
FORTINET
COLOMBIA
& ECUADOR
XPERTS26

FORTINET | COLOMBIA & ECUADOR

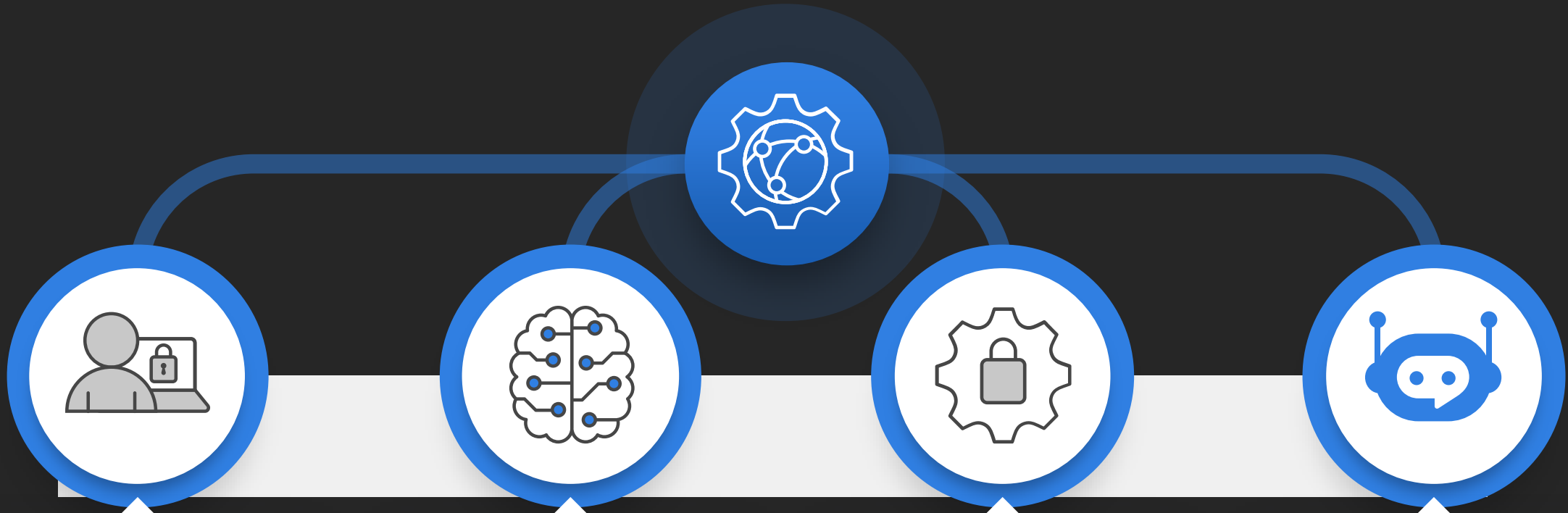
XPERTS26

FortiWeb AI Security

Fabián González Soto

Principal Systems Engineer

Agenda



Introduction

Machine Learning
Anomaly Detection

MCP Protection

Generative AI

WAF to WAAP: The Application Attack Surface Keeps Growing

Web Application and API Protection solutions today are expected to manage bot traffic, secure APIs, and mitigate DDoS Attacks

48% of the organizations have 100 or more unique applications in their environment

On average, companies publish **25** Software updates into production on a monthly basis

Over 85% of web traffic is API traffic

Nearly Half of internet traffic is bot-generated traffic

For the full report, go to https://go.fortinet.com/global-lp/aws-app-security-report

AI-Powered

WEB APPLICATION AND API PROTECTION

API Discovery and Protection

API Discovery using URL clustering with schema awareness, automatic schema generation, Anomaly Detection (HMM+SVM)

Threat Analytics

Analyze million of events using ML to identify common characteristics and patterns and group them into meaningful security incidents

Web Protection

Zero day attack protection using two layer solution (HMM and SVM), Anomaly verification, continuous learning

FortiAI-Assist

An AI SOC agent that accelerate threat detection, analysis, and response by providing business context and recommendations

Bot Mitigation

Behavioral learning using ML SVM based on 13 different traffic dimensions, automated verification using training samples

AI-Powered WAAP Protection

Detection

Learn application traffic to identify zero-day attacks, malicious bot behaviors and anomalous API calls

Risk Evaluation

Analyze suspicious patterns to get insights on severity levels

Decision Support

Translate insights to priorities and actions, and use the AI Assistant to investigate incidents further

Remediation

Take the necessary actions that reduce threat exposure substantially first, and correct misconfigurations

FortiWeb SOC-as-a-Service

24/7/365 Protection

Web application security around-the-clock

Incident Response

Triage, investigation and guidance

Security Hardening

Reports, reviews and prioritization

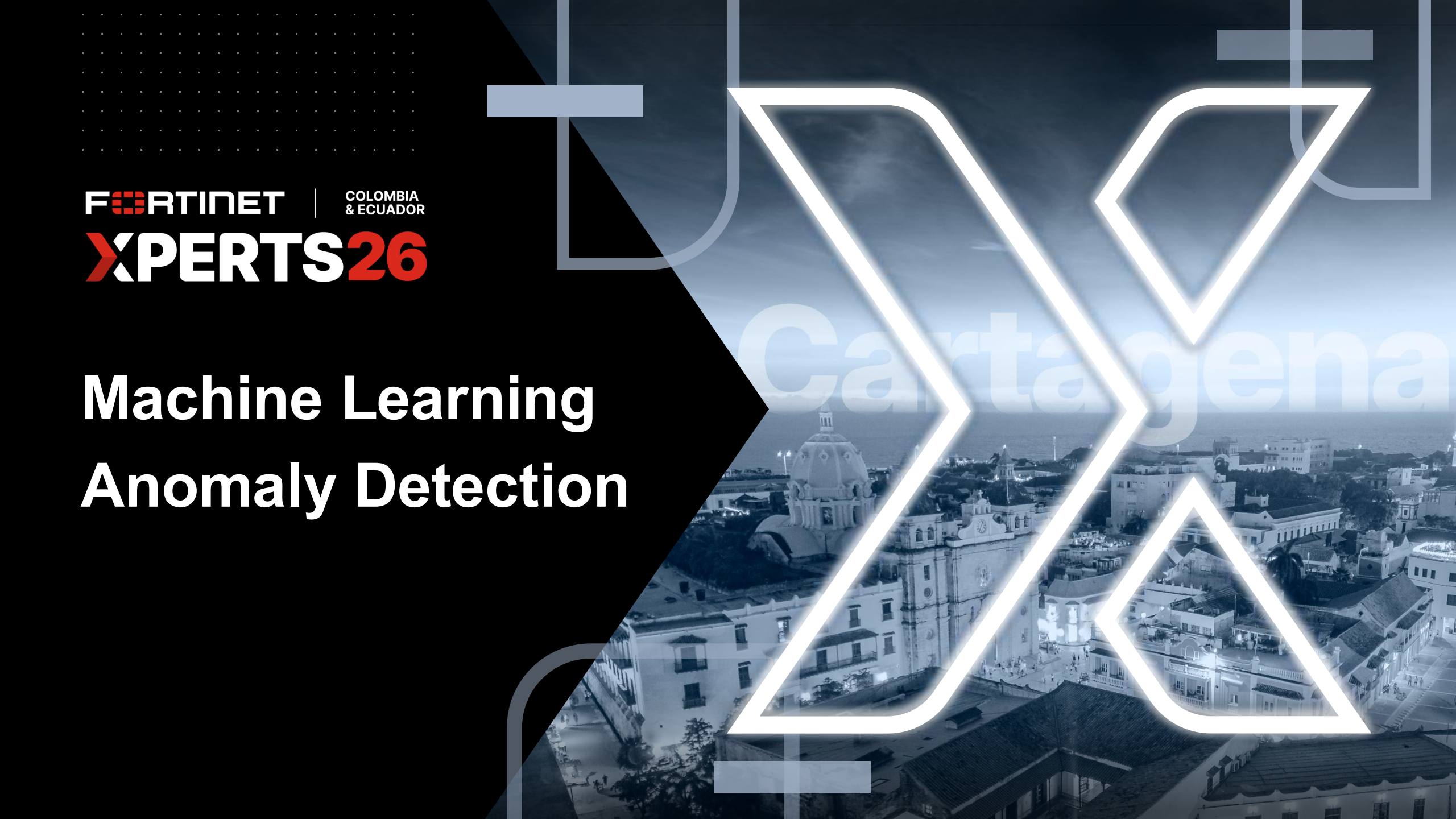
Cloud Service Portal

Continuous visibility into all protected assets

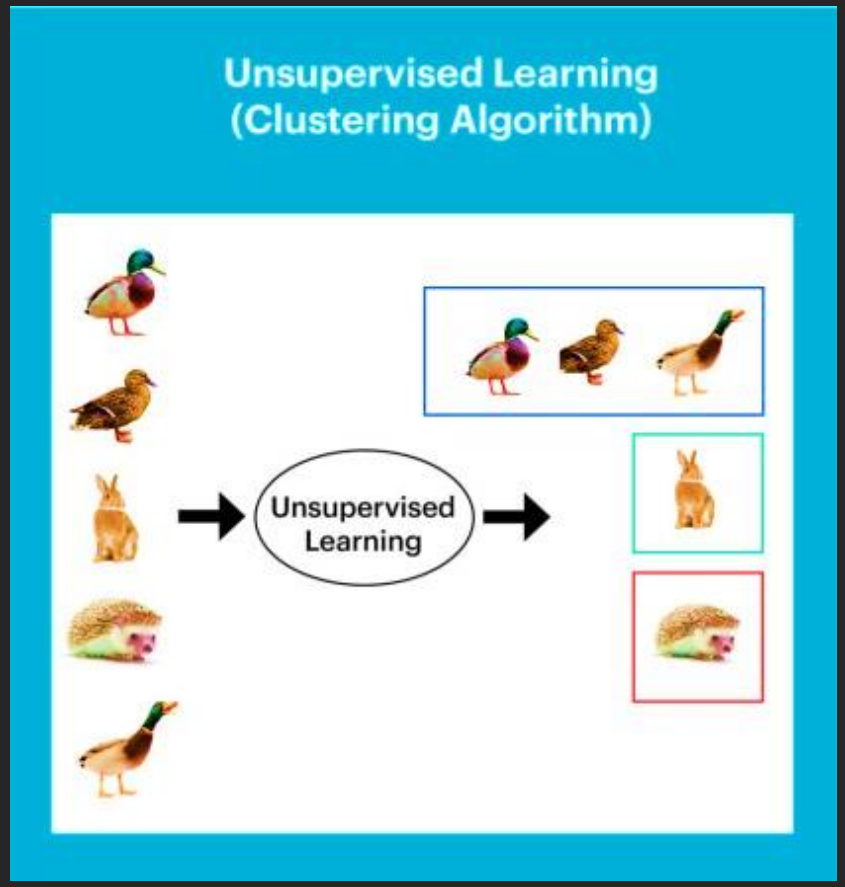
FORTINET | COLOMBIA & ECUADOR

XPERTS26

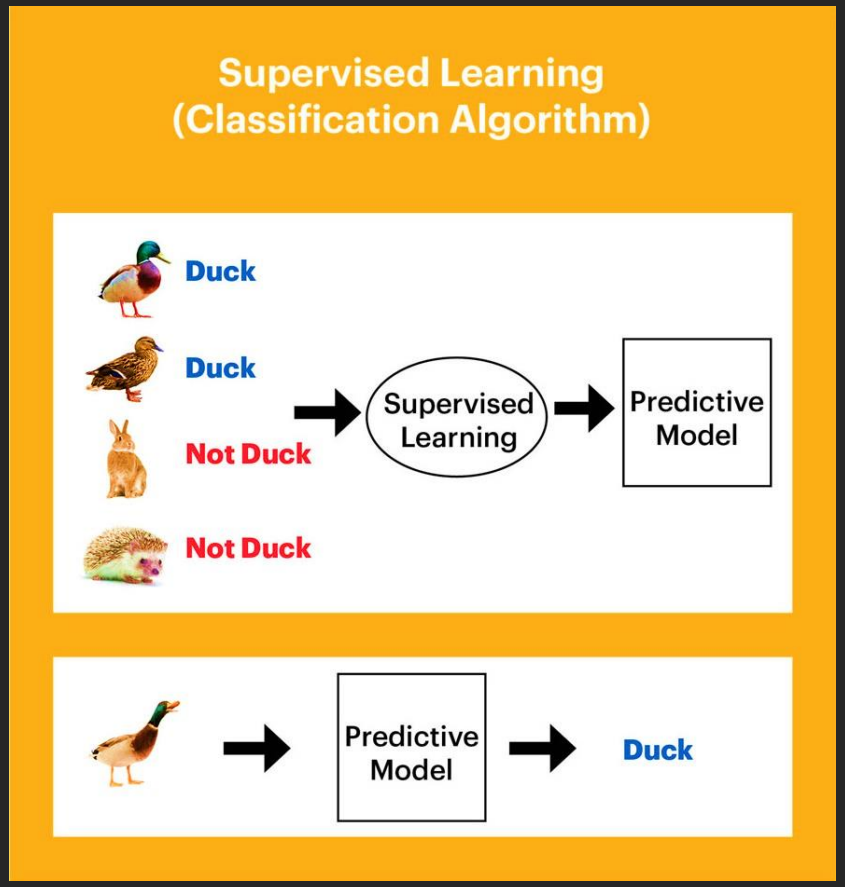
Machine Learning Anomaly Detection



Unsupervised vs Supervised Machine Learning



In Unsupervised Learning, the Machine Learning algorithm learns from Unlabeled Data



In Supervised Learning, the Machine Learning algorithm learns from Labeled Data

Unsupervised vs Supervised Machine Learning

USER	CONNECTION TIME	COUNTRY	NUMBER OF TRANSACTIONS
A	8:00 AM	Colombia	5
B	9:00 AM	Colombia	4
C	3:00 AM	Rusia	200

MAIL	LABEL
"Click here to earn money"	Spam
"Meeting tomorrow at 10 AM"	No spam
"Your account will be blocked"	Spam

The algorithm discovers patterns on its own.

Users who:

- Connect during working hours
- Connect from unusual locations
- Exhibit different behaviors

Then, when you receive a new email:
“Congratulations! You won a prize; click here”

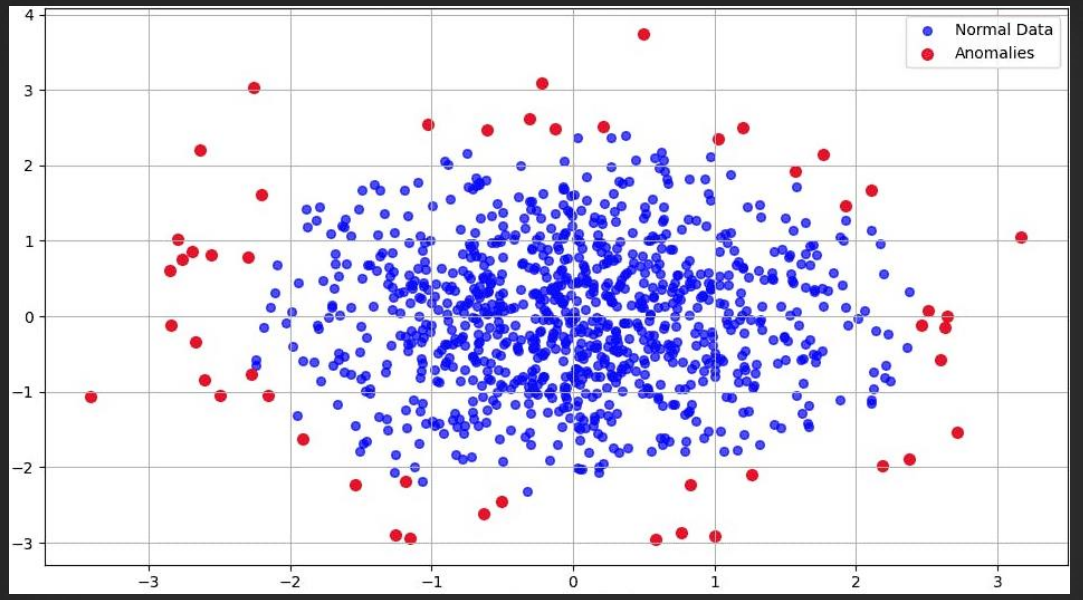
The model predicts:
→ **Probably Spam**

Machine Learning Anomaly Detection

Introduction

How it works?

- Behavior-based web traffic analysis (URLs, parameters, HTTP methods)
- Machine learning builds a baseline of normal application behavior
- Real-time anomaly detection by comparing requests to the learned model
- Two-layer ML architecture for higher accuracy



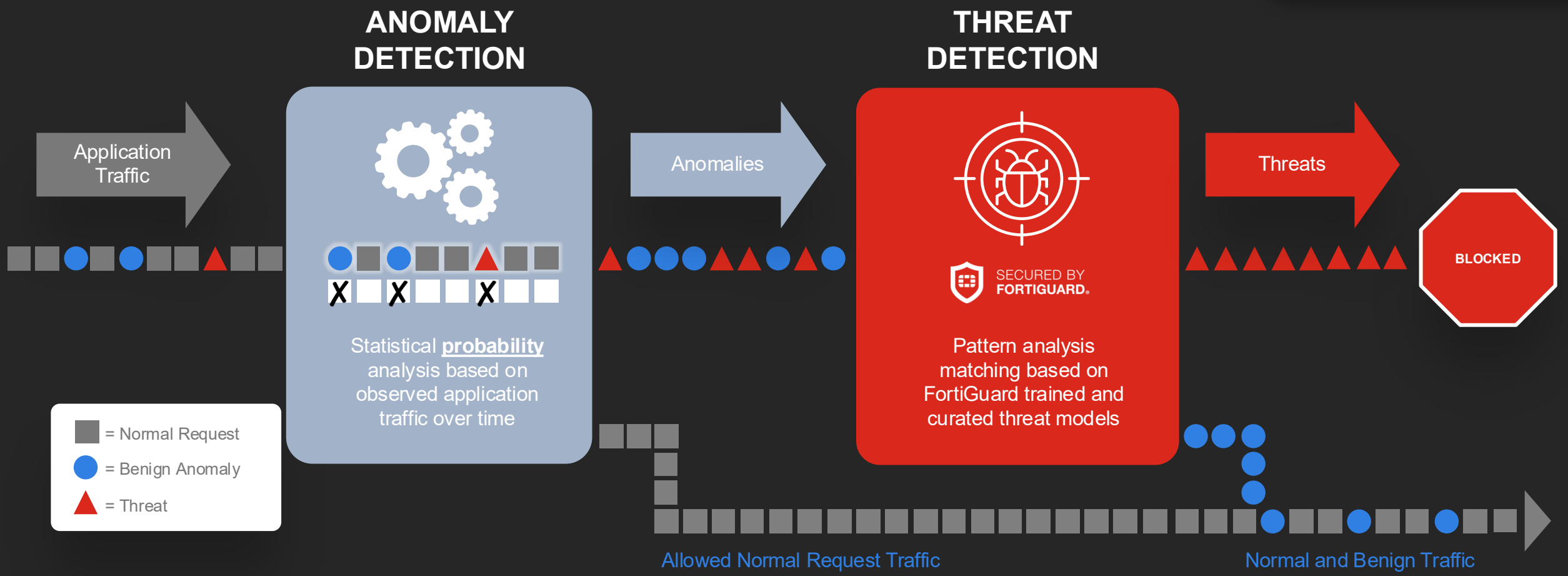
Zero-Day Protection | Behavioral Analysis | Adaptive Learning | Automated Protection

Low Latency Detection | False Positive Reduction | Accuracy

ML-Driven Highly Accurate Threat Detection

Reduce friction and false positives when deploying web applications

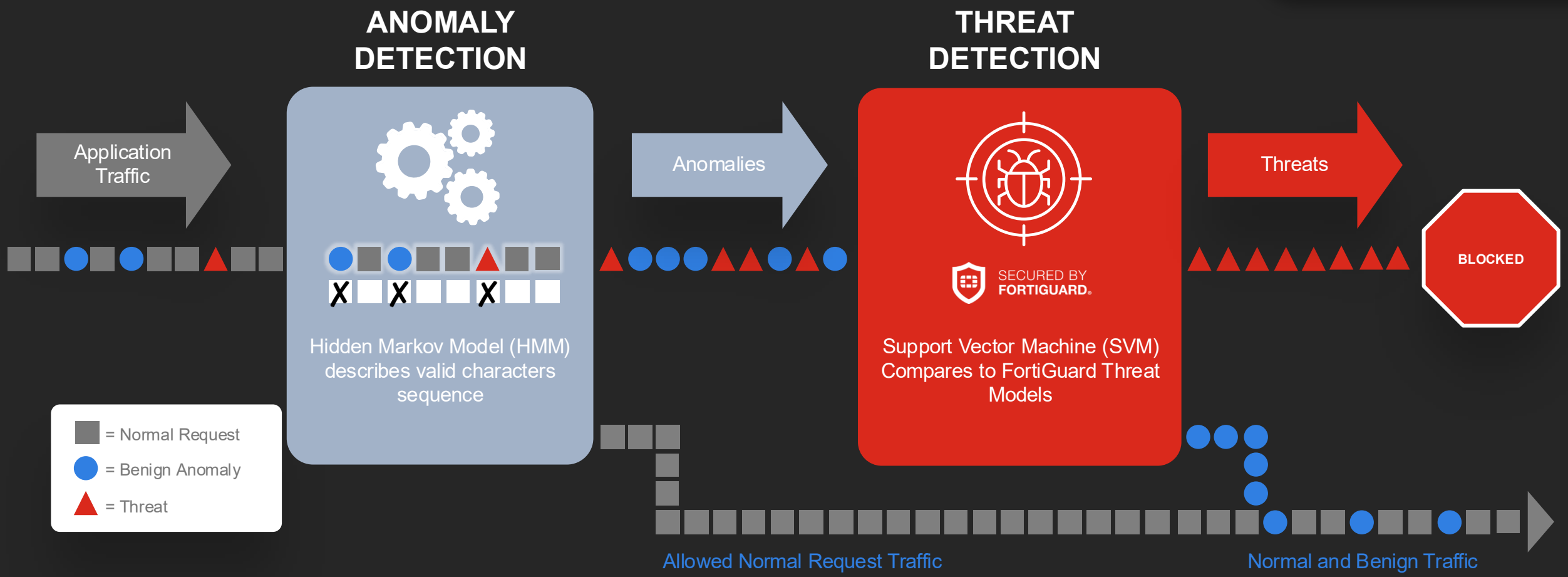
FortiAI-Protect
Protect Against AI Threats



ML-Driven Highly Accurate Threat Detection

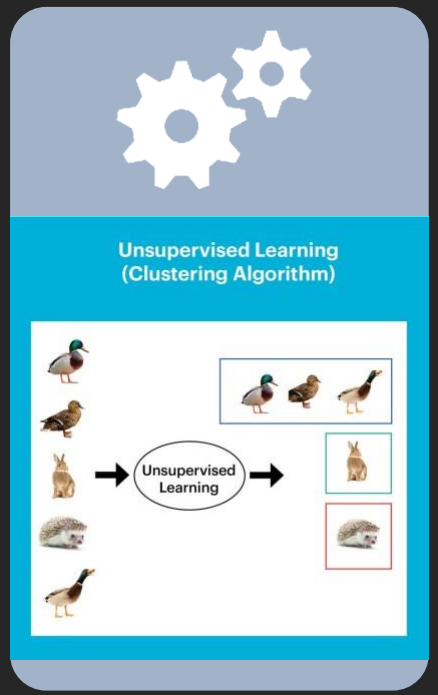
Reduce friction and false positives when deploying web applications

FortiAI-Protect
Protect Against AI Threats



Machine Learning Layer 1 for Anomaly Detection

ANOMALY DETECTION



1. **Phase 1**: Builds a State Machine Model per parameter that describes valid characters sequence input of Chars (**C**) Special Chars (**S**) Numbers (**N**)

2. **Phase 2**: Scores any new input to evaluate its level of anomaly

WEB APPLICATION

User ID: User Name

Password: ••••••••••••

LOGIN

abc_123@dom.com ➔ CSNSCSC

abc@dom.com ➔ CSCSC

<script>alert(hack)</script> ➔ SCSCSCSCS

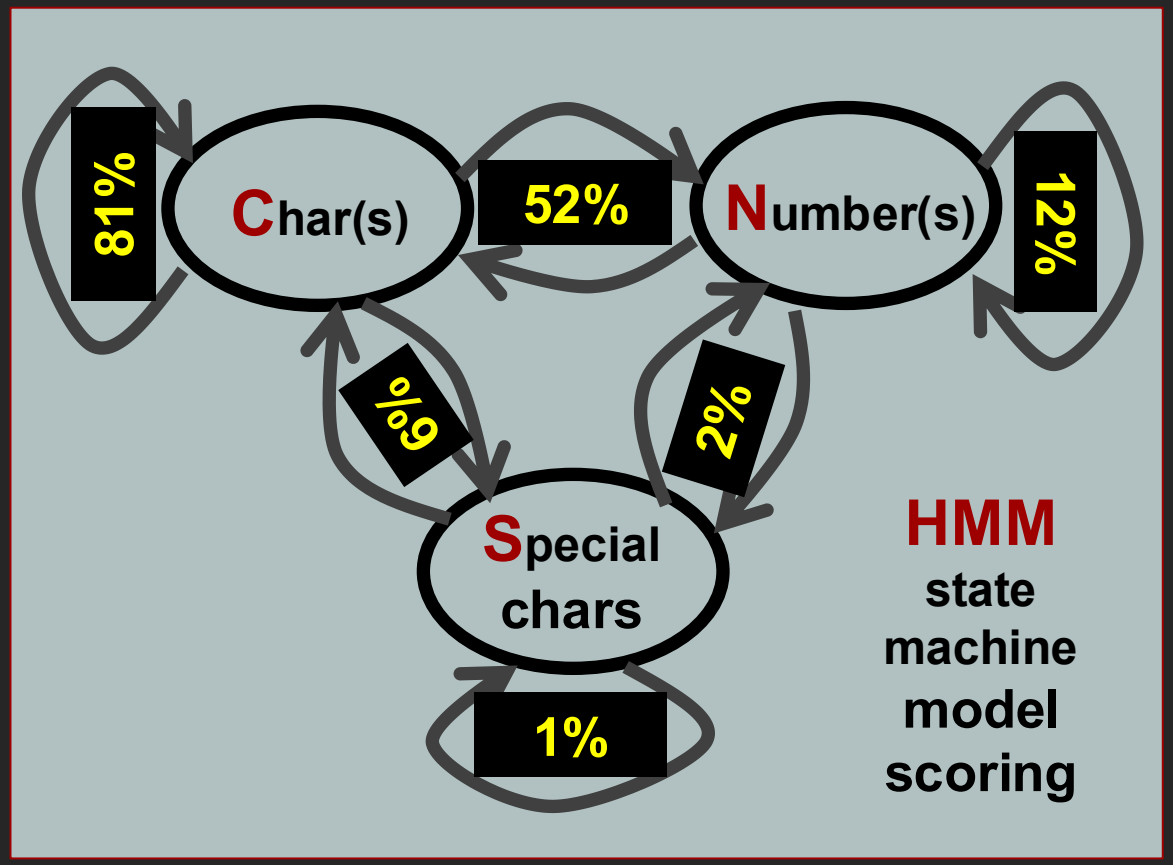
CSNSCSC ➔ Score = 0.5

CSCSC ➔ Score = 0.8

SCSCSCSCS ➔ Score = 4

Machine Learning Layer 1 for Anomaly Detection

Calculation of Threshold and Strictness



Threshold = μ + Strictness × σ

- **μ**

Average of the metric/observed probabilities in the model samples.

- **σ**

Standard deviation: represents the dispersion or variability of the samples.

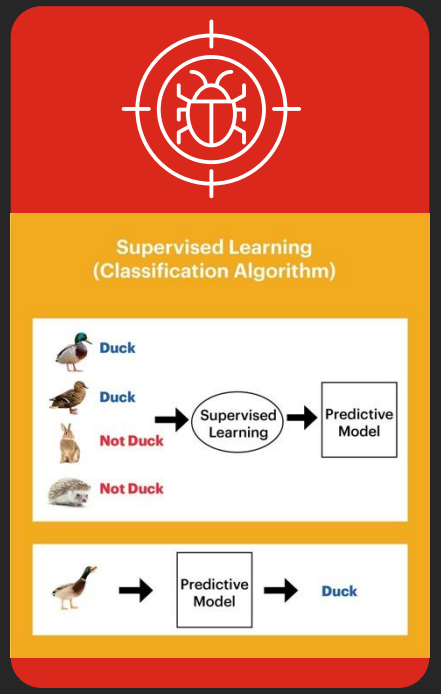
- **Strictness**

Sensitivity control: a lower value can make detection stricter.

NSE Important Changes

Starting on July 15, 2026

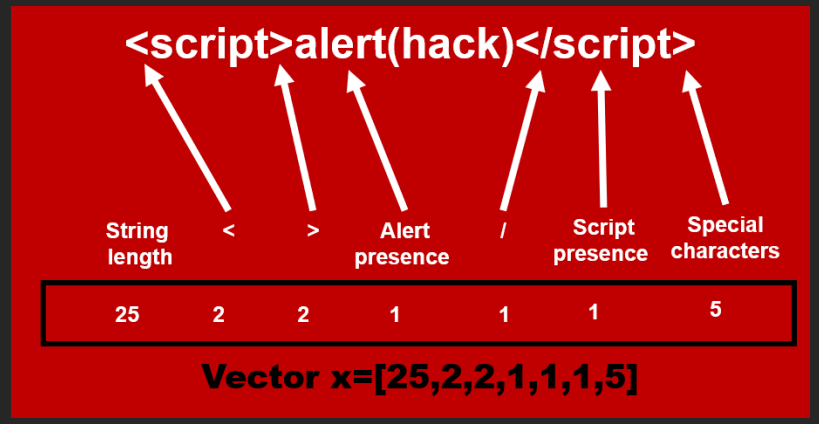
THREAT DETECTION

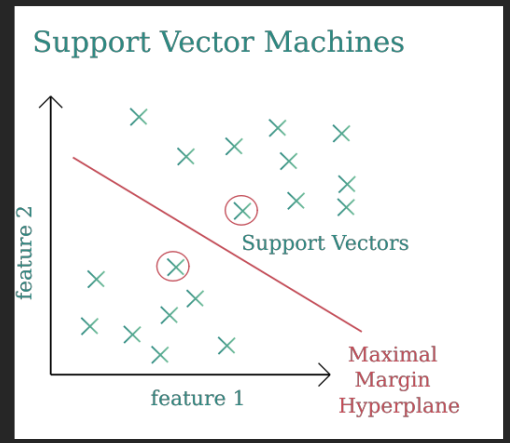


1. **Phase 1**: **converts** any detected anomaly from **text to vector**

2. **Phase 2**: compare it to **FortiGuard Threat Models** (SQLi, XSS, etc…) to evaluate if it's real attack or just a benign anomaly.

THREAT DETECTION

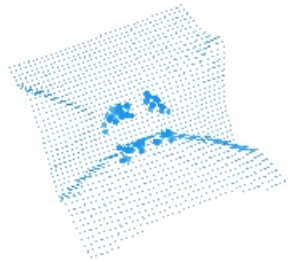




FortiWeb SVM Models

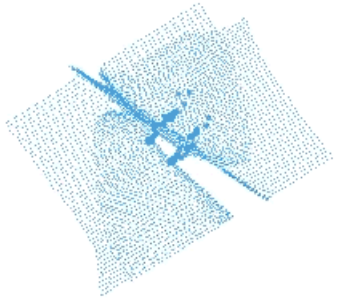
Well-trained Mathematical Model for Cross-site Scripting

Well-trained Support Vector Machine model with linear type kernel function for Cross-site Scripting attack.



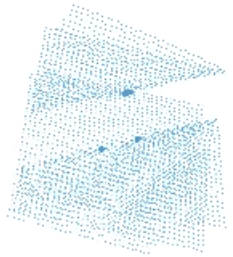
Well-trained Mathematical Model for Code Injection

Well-trained Support Vector Machine mode with sigmoid type kernel function for Code Injection attack.



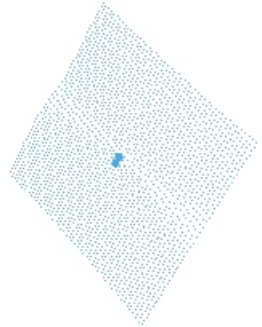
Well-trained Mathematical Model for Local File Inclusion/Remote File Inclusion

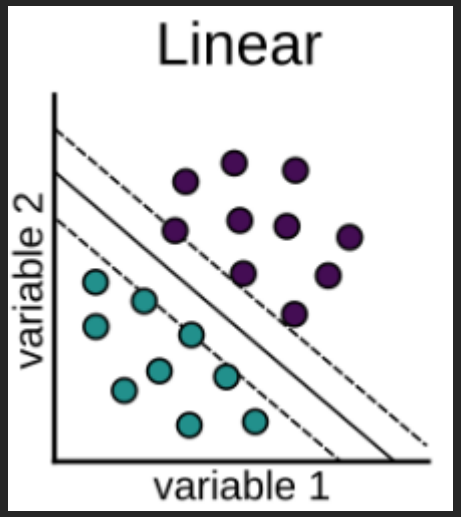
Well-trained Support Vector Machine model with radial basis type kernel function for Local File Inclusion/Remote File Inclusion attack.

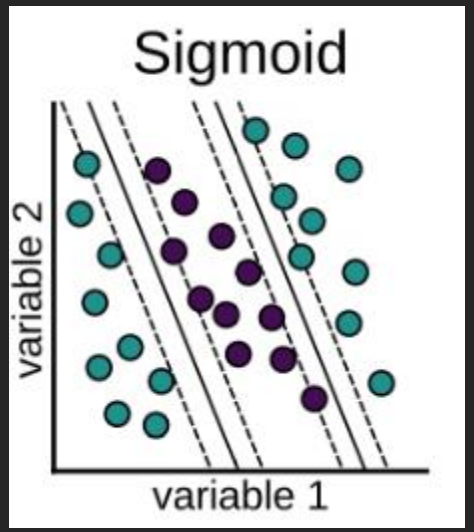


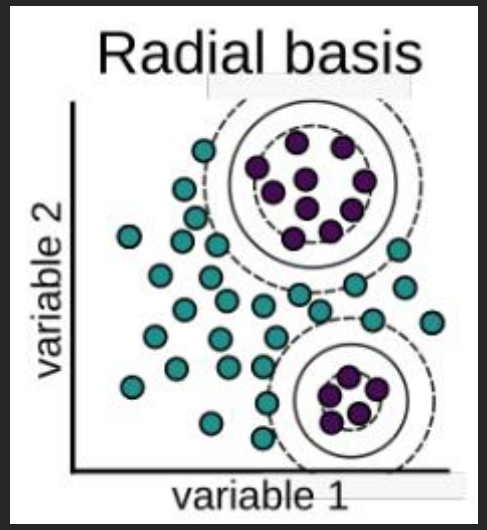
Well-trained Mathematical Model for Remote Exploits

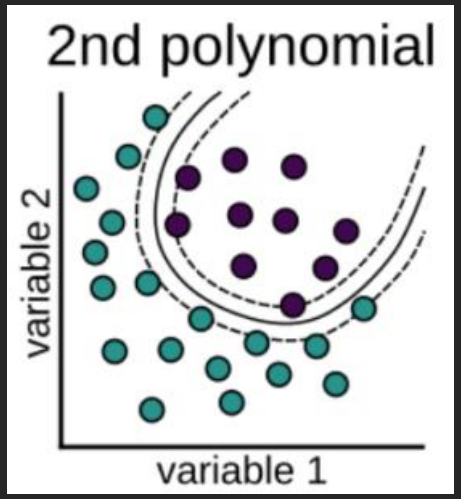
Well-trained Support Vector Machine model with polynomial type kernel function for Remote Exploits attack.



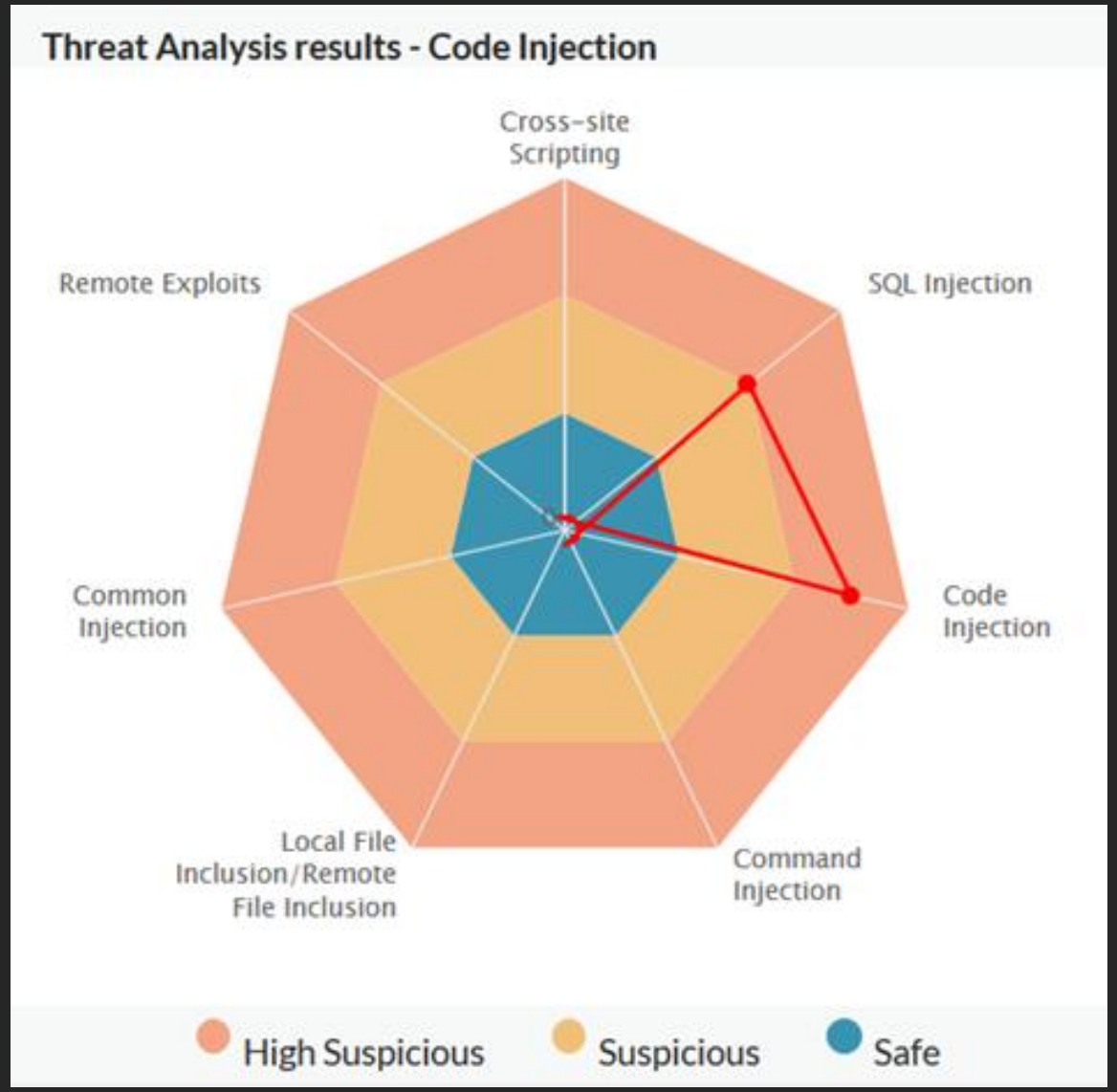








Block Multi-Vectors Attacks



Threat Model

- Well-trained Mathematical Model for Cross-site Scripting
  Well-trained Support Vector Machine model with linear type kernel function for Cross-site Scripting attack.
- Well-trained Mathematical Model for SQL Injection
- Well-trained Mathematical Model for noSQL Injection
- Well-trained Mathematical Model for Code Injection
- Well-trained Mathematical Model for Command Injection
- Well-trained Mathematical Model for Local File Inclusion/Remote File Inclusion
- Well-trained Mathematical Model for Common Injection
- Well-trained Mathematical Model for Remote Exploits
- Well-trained Mathematical Model for SSTI

FORTINET | COLOMBIA & ECUADOR

XPERTS26

MCP Protection

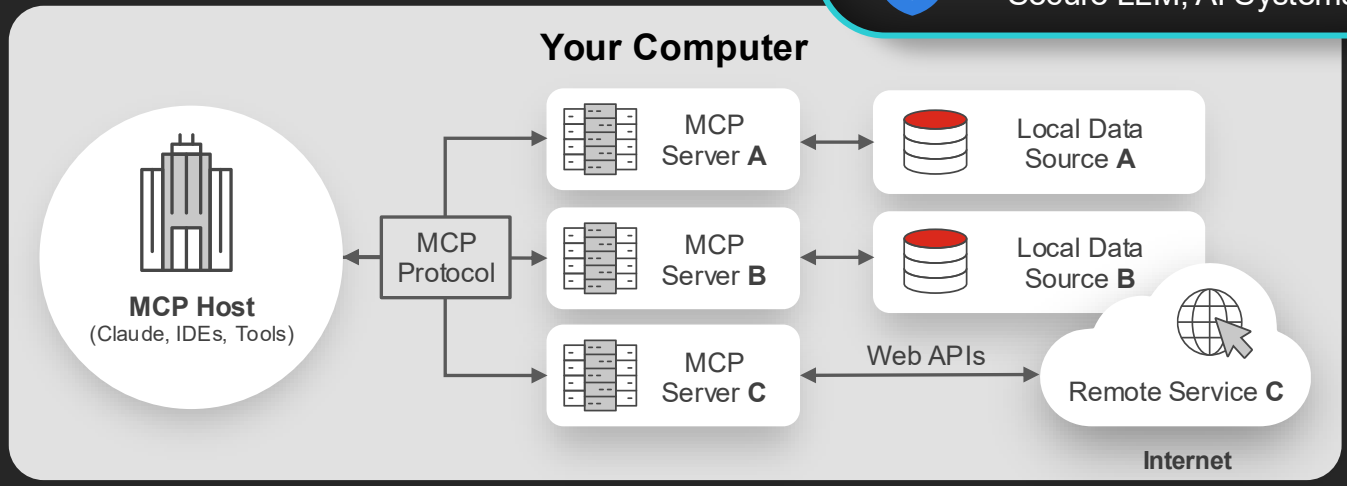
LLM Protection – MCP Protection

Model Context Protocol

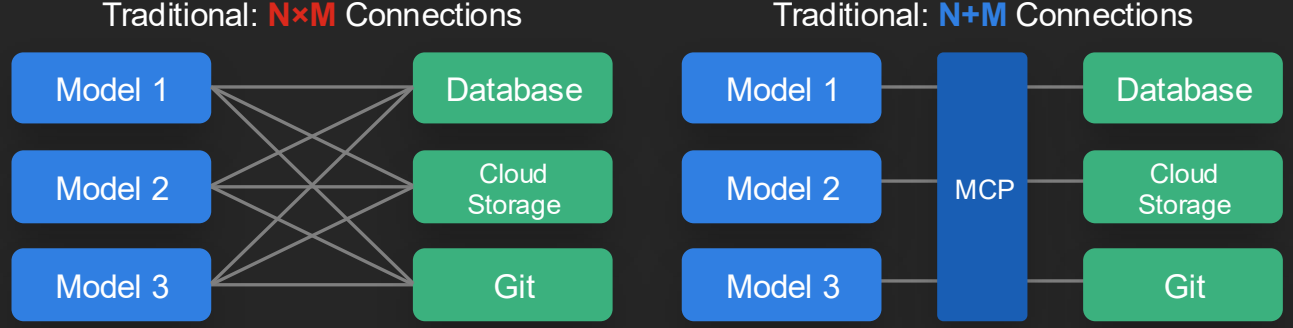
FortiAI-SecureAI
Secure LLM, AI Systems

Model Context Protocol

- Launched November 2024 by Anthropic the MCP standard allows LLMs to communicate with external services in a dynamic and modular way.
- Replaces static, narrow, specialized explicitly coded integrations for specific tasks
- Models and data sources only need to integrate once with MCP
- LLMs can now autonomously act across complex environments – but unguarded
- MCP Protection – another piece in the LLM protection puzzle



Traditional Integration vs MCP Approach



FortiWeb MCP Protection

Protect MCP servers from LLM abuse by enforcing API security policies

FortiAI-SecureAI
Secure LLM, AI Systems

The rapid evolution of MCP has also created a new and complex attack surface

Prompt Injection / Tool Poisoning

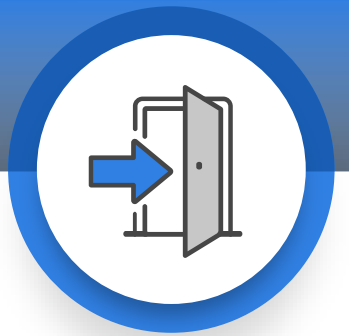
Attackers embed malicious instructions in tool des...

Continuous signature updates

Supply Chain Attacks

MCP is open source, attackers can publish malici... ...ckages

JSON schema validation



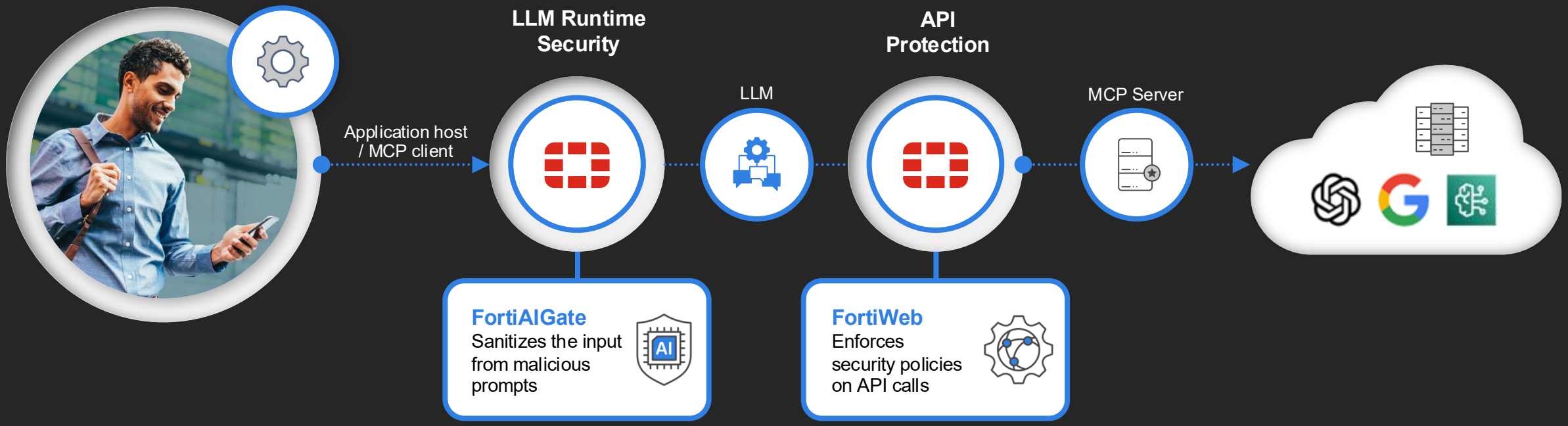
Architectural Flaws

Unauthorized access due to excessive pri...

Access lists, anomaly detection

LLM & MCP Protection

FortiAI-SecureAI
Secure LLM, AI Systems



FORTINET | COLOMBIA & ECUADOR

XPERTS26

Generative AI

FortiAI Assistant

FortiAI-Assist
Ai Assisted Operations

Proactive Alert Triage

Analyzing logs, identifying patterns, and automate fixes in an autonomous network

Agentic AI Reasoning

Autonomous, AI-driven decision-making that analyzes, reasons, and acts on threats or operational issues

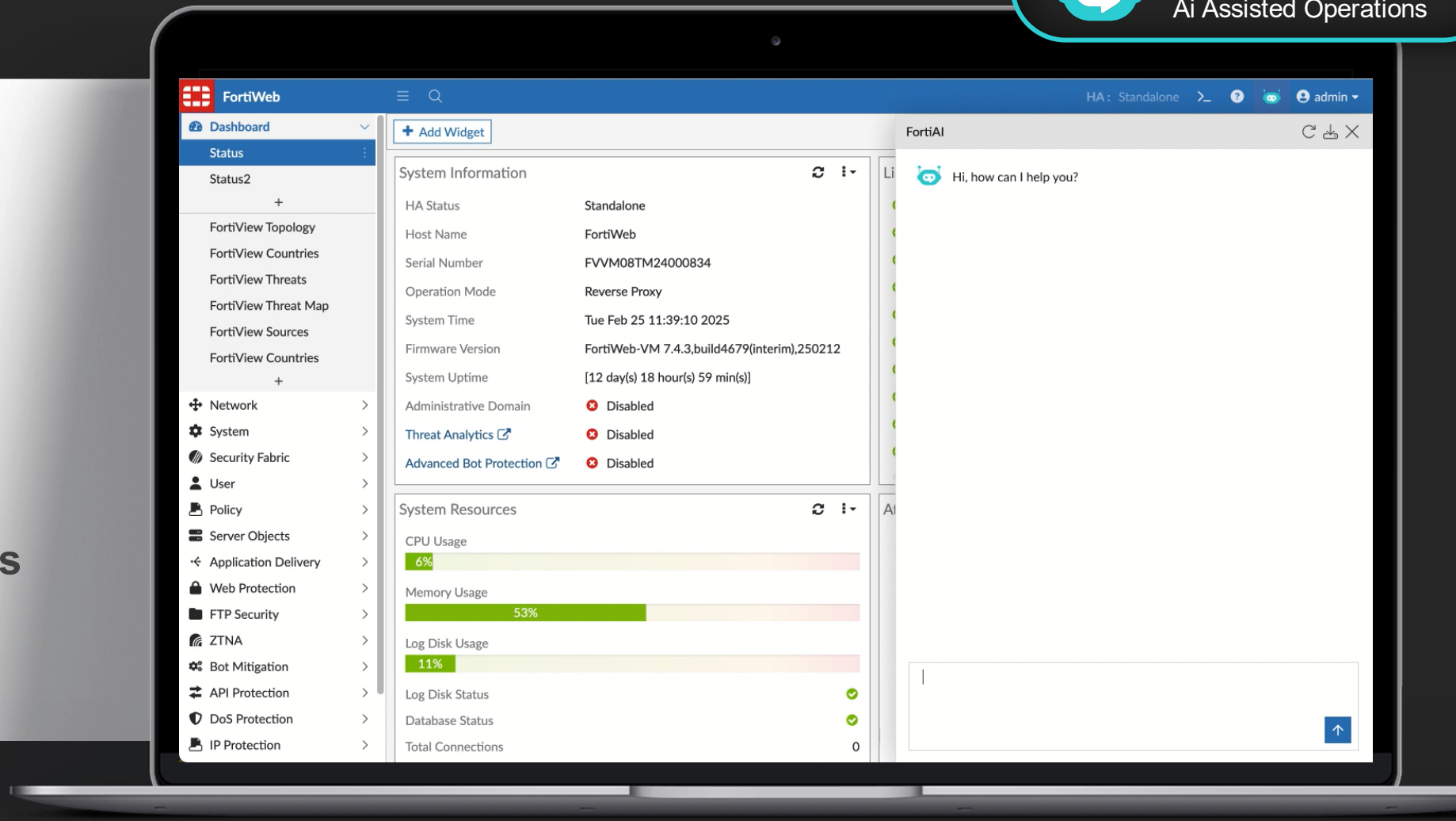
AI-driven Optimization

Predictive insights from correlated data to enhance network performance and resilience

FortiAppSec Cloud FortiAI-Assist Add-on

FortiAI-Assist
Ai Assisted Operations

- **Built for Security Analysts**
- **AI for Continuous Threat Analysis**
- **AI for Autonomous Response**



FortiAI-Assist Boosts Productivity and Saves Costs

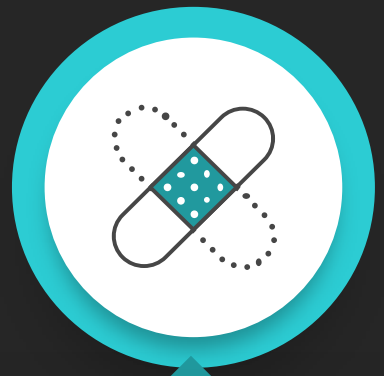
FortiAI-Assist
Ai Assisted Operations

Understand

- Who attacked your app?
- Why was a rule triggered?
- How can vulns. be exploited?
- What to do next?

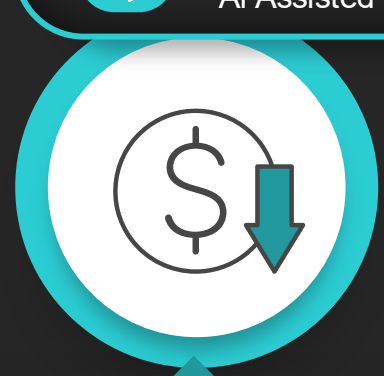
Enhance

- Share security knowledge with other teams
- Break silos and streamline remediation workflows
- Generate customized rules from simple text



Secure

- Make educated decisions
- Apply recommended mitigations
- Patch in advance



Assess

- Hours saved on investigation and remediation
- Improved collaboration
- Attack surface reduction
- Saved costs


FORTINET
COLOMBIA
& ECUADOR
XPERTS26