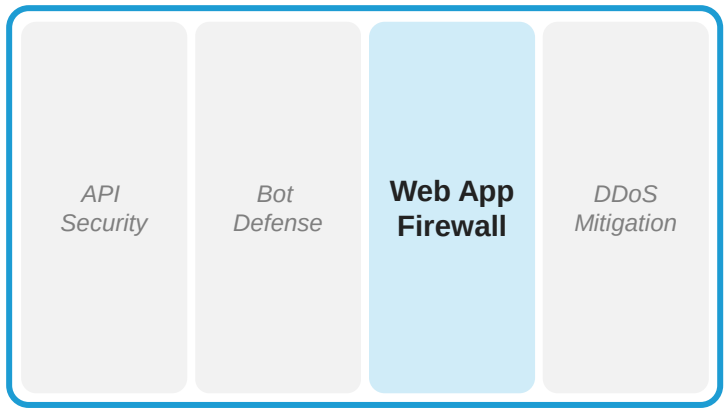
Standard Bot Defense

Highly effective real-time detection informs mitigation actions



F5 Distributed Cloud WAF - Identifying new threat actors

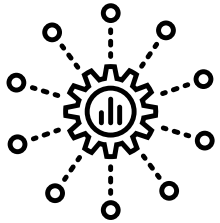
Moving beyond signature-based detection



Signature based identification

Identifies a bad request based on a match to one or more signatures in a database

- Protection against known attack signatures
- Live signature feed so you're always up to date with the changing threat landscape
- Threat campaigns that help you reduce false positives based on actor intent
- Evasion detection support finds potentially malicious requests that signatures alone don't find



Behavior based to identify threat actors and false positives

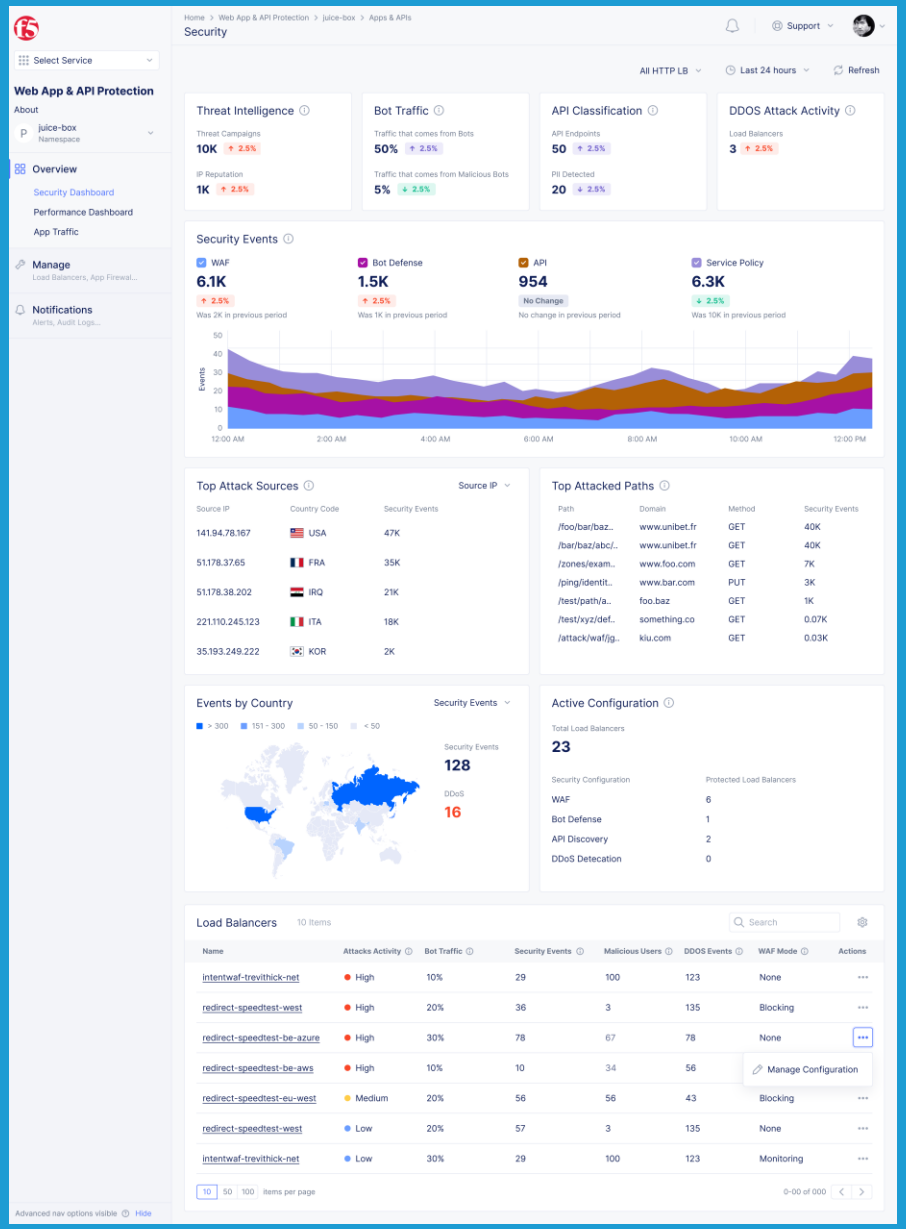
Identifies a client and follows their behavior

- Identifies anomalous user behavior and blocks malicious attacks
- Recognizes non-human, automated requests that can potentially be harmful
- Reduces the time spent resolving false positives

A Next Gen WAF

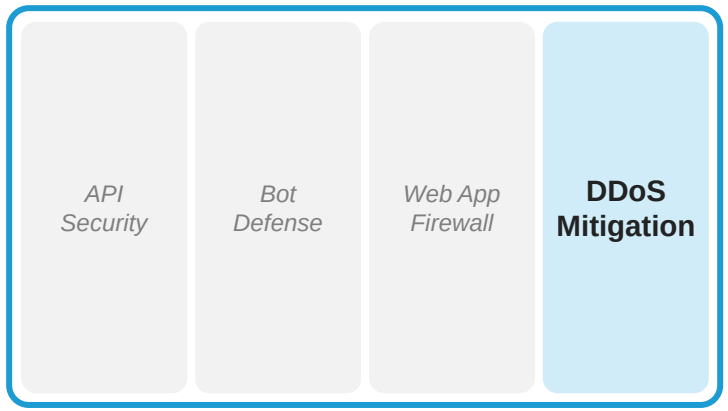
Streamlined set up and management with self-service or managed service options

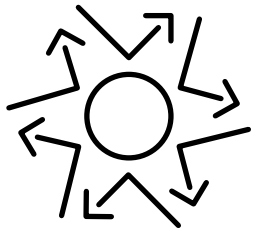
- **Robust Signature Engine including Threat Campaigns**
- **IP Reputation Service**
- **Advanced Behavior Engine**
- **Powerful Service Policy engine**
- **Automatic Attack Signature Tuning**



Better visibility for security events and traffic with drilldown

F5 Distributed Cloud DDoS Mitigation





L3-L7 DDoS mitigation

Ensure the availability of critical application and network resources.

- Block the malicious traffic while allowing the good, ensuring good user experience for applications and services
- Identify and mitigate sophisticated Layer 7 DoS attacks that exploit application & infrastructure weaknesses
- Block attacks closer to where they originate with a global backbone and distributed DoS mitigation technology
- Protect customer networks and services with Always On or Always Available routed and proxy DDoS Mitigation service

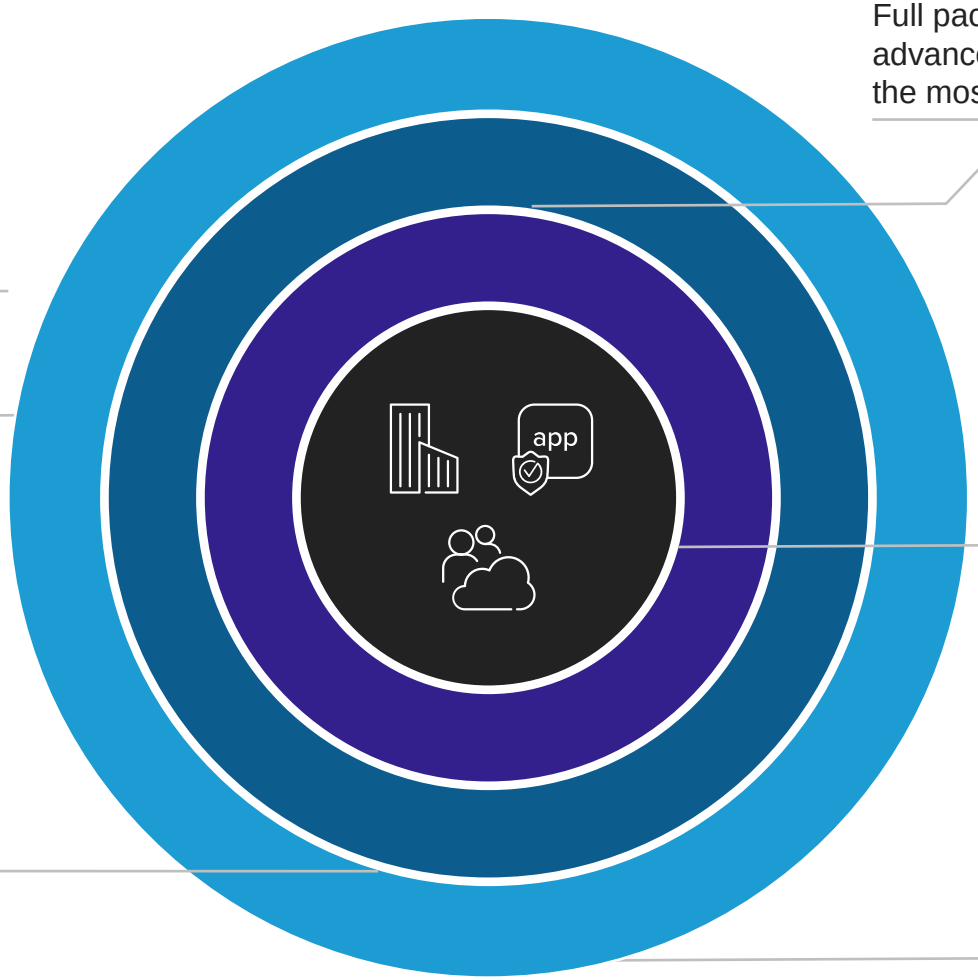
F5 Distributed Cloud DDoS Mitigation - Layers of Protection

Advanced Mitigation

Full packet analysis, custom filtering and advanced counter measures (scrubbing) for the most advanced attacks

CoreProtect

Pre-set rules that mitigate known-bad/known-useless traffic types that are always filtered immediately for all customer



Layer 7 and Proxy DDoS Protection

Protects apps and services from protocol attacks, L7 DoS and encrypted threats

Custom Mitigations

SOC analysis of traffic and implementation of any additional rules necessary to improve efficacy or reduce false positives of attack mitigation

Auto-Mitigation

Machine learning profiles traffic and automatically creates and deploys counter-measures for volumetric DDoS attacks

Key Differentiators

Efficacy + agility

Top-tier security controls provide higher efficacy, while SaaS model + unified management increase agility

Deploy anywhere

Operate on F5 Global Network, public / private clouds or edge sites – wherever apps are located

Common platform

WAAP combined with multi-cloud networking, edge computing and a global network in a single offering

Thank you!

