



# Fortinet Security Fabric Blueprint

Dr. Rattipong Putthacharoen, Com. Eng.  
Senior Manager, Systems Engineering

# Agenda

- 1 Company Overview
- 2 Fortinet Security Fabric Blueprint
- 3 Use Cases
- 4 Summary

# **Fortinet BluePrint**

# Fortinet is among the Top 3 Cybersecurity Companies in the World

**FOUNDED IN 2000**

Employees - 6250



**\$2.1B – 2018**

20% Growth



**ALMOST 500,000+  
CUSTOMERS**



**No. 1 SHIPMENTS**

**No. 2 REVENUE**

(IDC Firewall Tracker)



# Substantial Ongoing Investment in Innovation

## R & D CENTERS

U.S. (HQ)  
Canada



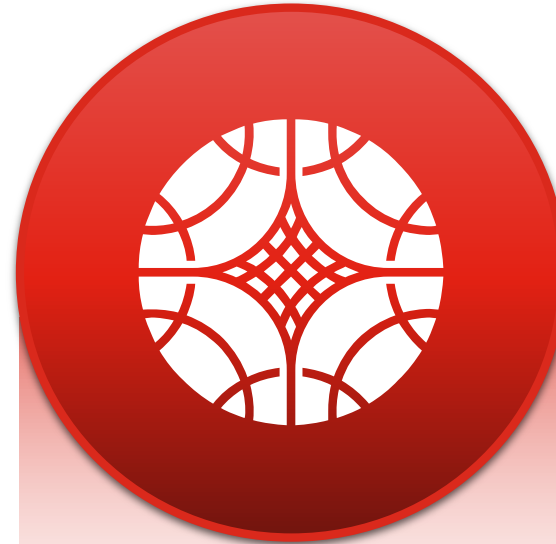
## SECURITY PROCESOR UNIT

(SPU)



## SECURITY FABRIC

(Platform)

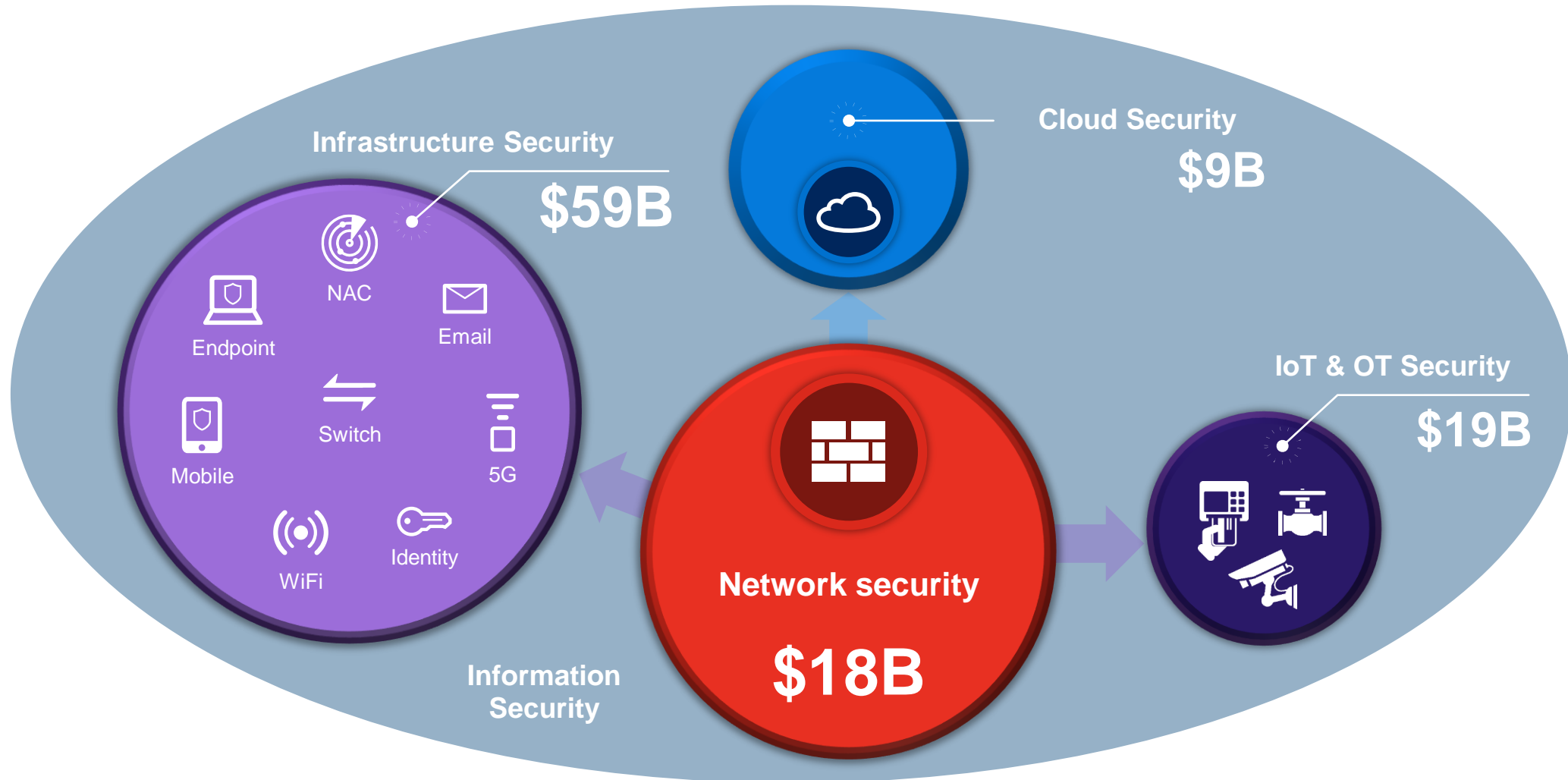


## PATENTS

600+



# Fortinet is Positioned for a Bigger Total Addressable Market



# Fortinet Security Fabric

## BROAD

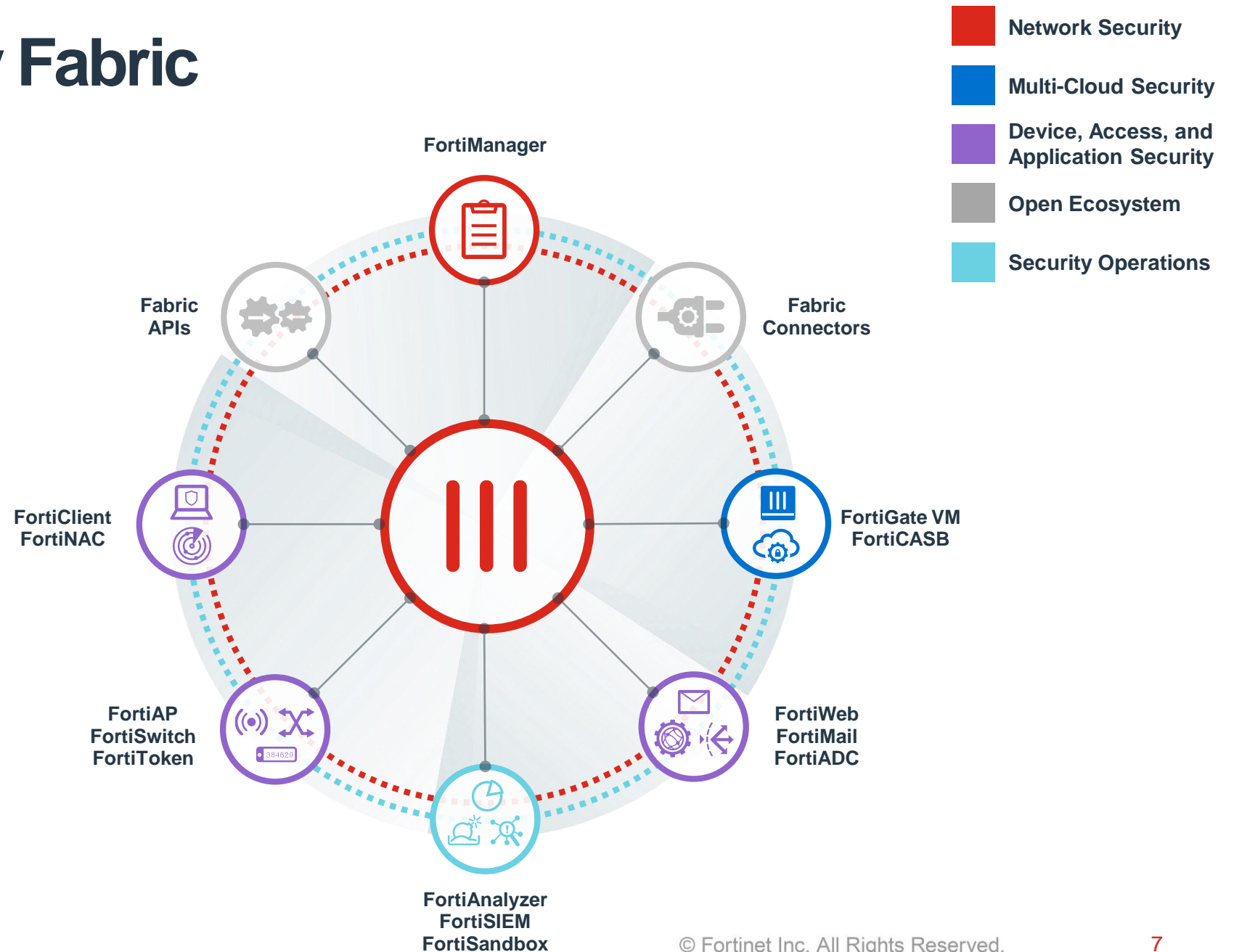
Visibility of the entire digital attack surface

## INTEGRATED

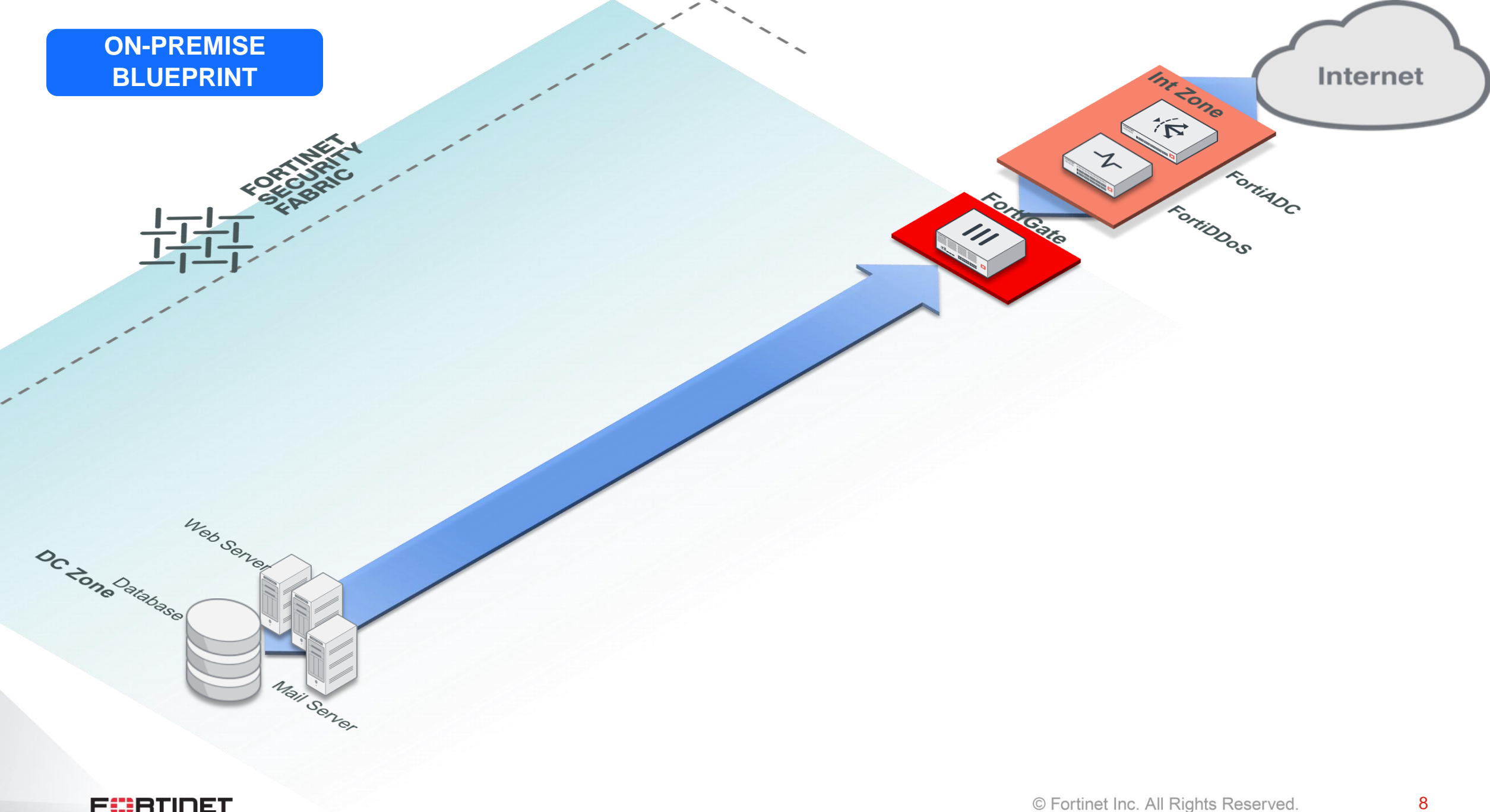
Protection across all devices, networks, and applications

## AUTOMATED

Operations and response driven by Machine Learning

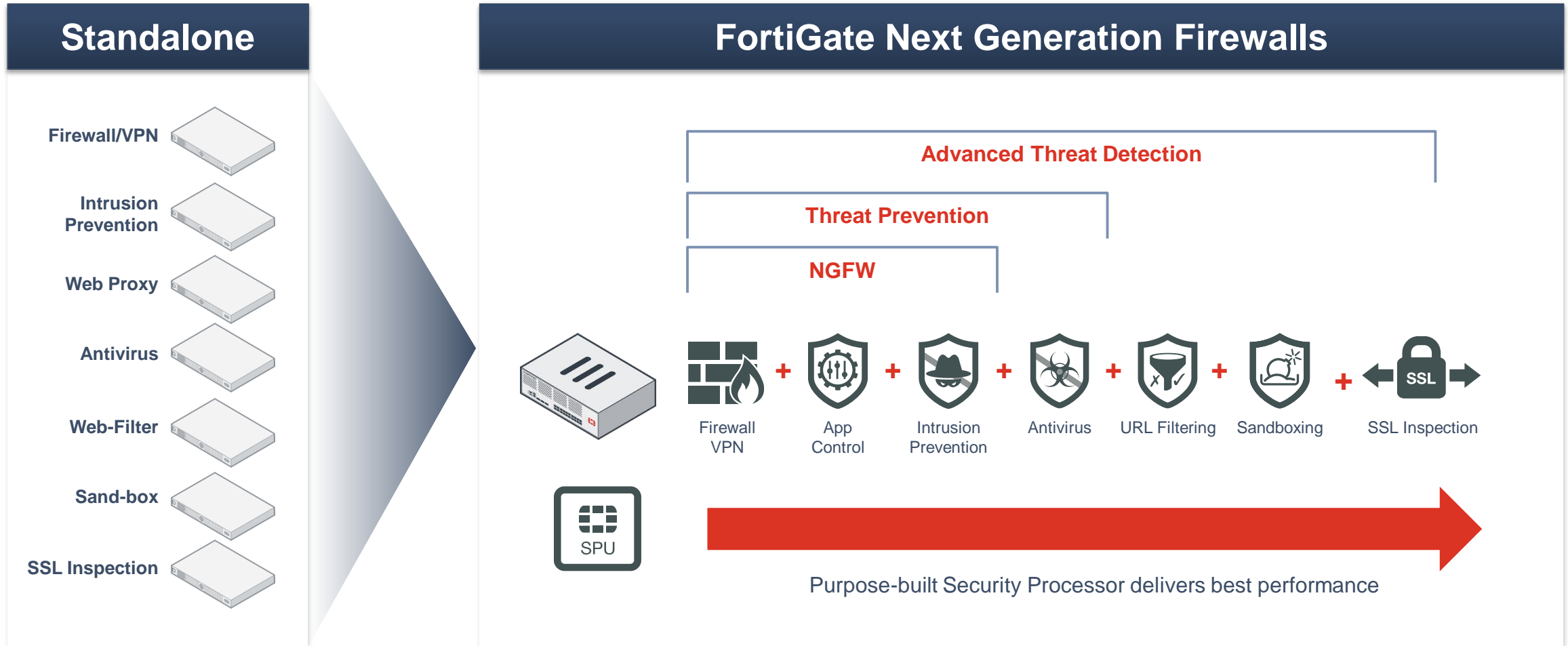


**ON-PREMISE  
BLUEPRINT**





# Fortinet NGFW – Reduce Complexity with Better Security

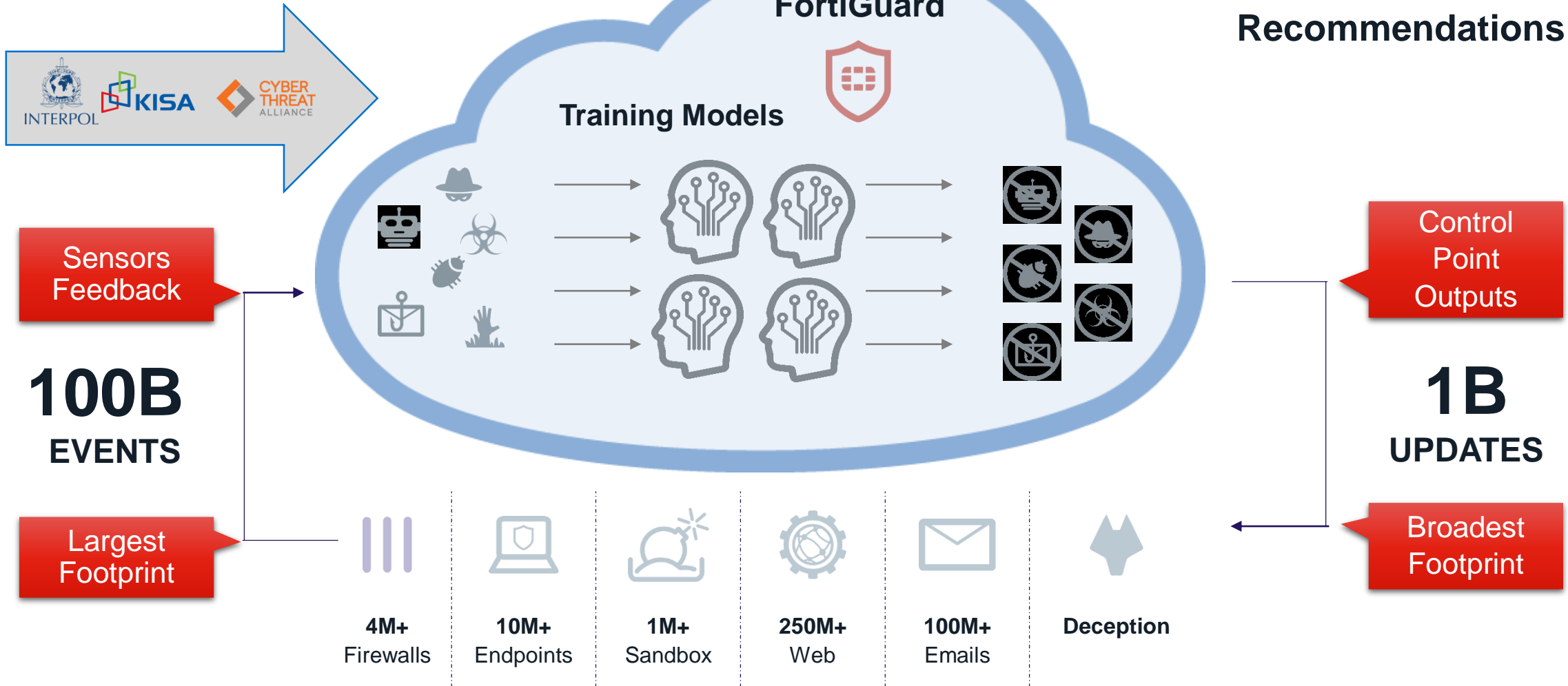


- Integrate various point products into NGFW Features

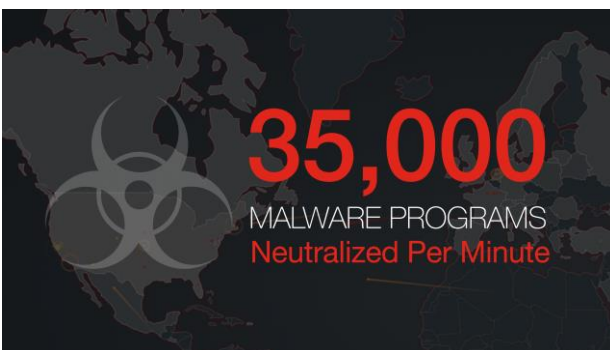
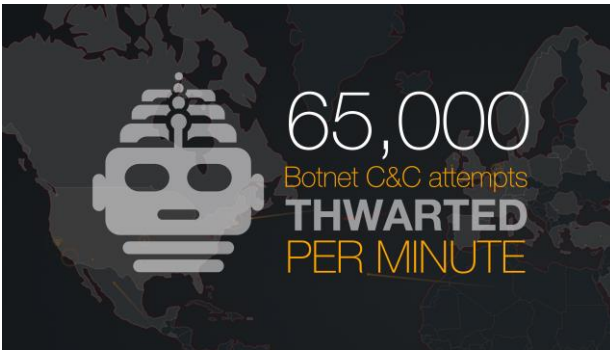
# FortiGuard - AI-Driven Security

Global and Customer-specific

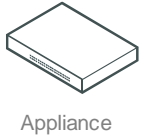
**9** **NSS** LABS  
Recommendations



# FortiGuard by the numbers



# Introducing FortiDDoS



## Hardware Accelerated DDoS Intent Based Defense



(SPU)-based layer 3, 4, and 7 DDoS protection



Behavior-based DDoS protection to eliminate need for signature files



Minimal false-positive detections through continuous threat evaluation



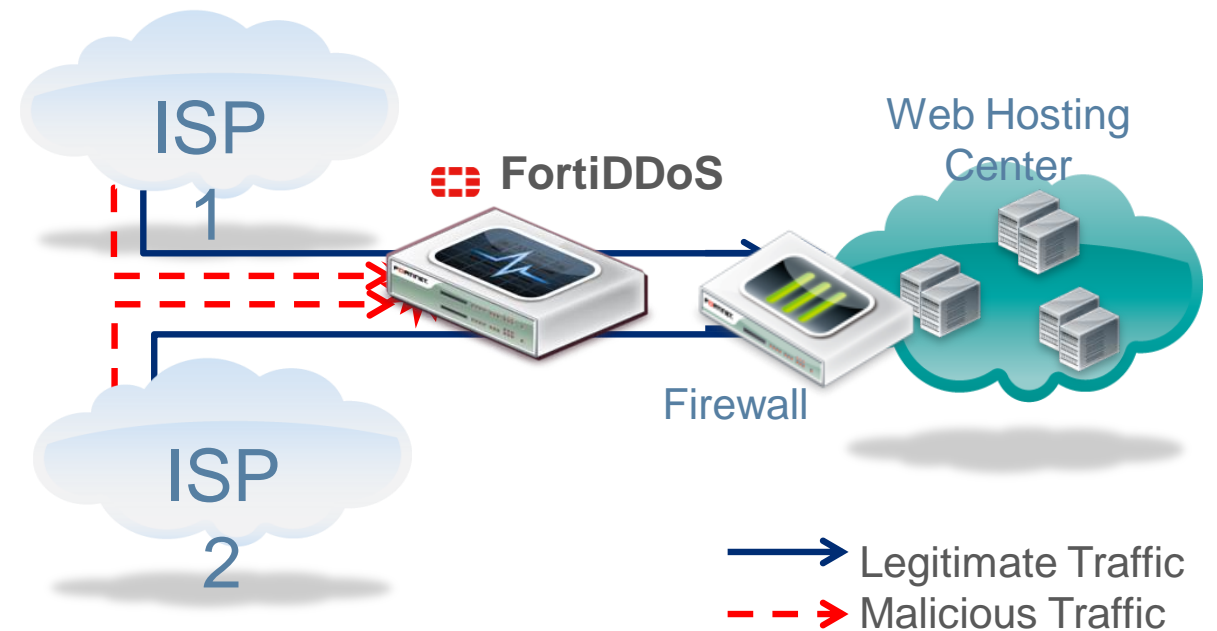
Ability to monitor enormous parameters simultaneously



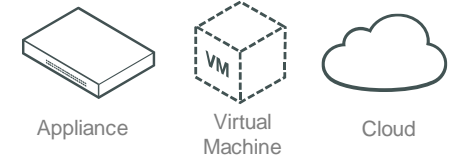
Advanced defense against bulk volumetric, layer 7 applications



Attack protection for DNS services via specialized tools



# Introducing FortiADC



Optimize the availability, performance and scalability of mobile, cloud and enterprise application delivery



Layer 7 Load Balancing



Secure Traffic Management



Application Optimization



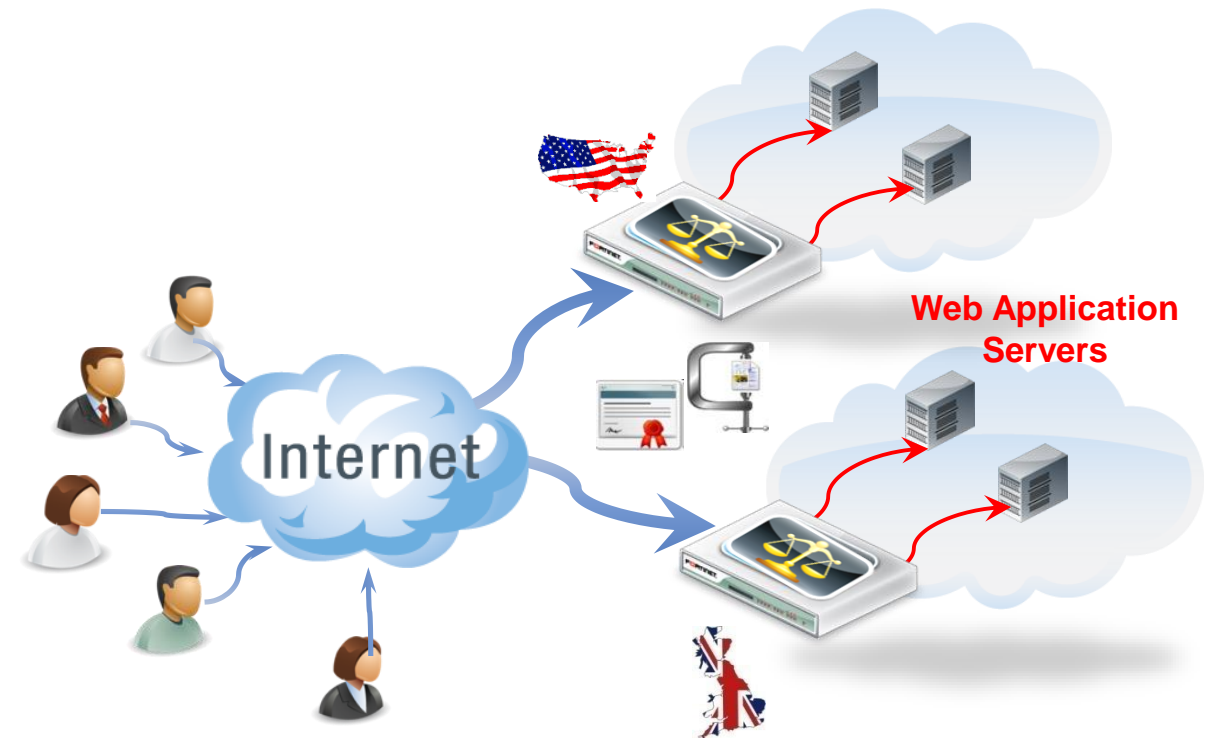
Security Fabric Integration



Global Server Load Balancing

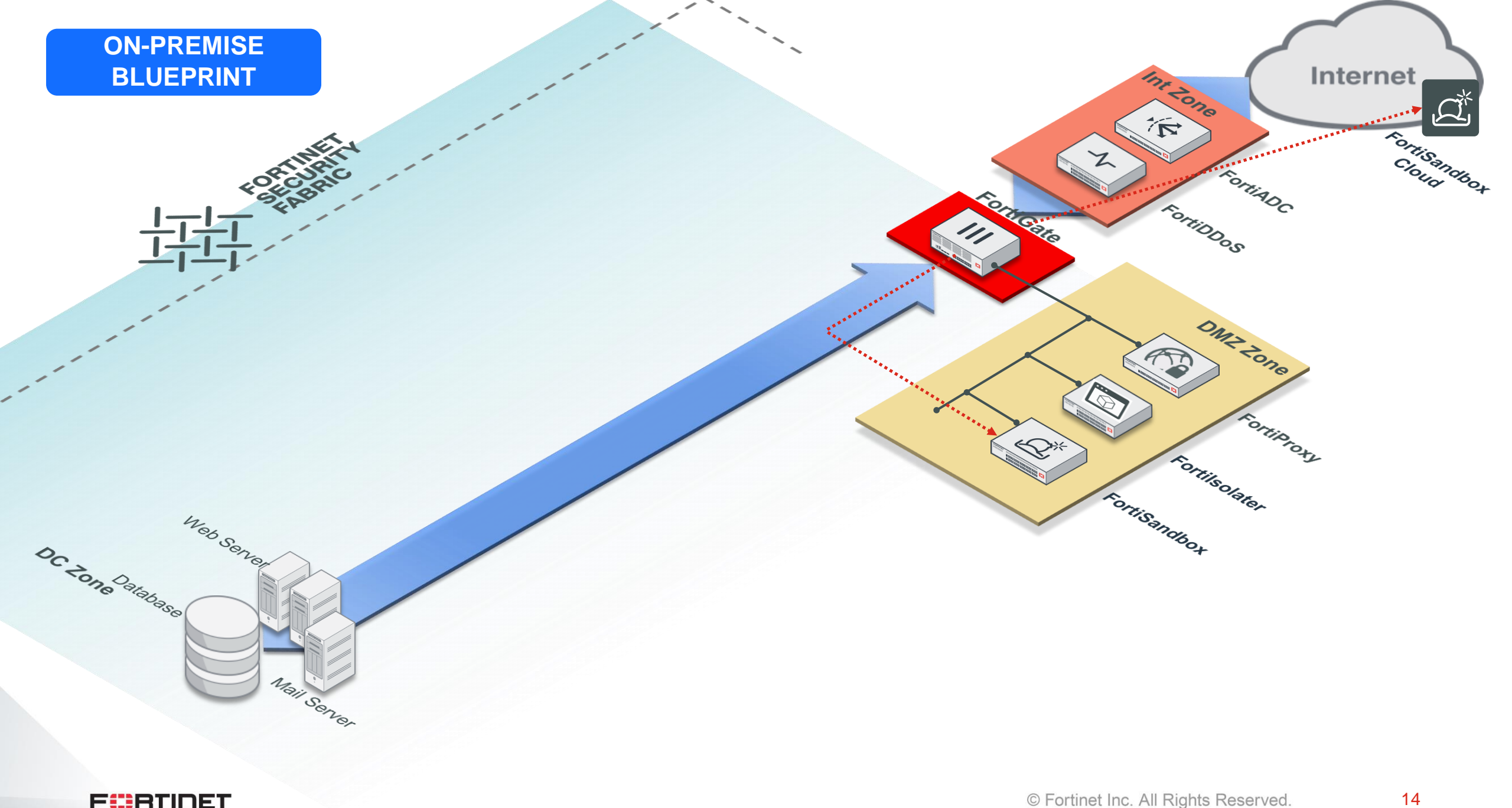


Value-added Security Features

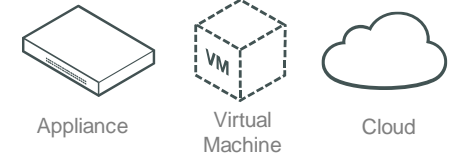




**ON-PREMISE  
BLUEPRINT**



# Introducing FortiProxy



Reduce the cost and impact of downloaded content, while increasing performance by improving the speed of access



Accelerated SSL deep inspection



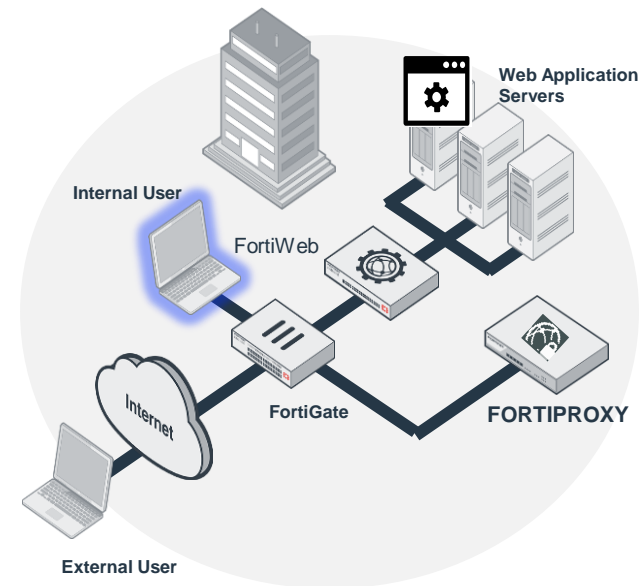
Protection against sophisticated web attacks



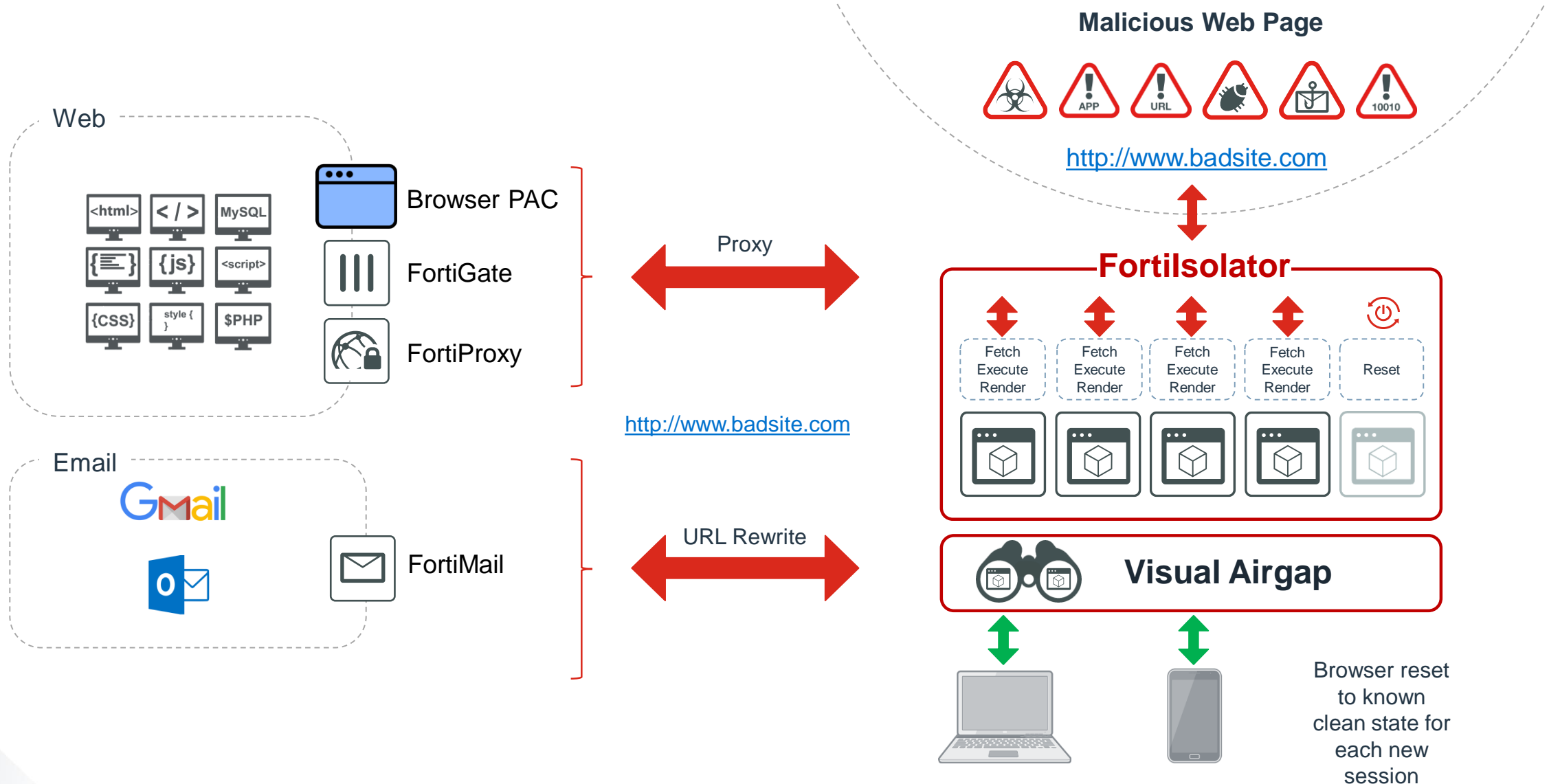
Authenticated web application control



WAN Optimization and Advanced Caching

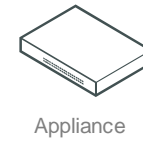


# Fortisolator Product Overview





# Introducing FortiSandbox



Appliance



Virtual Machine



Hosted



Cloud



Advanced Threat Protection solution designed to identify and thwart the highly targeted and tailored attacks



Independently top-rated



Broad integration



Intelligent automation



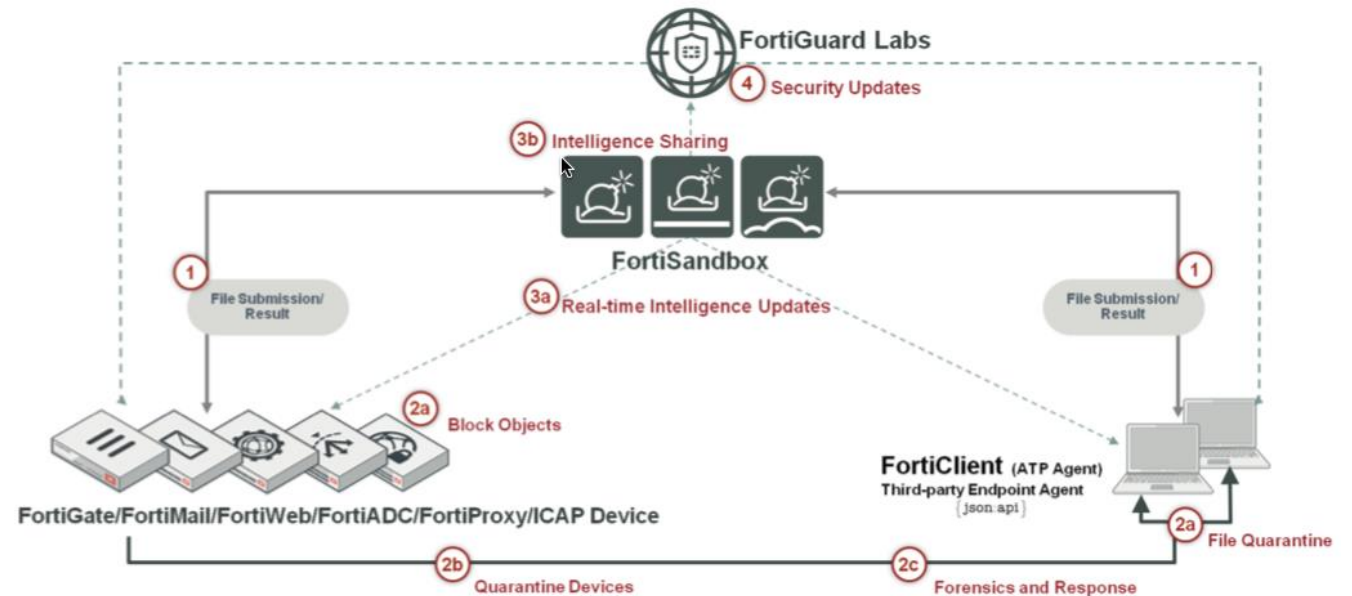
All-in-one



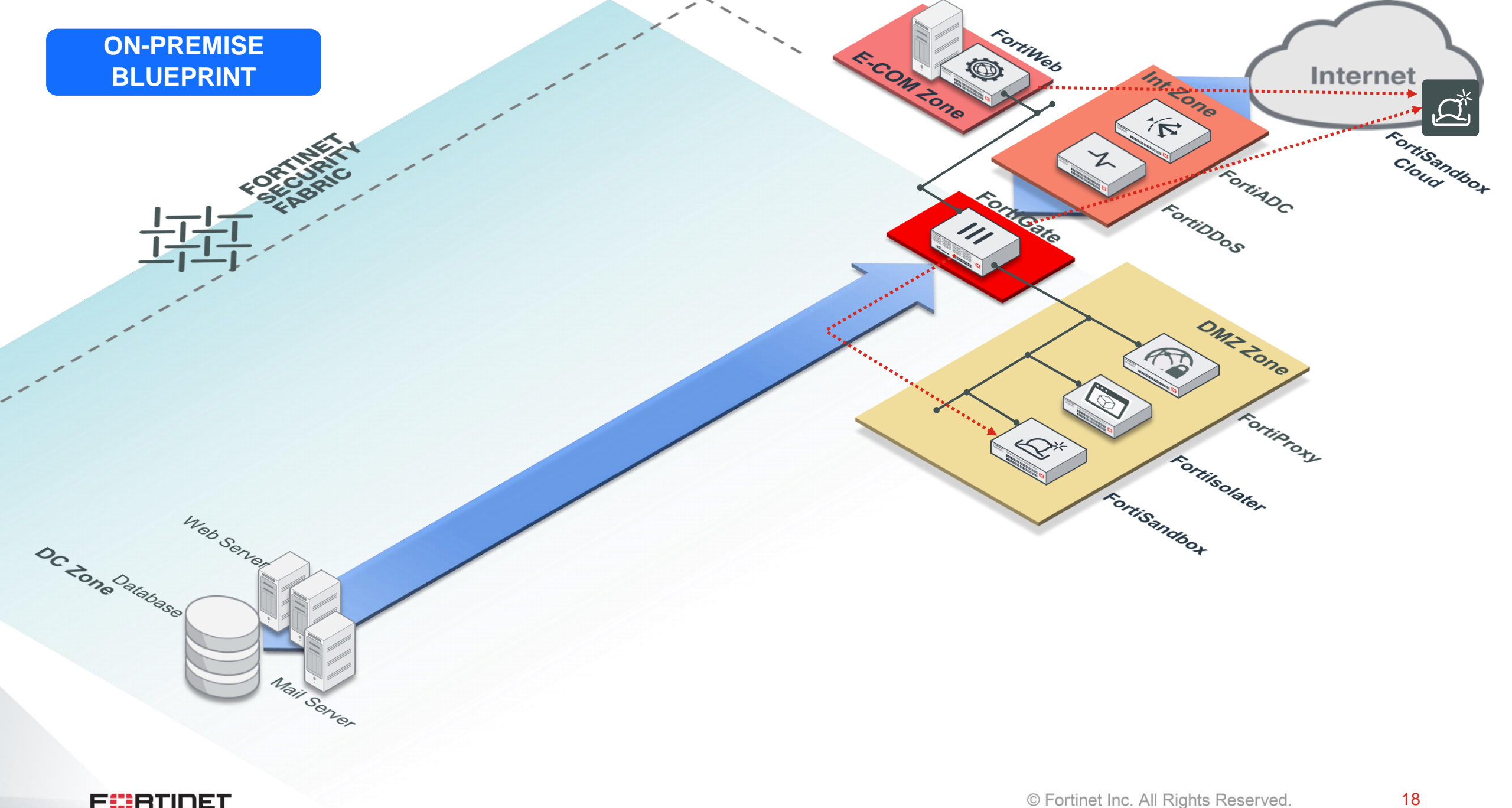
Flexible deployment



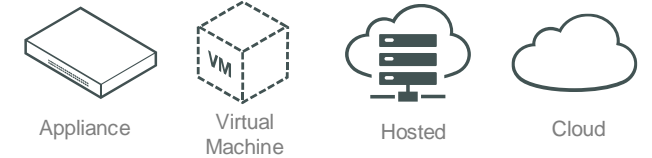
Open extensibility



**ON-PREMISE  
BLUEPRINT**



# Introducing FortiWeb



## Web application firewall to protect, balance, and accelerate web applications



Feature-rich product that consolidates NGFW and SWG services



Powerful hardware that can perform SSL deep inspection



Anti-malware techniques updated with the latest threat intelligence



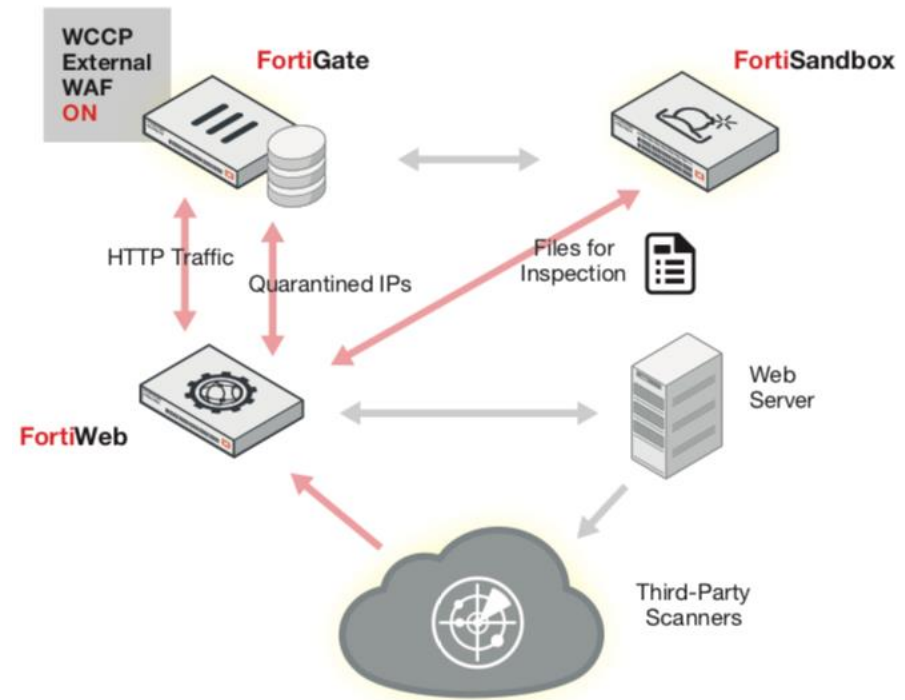
Single Pane of Glass management



Effectively remove blind spots in encrypted traffic

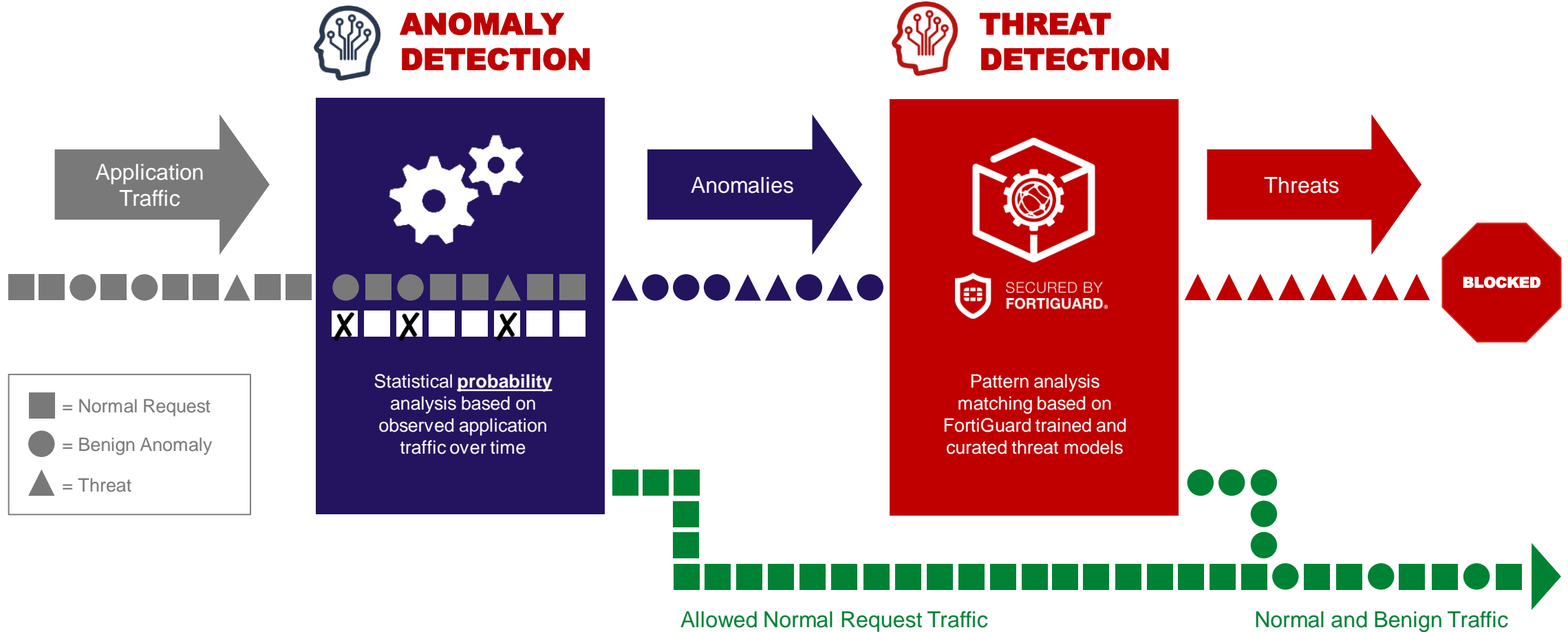


Stay protected against the latest known and unknown attacks



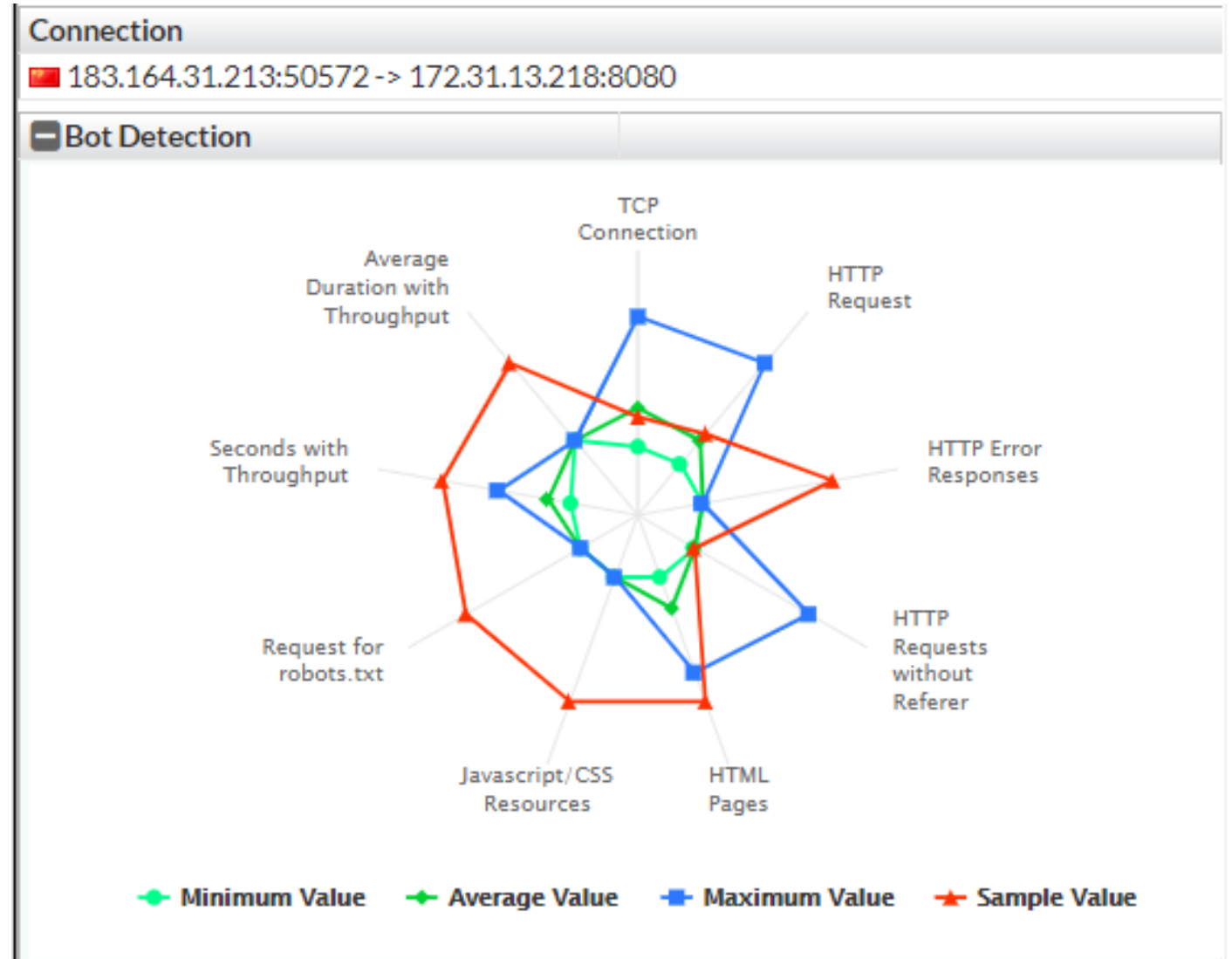
# Machine Learning-based Web App Protection

How it works?



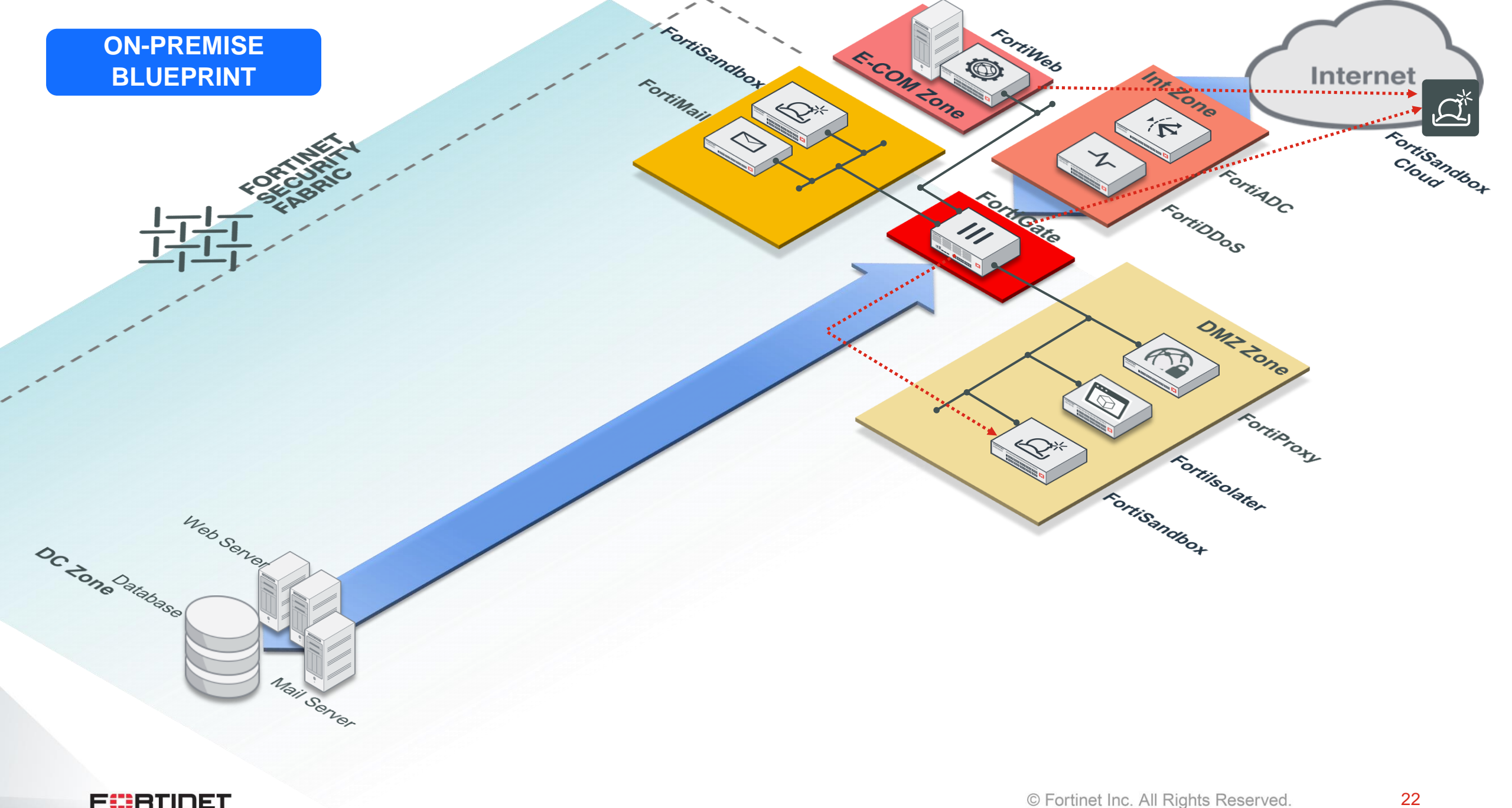
# FortiWeb adds Machine Learning

- FortiWeb identifies malicious bot activity by building a model based on live traffic

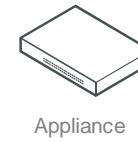




**ON-PREMISE  
BLUEPRINT**



# Introducing FortiMail



Appliance



Virtual Machine



Hosted



Cloud



**Advanced anti-spam and antivirus filtering solution, with extensive quarantine and archiving capabilities.**



Top-rated Antispam, Antiphishing and Business Email Compromise (BEC)



Independently certified advanced threat defense



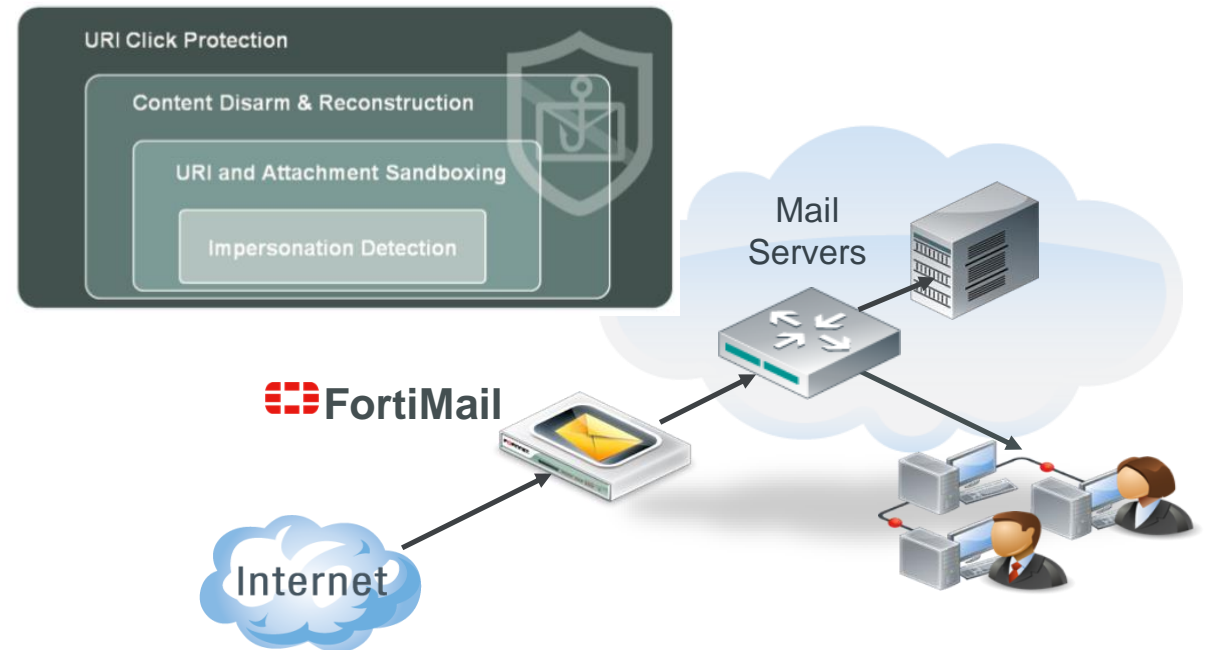
Integrated data protection



Enterprise-class management



High-performance mail handling







# Introducing FortiClient



## Comprehensive end-point protection & security enforcement



Broad endpoint visibility



Endpoint compliance and vulnerability management



Proactive endpoint defense



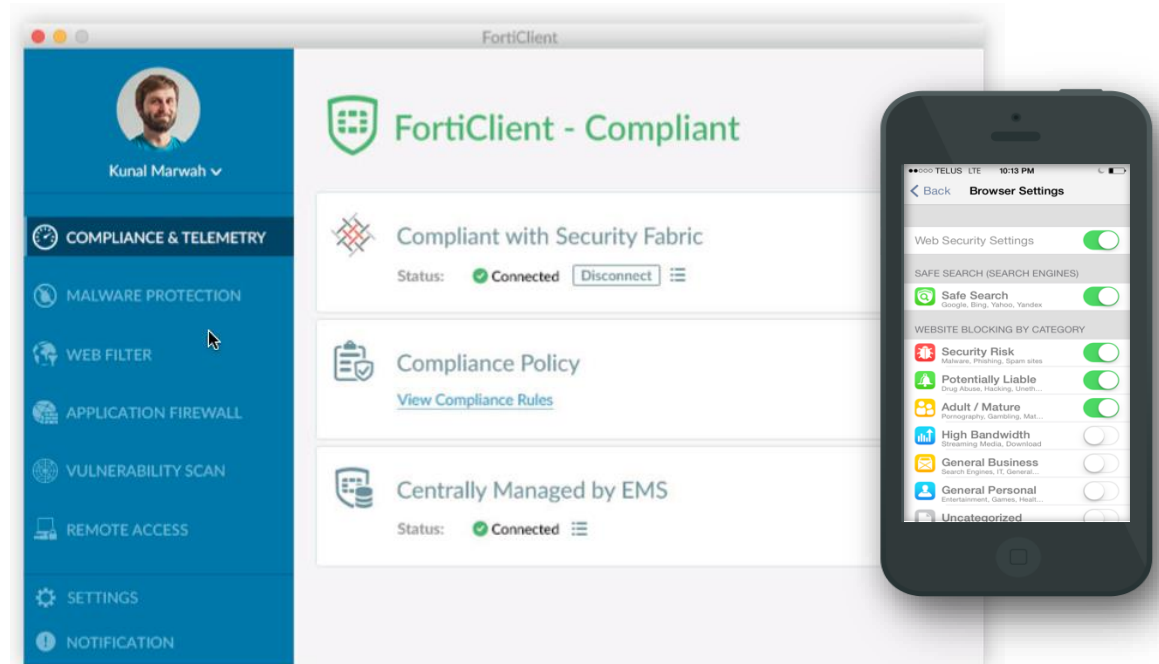
Automated threat containment



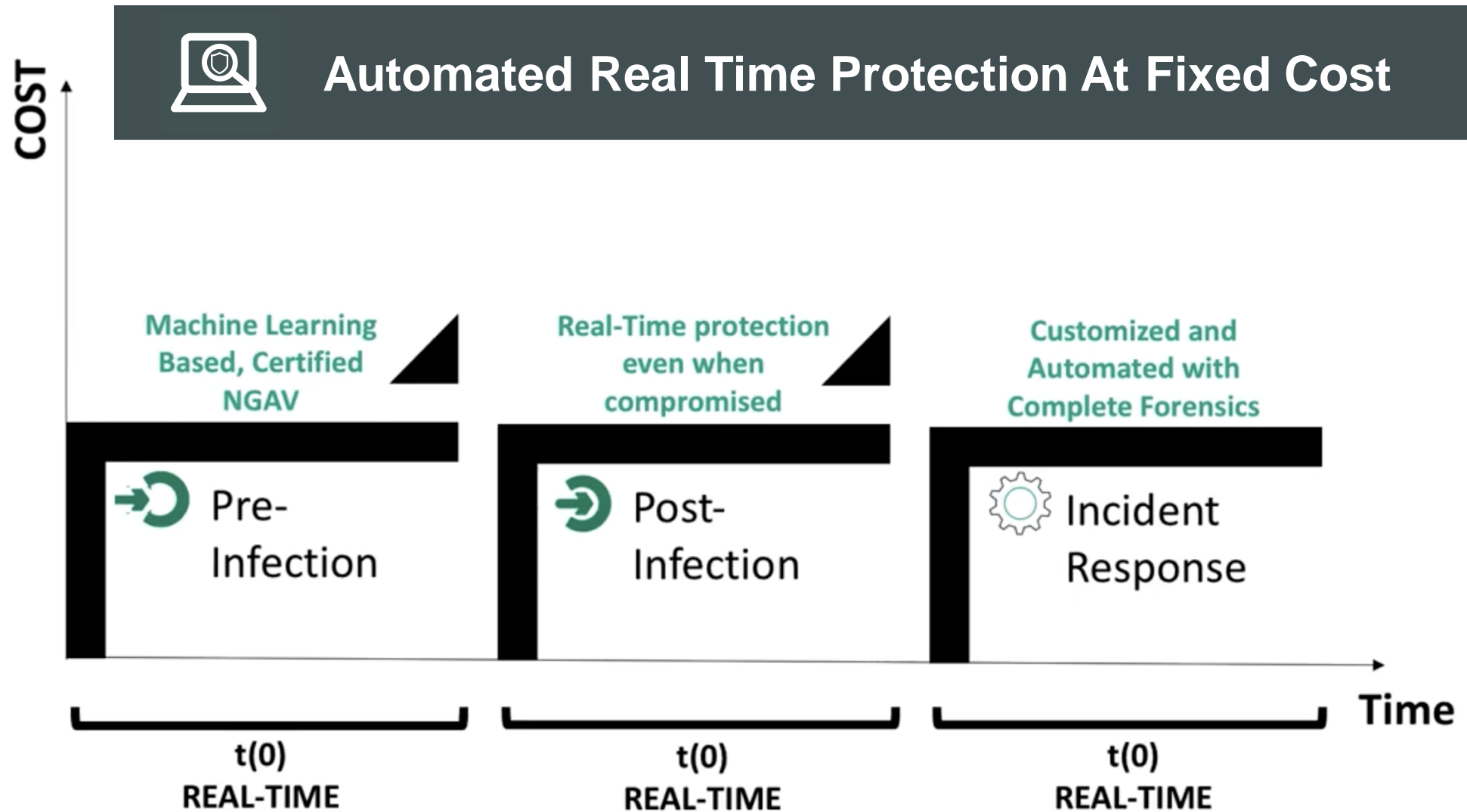
Secure remote access



Easy to deploy and manage



# Introducing FortiEDR



# Introducing FortiToken Mobile

384629

## Oath Compliant Time Based One Time Password Soft Token



Reduced costs by leveraging existing FortiGate as the authentication server



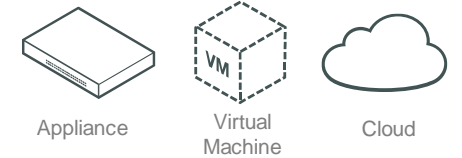
Minimized overhead with unique online activation option



A scalable solution for low entry cost and low total cost of ownership



# Introducing FortiAuthenticator



## Identity Management, User Access Control and multi-factor identification



Transparently identify network users and enforce identity-driven policy on a Fortinet-enabled enterprise network



Seamless secure two-factor/OTP authentication across the organization in conjunction with FortiToken



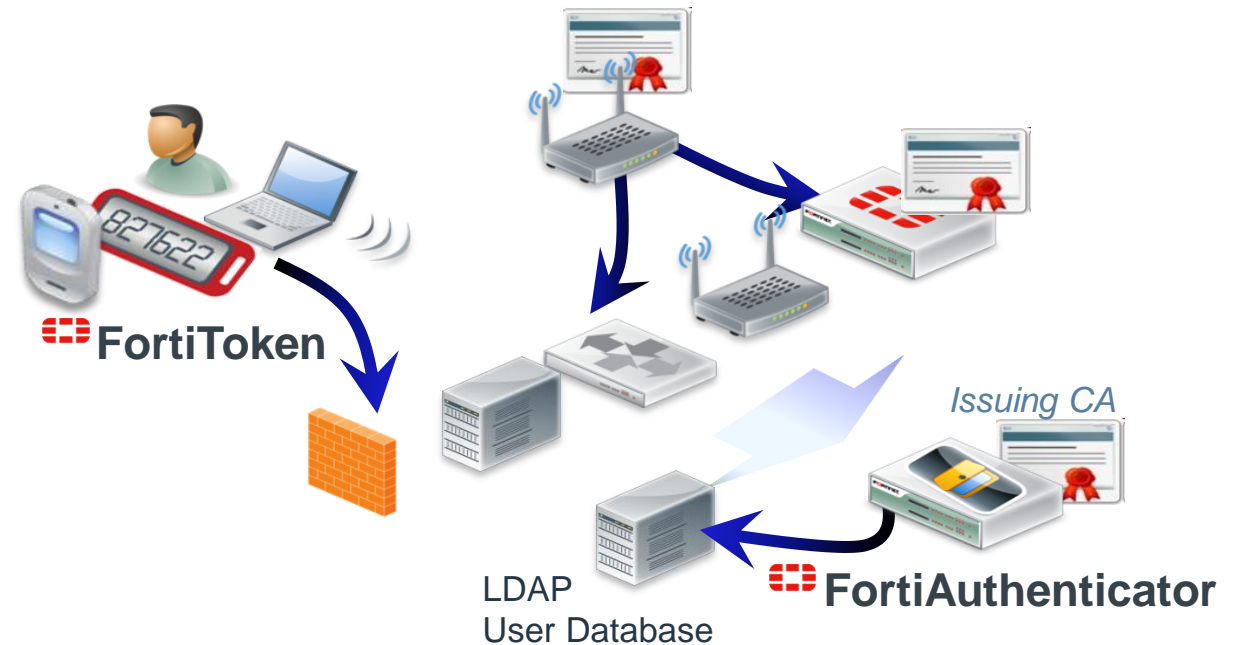
Certificate management for enterprise wireless and VPN deployment



Guest management for wired and wireless network security



Single Sign On capabilities for both internal and cloud networks



# Introducing FortiNAC



**Provides Visibility of Users and End points for Enterprise Networks and Automates Threat Response**



Device identification and profiling



Simplified guest access with self-registration



Continuous risk assessment



Micro-segmentation of endpoints

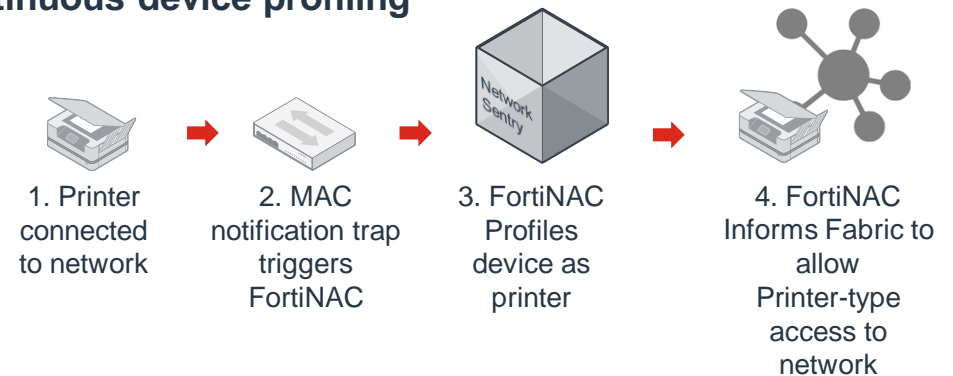


Automated response to identified risks

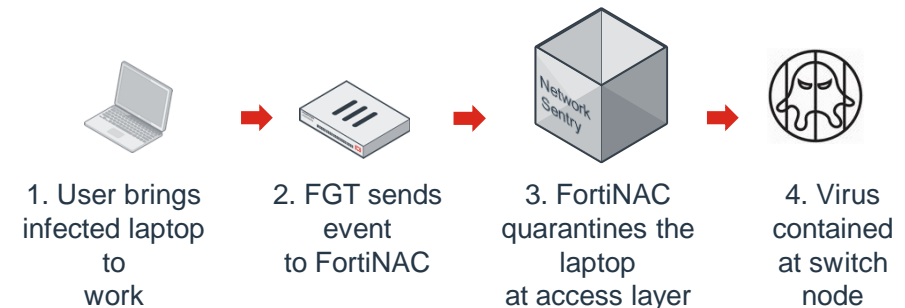


Orchestration of 3rd party devices

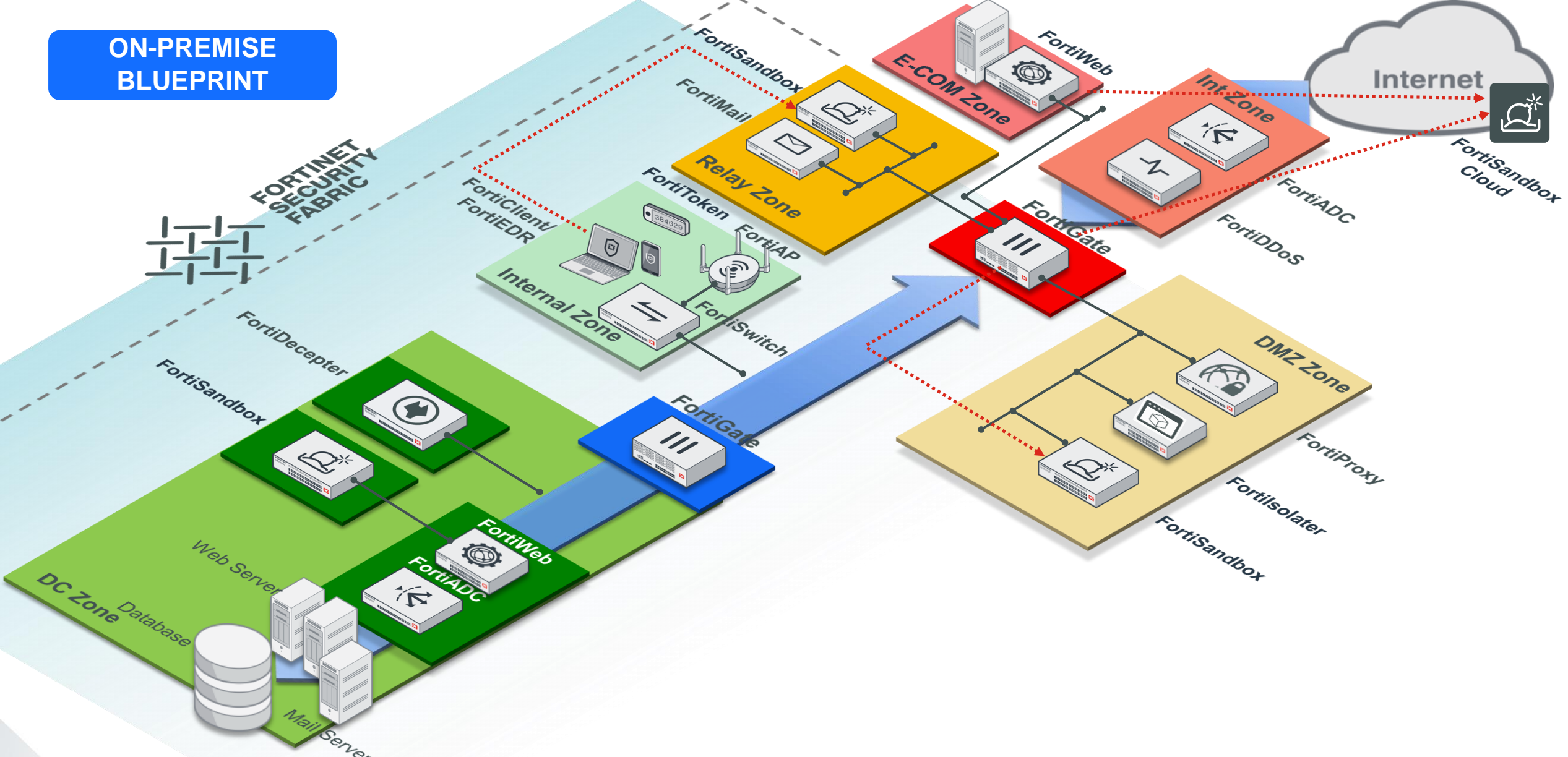
## Continuous device profiling



## Containment of lateral threats at Edge



**ON-PREMISE  
BLUEPRINT**





# Introducing FortiDeceptor



## Automated Detection and Response to External and Internal Threats



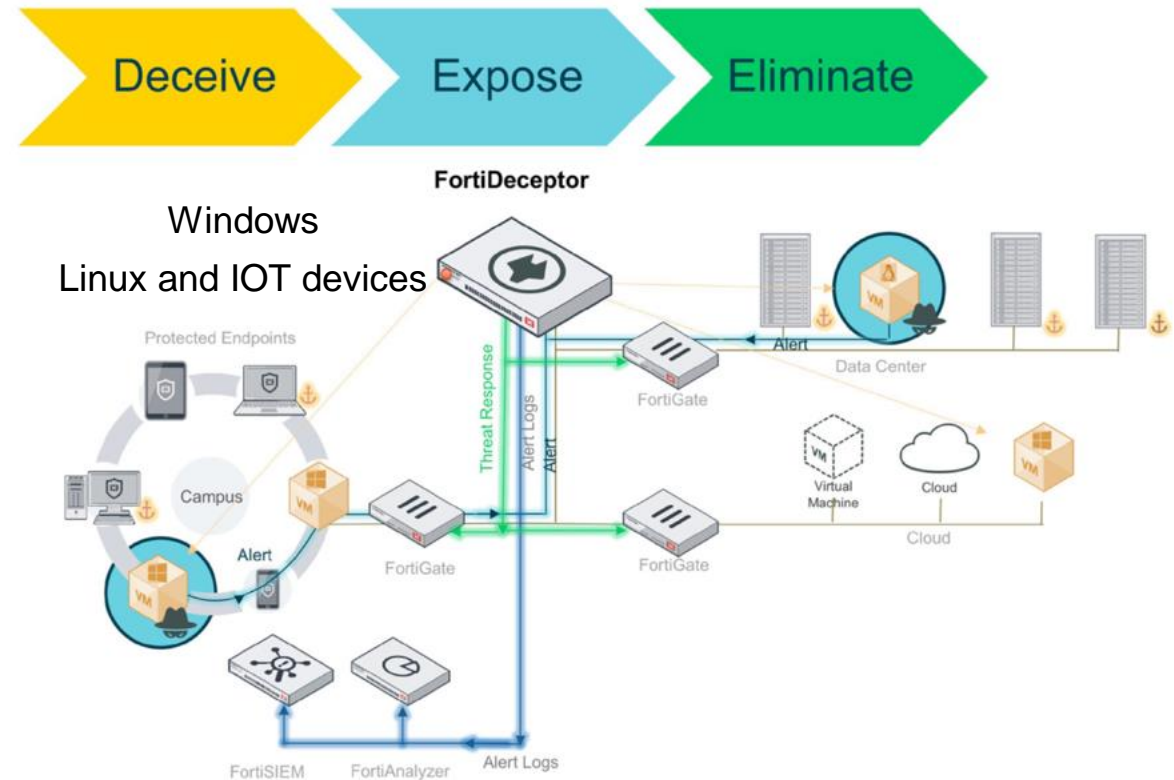
GUI driven threat map quickly uncovers threat campaigns targeting your organization



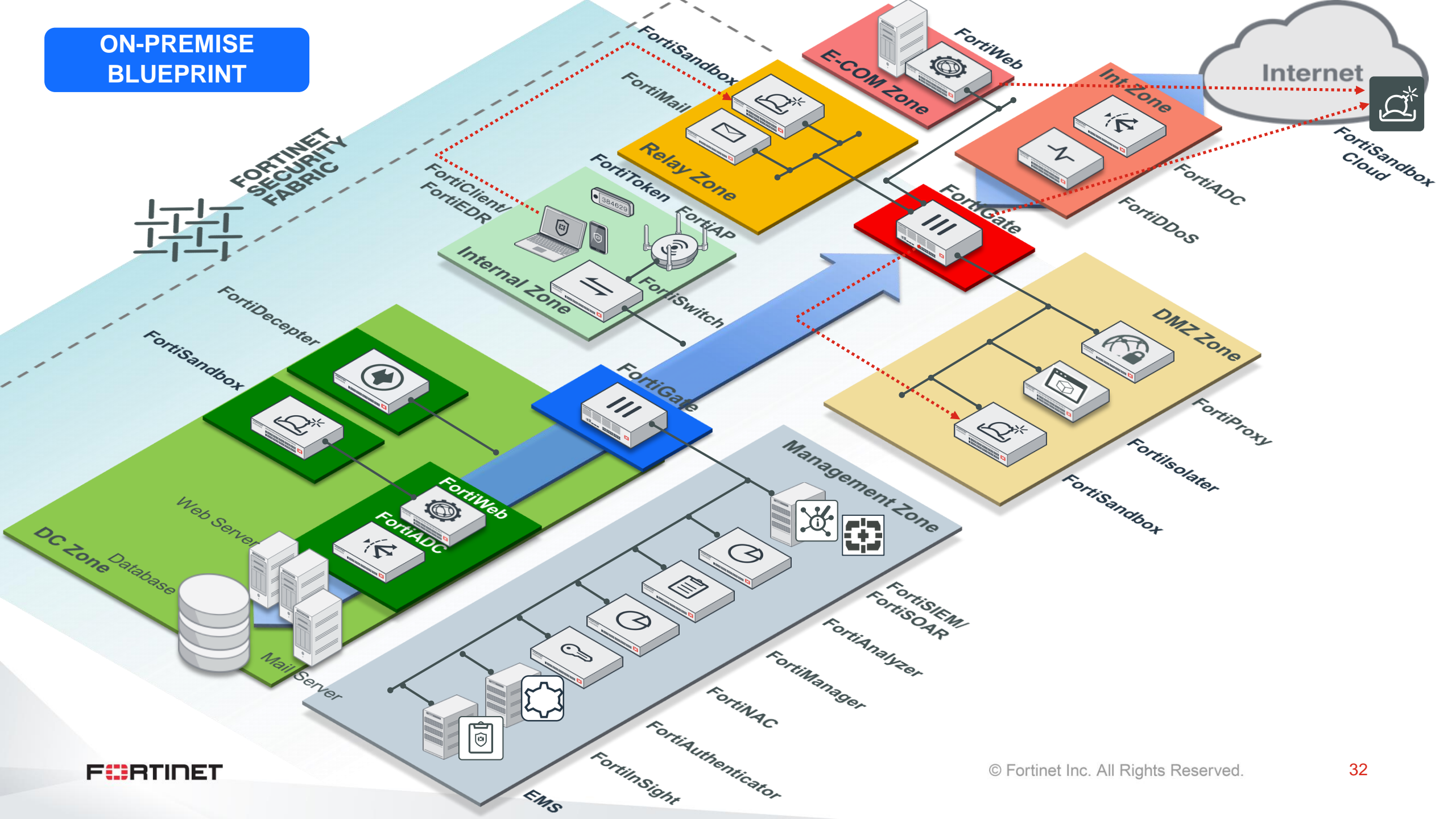
Security infrastructure integration provides real-time blocking of attackers before real damage occurs



Centrally manage and automate the deployment of deception VMs and decoys

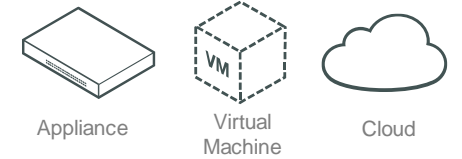


**ON-PREMISE BLUEPRINT**





# Introducing FortiSIEM



## Unified event correlation and risk management for modern networks



Asset Self-Discovery



Rapid Integrations and Scalability



Automated Workflow with Remediation Library



Single Pane of Glass to quickly remediate service issues



Multi-tenancy for role-based access to a unified platform



# Introducing FortiSOAR



## Security Orchestration, Automation and Response



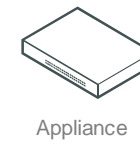
**Manage:** Alerts, Incidents, Indicators, Tasks across Tenants

**Measure:** MTTD, MTTR, ROI, Reports, Dashboards

**Respond:** Automate, Visual Playbook Designer, Out of Box Connectors

**Solutions:** SOC Automation, Vulnerability Management and BYOS

# Introducing FortiAnalyzer



Appliance



Virtual Machine



Hosted



Cloud



## Logging, reporting and analysis from multiple Fortinet devices



Centralized Search and Reports



Real-time and Historical Views into Network Activity



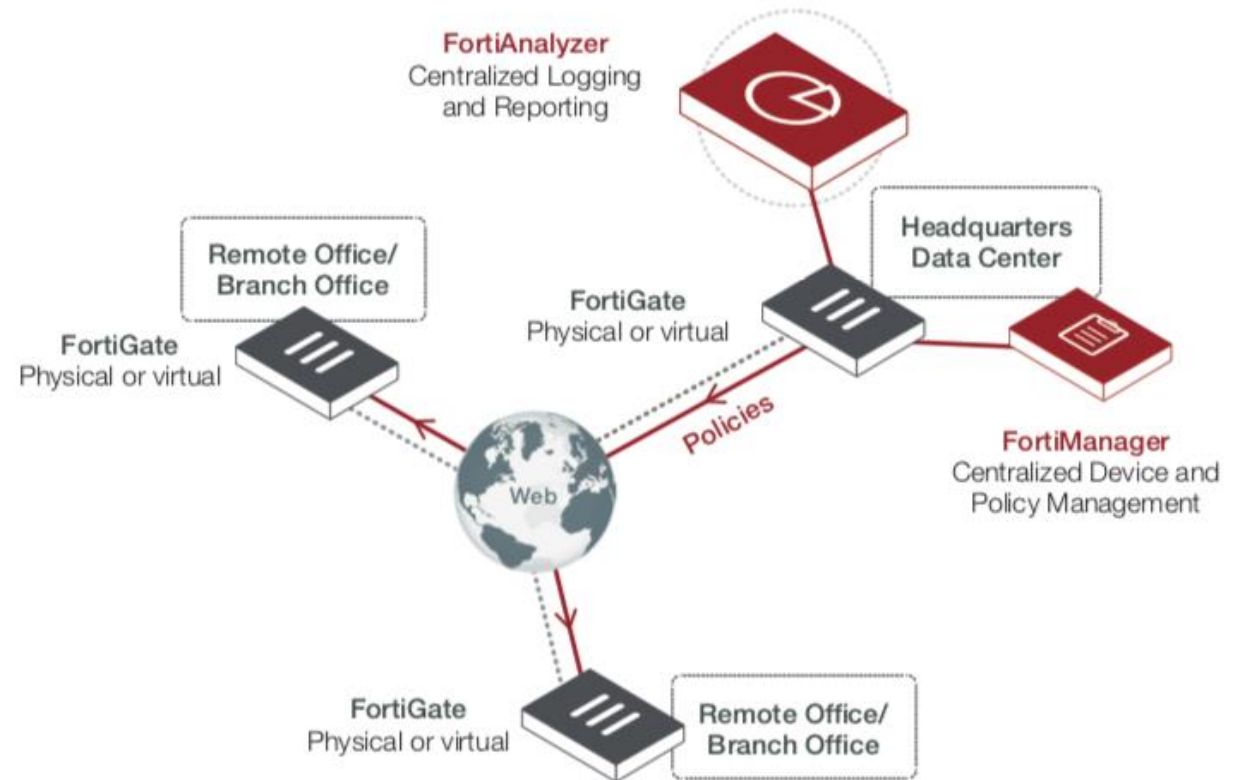
Scans security logs using FortiGuard IOC Intelligence for APT detection



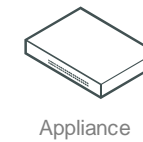
Light-weight Event Management



Seamless Integration with the Fortinet Security Fabric



# Introducing FortiManager



Tools that effectively manage any size Fortinet security infrastructure, from a few to thousands of appliances



Easy centralized configuration, policy-based provisioning, update management, and end to-end network monitoring



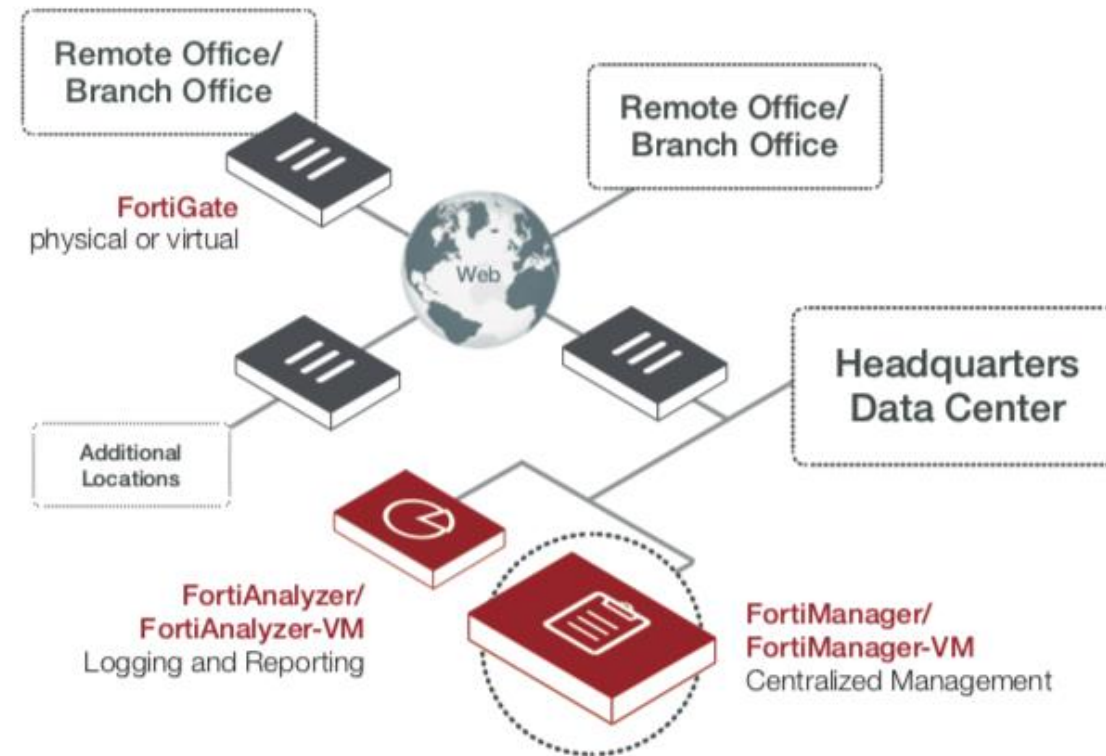
Segregate management of large deployments with ADOMs



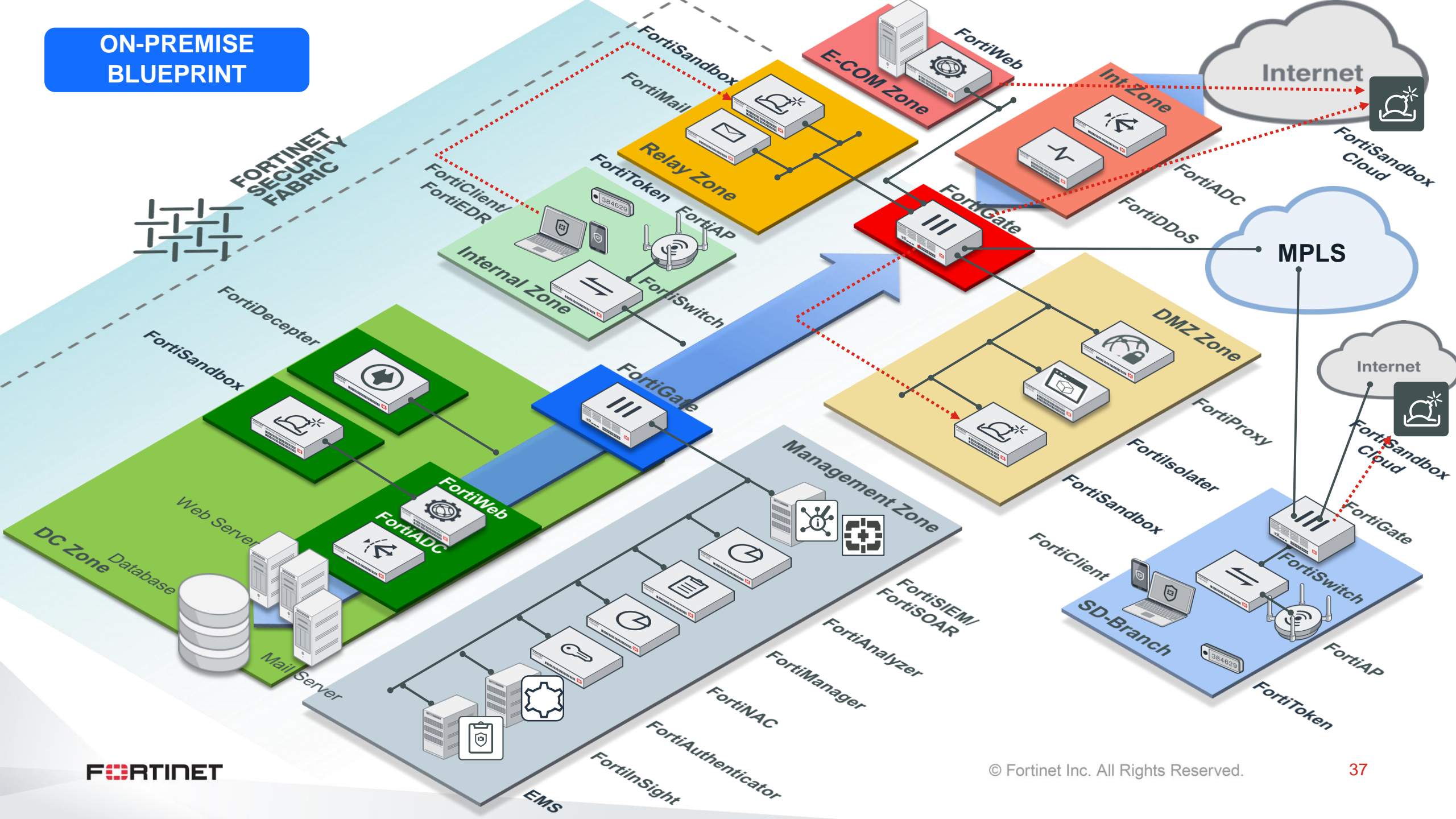
Single-pane-of-glass manages more than firewalls



Script and automation support with JSON/XML APIs with external systems



**ON-PREMISE BLUEPRINT**





# Next Generation Firewalls with Integrated SD-WAN

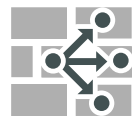
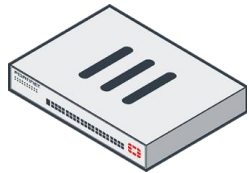
SD-WAN requires direct internet access which demands security at every branch

90% of the SD-WAN vendors only offer stateful firewalls which is not enough

## Secure SD-WAN

### SD-WAN

### NGFW



SD-WAN



Traffic Shaping

+



VPN

+



App Control

+



Intrusion Prevention

+



Antivirus

+



URL Filtering

+



Sandboxing

+



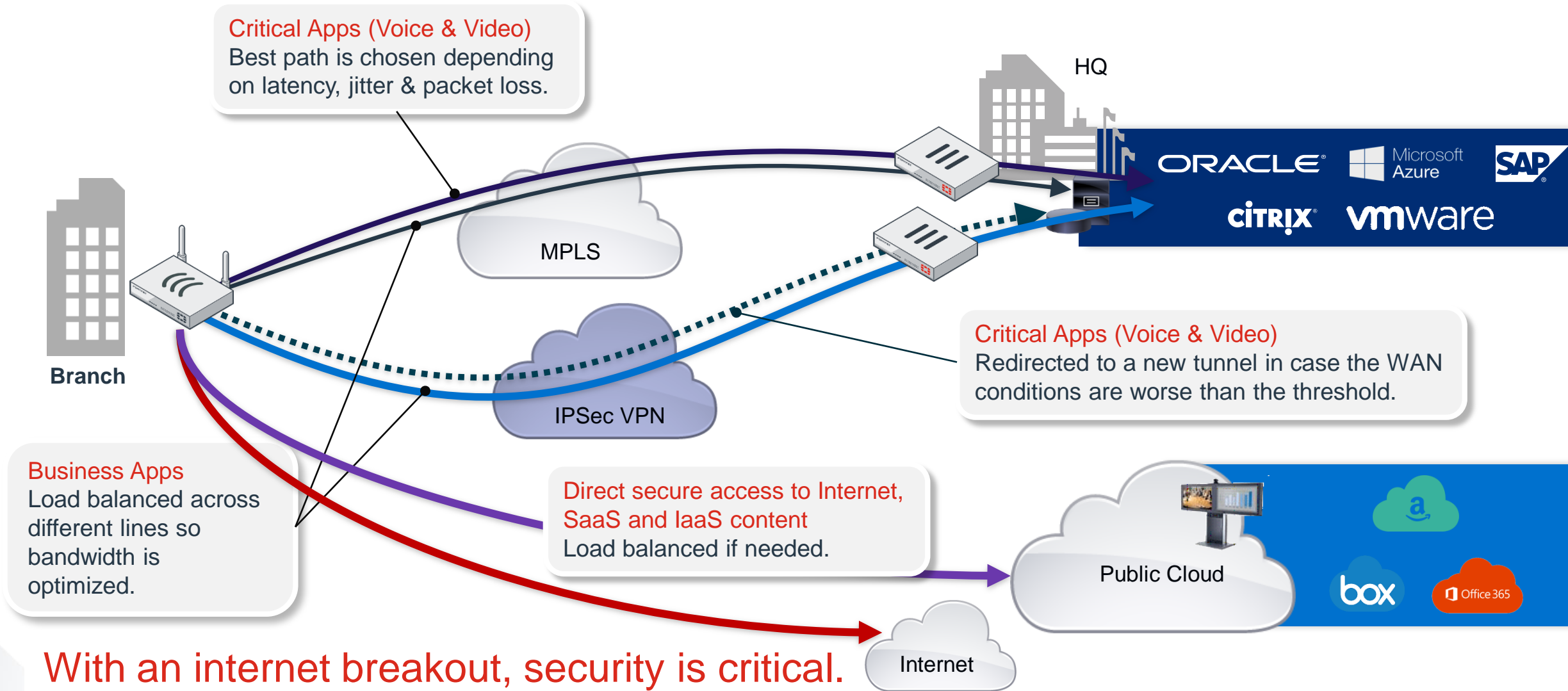
SSL Inspection

Scalable and Easy to Deploy

Unprecedented Integration and visibility

# Enterprise SD-WAN Use Cases - MPLS Migration

## MPLS backup with local breakout

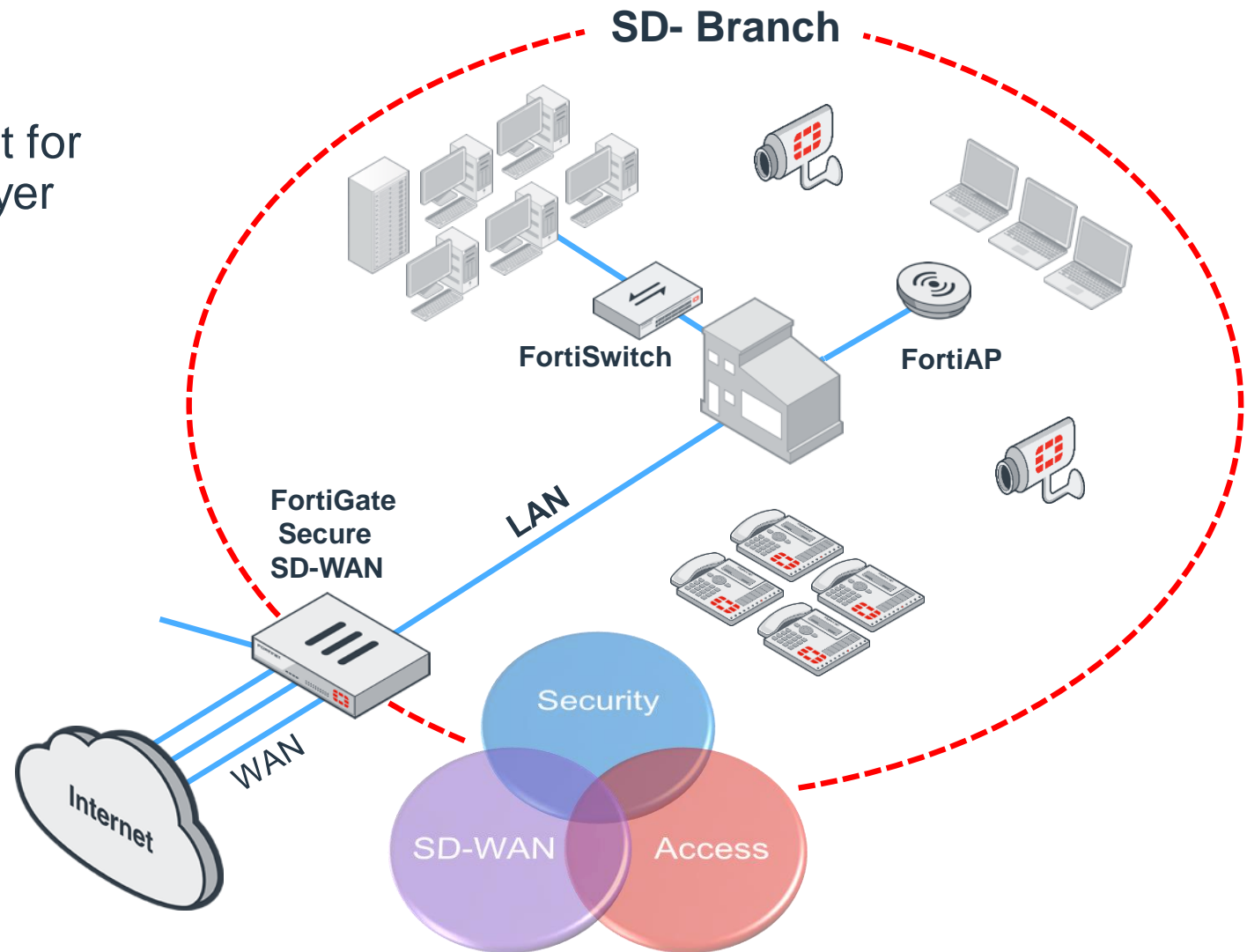


With an internet breakout, security is critical.

# Secure SD-Branch

## Software Defined Branch

- Single pane of glass management for SD-WAN, Security and Access layer (Switch & Wireless)
  - Network segmentation
  - Guest management
  - Network Access Control
  - User & Entity Behavior Analytics
  - Presence Analytics
  - Cameras, VoIP





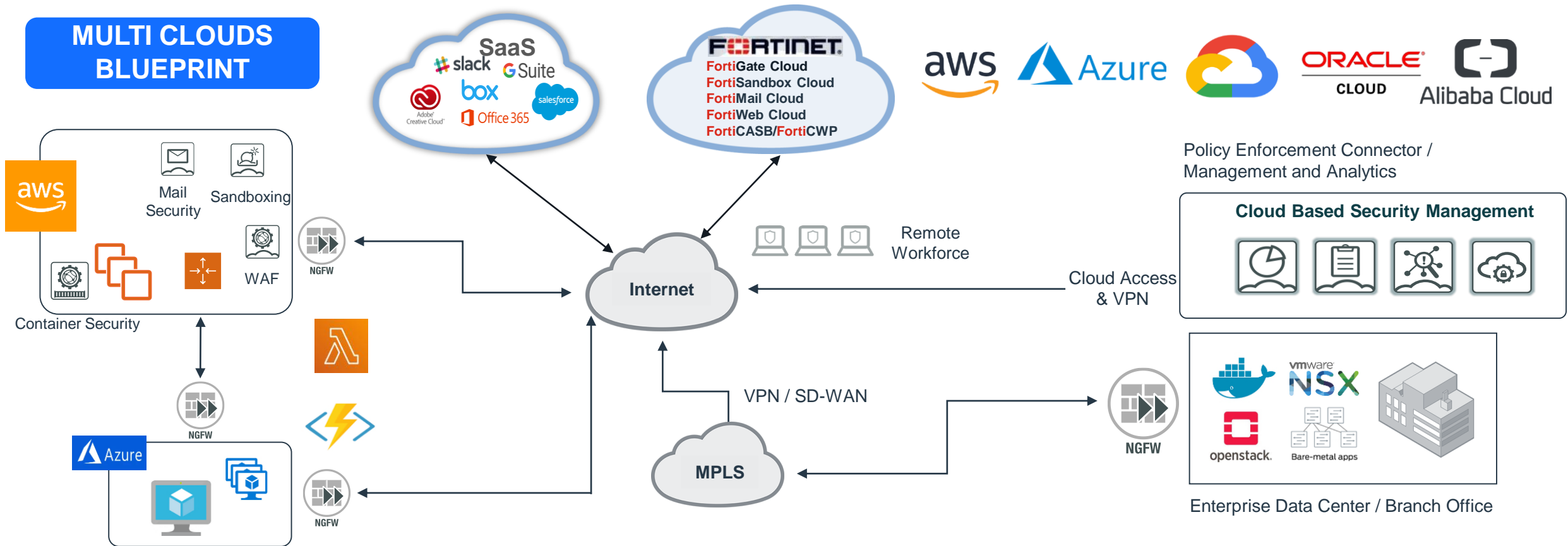
# Virtual Appliance Platforms

**B** BYOL **P** PAYG

	VMWare vSphere	Citrix Xen Server	Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Amazon AWS	Microsoft Azure	Oracle OPC	Google GCP	Aliyun
FortiGate-VM*	✓	✓	✓	✓	✓	✓	B P	B P	B	B P	B P
FortiManager-VM	✓	✓	✓	✓	✓	✓	B P	B	B	B	B
FortiAnalyzer-VM	✓	✓	✓	✓	✓	✓	B P	B	B	B	B
FortiWeb-VM	✓	✓	✓	✓	✓		B P	B P	B	B	
FortiWeb Manager-VM	✓						B				
FortiMail-VM	✓	✓		✓	✓	✓	B	B			
FortiAuthenticator-VM	✓		✓	✓	✓		B				
FortiADC-VM	✓	✓	✓	✓	✓	✓	B	B			
FortiVoice-VM	✓	✓		✓	✓		B	B			
FortiRecorder-VM	✓	✓		✓	✓		P				
FortiSandbox-VM	✓			✓			B P	P			
FortiSIEM	✓			✓			B				
FortiProxy-VM	✓			✓			B	B			

\* Also support AzureStack and RackSpace (PAYG)

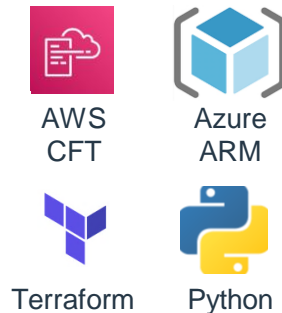
# MULTI CLOUDS BLUEPRINT



## Zero Trust Deployment

- Block lateral threat propagation in East-West direction
- Comprehensive protection in North-South direction
- Advanced security (L7 Firewall, IPS, and ATP) for all traffic paths
- Security workflows that adapt to deployment changes
- Auto-provisioning of security services across all platforms

## End-to-End Automation



## Operational Simplicity

- Single Policy Set across all deployments
- Leverage metadata instead of traditional IP in security policies
- Automated workload and metadata discovery
- Centralized management & analytics across deployments
- Intuitive visibility
- Automated VPN provisioning for multi-cloud connectivity
- Quarantine infected workloads automatically

## Cloud Security Components

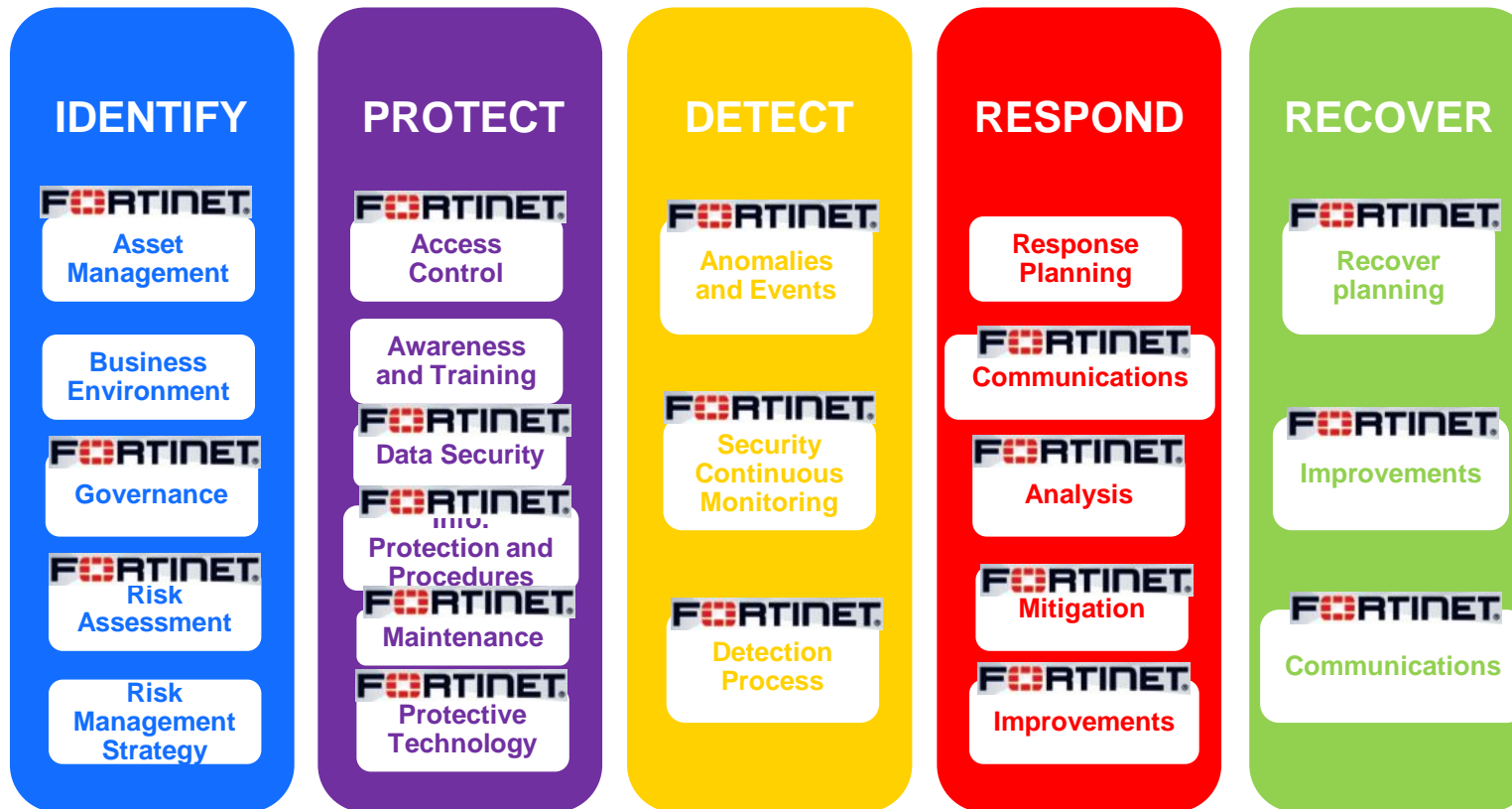
- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Auto Scaling Security
- Denial of Service Protection



# **Use cases:** **Fortinet for Thailand Acts**

# พ.ร.บ. การรักษาความปลอดภัยมั่นคงไซเบอร์

## NIST Cybersecurity Framework



**FORTINET**  
มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บไซต์  
(Web Application Security Standard : WAS)

**FORTINET**  
มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์  
(Web Security Standard : WSS)

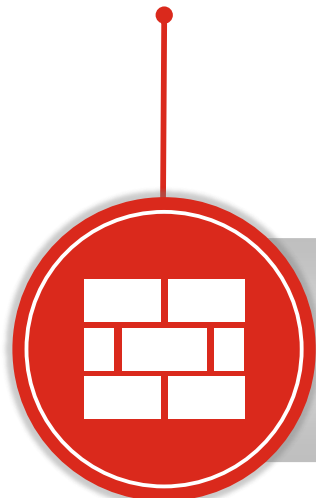
มาตรฐานการรักษาความมั่นคงปลอดภัยตามวิธีการแบบปลอดภัย พ.ร.บ. อุตกรรมทางอิเล็กทรอนิกส์

ที่มา NIST (National Institute of Standard and Technology) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ สหรัฐอเมริกา

ที่มา ETDA

# Fortinet สำหรับ พ.ร.บ. ไซเบอร์

## Network Security



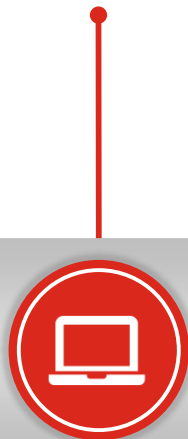
-   
**FortiGate**  
Enterprise Firewall
-   
**FortiProxy**  
Secure Web Gateway

## Multi-Cloud Security



-   
**FortiGate**  
Virtual Firewall
-   
**FortiGate**  
Cloud Firewall
-   
**FortiCASB**


## Endpoint Security



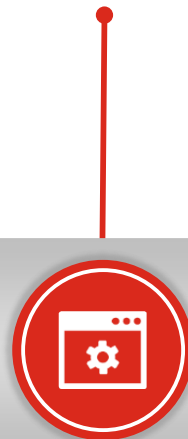
-   
**FortiClient**  
EPP
-   
**FortiSight**  
User and Entity Behaviors Analytics
-   
**FortiNAC**  
Network Access Control

## Email Security



-   
**FortiMail**  
Secure Email Gateway

## Web Application Security



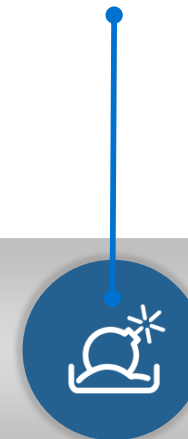
-   
**FortiWeb**  
Web Application Firewall
-   
**FortiADC**  
Load Balancer
-   
**FortiDDoS**  
Advance DDoS Protection

## Secure Unified Access



-   
**FortiAP**  
Access Point
-   
**FortiSwitch**  
Switching
-   
**FortiAuthenticator**  
Identity and Access Management


## Advanced Threat Protection



-   
**FortiSandbox**  
Advanced Threat Protection
-   
**FortiDeceptor**  
Insider Threat Detection
-   
**Fortisolator**  
Remote Browser

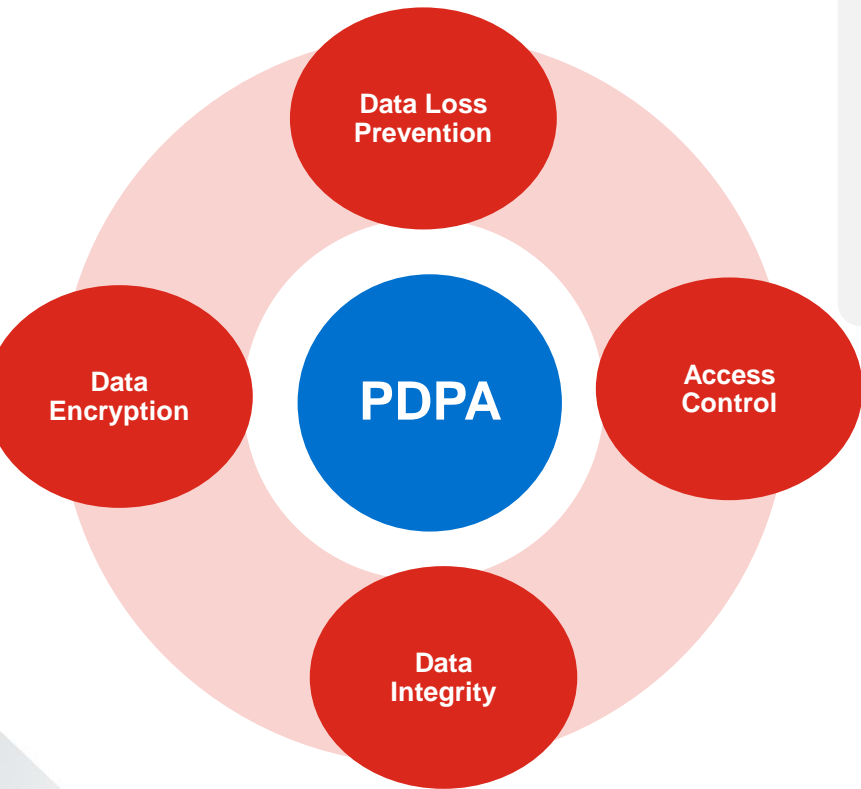
## Management - Analytics



-   
**FortiAnalyzer**  
Central Logging /Reporting
-   
**FortiManager**  
Central Security Management
-   
**FortiSIEM**  
Security Information & Event Management

# Fortinet สำหรับ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

Data Loss Prevention, Access Control, Data Integrity, Data Exposure and Data Encryption



**Built-In DLP**

<b>FortiGate</b>  Security Gateway	<b>FortiProxy</b>  Secure Web Caching Server	<b>FortiWeb</b>  Web App. Firewall	<b>FortiMail</b>  Mail Sec. Gateway
--	--	--	---

**Access Control**

<b>FortiToken</b>  2 Factor OTP Token	<b>FortiNAC</b>  IoT Access Control
---	---

**Built-In DLP**

FortiGate Cloud  
FortiMail Cloud  
FortiWeb Cloud  
FortiCASB

FTNT Hosted Services

**Built-In DLP**

aws  
Azure  
ORACLE® Cloud Infrastructure  
Alibaba Cloud

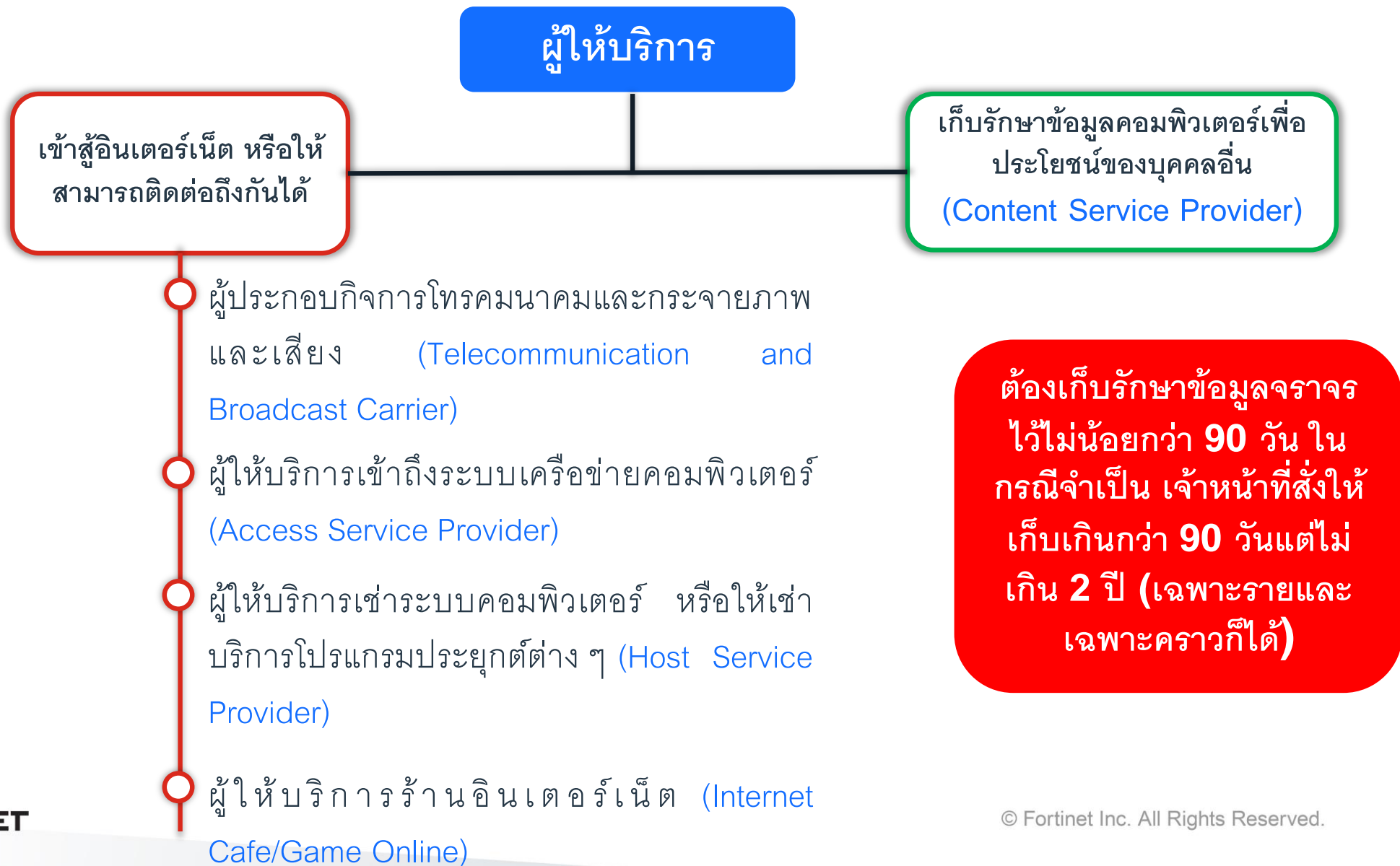
Public Cloud Instances

**Data Integrity**

<b>FortiWeb</b>  Web App. Firewall	<b>FortiClient</b>  Endpoint Security
--	---



# พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์



# Fortinet สำหรับ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์

เกินในสื่อ ที่รักษา  
ความครบถ้วน  
ถูกต้อง และ  
สามารถระบุตัวตน  
ผู้เข้าถึง

รักษา  
ความลับ  
และกำหนด  
ชั้นความลับ

จัดให้มีผู้  
ประสานงาน

ระบุ  
รายละเอียด  
ผู้ให้บริการ  
เป็น  
รายบุคคล

ถ้าใช้ระบบของ  
บุคคลที่สาม ผู้  
ให้บริการต้อง  
ดำเนินการให้มีการ  
ระบุและยืนยันตัวตน

LOG

FortiCloud Logs



Central Cloud  
Log & report

FortiAnalyzer



Central Log &  
report & Incident

FortiSIEM/SOAR

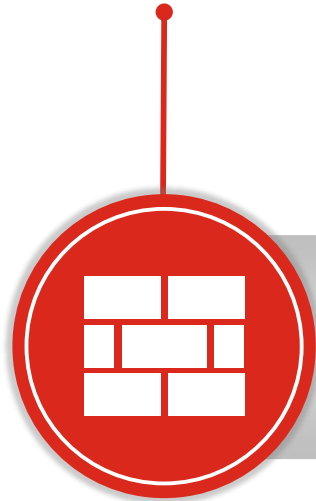




SIEM/SOAR

# Summary

# Fortinet Solutions



## Network Security



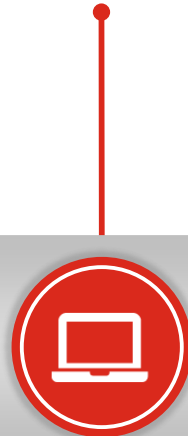
-   
**FortiGate**  
Enterprise Firewall
-   
**FortiProxy**  
Secure Web Gateway

## Multi-Cloud Security



-   
**FortiGate**  
Virtual Firewall
-   
**FortiGate**  
Cloud Firewall
-   
**FortiCASB**


## Endpoint Security



-   
**FortiClient**  
EPP
-   
**FortiSight**  
User and Entity Behaviors Analytics
-   
**FortiNAC**  
Network Access Control

## Email Security



-   
**FortiMail**  
Secure Email Gateway

## Web Application Security



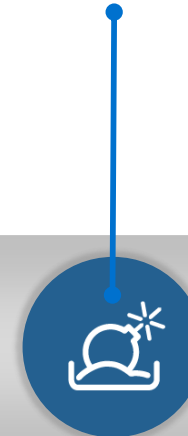
-   
**FortiWeb**  
Web Application Firewall
-   
**FortiADC**  
Load Balancer
-   
**FortiDDoS**  
Advance DDoS Protection




## Secure Unified Access



-   
**FortiAP**  
Access Point
-   
**FortiSwitch**  
Switching
-   
**FortiAuthenticator**  
Identity and Access Management

## Advanced Threat Protection



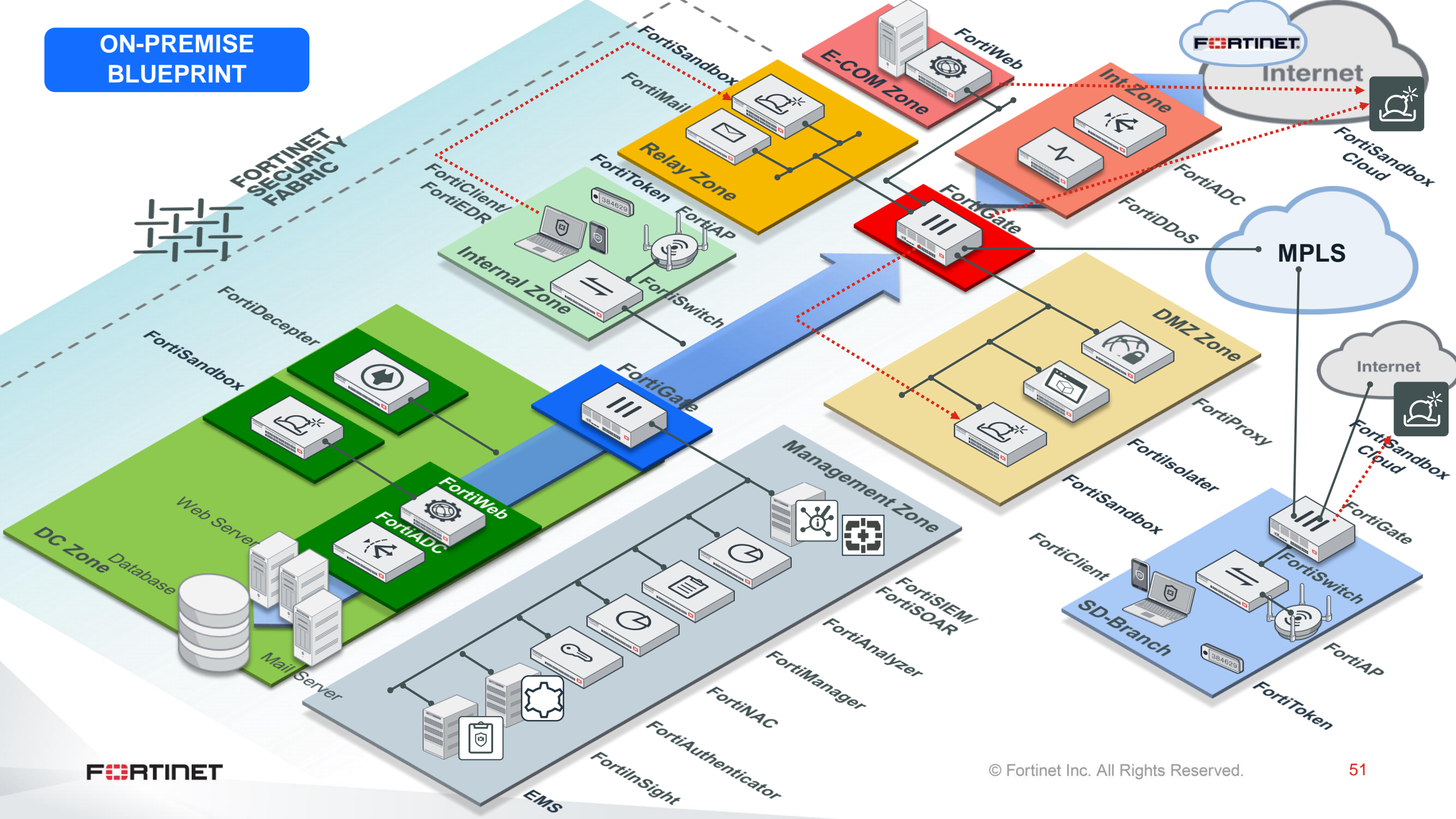
-   
**FortiSandbox**  
Advanced Threat Protection
-   
**FortiDeceptor**  
Insider Threat Detection
-   
**Fortisolator**  
Remote Browser

## Management - Analytics

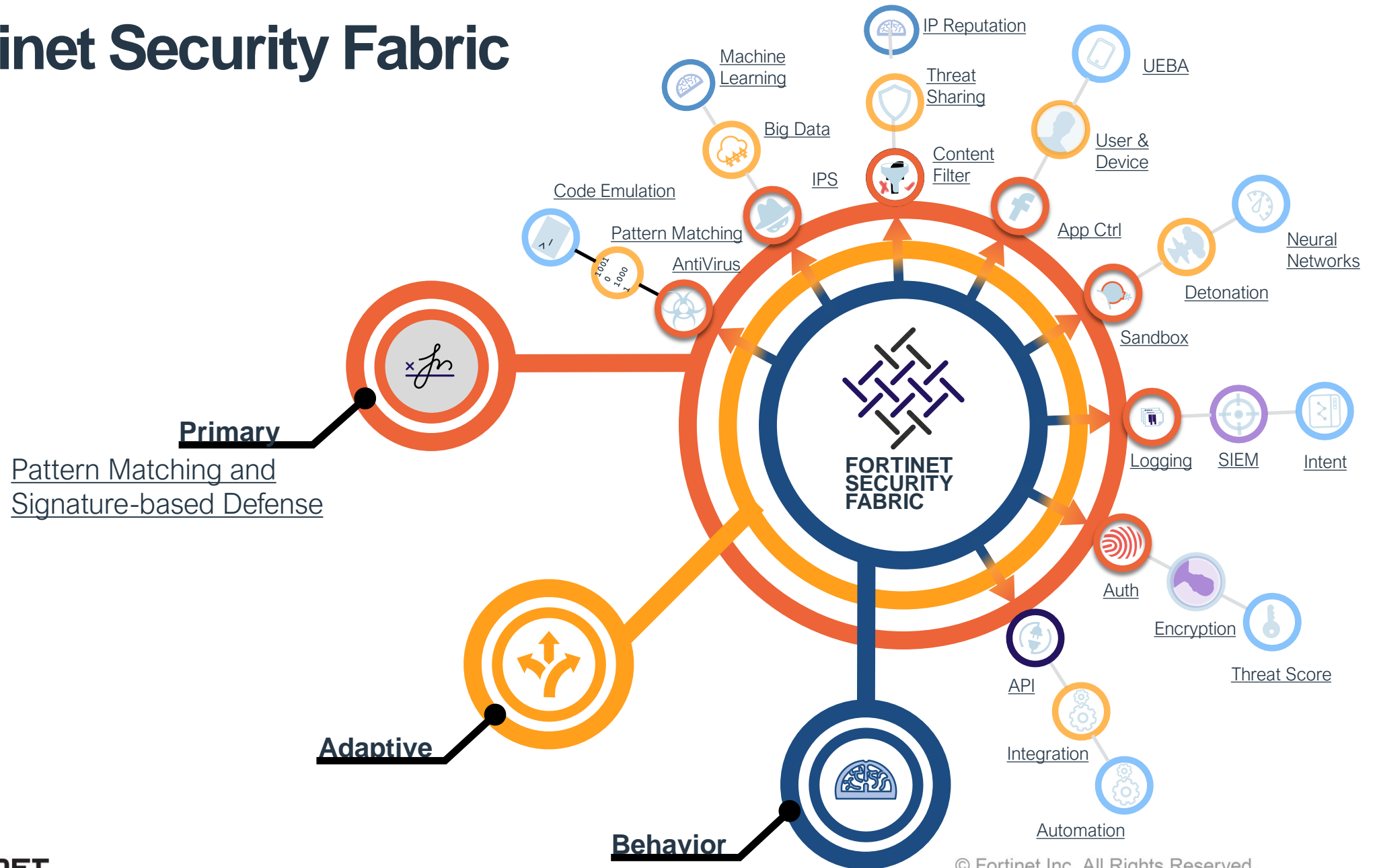


-   
**FortiAnalyzer**  
Central Logging /Reporting
-   
**FortiManager**  
Central Security Management
-   
**FortiSIEM**  
Security Information & Event Management

**ON-PREMISE BLUEPRINT**



# Fortinet Security Fabric





**F**ORTINET®