
Nomios Security Cup
7-8 maja 2026
Hotel Mazurski Raj
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ectacom
EXCLUSIVE NETWORKS
CLICO

Applications Under Attack: API, Boty, oraz nowa wojna o aplikacje

Paweł Skowroński
Security Engineer @ Nomios

Michał Zbroziński
Solutions Engineer @ F5

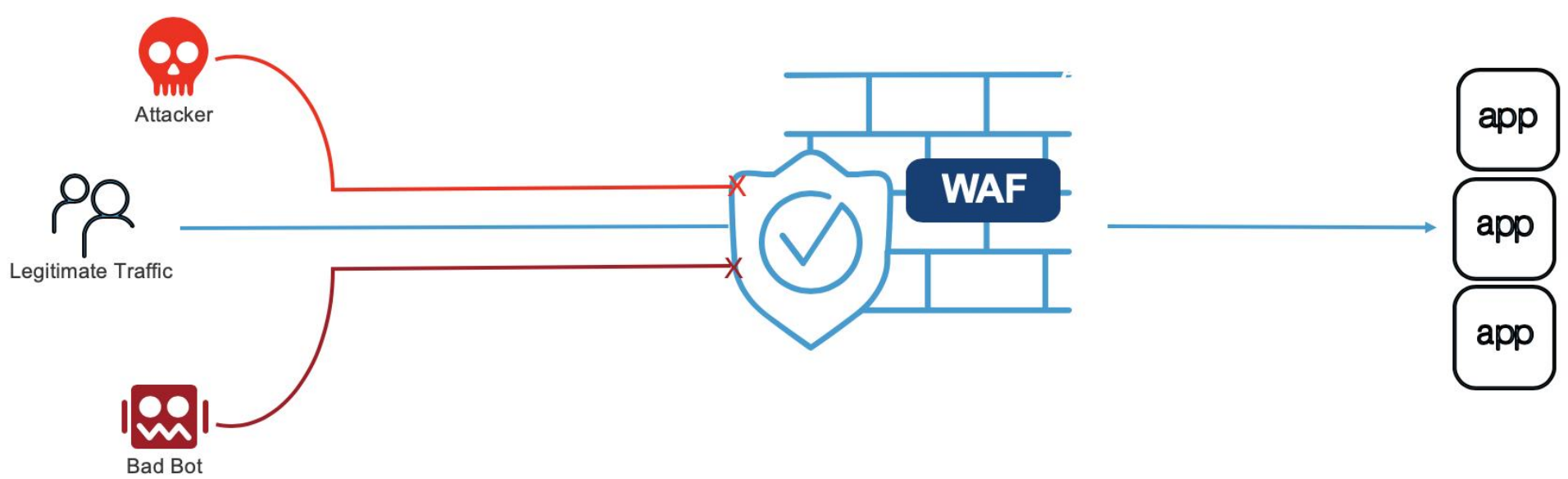
Mikołaj Borecki
Security Expert @ Nomios

CROWDSTRIKE | ExtraHop | FORTINET | F5 | HPE JUNIPER networking | infoblox | Trellix

nomios | ARROW | ectacom | EXCLUSIVE NETWORKS | CLICO

What is a WAF?

Web Application Firewall – comprehensive security solution

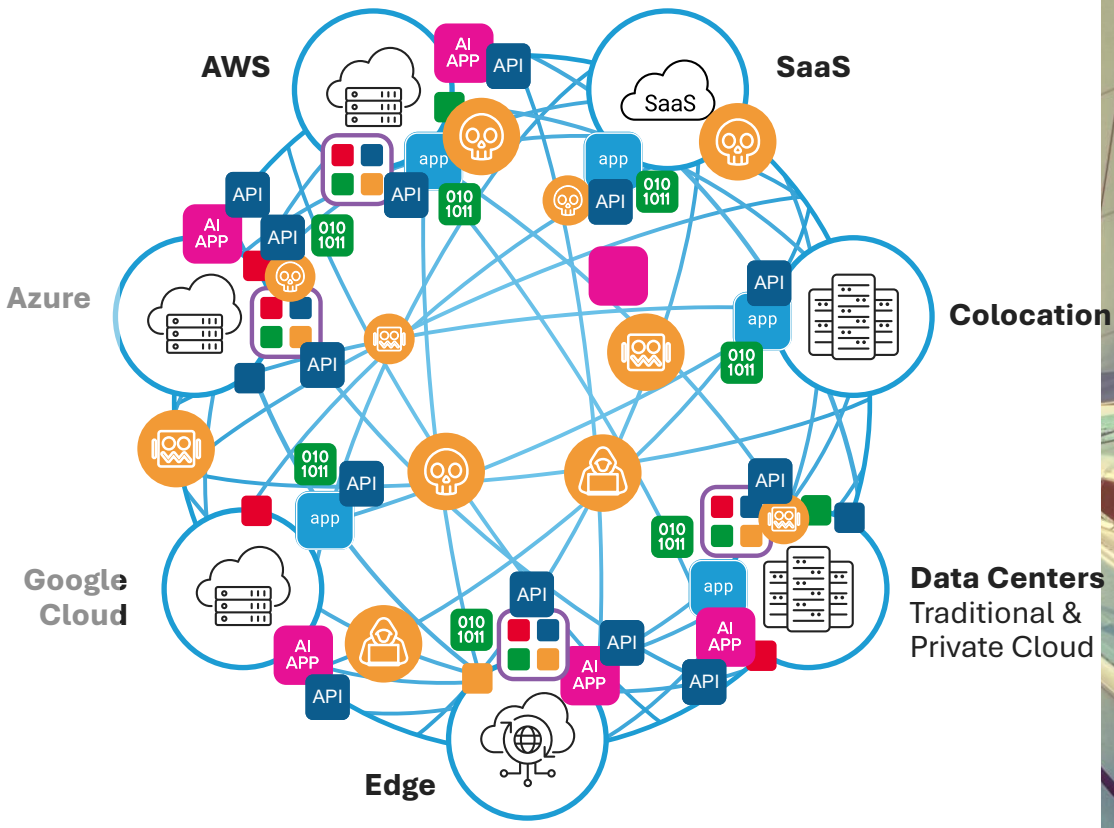


designed to protect:
- Web Applications
- APIs
from layer 7 attacks, including the OWASP Top 10 risks.

API Discovery and Security in Modern Enterprise

API Discovery is key for visibility and insights and is the foundation of security

- **Hybrid Environments**
  (on-premises, private cloud, public cloud)
- **Diverse Tools**
  (API GWs, Load Balancers, WAFs, Service Meshes, Ingress Controllers)
- **Multiple Owners**
  (AppDev and DevOps, Platform teams, API GW owners, SecOps)



CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix

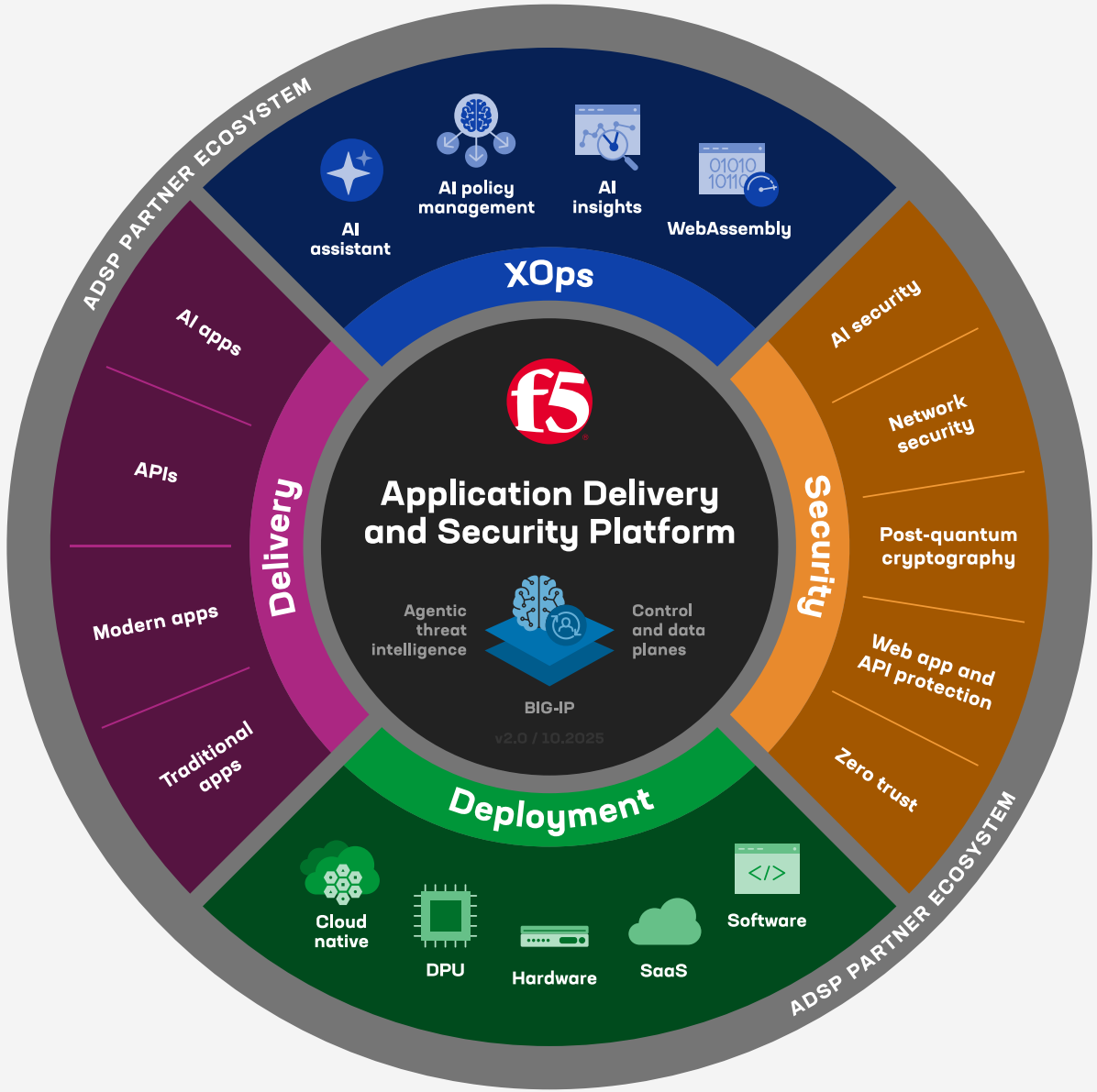
nomios | ARROW | ectacom | EXCLUSIVE NETWORKS | CLICO

Deliver and secure every application, every API – and now every model, agent, and connected data set – with F5 ADSP

Uniform AI policy management across **all environments**

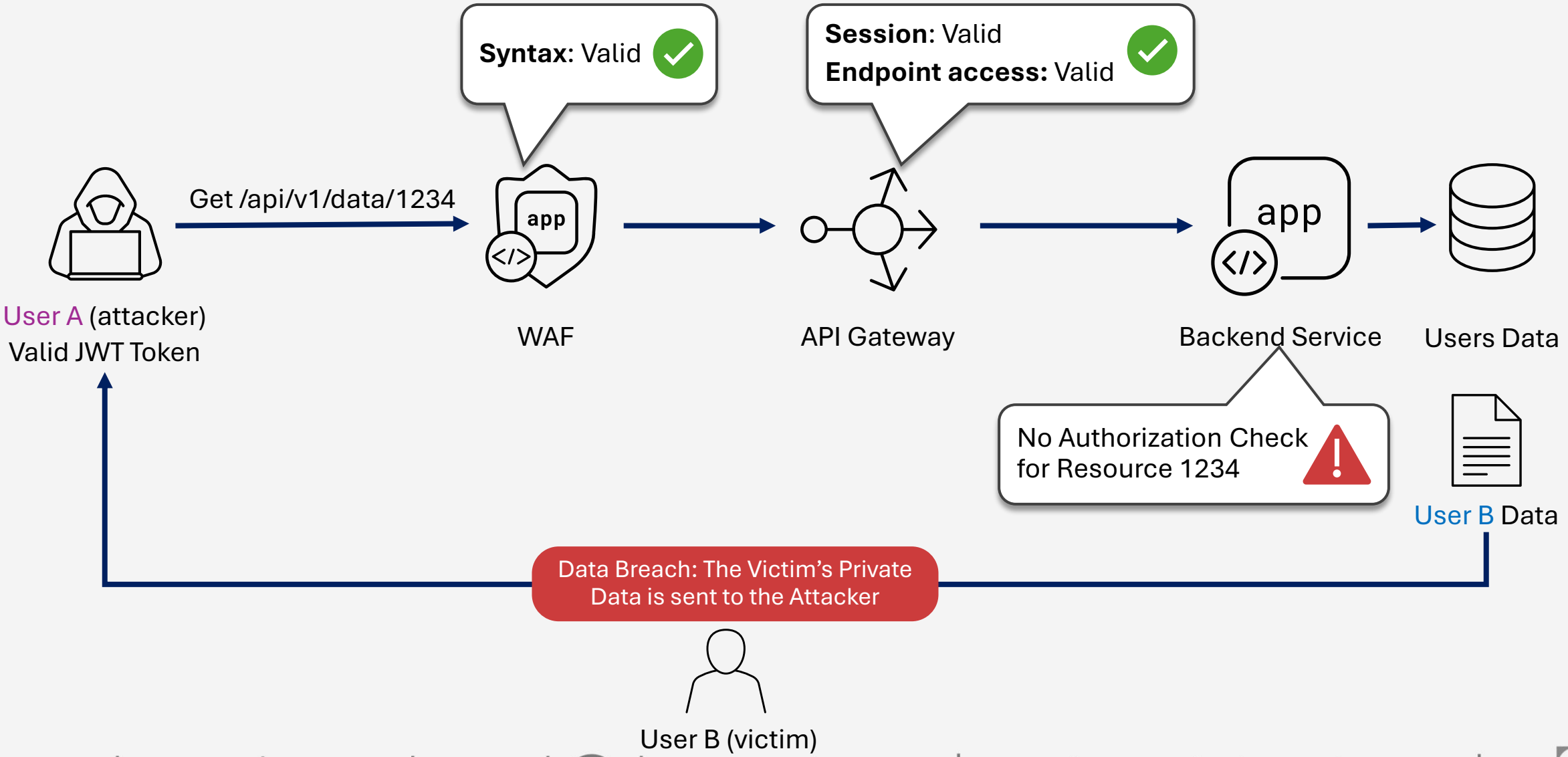
Discover and secure every API with **F5 Distributed Cloud Web App and API Security**

Mitigate shadow AI with **BIG-IP SSL Orchestrator**



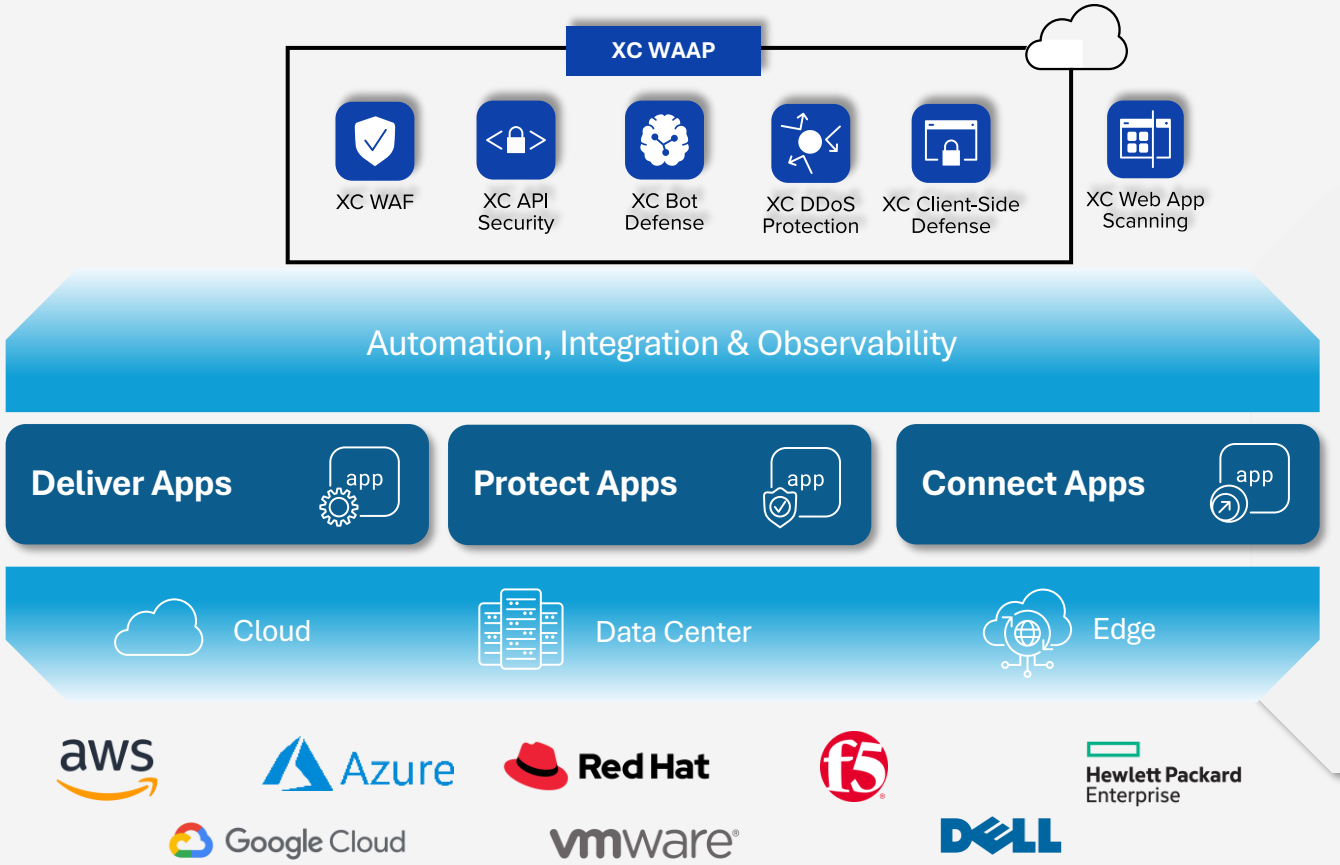
nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

API GW & WAF Cannot Protect Against Logic Abuse



Secure, Deliver, and Optimize Every App and API Anywhere

Why app security (WAAP) should not be decoupled from app delivery and app connectivity



APP SERVICES

Deliver, Protect, Connect

LOCATIONS & ENVIRONMENTS

Data Center, Cloud, Edge

CONSUMPTION MODELS

Hardware, Software, SaaS

From dauntingly complex to ridiculously easy

nomios | CROWDSTRIKE | ExtraHop | FORTINET | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

What value does WAAP deliver across DevOps, SecOps & NetOps teams?

Simpler, more agile operations via easy-to-use SaaS services

End-to-end visibility and policy enforcement

More effective for **modern, distributed apps and multi-cloud**

Lower TCO with SaaS model, **multiple services, unified mgmt**

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox. | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

Distributed Cloud WAF core capabilities

Robust attack signature

Captures Common Vulnerabilities and Exposures (CVEs) plus known vulnerabilities and techniques identified by F5 Labs, including *Layer 7 DDoS*, *bots*, automated threats, and OWASP Top 10

Advanced behavior engine

Leverages AI/ML to monitor and score client interactions, deciphering intent based on the number of WAF rules hit, forbidden access attempts, login failures, error rates, Malicious User Detection, and more to help identify an app's highest-priority threats.

Powerful custom rules engine

Enables micro-segmentation and advanced security at the application layer, utilizing IP reputation and allow/deny lists to block clients with known bad TLS fingerprints, ASNs from suspicious countries, and more.

Automatic attack signature tuning

Easily determines if a signature-identified attack is really a threat, helping reduce the number of false positives.

AI assistant

Simplify delivery and security of distributed apps and APIs using a natural language interface with real-time insights, actionable recommendations, and summary of data reports.

Threat intelligence

Dedicated team to research new threats and characterize them to incorporate this feed into Distributed Cloud WAF (ex. Threat Campaigns, Threat mesh)

Streamlined set-up and management

Deploy through a simple UI or automate via APIs including best-practice default protections and the flexibility to create custom rules.

Bot protection

Bot protection provides basic bot protection by detecting bot signatures in the user-agent header and URL.

API security

API Discovery through traffic, and starter API protection

Global Network

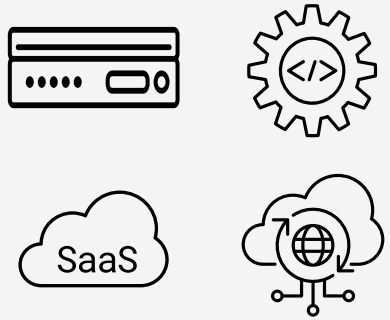
Clients connect to the nearest F5 Global Network RE; traffic is targeted to be a determined load balancer configuration, and security services are applied.

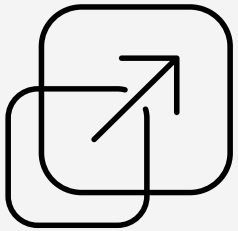
Load balancing

Unlimited number of endpoints (i.e., origin servers). Unlimited number of endpoint locations for health checks. The granularity of health checks for endpoints is one second. This includes one load balancer

F5 delivers the *most comprehensive and flexible market leading* WAF solution delivered wherever customers' apps live.

Available in different deployment models and form factors to meet any app and API security requirement





Available in multiple delivery models

Appliance, software, SaaS, and edge

Supports most deployment types

Hybrid, multicloud, on-premises / data center, VM, public cloud, private cloud, edge, and containers (Kubernetes)

Designed to protect all types of apps

Traditional, multicloud, hybrid, cloud-native, modern containerized, and microservices

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

Why organizations need F5 WAF.

Delivering security closest to apps and APIs in the needed deployment model

XC WAF

- Malicious User Detection
- Simple setup and deployment
- Consistent security across app suites and distributed environments
- Advanced AI / ML–based behavioral engine
- Automatic attack signature tuning

BIG-IP
Advanced WAF

- Comprehensive protection for a full range of app and API security needs
- Customizable to meet different security use cases
- Higher security efficacy via fine-grained controls
- OWASP Top 10 Compliance Dashboard

NGINX App
Protect

- Easy integration into DevOps environments
- Low-latency security solution
- Protection for container-, Kubernetes-based apps
- Flexible deployment options

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

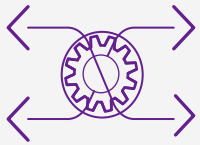
Secure your apps and APIs with BIG-IP Advanced WAF

Common WAF security

Layer 7 DoS mitigation

Credential Protection

API security



DevOps and Security Automation

Integrated LTM

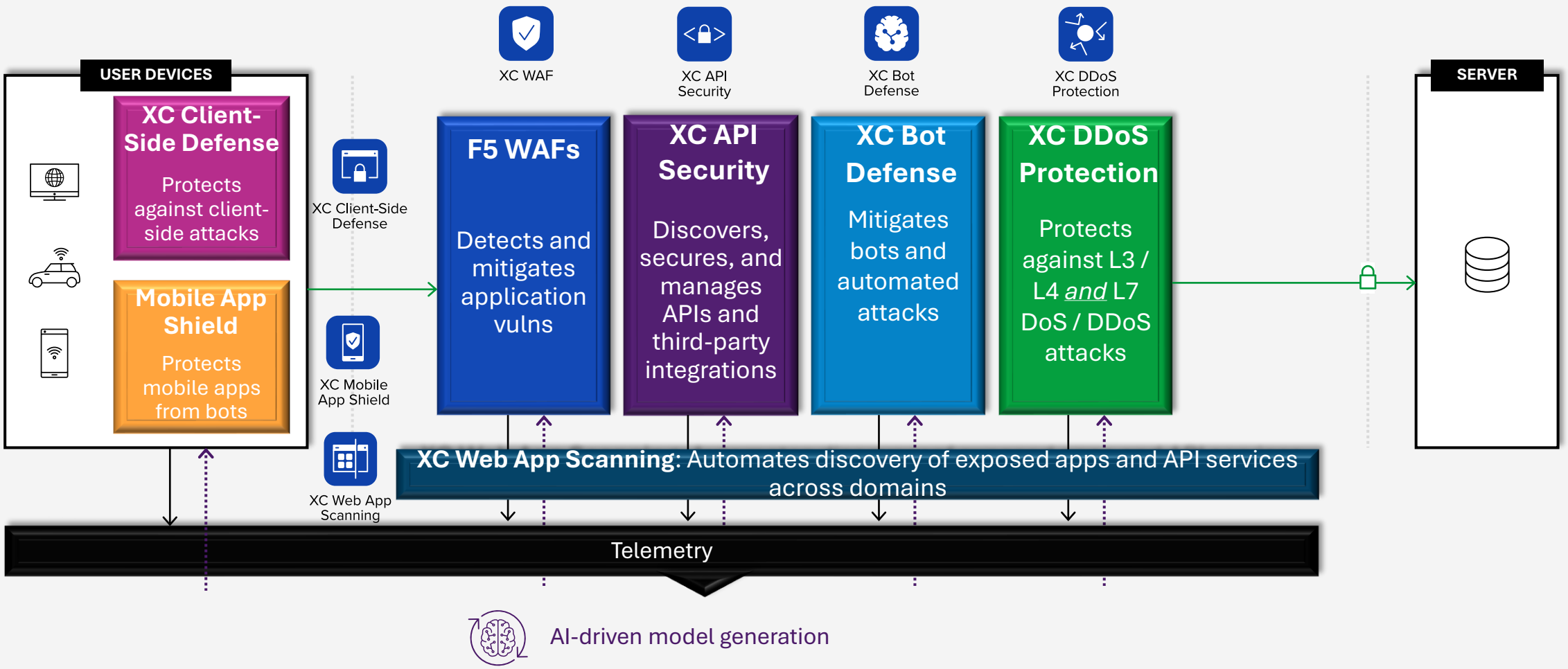
F5 Threat Campaigns

Bot protection

F5 IP Intelligence

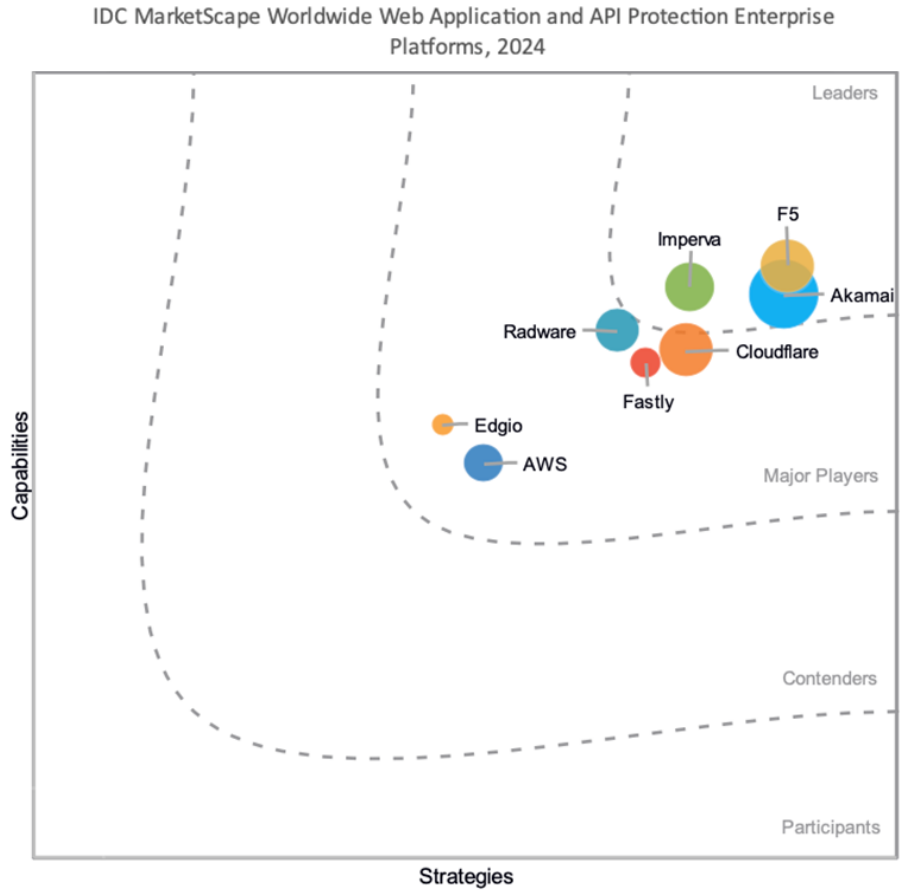
nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox. | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

F5 WAAP delivers holistic security that's simple to deploy and use, and just works in hybrid and multi-cloud environments.



nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

F5 was named a leader in the IDC Marketscape Worldwide Web Application and API Protection (WAAP) Enterprise Platforms Vendor Assessment for 2024



Source: IDC, 2024

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

BIG-IP Advanced WAF Bot defense and XC integration

WAF-based bot defenses were once sufficient and adequately addressed bots

HOWEVER, today's advanced bots need a specialized, dynamic solution

Today's advanced bots:

- *Retool in hours*
- *Apply ML to bypass CAPTCHA*
- *Mimic humans*
- *Introduce subtle randomness to avoid detection*

Customers need to add best-in-class F5 XC Bot Defense to their best-in-class WAF

XC Bot Defense is a *specialized bot management solution*

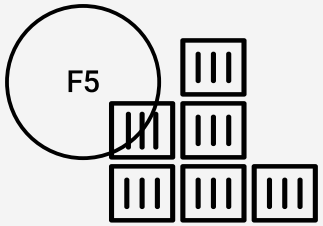
- Mobile and web signal collection covering environment and behavior
- Telemetry to XC Bot Defense service
- ML-based analysis to discover bot retooling
- Dynamic updates to the rules that mitigate advanced bots in real-time

XC Bot Defense integration available with Adv WAF

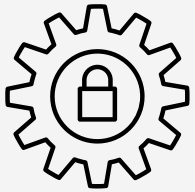
BIG-IP
Advanced WAF

+

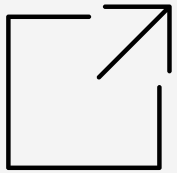
XC Bot
Defense



One vendor responsible for the security stack



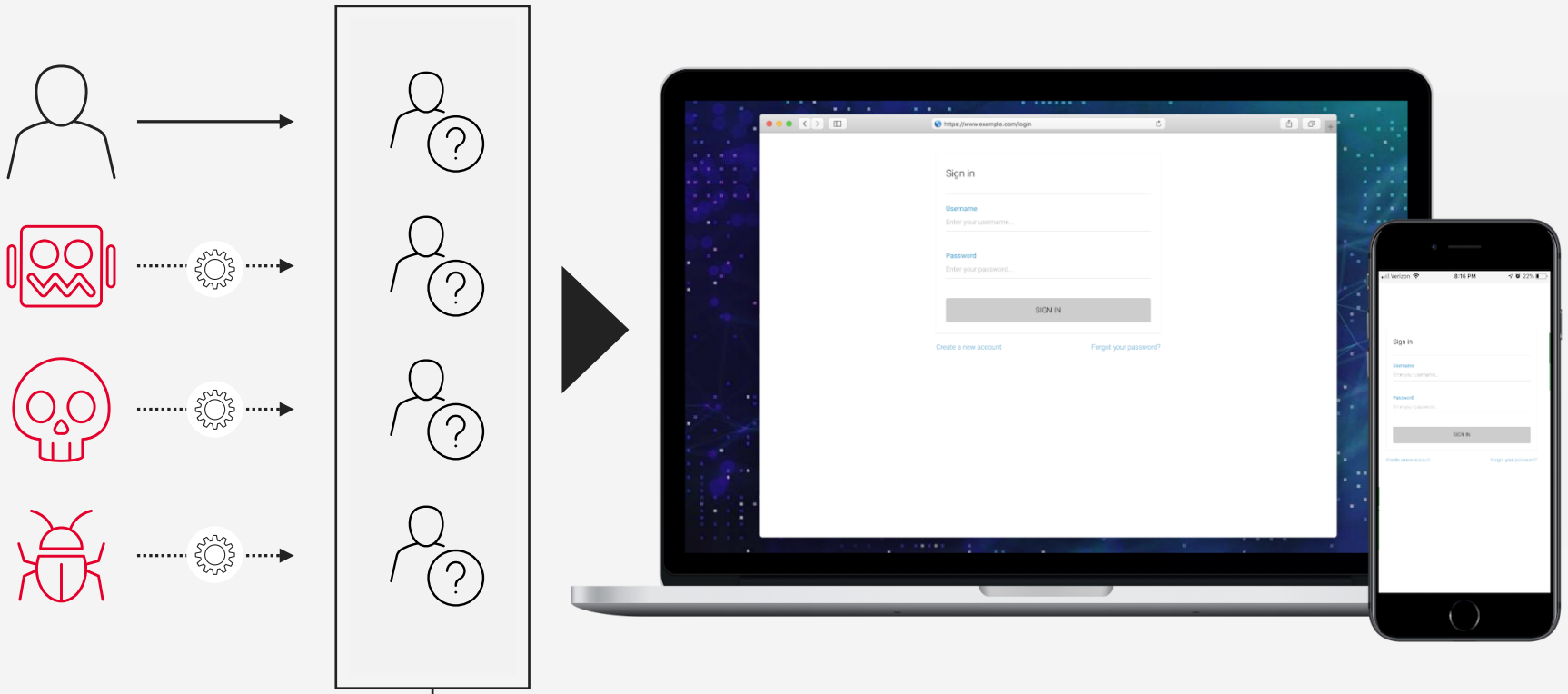
One skillset to manage products



Extends the F5 BIG-IP security stack

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

Bots are a **fundamentally different** type of threat



Bots look like customers and abuse inherent app functionality

> **Using our WAF and traditional firewalls** to manually block IP addresses was a **horribly ineffective** way to mitigate the very real threat posed by bots.
>
> —CISO, Major US Retailer

Bots have costs across your organization

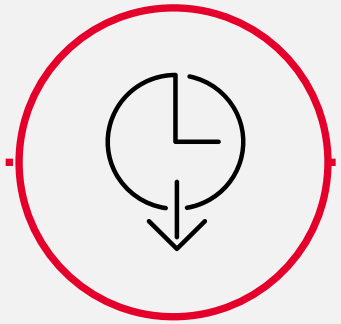
ATO and Fraud

$500k lost annually per organization due to credential stuffing

Manual bot blocking

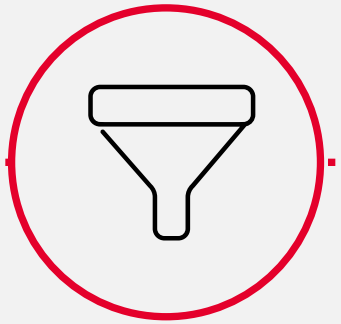
10k hours manually blocking bots per year

Downtime



80% of traffic potentially unwanted automation

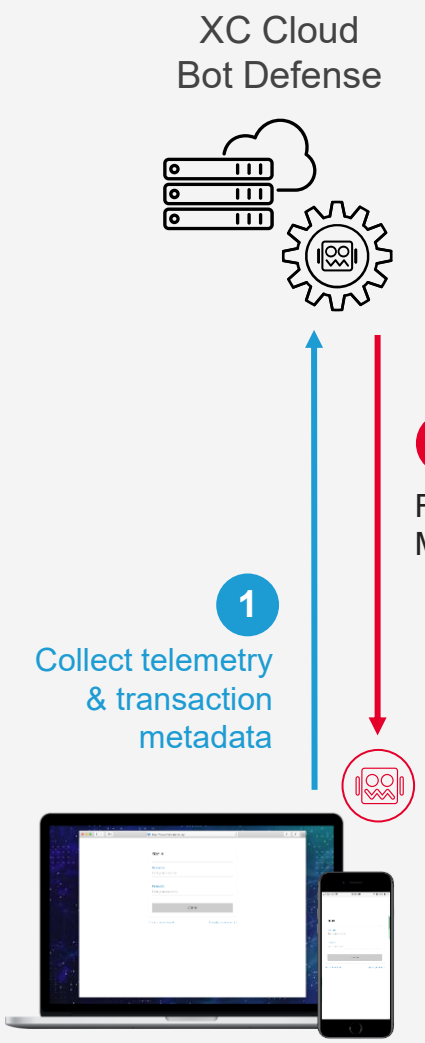
Poor customer experience

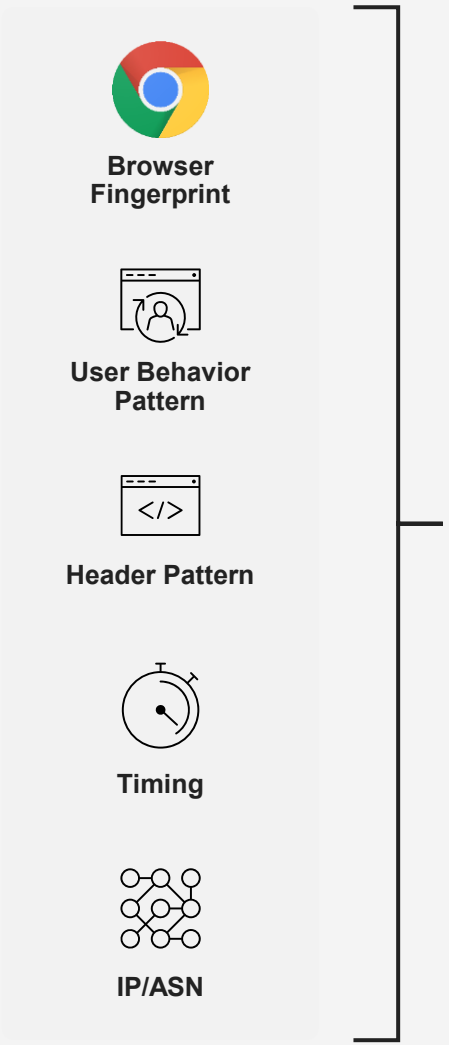


4 out of 5 global brands suffer churn due to bots

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox. | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

Highly effective real-time detection informs mitigation actions





Less Complex

- Are the headers in the right order?
- Did the client execute JavaScript?
- Is the client what it claims to be?
- Is the client reusing payloads?
- Is the client exhibiting human behavior?
- Are their signs of reverse engineered responses?
- …

More Complex

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

AI is the most vulnerable technology to ever be deployed at scale

Models are unpredictable

AI is non-deterministic which means you can never trust a prompt or an output.

Hallucinations

Data leakage

Escalation of model privileges

New attack types

Bad actors are using AI to exploit new threat surfaces.

Prompt injection

Jailbreak attacks

Model distillation

Data exfiltration

Anyone can use it

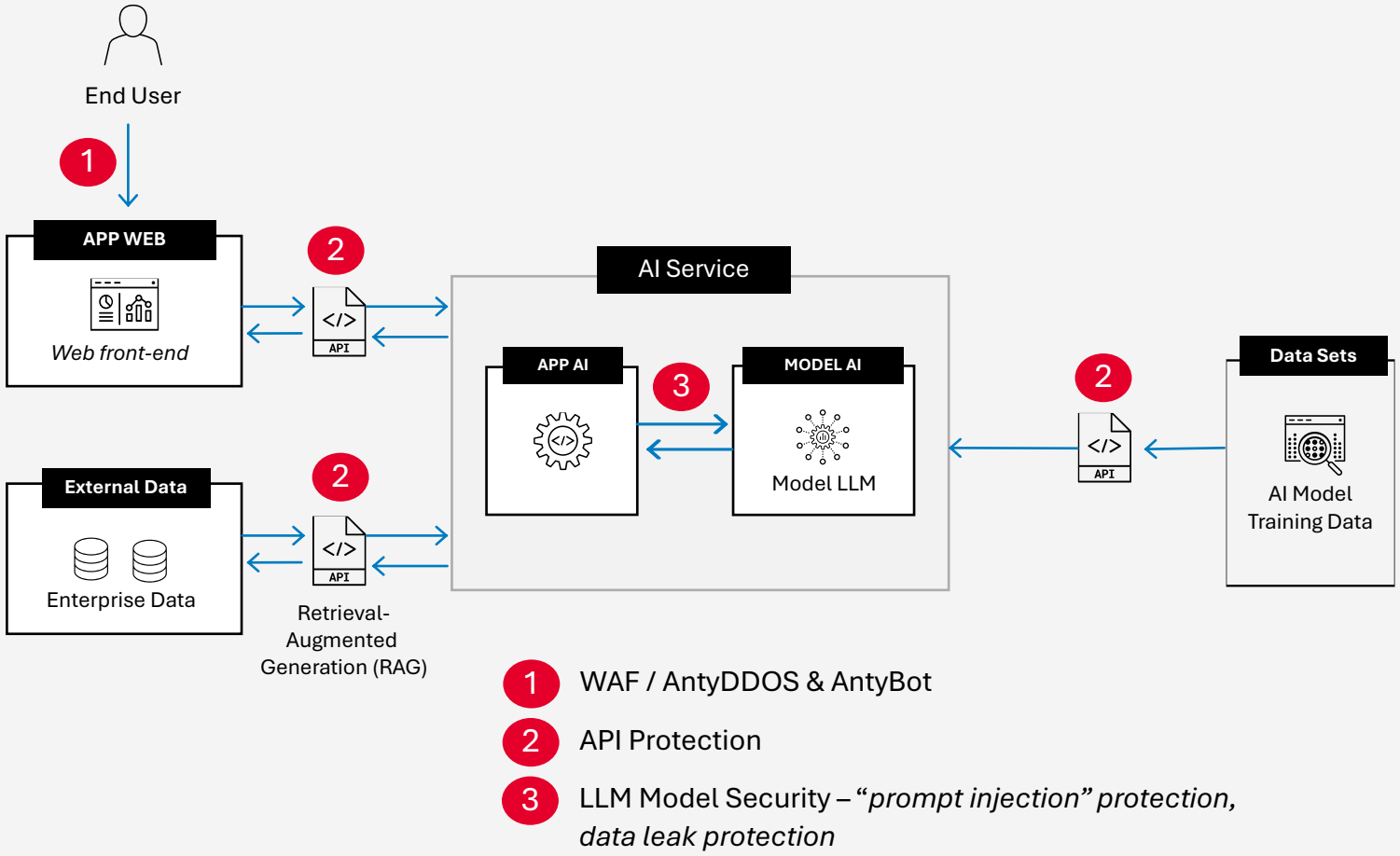
With AI everywhere, it increases the breadth of risky behaviors.

Shadow AI usage

Sensitive data disclosure

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

AI Ecosystem Challenges



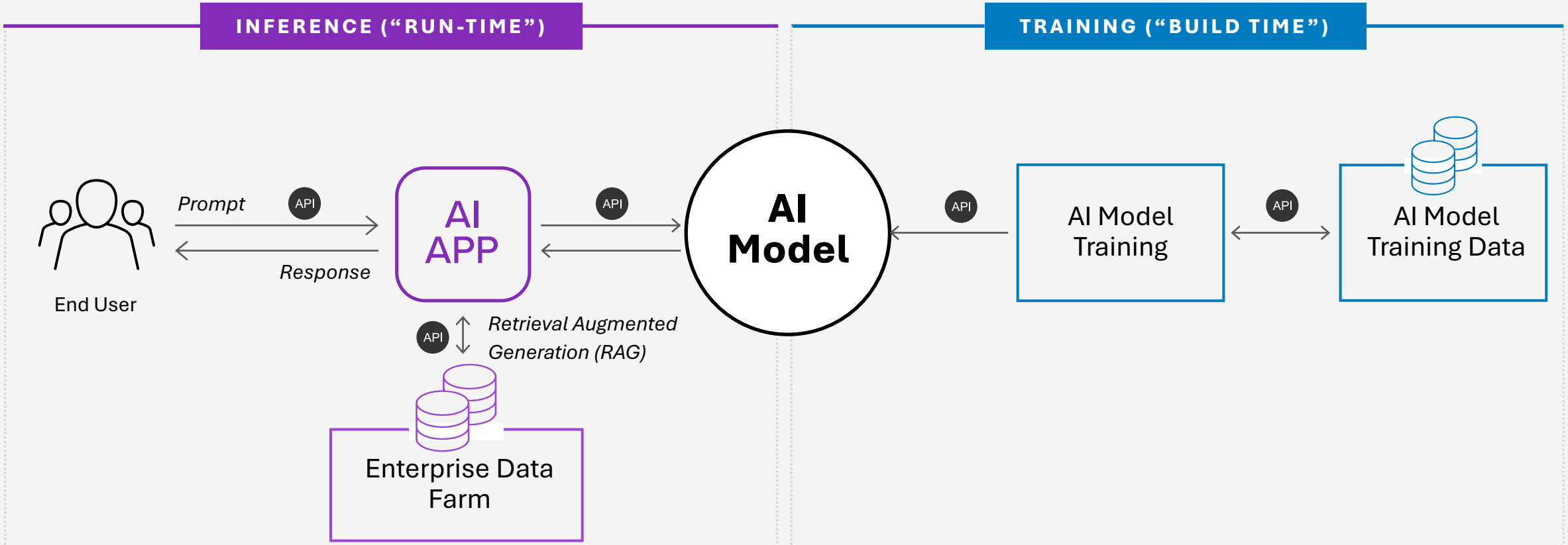
1. WAF / AntyDDOS & AntyBot
2. API Protection
3. LLM Model Security – "*prompt injection*" protection, *data leak protection*

AI Application & Services need:

- *Web Application Firewall* (WAF)
- AntyDDoS Protection
- Anty-Bot Defense
- API Protection
- AI/LLM Data Flow Security

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

AI Applications architecture is more complex than legacy Apps



Response is being generated based on the prompt

AI Data Farms are crucial in AI model lifecycle

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

F5 AI Guardrails

Define and observe how your AI models and agents interact with users and data, and defend against attackers

Combat adversarial threats

Safeguard AI from runtime threats like prompt injection and jailbreaks with 10,000+ monthly attack patterns continuously updated by real-world examples

Secure AI data

Detect and prevent data leakage from sensitive disclosures and policy violations at runtime

Govern responsible AI

Ensure regulatory compliance, obstruct harmful outputs, and enforce restrictions on model and agent privileges

Continuous Observability

Achieve continuous visibility and traceability across all AI interactions.

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox. | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

F5 AI Red Team

Command a swarm of agents to identify threats both obvious and obscure, translating those discoveries into new Guardrails

Harden AI Systems

Ensure your defenses grow smarter and more resilient with agentic threat intelligence regularly trained on **10,000+ new attack prompts created per month** from the preeminent AI CVE database

Attacker Chain of Thought

Explain and trace where and why threats arise with streamlined dashboards and 3rd Party SIEM/SOAR integrations

Automate the Repetitive, Augment the Strategic

Automate discovery of routine CVEs to free up team members for more sophisticated threats

Agentic Fingerprints

Gain insight into broader trends across the attack surface and trace ground-level knowledge of how each agent did its work

Insights → **F5 AI Guardrails**

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox. | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

F5 AI Guardrails delivers real-time security for AI models, agents, and data from pilot to production.

CHALLENGE

Limited visibility of AI deployments

Enterprises lack real-time insights into:

- Threat exposure
- User behavior
- Model performance,
- Areas of non-compliance

Without visibility, security teams struggle to detect and mitigate evolving risks.

Growing threat vectors

GenAI systems remain vulnerable to:

- Prompt injections
- Jailbreaks
- Adversarial attacks

These gaps expose enterprises to security breaches and reputational damage.

Uncontrolled AI interactions

Organizations are more exposed to:

- Data leaks
- IP loss
- Regulatory violations
- Unmoderated app interactions

Without enforcement at the inference layer, sensitive data and compliance are at risk.

SOLUTION

Full visibility

Real-time monitoring of threats, usage, and compliance

Proactive defense

Custom scanners to detect and prevent adversarial threats in real-time

Runtime control

Policy enforcement prevents data loss, risk, and non-compliance while enabling content moderation in line with specific needs

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO

4 key areas where F5's AI Security solution stands out

Custom Guardrail Creation

Pair plug-and-play presets with bespoke, customizable policy enforcement by regulatory framework or unique organizational requirements

Model-Agnostic

Protections apply to every model and fine-tuned variation, regardless of source

Privacy

Proxy layer that can run asynchronously or offline without outbound calls to a 3rd party cloud services or security-as-code

AI Threat Research

Preeminent AI vulnerability database updated with 10,000 attack patterns every month based on emerging trends and adversarial techniques

nomios | CROWDSTRIKE | ExtraHop | FORTINET | f5 | HPE JUNIPER networking | infoblox | Trellix | ARROW | EXCLUSIVE NETWORKS | ectacom | CLICO


Dziękujemy za uwagę!
CROWDSTRIKE
ExtraHop
FORTINET
HPE JUNIPER networking
infoblox
Trellix
nomios
ARROW
ectacom
EXCLUSIVE NETWORKS
CLICO