FORTINET | USA
XPERTS
SUMMIT 2025

Helping you create a digitally secure future.

FortiADC Secure Application Delivery

David Parisie & Nishant Dhawan
Cloud CSE Team

Disclaimer

Fortinet Confidential

This document contains confidential material proprietary to Fortinet, Inc.

This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside Fortinet, Inc. without prior written consent of Fortinet, Inc.

This information is pre-release and forward looking and therefore is subject to change without notice.

The purpose of this document is to provide a statement of the current direction of Fortinet's product strategy and product marketing efforts.

Please note that this Product Roadmap is neither intended to bind Fortinet to any particular course of product marketing and development nor to constitute a part of the license agreement or any contractual agreement with Fortinet or its subsidiaries or affiliates.

Agenda

- Market Overview
- FortiADC Technology and Use-Cases
- Deployment Options and Licensing
- Summary
- Competition
- Lab

Market Overview

Technical Challenges

1 Architecture Flexibility

Appliances → Hybrid Cloud

2 IT Technologies

Monolithic → Microservices

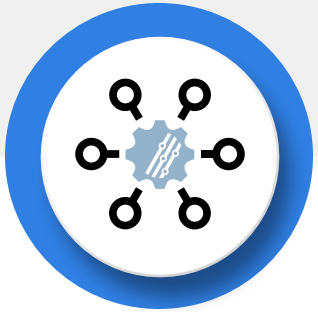
3 CI/CD Tools

Manual → Automation

4 Increased Attack Surface

Web apps → API, Files, Bots

Solution Requirements



Automation and Scale

Applications are extremely dynamic

- Automate traffic steering and optimize resource utilization
- React to real-time events
- Scale up and down effectively
- Set up adaptive security policies

Service Optimization

Ensure uptime via distribution

- Downtime and delays have cost
- Applications MUST be accessible from anywhere
- Enable users to work remotely and securely

Application Security

Applications are a common target

- Protect apps from a variety of threats
- Keep security policy up to date
- Meet compliance requirements
- Secure availability

FortiADC
Technology and Use-Cases

FortiADC Core Offering

Automation and Scale

- Cloud Connectors
- DevOps tools
- Application LB

Service Optimization

- GSLB
- Application Acceleration
- Automation

Extensive Security

- WAF: Adaptive Learning & OWASP Top-10
- Threat intelligence and analytics
- Bot Protection

Integrations

SAP, aws, ORACLE CLOUD, splunk>, openstack, ANSIBLE, cloud-init, API, CloudFormation, Terraform

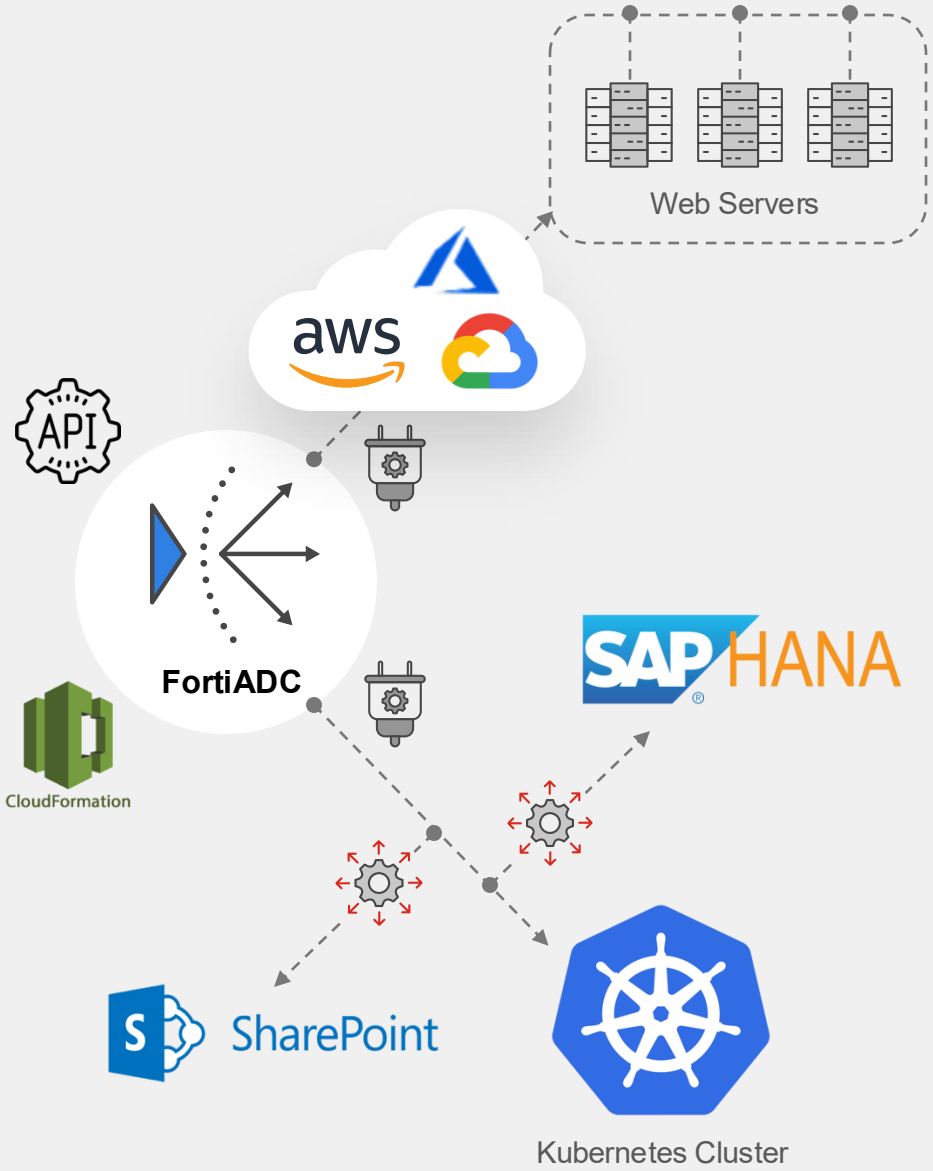
Application Availability

Application Load Balancing
- L7 HTTP & HTTPS LB
- Advanced Health Check
- SSL Offloading and Inspection

Scripting & Automation
- Support any customer requirements
- React to real-time events via Automation

Global LB
- Ensuring Business Continuity
- Support traffic rerouting based on health checks, Geolocation, and application RTT

Optimization
- Improve User Quality of Experience
- Provide website performance enhancement tools



Application Security

Web Application and API Protection

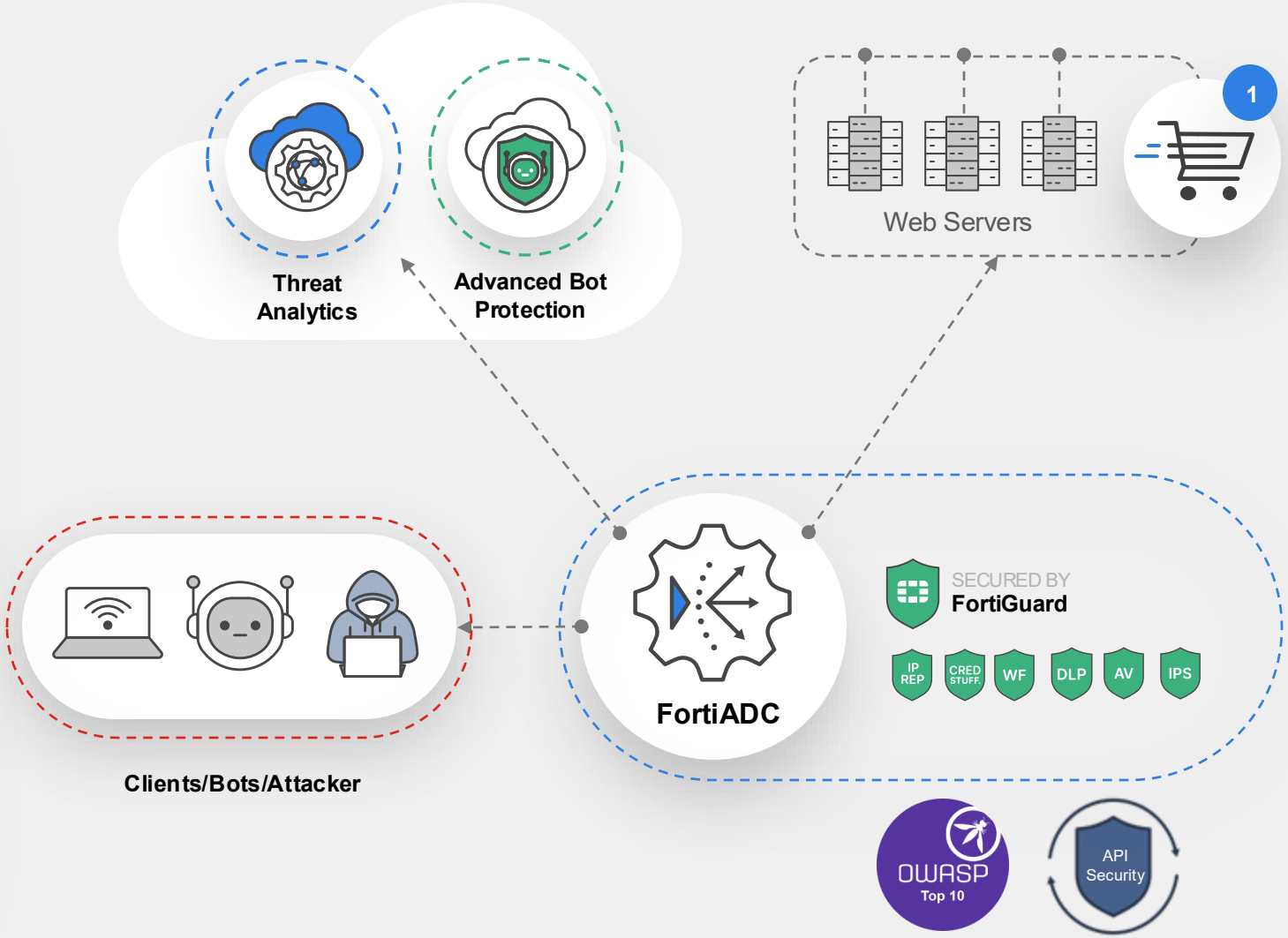
- Protects against common web threats, including SQL injection, XSS, and other OWASP Top 10 risks
- Adaptive traffic learning for continuous threat detection and response
- Monitors and controls API traffic to prevent data breaches and unauthorized access

Bot Protection

- ML-driven, biometric, and behavior-based detection of malicious bots to protect online services and free up network resources

Threat Analytics

- Reduces alert fatigue by speeding up incident investigation and provides SOC analysts with insights to prioritize mitigations and workload



Application Access

Agentless Application Gateway

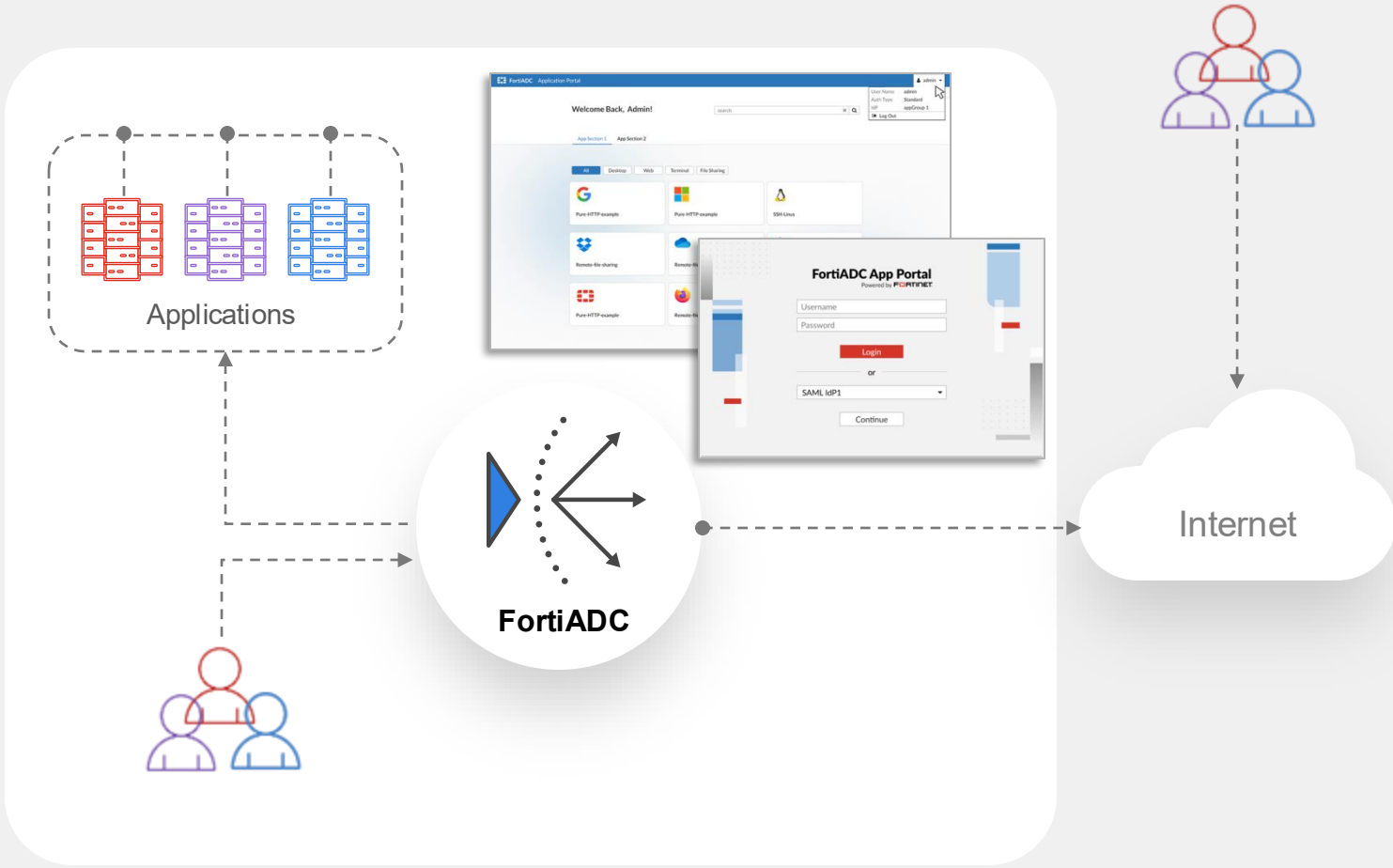
- Access internal applications with **no client-side agents**
- secure access to corporate resources from **any location,** enabling a global workforce to work efficiently and securely
- Publish RDP, VDI, SSH, and web applications through a centralized portal

Strong Security & Authentication

- Support multi-factor authentication (MFA) and SSO
- Enforce granular user access policies for enhanced security

Real-Time Visibility & Control

- Monitor user sessions and application access

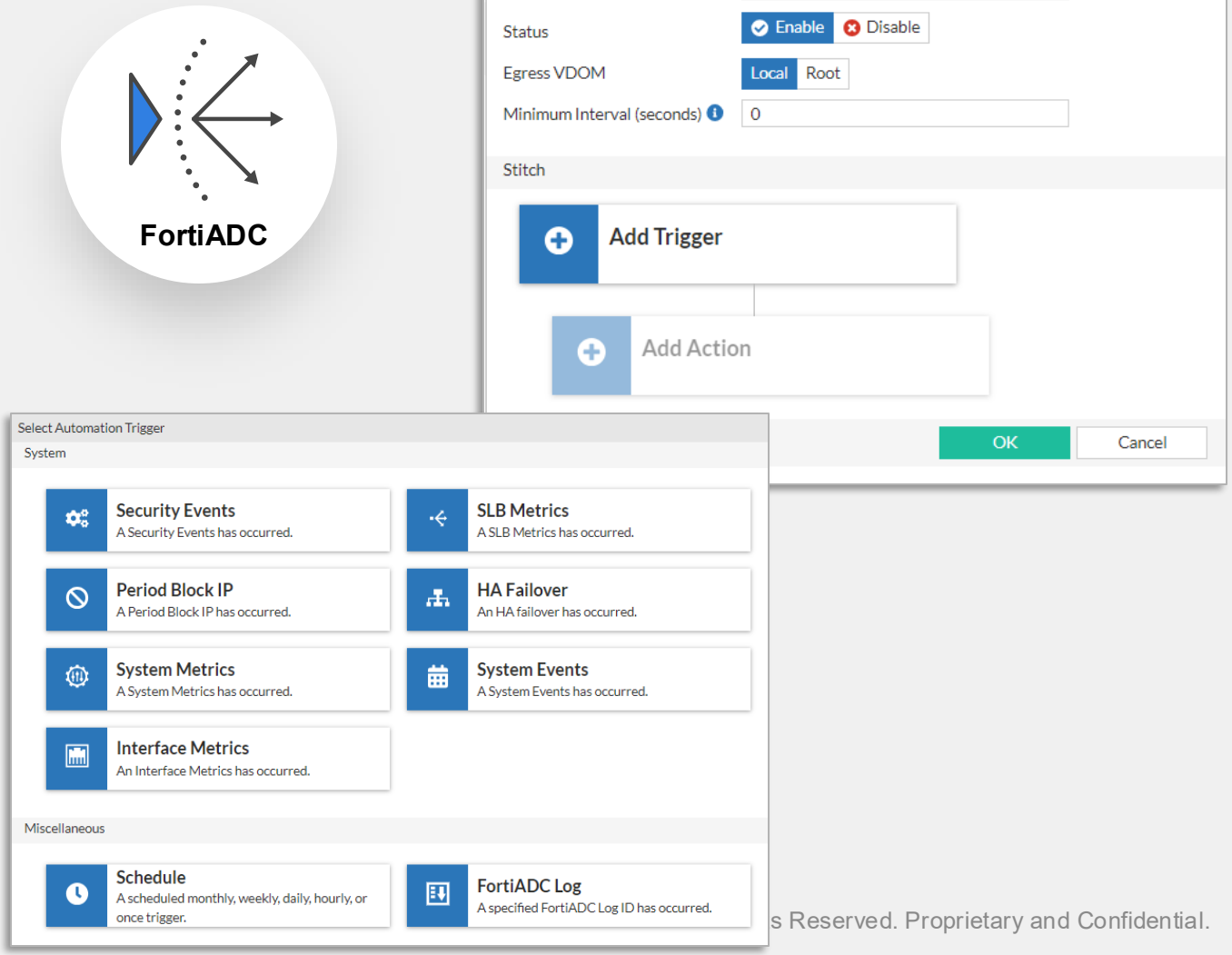


Application Automation

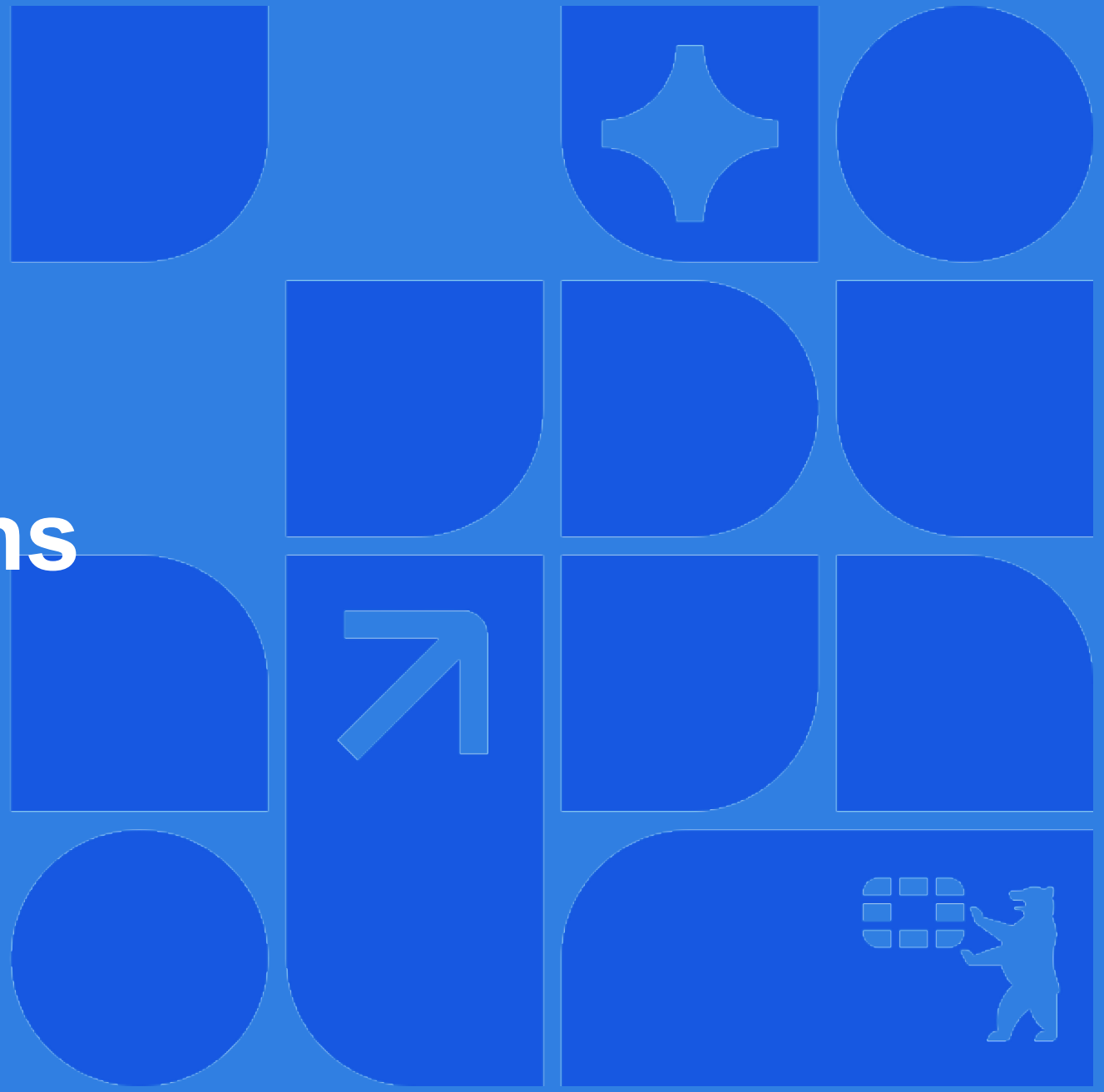
Automation Stitches

Improve productivity via automating actions and response to events

- Ensure application automation and application security using automation stitches.
- An event triggers the predefined condition on the FortiADC that activates the action. (For example, a failed login attempt).
- FortiADC then acts in response to the trigger. (For example, changing the configuration).



Deployment Options and Licensing



Options For Any Organization Size And Deployment

Full Control

Solutions for organizations that prefer full control and management over their Application Delivery Controller.

Appliances

- From 5Gbps - 250Gbps
- Hardware ASICs
- Support for 100GE

FORTINET

Virtual Machines

- 6 VM models
- CPU-based
- Subscription licensing

vmware Hyper-V CITRIX XenServer KVM

Cloud

- 5 Cloud models
- BYOL/PAYG Support
- Multiple Templates for easy deployment

aws Azure Alibaba Cloud ORACLE CLOUD Google Cloud

FortiFlex

- Simplified, Flexible Licensing
- Simplified Deployment and Purchasing Decisions
- Cloud & Platform Agnostic

FortiADC Ecosystem

Public Cloud

aws · Azure · Google Cloud · Alibaba Cloud · ORACLE CLOUD · IBM Cloud

NEW

Private Cloud

vmware · Hyper-V · KVM · CITRIX XenServer · IBM · openstack

API Connectors

SAP · aws · ORACLE CLOUD · splunk> · NEW

DevOps and IaaC

ANSIBLE · cloud-init · API · CloudFormation · Terraform · NEW

FortiADC Security Bundles

		Network Security	Application Security	AI Security
Network Security	IP Reputation and GeoIP	✓	✓	✓
	FortiGuard AntiVirus	✓	✓	✓
	Intrusion Prevention	✓	✓	✓
Application Security	Web Security Signatures & Adaptive Learning		✓	✓
	Credential Stuffing Defense		✓	✓
	Sandbox Cloud		✓	✓
	FortiGuard DLP		✓	✓
AI Security	Threat Analytics			✓
	Advanced Bot Protection			✓

* Agentless Application Gateway is included in each of the bundles

Security Fabric Integrations

3rd Party Scanners

FortiWeb

FortiGate

File Scanning

FortiSandbox / FortiSandbox Cloud

Web Vulnerabilities / custom rules

HTTP Traffic

Ban IPs

SECURED BY FortiGuard

IP REP

CRED STUFF.

WF

DLP

AV

IPS

FortiADC

File Scanning

ZTNA Client Verification

FortiClient / FortiClient EMS

Protected Web Applications

FortiAnalyzer

Analytics Reports

Unified Threat Analytics dashboard

Threat Analytics

FortiSIEM

Security Reports

Advanced Bot Protection

Bot Protection

Summary

FortiADC Summary

Cost-Effective, Secure Application Delivery

Improve application experience, security, and availability

1. Most complete ADC security solution (WAF, API Security, DLPIP Rep, AV, IPS, Sandbox, and FW)
2. Fortinet Security Fabric Integration (FortiGate, FortiSIEM, FortiAnalyzer, FortiSandbox)
3. Cloud and fabric connectors
4. Application automation and scripting (SAP, K8s, OCP, Oracle, and AWS)
5. Best price/performance in the market

Application Delivery Controllers - Competitive

Let's see WAF on ADC competitive offerings

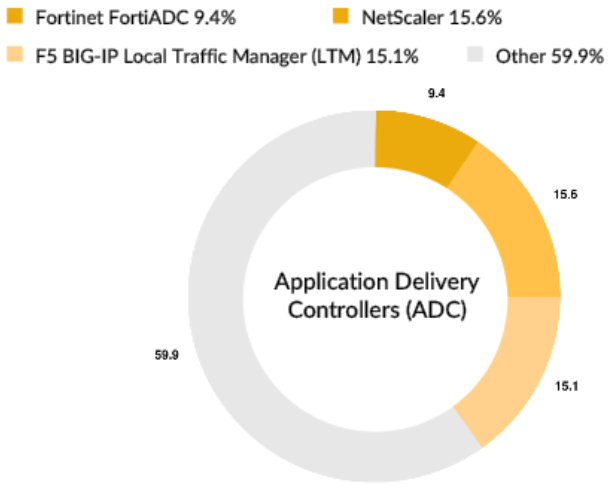
	FortiADC	F5	Citrix	Radware	A10
Signatures	**Yes**	Yes	Yes	Yes	3rd party (fastly)
Traffic Learning	**Yes**	Yes	No	Yes	No
Policy Recommendations	**Yes**	No	No	Yes	No
Threat Intelligence	**Yes**	Limited	No	Limited	No
Bot Protection	**Add-on**	Add-on	Limited	Add-on	3rd party add-on
Threat Analytics	**Yes**	No	No	No	No

PeerSpot – FortiADC reviews

Mindshare And Ranking

As of **December 2024**, the mind share of **Fortinet FortiADC** in the Application Delivery Controllers (ADC) category stands at **9.4%**, up from 7.3% compared to the previous year, according to calculations based on PeerSpot user engagement data.

Primary Category



"I am impressed with the product's load-balancing feature."

Aymar Tala Defo
Cyber Security Analyst at COLLEGE BOREAL

"We can do patches offline without causing customers outages. The web application firewall features, especially those related to the OWASP Top Ten, provide automated protections. This allows more flexibility in patching the backend applications. Additionally, it offers visibility into the requests being made to the applications, and you can't protect what you can't see."

Andrew Reynolds
Senior Technical Consultant at CBR Cyber Pty Ltd

"Although FortiADC has multiple features that I like, the global DNS is the most helpful. It is primarily useful for customers with huge environments and at least two data centers. FortiADC can act as your DNS server. It can check which data center has the lowest latency, and route traffic to that one. It's an intelligent DNS."

Bruno Moreira
Network Security Consultant at SigmaTelecom

Source: https://www.peerspot.com/products/fortinet-fortiadc-reviews

F5 Customer Experience

From product disruption to security exposure

May 2023

August 2025

October 2025

BIG-IP iSeries EoS:
Forcing customers to undergo complete HW and OS. Customers reported concerns

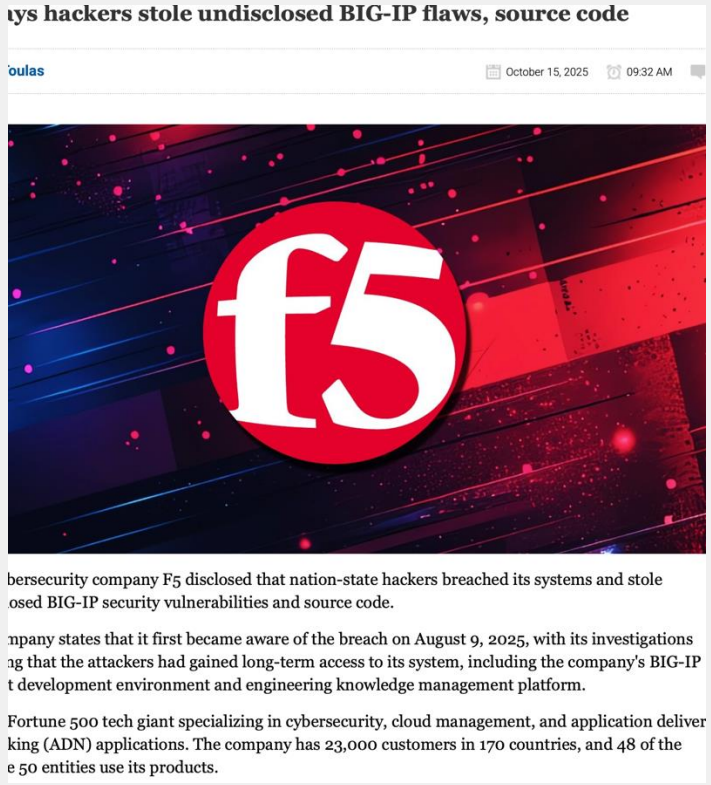
Terminated BIG-IP Next
advising HW/VE customers to roll back to the previous OS

Security Breach
leaving customers exposed and vulnerable to a threat actor holding access to their networks and apps

F5 Says Hackers Stole Undisclosed BIG-IP Flaws, Source Code

F5 Customers are unsafe

What Happened



ıys hackers stole undisclosed BIG-IP flaws, source code

oulas October 15, 2025 09:32 AM

bersecurity company F5 disclosed that nation-state hackers breached its systems and stole osed BIG-IP security vulnerabilities and source code.

npany states that it first became aware of the breach on August 9, 2025, with its investigations ıg that the attackers had gained long-term access to its system, including the company's BIG-IP t development environment and engineering knowledge management platform.

Fortune 500 tech giant specializing in cybersecurity, cloud management, and application deliver king (ADN) applications. The company has 23,000 customers in 170 countries, and 48 of the e 50 entities use its products.

The Impact

Ramifications

- 266,000 systems exposed WW
- A hostile entity now holds BIG-IP source code, undisclosed vulnerabilities, and customer configuration data.
- Can access any device and reverse engineer software updates and security patches
- Customers are required to continuously invest in upgrading compensating controls
- F5 is trying to rectify the situation and stop customer attrition as the stock price drops

UNC5221

UNC5221

Chinese espionage group

Linked to the exploitation of at least seven specific CVEs:

- CVE-2023-46805 (Ivanti Connect Secure authentication bypass)
- CVE-2024-21887 (Ivanti Connect Secure command injection)
- CVE-2023-4966 (NetScaler ADC and NetScaler Gateway vulnerability)
- CVE-2025-22457 (Ivanti Connect Secure stack-based buffer overflow)
- CVE-2025-0282 (Ivanti Connect Secure stack-based buffer overflow)
- CVE-2025-4427 (Ivanti Endpoint Manager Mobile (EPMM) unauthenticated RCE)
- CVE-2025-4428 (Ivanti EPMM unauthenticated RCE)

The group has also been linked to a breach of F5, where they likely exploited an undisclosed zero-day vulnerability

BRICKSTORM

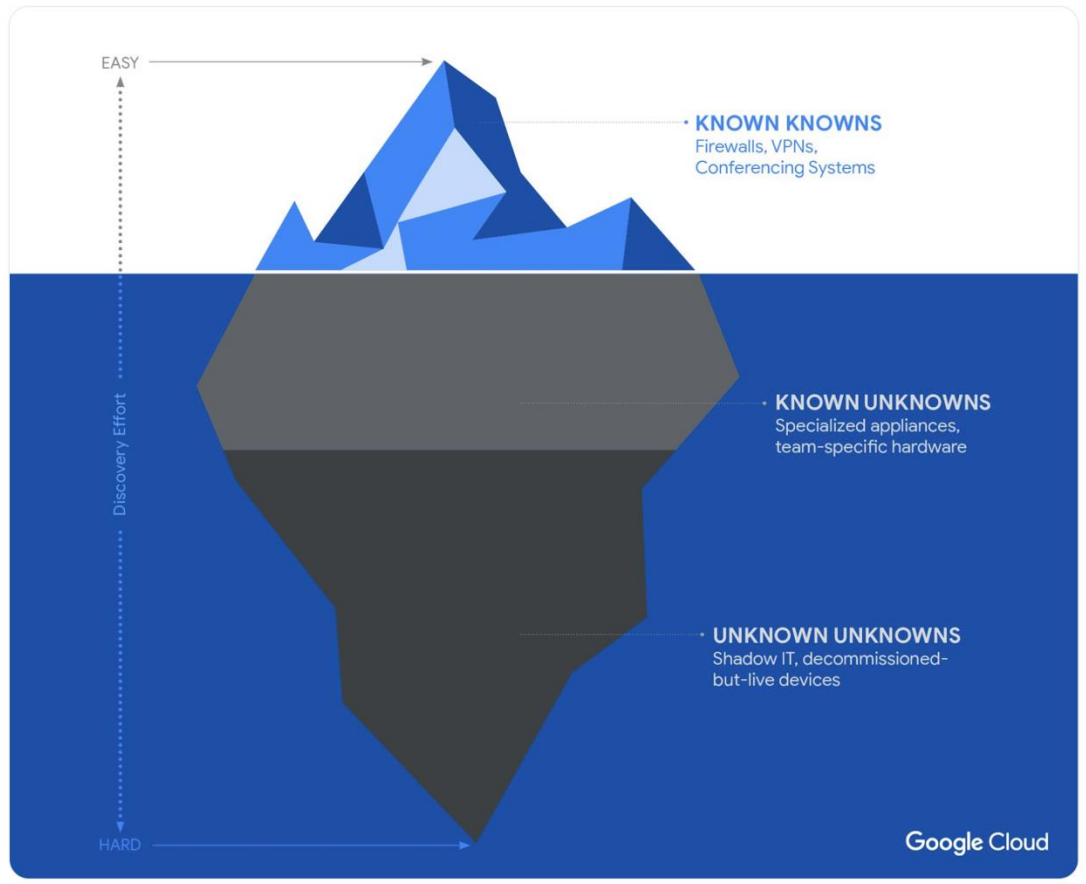
Malware used to maintain persistent access

- Closely related to group “UNC5221”
- Targeting appliances that do not support EDR
- Generates very little to no security telemetry
- Initial logs are usually gone by the time the breach is discovered
- May wait months after the breach before beaconing back to command and control
- Averages 393 days before discovery
- Using the BRICKSTORM SOCKS proxy to tunnel into victim computers.
- UNC5221 more often targets ESXi and vCenter
- Google Threat Intelligence has a BRICKSTORM scanner: https://github.com/mandiant/brickstorm-scanner

BRICKSTORM

Threat hunting

Step	Hunt	Data Sources
0	Create or update asset inventory that includes edge devices and other appliances	N/A
1	File and backup scan for BRICKSTORM	Appliance file system, backups
2	Internet traffic from edge devices and appliances	Firewall connection logs, DNS logs, IDS/IPS, netflow
3	Access to Windows servers and desktops from appliances	EDR telemetry, Security Event Logs, Terminal Service Logs, Windows UAL
4	Access to credentials and secrets	Windows Shellbags, EDR telemetry
5	Access to M365 mailboxes using Enterprise Application	M365 UAL
6	Cloning of sensitive virtual machines	vSphere VPXD logs
7	Creation of local vCenter and ESXi accounts	VMware audit events
8	SSH enablement on vSphere platform	VMware audit events, VAMI logs
9	Rogue VMs	VMware audit events, VM inventory reports



FortiGuard BRICKSTORM coverage

FortiGuard specific BRICKSTORM mitigation actions

- Antimalware Service: Released AV detections for known BRICKSTORM binaries, webshells, and YARA rules.
- Indicators of Compromise (IOC) and Web Filtering Service: Implemented protections against malicious traffic and C2 infrastructure observed in this campaign.
- FortiGuard Sandbox Service: Delivers protection against known malware and uses advanced behavioral analysis to detect and block unknown threats.
- Organizations suspecting a compromise can contact the FortiGuard Incident Response team for rapid investigation and remediation support.

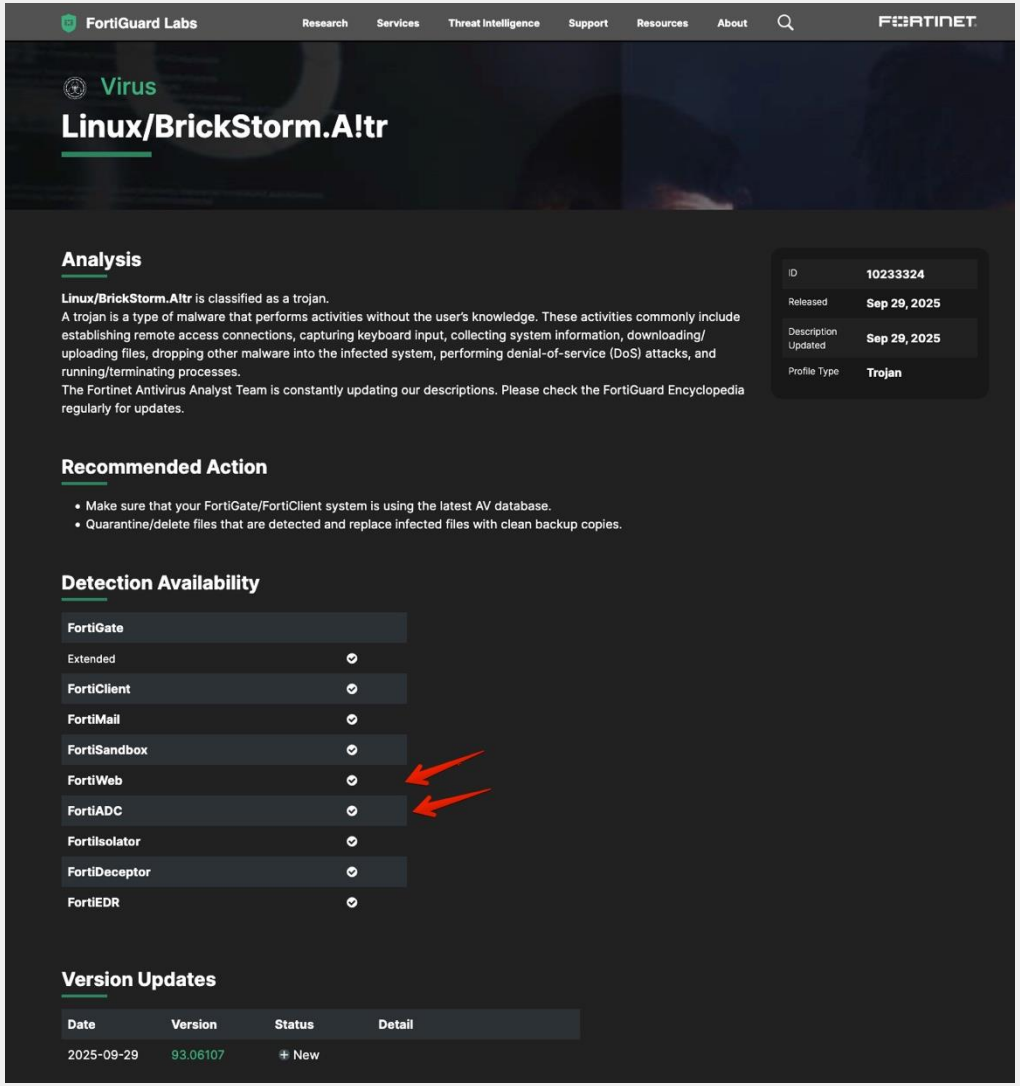
FortiADC - FortiWeb specific BRICKSTORM coverage

FortiADC - FortiWeb specific BRICKSTORM mitigation actions

- Antivirus
- FortiSandbox
- Automation Stitches

FortiGuard specific BRICKSTORM coverage

FortiGuard specific BRICKSTORM mitigation actions



BRICKSTORM

References

BRICKSTORM Espionage Campaign

https://www.fortiguard.com/threat-signal-report/6204/brickstorm-espionage-campaign

Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors

https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign

Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457)

https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability


FORTINET