FORTINET | USA

XPERTS

SUMMIT 2025

Helping you create a digitally secure future.

FortiAppSec Cloud

Cloud CSE Team

Agenda

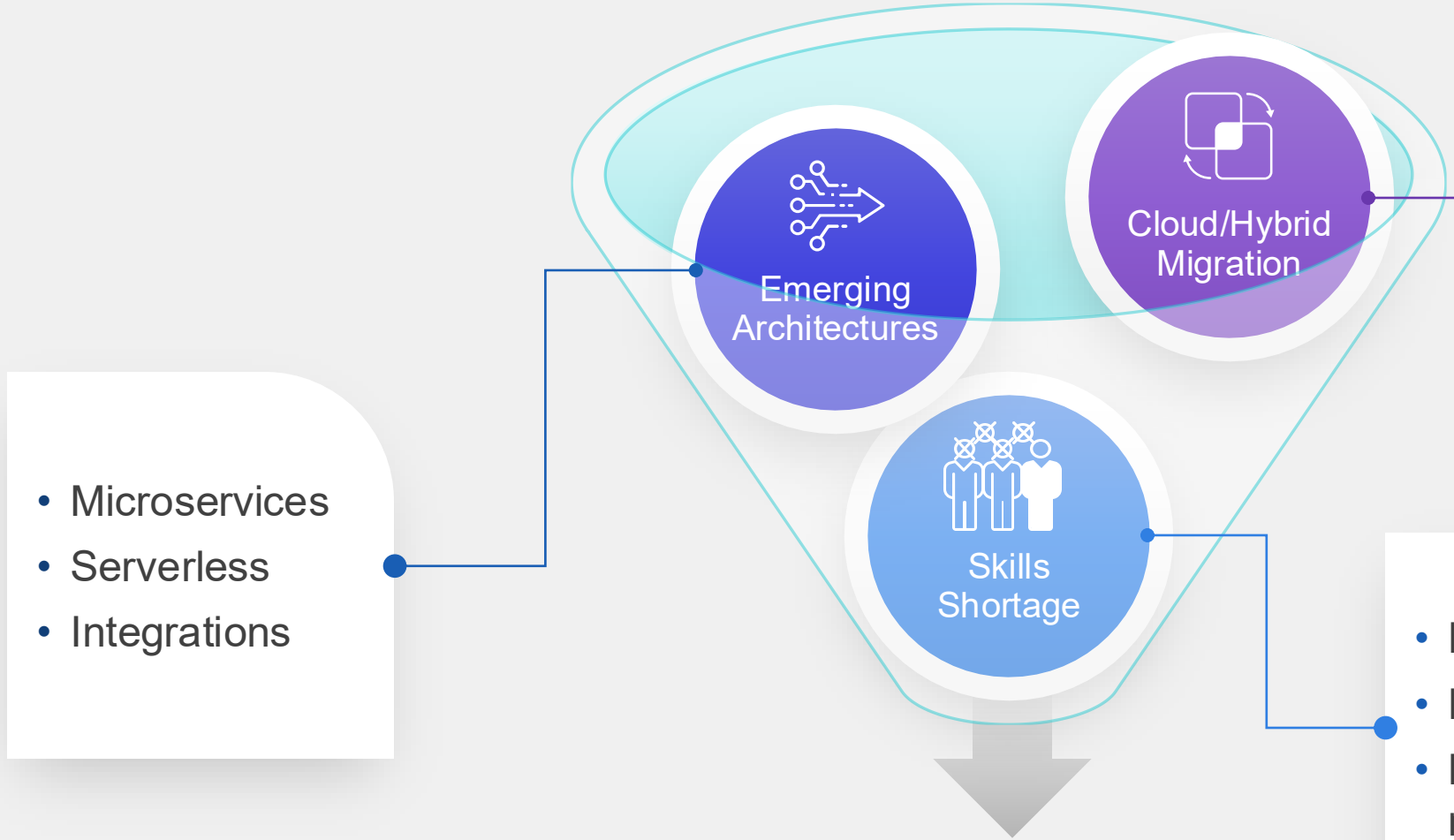
- Need for Application Security
- Introducing FortiAppSec Cloud
- Review Hands on Lab
  - Initial Setup
  - Web Application Firewall rules
  - Machine learning
  - Bot mitigation
  - API protection
- Summery

FORTINET | USA XPERTS SUMMIT 2025

FortiAppSec cloud

Initial setup

Modern Applications Architectures Create Blind Spots



- Microservices
- Serverless
- Integrations

- Multiple environments
- Access management
- SaaS

- New threats
- New solutions
- Limited resources

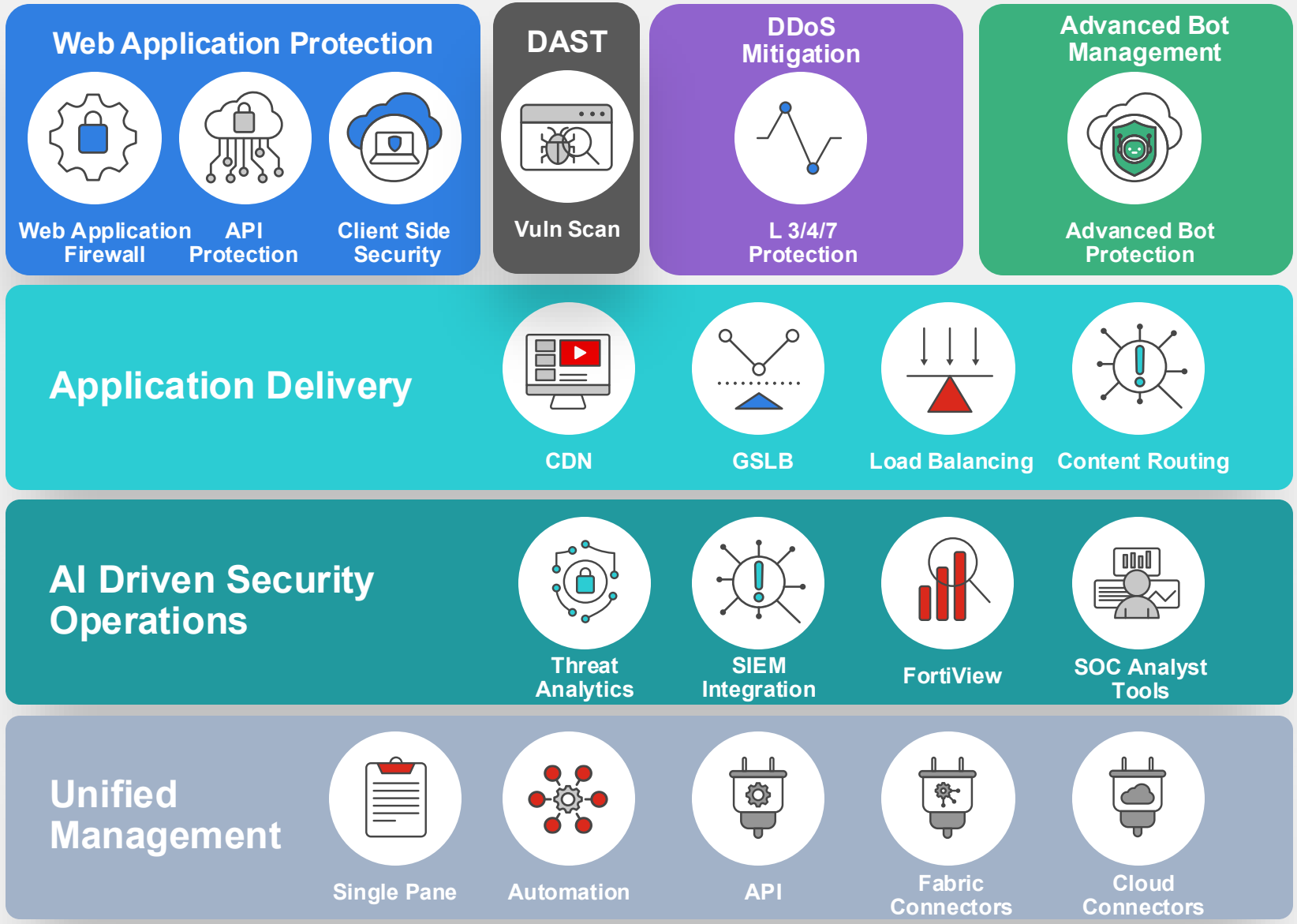
Customers expect security solution that is

- **Seamless** – Built-in, not bolted on; protection that doesn't slow down innovation.
- **Cloud-Ready** – Works across on-prem, cloud, and hybrid environments.
.
- **Intelligent** – Uses AI/ML to detect and respond to evolving threats automatically.
- **Comprehensive** – Covers web apps, APIs, and bots under one platform.
- **Visible and Actionable** – Offers unified analytics and simplified management.
- **Integrated** – Works with existing DevOps and CI/CD pipelines.
.

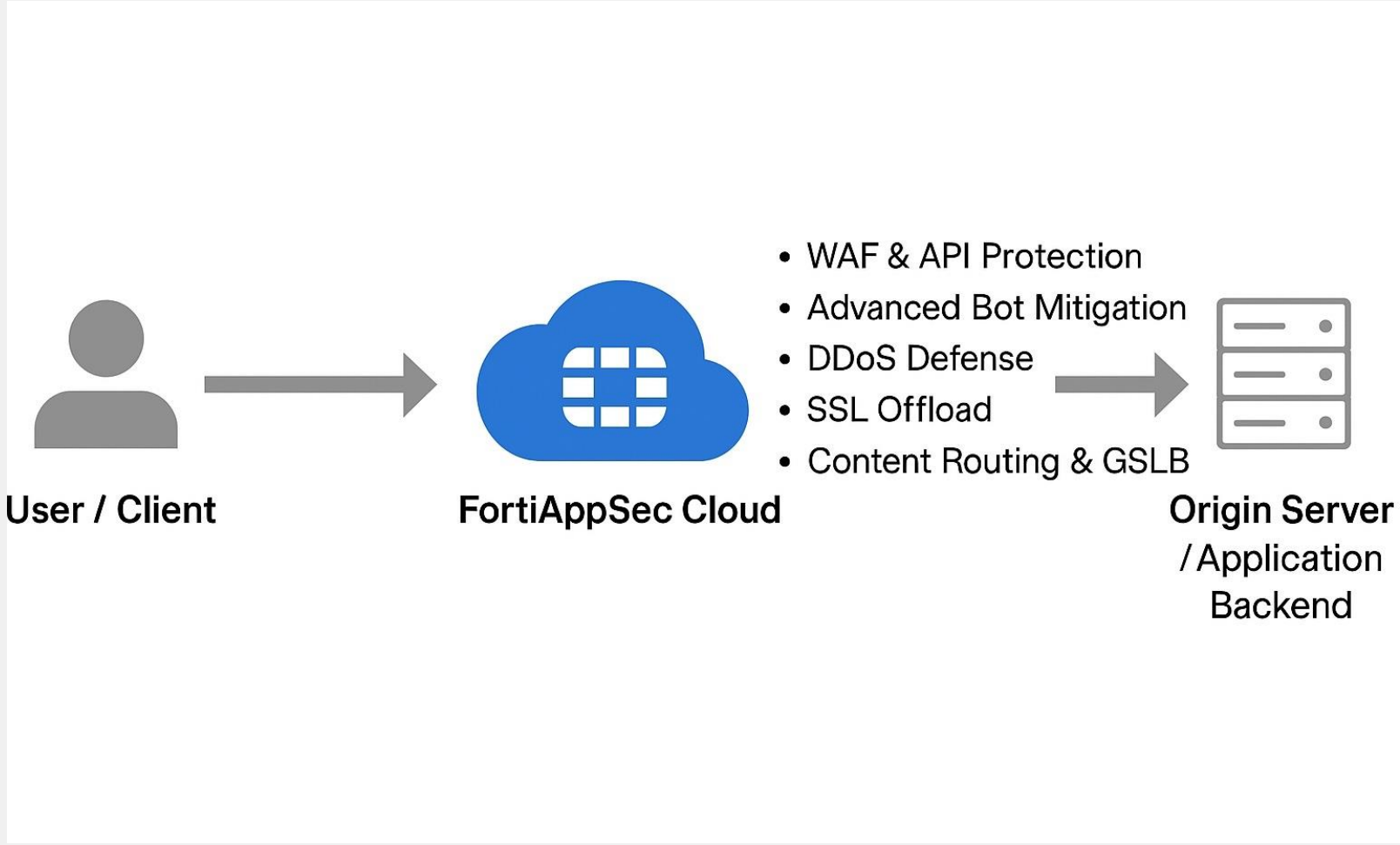
FortiAppSec Cloud

Customer Benefits

- Cover the application attack surface
- Simplify detection and response
- Deliver consistent security policy
- Ensure availability and continuity
- Optimize application performance
- Central management and visibility



How FortiAppSec Works



Traffic Flow Overview:

1. **User / Client** – Sends web or API requests to the application's public URL.

2. **FortiAppSec Cloud** – Intercepts and inspects all HTTP/S traffic before it reaches the origin.

WAF & API Protection

Advanced Bot Mitigation

DDoS Defense

SSL Offload

Content Routing & GSLB

3. **Origin Server / Application Backend** – Only clean, legitimate traffic is forwarded to the application.

Outcome:

Enhanced security

Improved performance

Simplified management

Global Coverage: Simple. Fast. Secure.

Deployment across all major Cloud Providers

- **Unlimited elasticity**
- **Simplified regulatory environment**
- **Proximity, 0 latency**
- **Multi-tenancy**
- **Only intra-region traffic is charged**

FORTINET | USA

XPERTS

SUMMIT 2025

Lab Review

Section 1 Create Your Environment

Getting Started – Goal and Context

Objective: Provisioning Your Azure Environment. Each student receives an isolated environment with prebuilt components for hands-on exercises.

1. Provision your personal Azure lab instance
2. Configure and access Azure Cloud Shell
3. Deploy lab resources using Terraform
4. Connect to your Kali Linux and Juice Shop servers

Protect Application – What You Will Do

Hands-On Setup Steps:

1. **Provision Azure Environment** – Submit your email and receive Azure credentials.
2. **Set Up Azure Cloud Shell** – Login → Select Bash → Mount the training storage account.
3. **Run Terraform** – Clone the repo and apply the template to deploy all lab resources.
4. **Start Kali RDP** – Use Guacamole to connect via browser and verify access.
5. **Check Juice Shop** – Browse to http://<ubuntu-ip>:3000 to confirm the app is running.

.

End Goal: Both Kali and Juice Shop accessible — ready for vulnerability labs.

FORTINET | USA

XPERTS

SUMMIT 2025

Lab Review

Section 2 On board the Application

On Board your Application – Goal and Context

From Deployment to Protection

Objective

Establish secure protection for a live web application by onboarding the **Juice Shop** into **FortiAppSec Cloud**, enabling cloud-based inspection and control.

1. All application traffic is routed **through FortiAppSec Cloud** for visibility and protection.
2. The **origin server is isolated** — only FortiAppSec Cloud can communicate with it.
3. **DNS and Azure NSG updates** ensure a hardened, trusted traffic path.
4. This setup lays the **foundation for hands-on attack simulation and mitigation labs**.

Protect Application – What You Will Do

In This Section You Will:

1. **Access FortiAppSec Cloud** — log in with your student credentials.
2. **Onboard the Juice Shop App** — register it as a protected application.
3. **Connect the Backend** — verify origin server and CNAME resolution.
4. **Update DNS & Azure NSG** — restrict access to FortiAppSec Cloud only.
5. **Verify Protection** — confirm traffic flows securely through FortiAppSec Cloud.

.

Result:
Your application is now live, protected, and ready for the upcoming attack-simulation and mitigation labs.

FORTINET | USA

XPERTS

SUMMIT 2025

Lab Review

Section 3 Simple Attacks

Simple Attacks– Goal and Expected Outcome

Defending Against Known Web Application Attacks

Goal

Understand and demonstrate how FortiAppSec Cloud detects and blocks *known web application attacks* such as **SQL Injection**.

1. FortiAppSec Cloud uses **signature-based detection** to quickly identify these patterns.
2. Students will observe how enabling **Block Mode** stops malicious input and records it as a *known attack event* in the dashboard

Outcome: Recognize how WAF signatures provide immediate protection against known threats while highlighting where additional defenses (positive security, parameterized queries) fit in.

FortiGuard Services for FortiAppSec Cloud

SECURED BY FORTIGUARD®

WAF Security Service

- Application layer signatures
- Web Application signature to prevent any web attack
- Machine learning threat models
- Malicious Bots

IP Reputation

- Protection for automated attacks and malicious sources
- DDoS, Phishing, Botnet, Spam, Anonymous proxies and infected sources

Antimalware

- Scan file uploads
- Regular and extended AV databases
- Protect the network against exploitable vulnerabilities

FortiSandbox Cloud

- FortiSandbox hosted by Fortinet
- Subscription-based
- No separate sandbox required

Credential stuffing Defense

- Identifies login attempts using stolen credentials from numerous sources
- Automatic updates
- Prevents unwanted access and defends against data breaches

Threat Analytics

- AI based Threat Analytics
- Identifies common characteristics and patterns and groups them into meaningful security incidents
- Incident risk prioritization

Simple Attacks– What You Will Do

In This Section You Will:

1. **Enable Block Mode** – Navigate to **Applications** → **Block Mode**, toggle ON.
2. **Run a SQLi Test** – In your browser, append a test payload (e.g., ?id=1 OR 1=1--) to the target URL.
3. **Observe the Result** – A block page appears; FortiAppSec logs the event as *A03:2021 Injection – SQL Injection*.
4. **Inspect the Console** – Go to **Threats** → **Known Attacks** and expand the entry to view: Matched signature ID pattern, Request headers and payload, OWASP Top-10 reference and timestamp
5. **(Optional)** Explore the **Search Signature** view to see how the detection pattern matches known SQL injection keywords and encodings.

.

FORTINET | USA

XPERTS

SUMMIT 2025

Lab Review

Section 4 Web Attacks

Advanced Attacks: Goal and Context

Objective
recognize attack patterns, understand why classic defenses fail, and validate signature & token-based mitigations.

1. Move beyond simple scans — we're testing *more sophisticated* web attacks.
2. Focus: **SQL Injection** and **Cross-Site Request Forgery (CSRF)**.
3. SQL Injection → direct data compromise, privilege escalation, data exfiltration.
4. CSRF → unauthorized actions performed in an authenticated user's context.

Learning goal: demonstrate FortiWeb signature behavior with advanced tooling and validate token-based mitigation techniques.

SQL Injection

Brief Explanation

- **What it is:** An attacker injects unexpected SQL into an input so the application runs unintended database commands.
- **Why it is dangerous:** Can read, modify, or delete sensitive data and escalate privileges.
- **Common indicators:** unusual WHERE clauses, sudden large data returns, errors with SQL keywords, unexpected SELECT/UNION in requests.
- **High-level example:** user input like ' OR '1'='1' -- could alter a query's logic.
- **Primary defenses:** parameterized queries / prepared statements, strict input validation & whitelisting, least-privilege DB accounts, WAF signatures and anomaly detection.

Understanding CSRF (Cross-Site Request Forgery)

When Trusted Sessions Are Tricked. Brief Explanation

- **What it is:** An attacker tricks a logged-in user's browser into sending unwanted requests to a trusted site.
- **How it works:** The user is *already authenticated* — so the malicious request carries their valid session cookies.
- **Impact:** Unauthorized actions (money transfer, password change, data deletion) executed as the victim.
- **Example:** A hidden form or image on an attacker's site silently submits a "Transfer $100" request to victim.bank.
- **Defense strategies:**
  - Use **CSRF tokens** for every state-changing request.
  - Enforce **SameSite cookies**.
  - Verify **Referrer / Origin** headers.
  - Combine with WAF and behavior-based detection.

Advanced Attacks– What You Will Do

In This Section You Will:

1. **Observe** — review sample HTTP requests and server logs to identify suspicious patterns.
2. **Exploit demo** — safe, contained demo: trigger SQLi read and a CSRF action on the test app.
3. **Analyze** — map attack vectors to vulnerable inputs and session flows.
4. **Apply defenses**
   - Deploy/verify WAF signatures & parameter validation for SQLi.,
   - Enable/validate anti-CSRF tokens and SameSite cookie settings for CSRF.
5. **Tune & retest** — refine signature thresholds, false-positive checks, and re-run test cases.
6. **Validate telemetry** — confirm alerts, logs, and blocking behavior; capture evidence for the report.

.

FORTINET | USA

XPERTS

SUMMIT 2025

Lab Review

Section 5 API protection

Protecting APIs – Goal and Context

Objective
Introduce **API Gateway** and **Schema Validation** — key features for controlling and securing API traffic.

1. FortiAppSec Cloud protects APIs by enforcing authentication (API keys) .

2. FortiAppseec validating requests against OpenAPI schemas

Protecting APIs - Use-Cases and Protections

JSON/XML bombs

Advanced Bot Protection

Object Access Control, token security

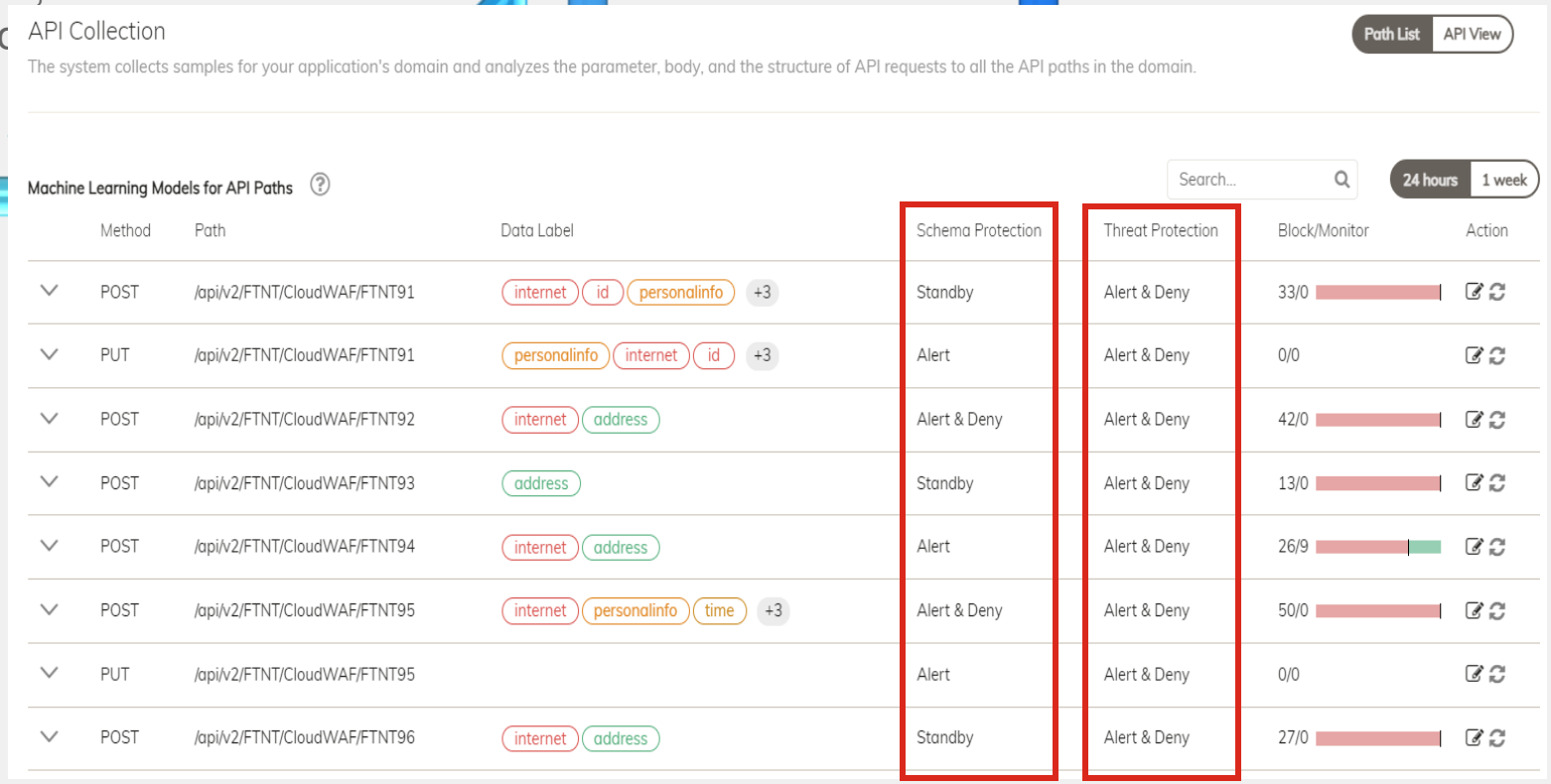
Anomaly Detection, limit HTTP methoc

Mitigate Denial of Service

For REST API

API Discovery and PII Catalog

Validate and enforce schemas and API endpoint access



Protecting APIs – What You will Do

In This Section You Will:

1. **Call an API using Postman** – verify how API data is retrieved.
2. **Enable API Gateway** – configure key-based access control for your Juice Shop API.
3. **Apply Schema Protection** – upload and test OpenAPI validation to block malformed requests.
4. **Validate Results** – use Postman to confirm allowed and blocked requests and review logs in FortiAppSec Cloud.

FORTINET | USA

XPERTS

SUMMIT 2025

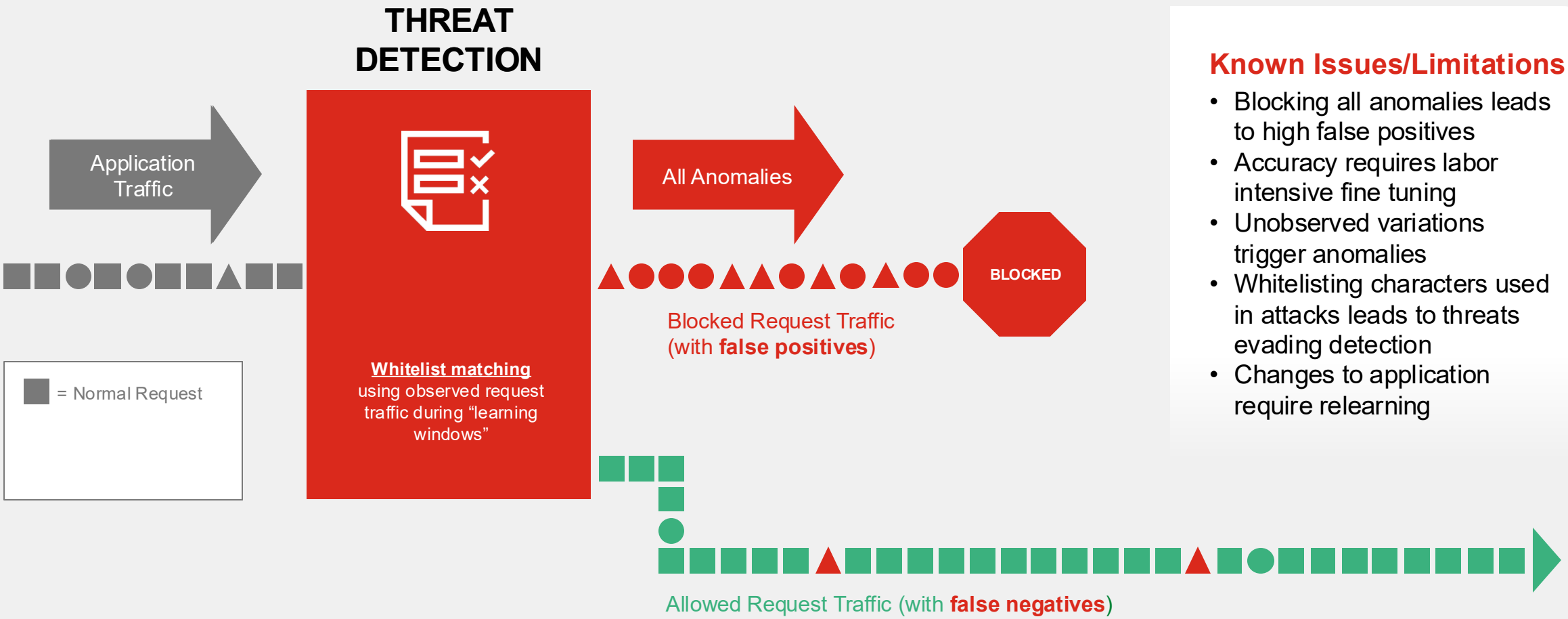
Lab Review

Section 6 Machine Learning

Positive Security Model and Machine Learning – Goal & Context

- FortiAppSec uses **machine learning** to make this approach practical — it learns normal URL, parameter, and method patterns and spots anomalies automatically.
- Two ML layers:
  - **Anomaly Detection** — builds baseline of legitimate activity.
  - **Threat Detection** — checks if flagged anomalies match known attack types (SQLi, XSS, etc.).
- This combination provides strong protection against **zero-day and evolving threats**.

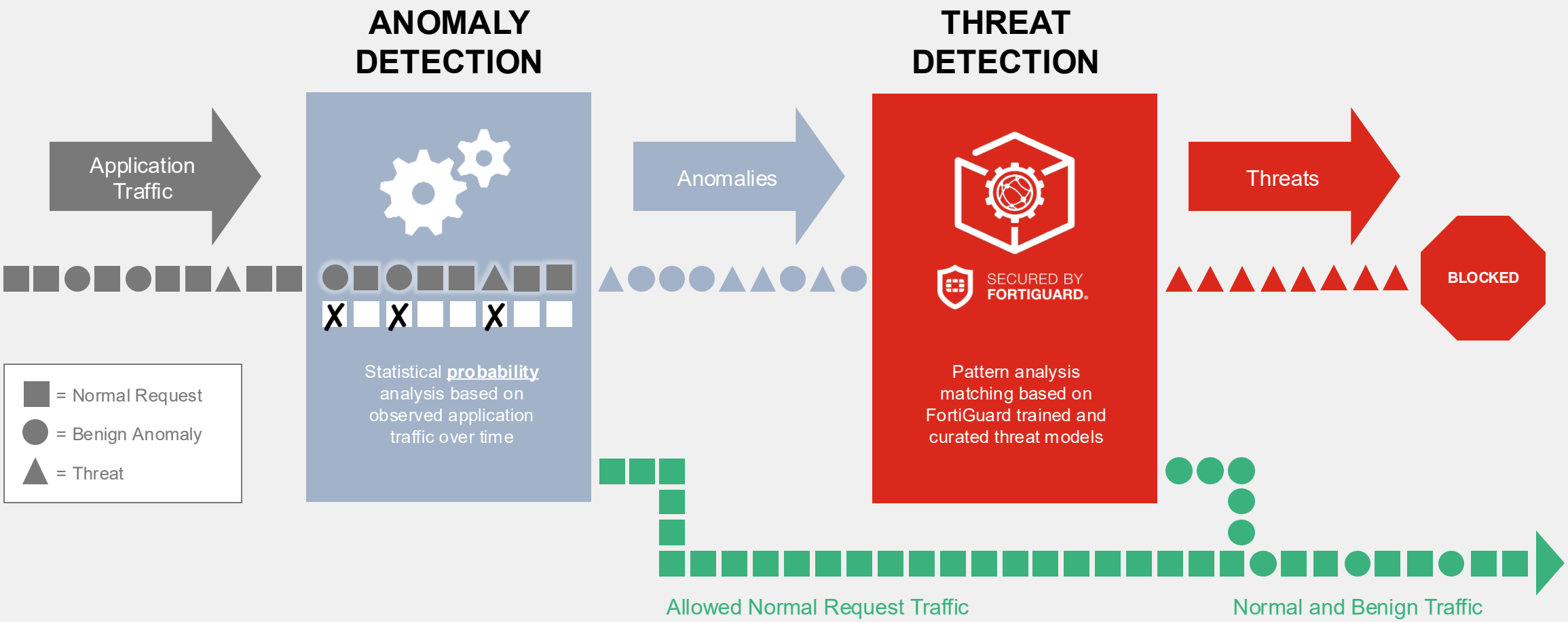
Common WAF Learning



Known Issues/Limitations

- Blocking all anomalies leads to high false positives
- Accuracy requires labor intensive fine tuning
- Unobserved variations trigger anomalies
- Whitelisting characters used in attacks leads to threats evading detection
- Changes to application require relearning

FortiAppSec WAF Machine Learning



Reduce friction when deploying web applications!

How FortiWeb ML Works - Simplified

https://www.example.com/insert?firstname=Mark&lastname=Smith

User sends "Mark Smith" in application form field for NAME

FortiWeb ML expects letters only in this field.

FortiWeb ML see this as **Normal Application Traffic**

ALLOWED

Normal Application Traffic

FortiWeb ML matches entry against characters normally expected for the field and typical length of field entry

https://www.example.com/insert?firstname=Janette&lastname=Smit&

User accidentally sends "Janette Smit&" in application form field for NAME

FortiWeb ML predicts that this as **an Anomaly from normally expected field entries but not a threat**

ALLOWED

Anomalies

ATTACKS

SECURED BY FORTIGUARD®

Support Vector Machine (SVM) separates threats from anomalies using vector patterns from FortiGuard Labs

User sends "SELECT *.* FROM CUSTOMER" in application form field for NAME

FortiWeb ML with FortiGuard SVM predicts that this as **an Anomaly AND AN ATTACK**

BLOCKED

https://www.example.com/insert?firstname="SELECT *.* FROM CUSTOMER"

Protect Application – What You Will Do

In This Section You Will:

1. **Enable** the Anomaly Detection module in FortiAppSec Cloud.
2. **Generate legitimate traffic** with ml-mix to let the model learn baseline patterns.
3. **Monitor model building** stages — Collecting → Building → Running.
4. **Run attack traffic** (≈ 30 %) to see ML detect SQL Injection, Command Injection, and XSS automatically.
5. **Review logs** in FortiAppSec Cloud to verify detections.

.

FORTINET | USA

XPERTS

SUMMIT 2025

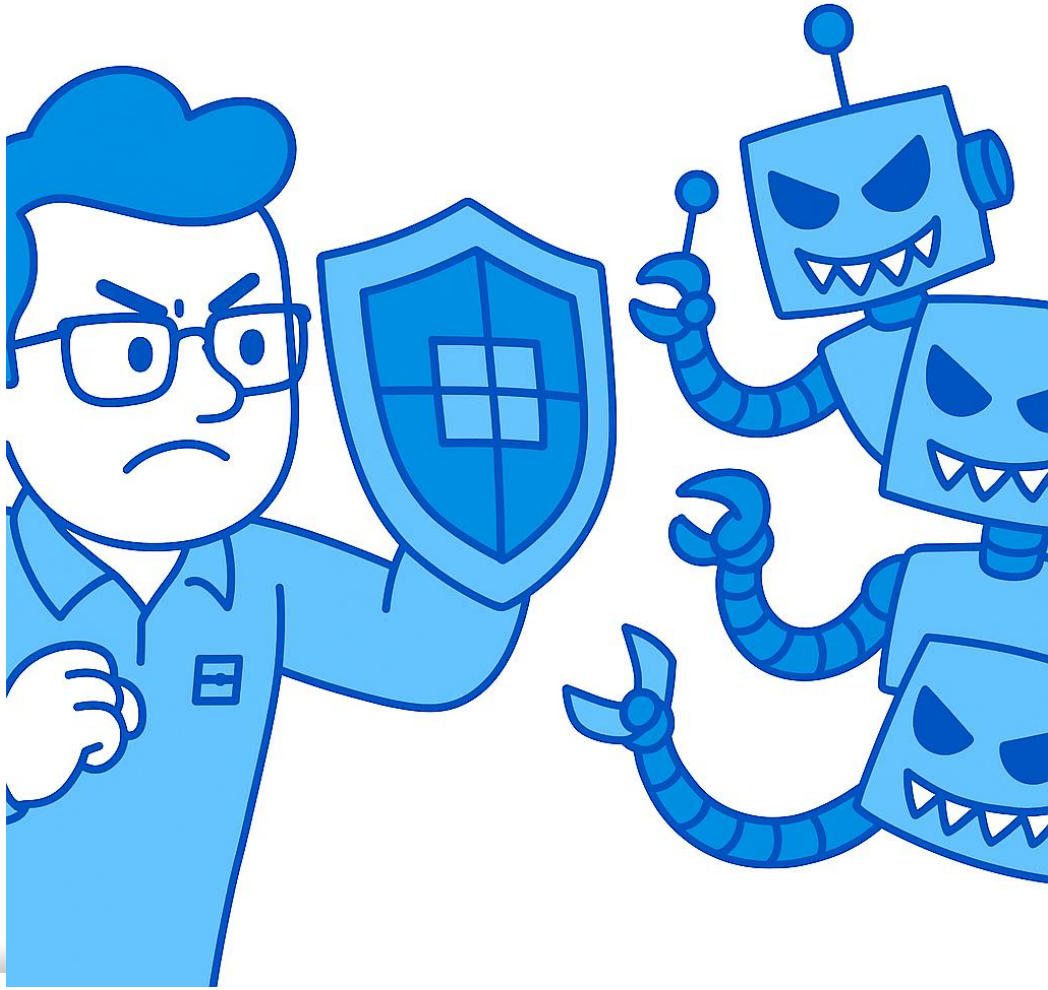
Lab Review

Section 7 Bot Mitigation

What Are Bots

Brief Explanation

- **What Are Bots?**
- Automated software programs that perform tasks over the internet — some helpful, others harmful.
- **Good Bots:**
  - Search engine crawlers (Google, Bing)
  - Monitoring or uptime services
  - Chatbots that assist users
- **Bad Bots:**
  - Credential stuffing and brute-force attacks
  - Data scraping and price scraping
  - DDoS and spam campaigns
- **Why They Matter:**
  - Nearly half of all internet traffic is bot-driven.
  - Without proper controls, bad bots can steal data, overload servers, and distort analytics.
- **How FortiAppSec Cloud Helps:**
  - Uses **behavioral analysis, deception, and machine learning** to separate humans from malicious automation



Bot Mitigation – Goal and Context

Objective

By the end of this chapter, you will understand how FortiAppSec Cloud detects and mitigates automated bot attacks using layered protection techniques.

1. **Biometric-Based Detection** – verifies human interactions.
2. **Threshold-Based Detection** – identifies abnormal frequency or timing.
3. **Bot Deception** – plants invisible “traps” for bots.
4. **Known Bots** – allows or blocks based on reputation and intent.
5. **Machine-Learning Detection** – uses ML to learn traffic profiles and detect anomalies.

Bot Mitigation

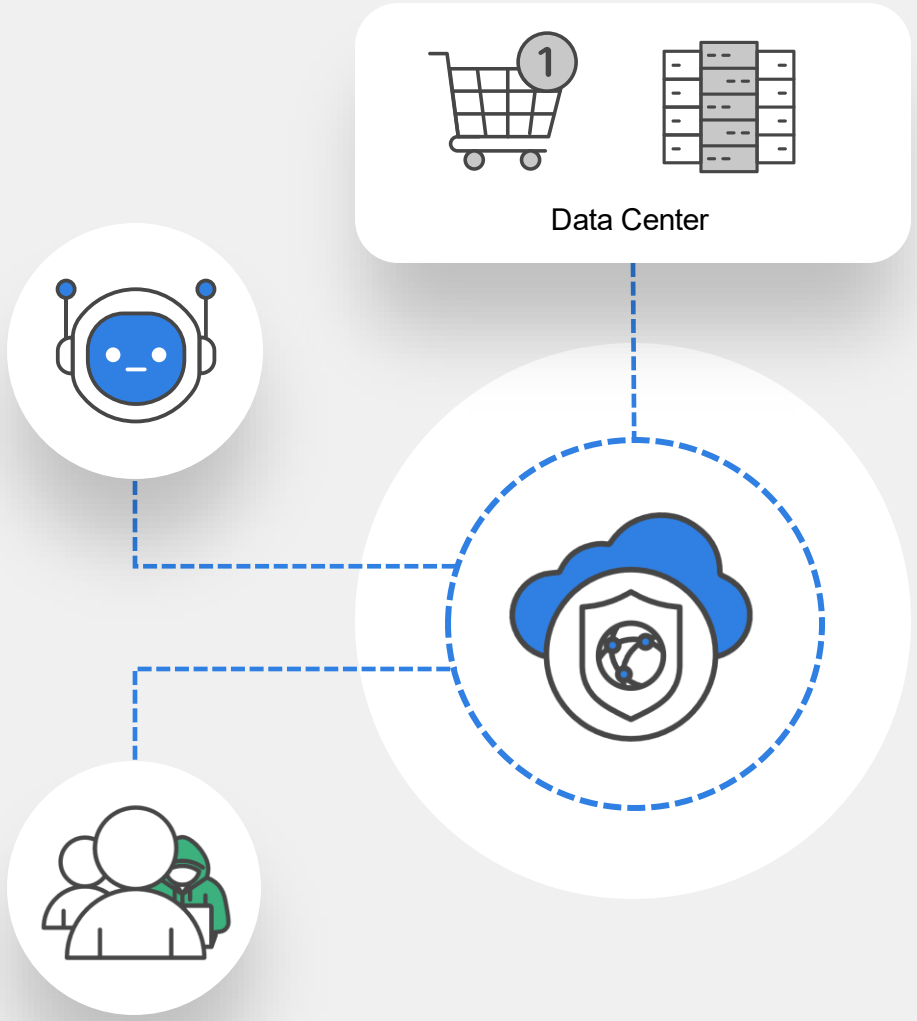
Bot Defense

Known Bots/ Signatures
- Crawler Detection/Limit

Browser Fingerprinting Detection
- Detecting Crawler-Specific Attributes
- Checking Browse/OS Inconsistencies

Biometric-based Detection
- Monitor client events

AI Analysis
- Deep Learning & Data Correlation
- Multiple Dimensions Comparing



Protect Application – What You Will Do

In This Section You Will:

1. **Enable Modules:** In *WAF > Add Modules*, switch on *Known Bots*, *Threshold*, *Biometric*, and *Bot Deception*.
2. **Configure Each Module**
3. **Known Bots:** set *Alert & Deny*, enable *Known Bad Bots*.
4. **Threshold:** enable *Crawler*, *Vulnerability Scanning*, *Slow Attack*, *Scraping*, *Brute Force*.
5. **Biometric & Deception:** create sample rules (e.g., /photo, /about).
6. **Simulate Bot Traffic:** Run the ./bots tool from Kali to generate mixed traffic.
7. **Verify Results**
8. Check *Threat Analytics → Bot Attacks* and *Attack Logs* to confirm blocked bots.

FORTINET | USA

XPERTS

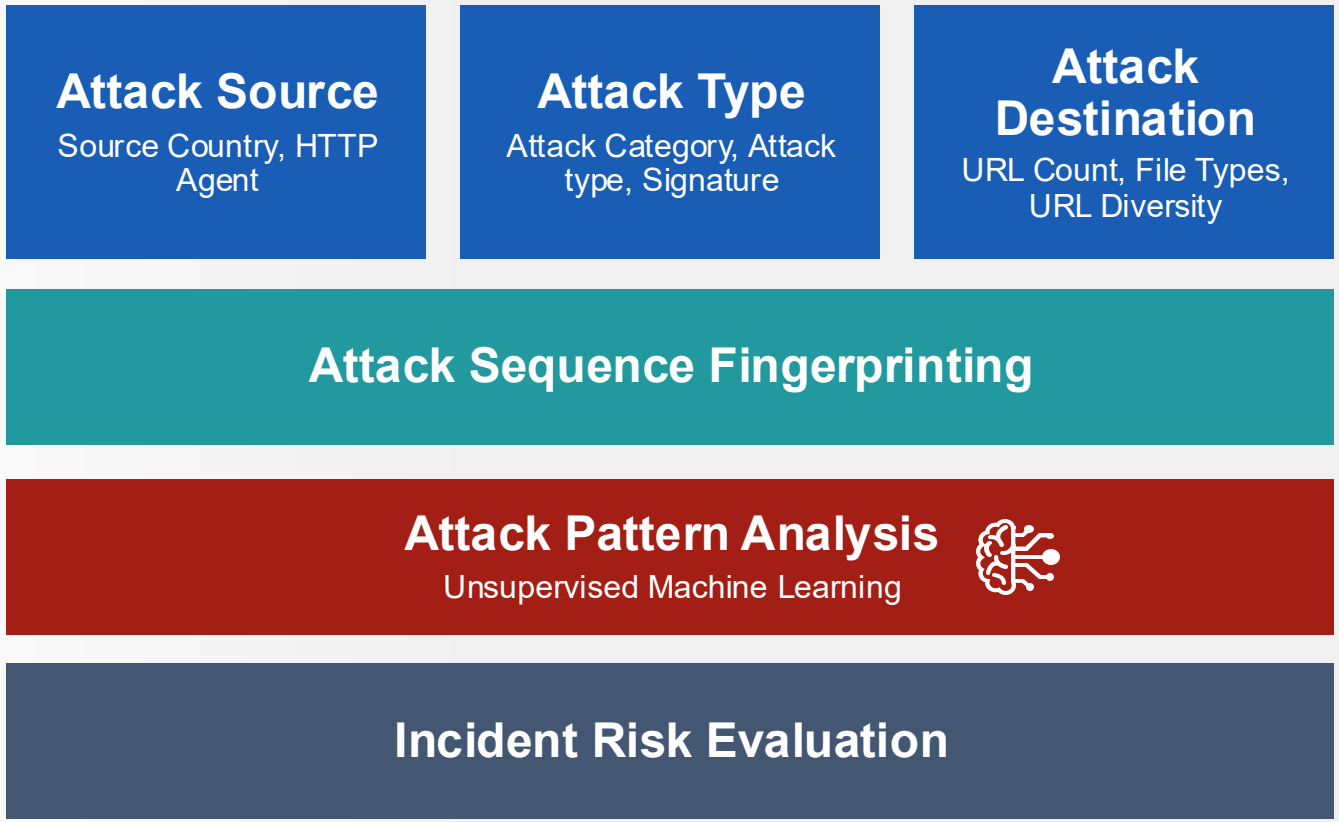
SUMMIT 2025

Threat Analytics

Threat Analytics

FortiWeb Threat Analytics uses machine learning algorithms to identify attack patterns and aggregate them into security incidents across customer entire application assets.

- Aggregate attacks into sequences
  - Same source and destination
  - No match for 60 min
- Create fingerprints for attack sequences
- Use ML to identify patterns in fingerprints
- Aggregate sequences into incidents
- Evaluate incident risk. Severity is impacted by –
  - Severity of every attack in incident
  - Number of attacks in incident
  - Variety of attack types



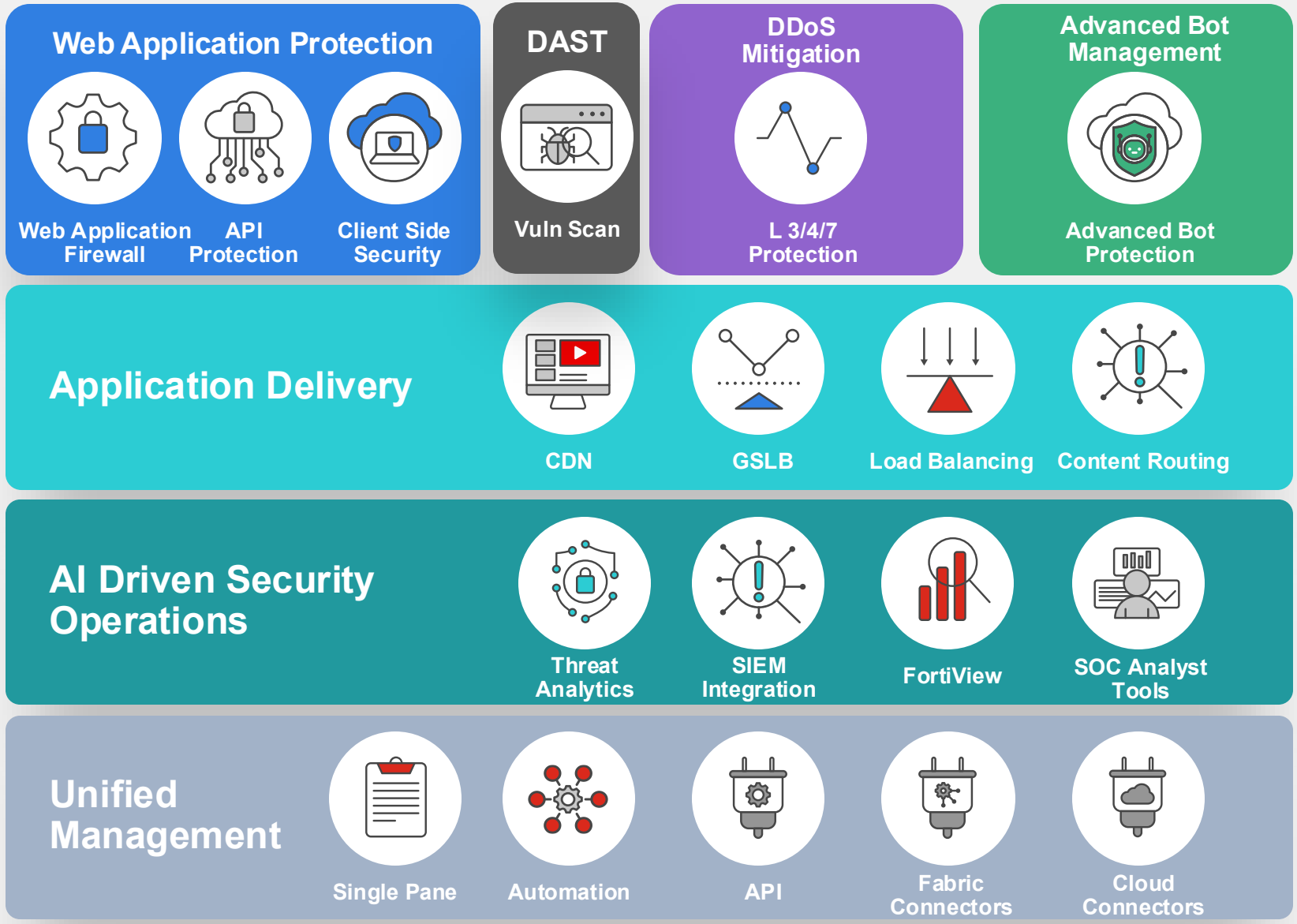
FORTINET | USA
XPERTS
SUMMIT 2025

Summary

FortiAppSec Cloud

Customer Benefits

- Cover the application attack surface
- Simplify detection and response
- Deliver consistent security policy
- Ensure availability and continuity
- Optimize application performance
- Central management and visibility



Industry Context

Always-on

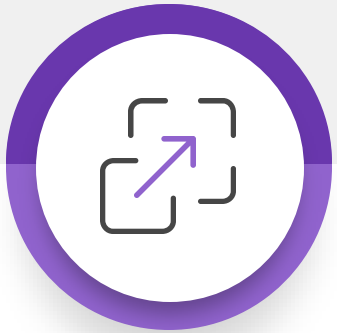
Need for integrated, scalable, and secure application delivery services to ensure uptime.

Cloud Adoption

The growing complexity of managing security across hybrid and multi-cloud environments.

Evolving Threats

Rise in sophisticated cyberattacks targeting web applications and APIs.



Solution Consolidation

Demand for unified, scalable solutions with consistent policies to protect critical applications.

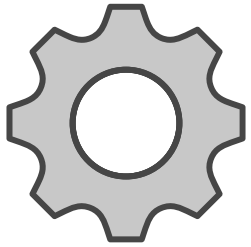
FortiAppSec Business Advantages

Cost-effective exposure management as the business value extends beyond security

Zero-day Protection

at high accuracy & min. false positives

Simplify Operations



Prioritize risk mitigations and increase productivity

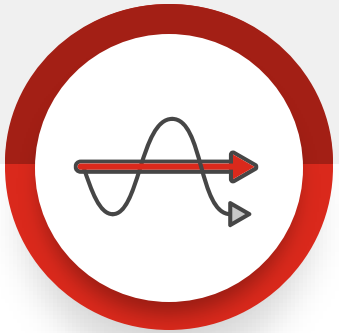
Flexible Consumption, Predictable Spend

With the upcoming FortiFlex Program

Visibility and Control

Consistency in management and enforcement

Business Benefits



Complexity Reduction

Simplify management of multiple security solutions across hybrid and multi-cloud environments, reducing resource intensity.

AI Generated Attacks

Adaptive protection against increasing zero-day exploits and sophisticated bot attacks targeting web and API applications.

Global Availability

Ensure consistent application availability across diverse global environments.

Compliance

Provide 360-degree observability for compliance management across applications.

Gartner Peer Insights

"The set-up and configuration of this product… was completed in 1 hour… Very satisfied with this solution."

50 ★★★★★

"Substantially improved the security and detection of attacks on our web applications"

50 ★★★★★

"Excellent Products and Services, Easy Management and Usage"

50 ★★★★★

"Very easy to onboard and has many useful functions to protect our business."

50 ★★★★★

"Also, Fortinet Support is very responsive"

50 ★★★★★


FORTINET

FortiWeb Security Fabric Integration

FortiWeb can be configured to join a Security Fabric through the root or downstream FortiGate