Vertrauen ist gut, Kontrolle ist besser

Warum *Good enough* WAAP Lösungen nicht ausreichend sind

Frank Thias

Principal Solutions Engineer, Financial Services

23rd September 2022

Agenda

Drivers for WAF and Use-Cases

Good enough WAFs vs. Enterprise Grade WAFs

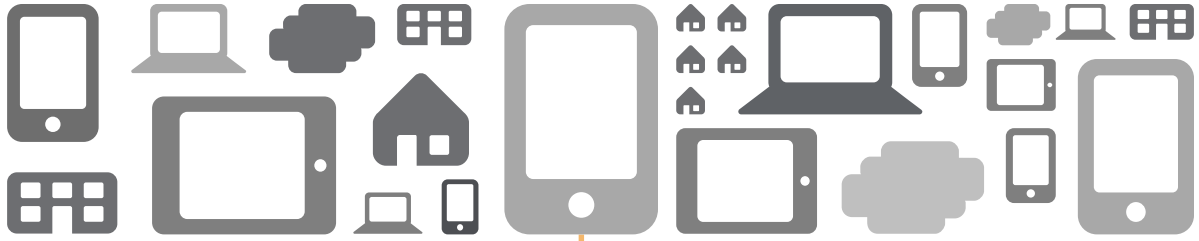
Deployment Options and Management

WAAP

Conclusion

Drivers for WAF and Use-Cases

The 21th Century Application Infrastructure



Users are going to access application

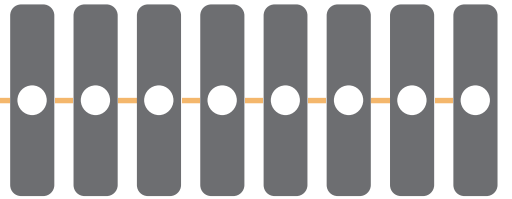
Mobile/VDI/XaaS/OS

Security

Network, Application, DDoS

Every application is a

Web Application



Application Attacks are Real & Direct Threats to Business

“TECHNICAL THREATS”

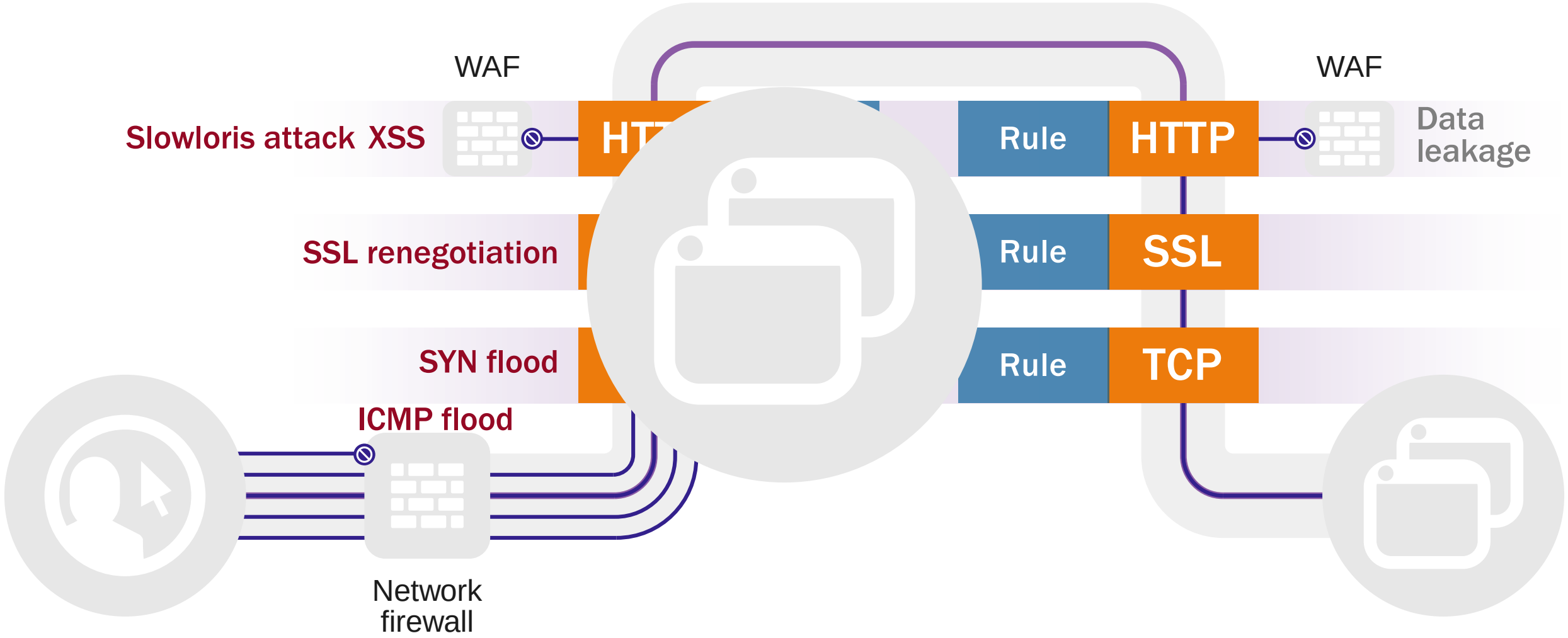
- OWASP Top 10: Cross-Site Scripting, SQL Injection etc.
- OWASP Automated Threat
- Exploitation of known & unknown web applications vulnerabilities

“BUSINESS THREATS”

- Credential Attack, Phishing, Fraud
- Web Scraping
- L7 DDoS

Sensitive Data Leakage, Outages → **Loss of Revenue – Against Competition**

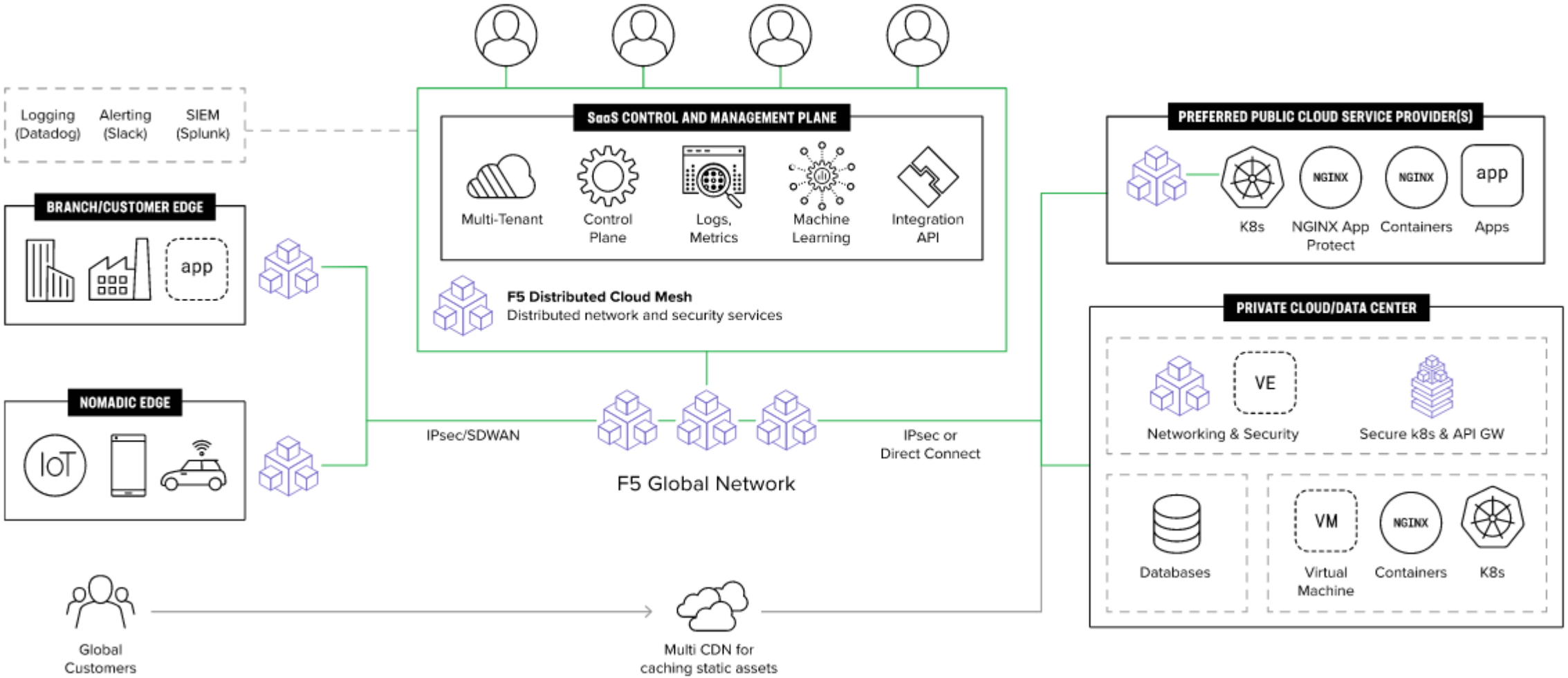
What is a WAF?



Real life customer use-cases

- OWASP Top 10 Protection
- Bot Prevention
- Layer 7 DDoS Mitigation
- API Security
- Very often in combination with:
  - Traffic Management
  - Scalable and secure TLS/HSM
  - Authentication Proxy – Federation, Formbased, Client-Cert
- Trend: WAF also internally used with our customers

Welcome to the century of Multi-Cloud networking



Good enough WAFs vs.

Enterprise Grade WAFs

Comparison Cloud Vendor WAFs vs. Enterprise Grade WAFs

Cloud native WAF

Advantages:

- Good integration in automation Frameworks – but for only one specific environment

Enterprise WAF

Advantages:

- Good integration in automation Frameworks for any environment:
  - ➢Customer Edge - On-Premises
  - ➢Regional Edge – These are F5 distributed POPs
  - ➢Public Cloud - In the Hyperscaler
- Centralized Management and Reporting for all deployments
- Strong security posture because this is the main business of enterprise cloud vendors

Deployment options and Management

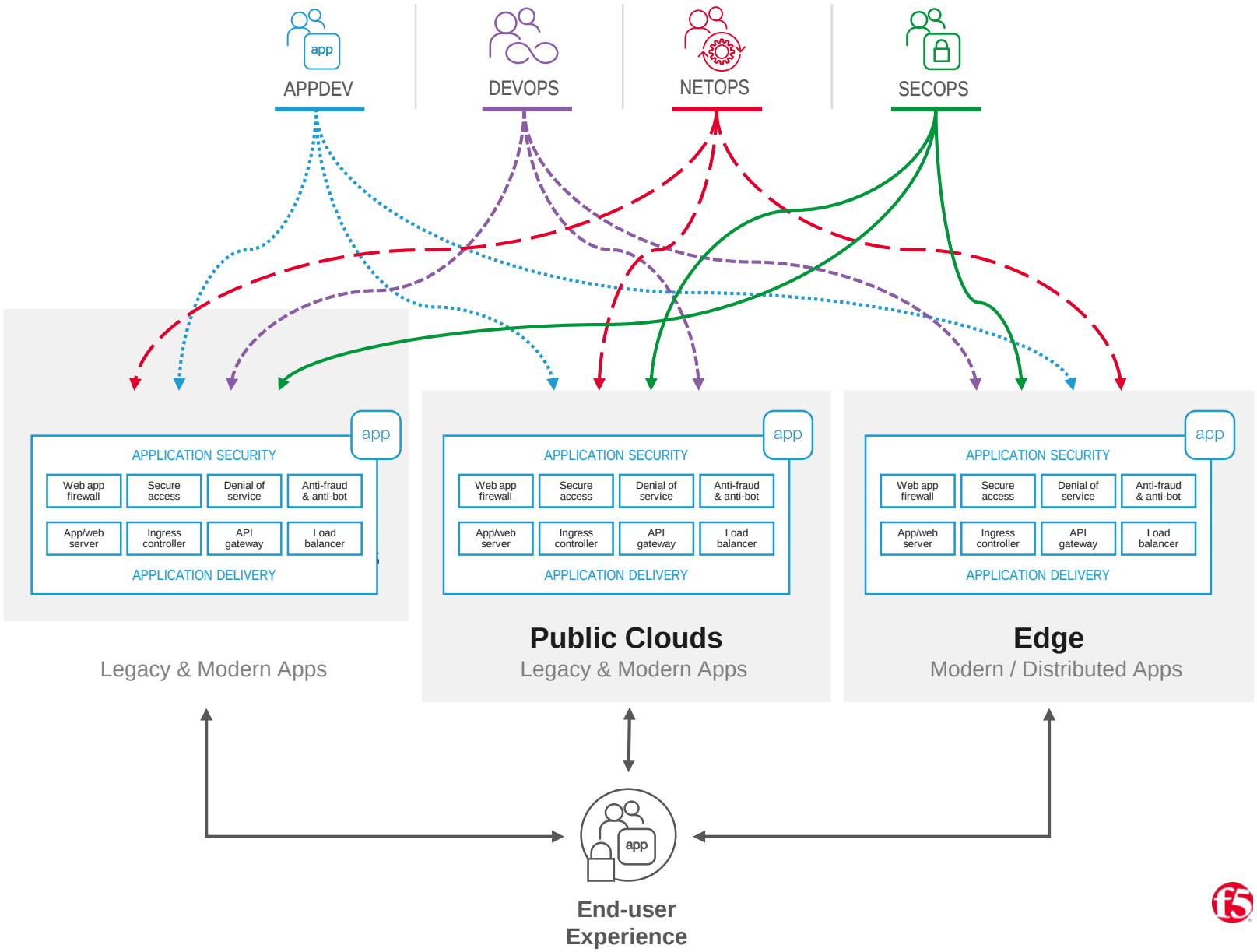
App Services without Mesh and centralized management

#1 Complex coordination because of technology inconsistencies between teams and across environments

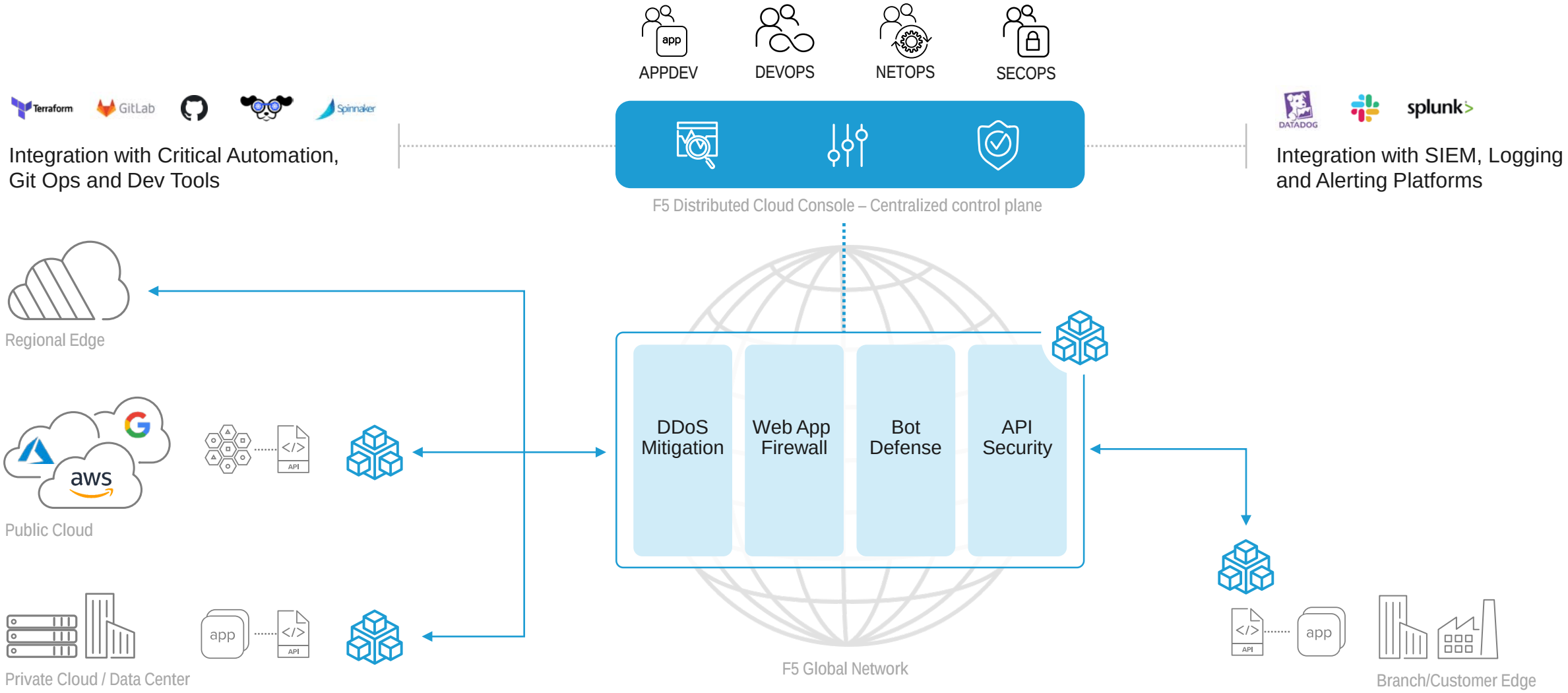
#2 Automation challenge ”stitching” multiple environments, layering net, security, and apps, at scale

#3 Security difficulties due to multiple different attack surfaces and sophistication of bad actors

#4 Limited observability of silo’d telemetry trapped in disjointed systems & environments



Centralized control and flexible deployments



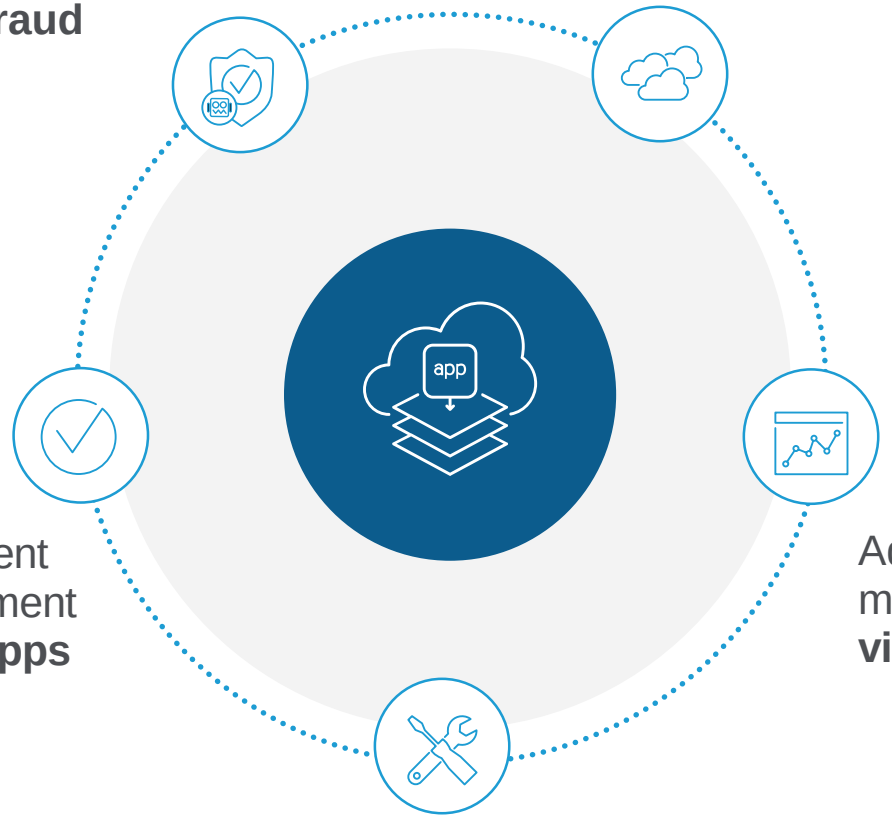
F5 Distributed Cloud Web App and API Protection (WAAP)

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**



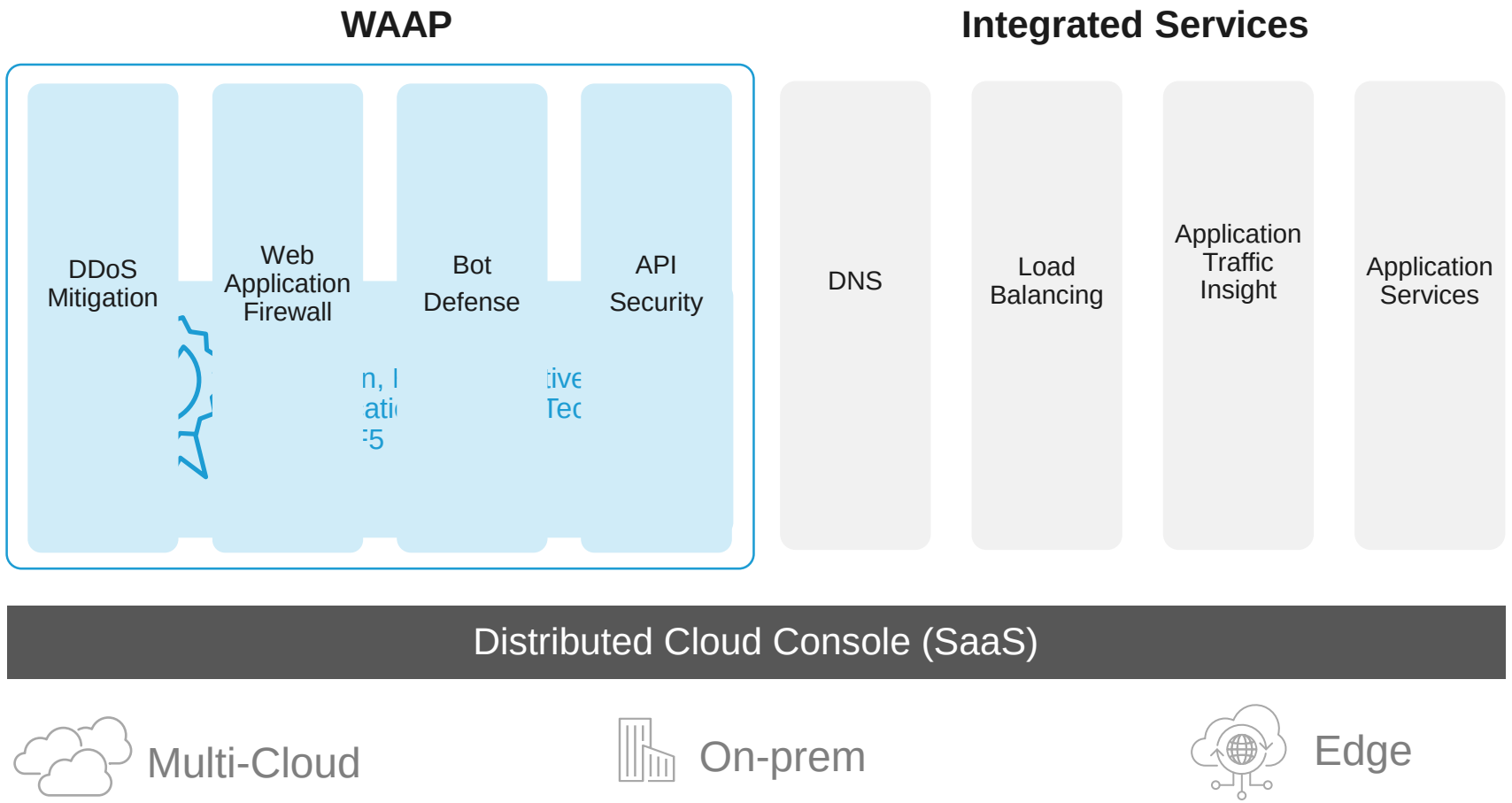
Simplify management and policy enforcement – **deploy secure apps faster**

Advanced monitoring and **visualization**

Securely and efficiently **handle increasing request traffic**

WAAP-as-a-Service

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



Mitigate Large, Sophisticated DoS Attacks

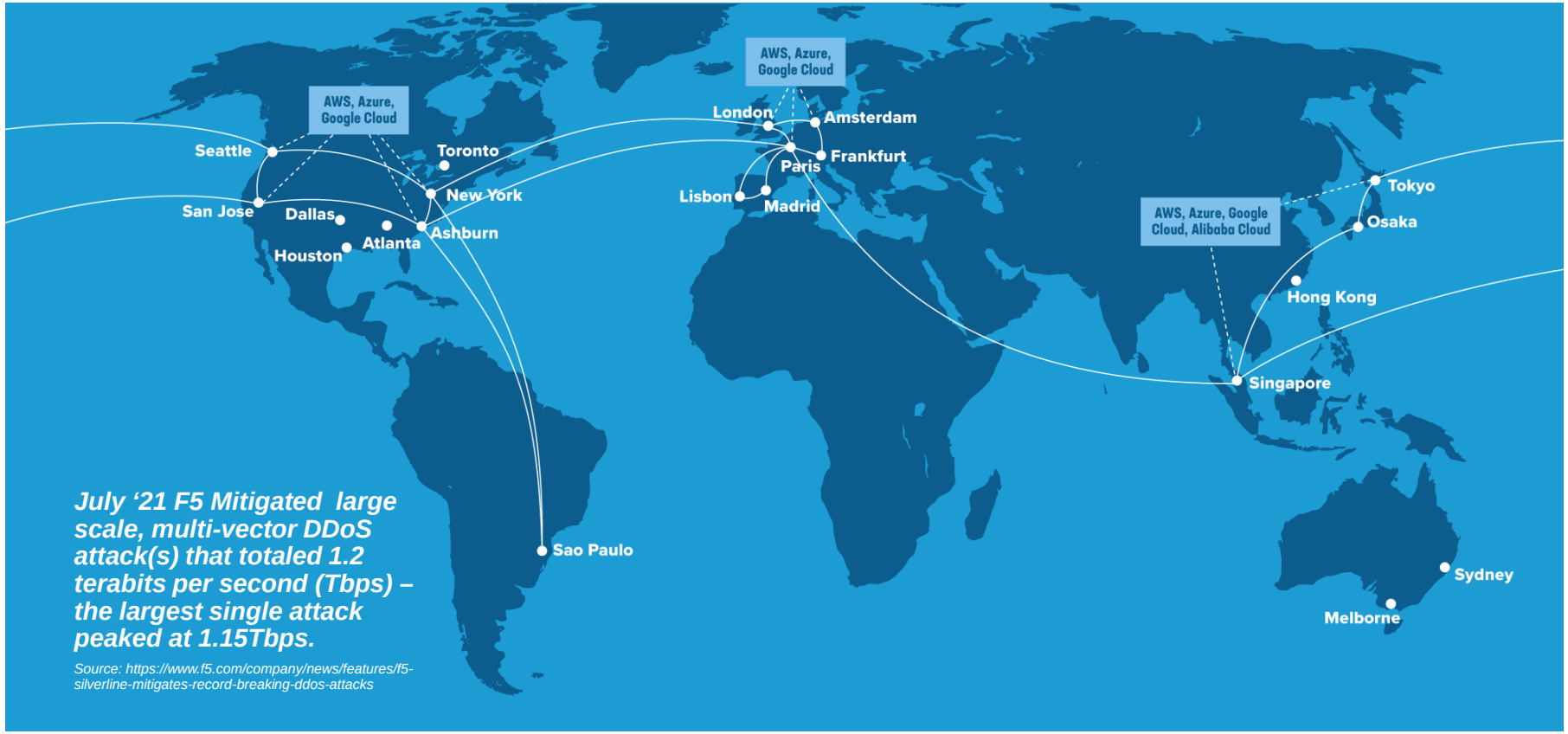
Mitigate closer to the origin away from critical apps and infrastructure

World Class Global Security Operations Center responds to DDoS attacks in < 2 minutes on average.*

Global DDoS Protection Network with 12+ Tb of scrubbing capacity**.**

Flexible Service Options including Always Available or Always On deployments

Connect how and where you need with BGP-based traffic redirection and direct connections, peering or GRE tunnels.

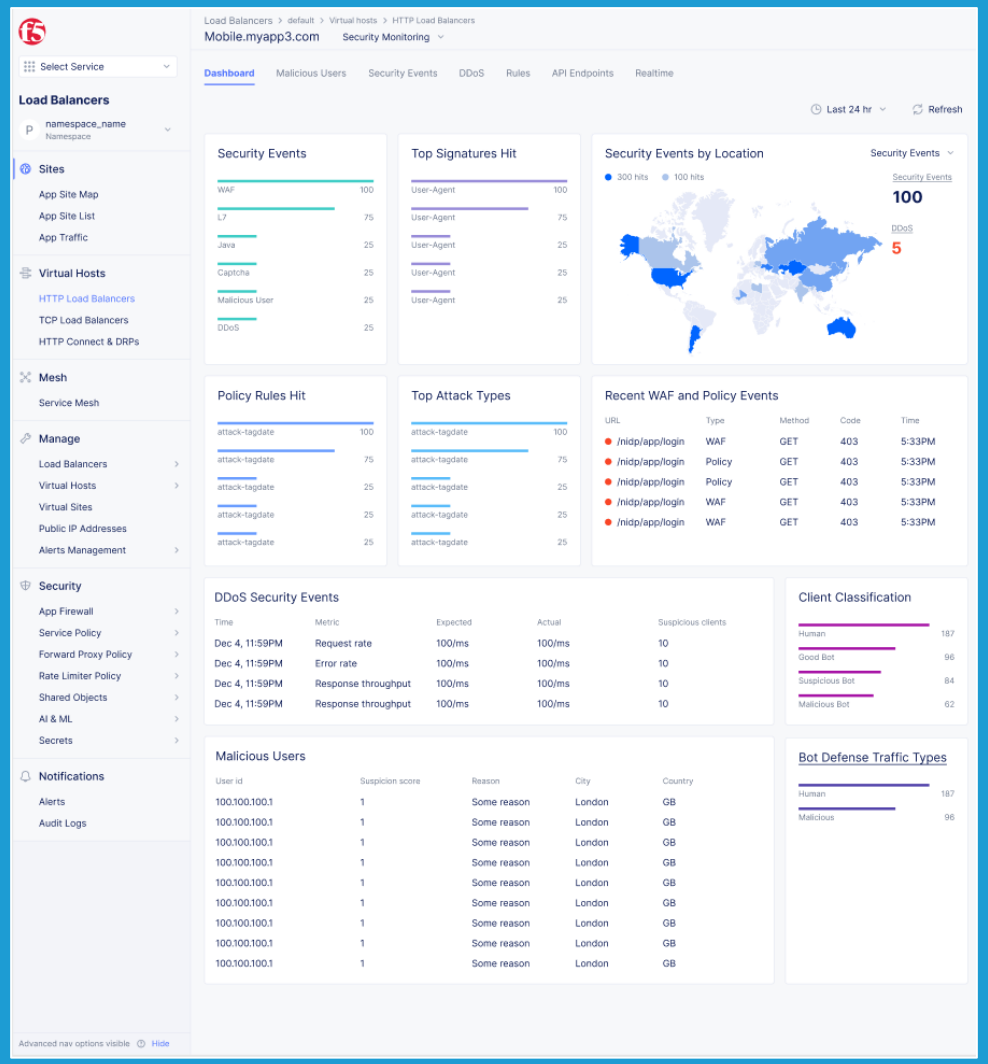


Note: Network PoPs without network lines are planned.
Standard DDoS Service offering MSA specifies a 15 Minute Response SLA.

A Next Gen WAF

High efficacy, low false positives

- **Streamlined set up and management**
- **Robust Signature Engine**
- **Advanced Behavior Engine**
- **Powerful Service Policy engine**
- **Automatic Attack Signature Tuning**



Better visibility for security events and traffic with drilldown

Bot support for **full-site protection** with option of **expanded bot defense security** for specific URLs

User Behavioral Analysis
Utilizes the Machine Learning / AI Engine to identify malicious clients.

+

Signature Based Bot Detection
Identifies bots by matching signatures or anomalous behavior

Good

- Both are **included** with the base WAF Service
- Protects both web content and APIs

+

Bot Defense

- Integrated **premium** option
- Designed to **protect highly sensitive parts** of a site or API, such as a login page
- Richer set of specific threat detections that identifies intent such as scraping, account takeover and carding
- A curated active database of known specific threats

Best

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

OWASP API Coverage

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

Automated Discovery

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

Importing Swagger

Integrate with your CI/CD pipeline when an API changes. The WAAP will know exactly what endpoints, methods and payloads are valid, tightening security against abuse.

Determine the Response

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

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.

Behavior and Time

By analyzing what endpoints are used, in what order and the frequency, API Protection can identify bad actors not obeying normal behavior and act.

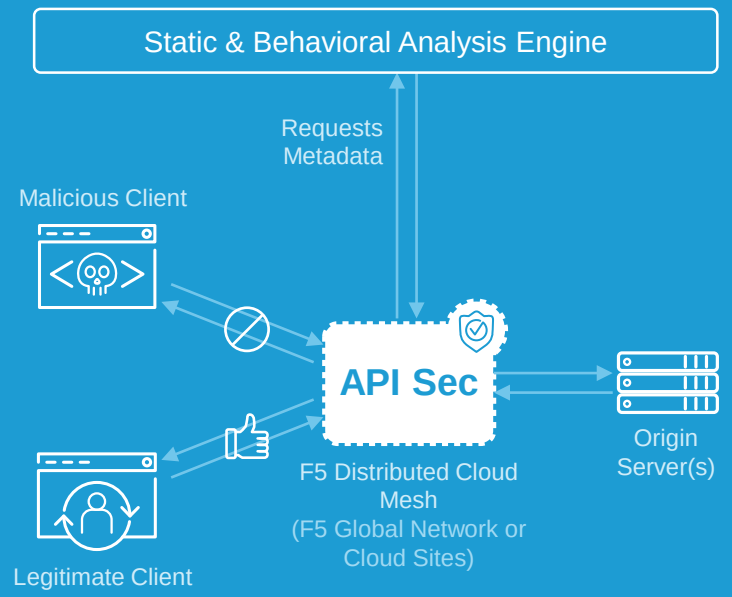
Forensics

Once a bad actor is identified, track their history of what they have been trying to exploit and take action.

Visualize API Usage

Identify usage patterns for APIs, correlate good and bad actor activity to optimize APIs for a better client experience.

Automated API Protection



Conclusion

- App Security is a basic need for applications
- It‘s a wide umbrella of security functions:
  OWASP Top 10, Bots, Layer 4/7 DDoS etc.
- Centralized Management is a requirement:
  This includes automation, logging and reporting
- Meshing components reduce the complexity on Layer 3
- F5 Technology can be used for all above