FORTINET®

Security Ready for Multi-Cloud

Sumit Onphaeng, System Engineer

Agenda

TODAY MULTI-CLOUD CHALLENGE

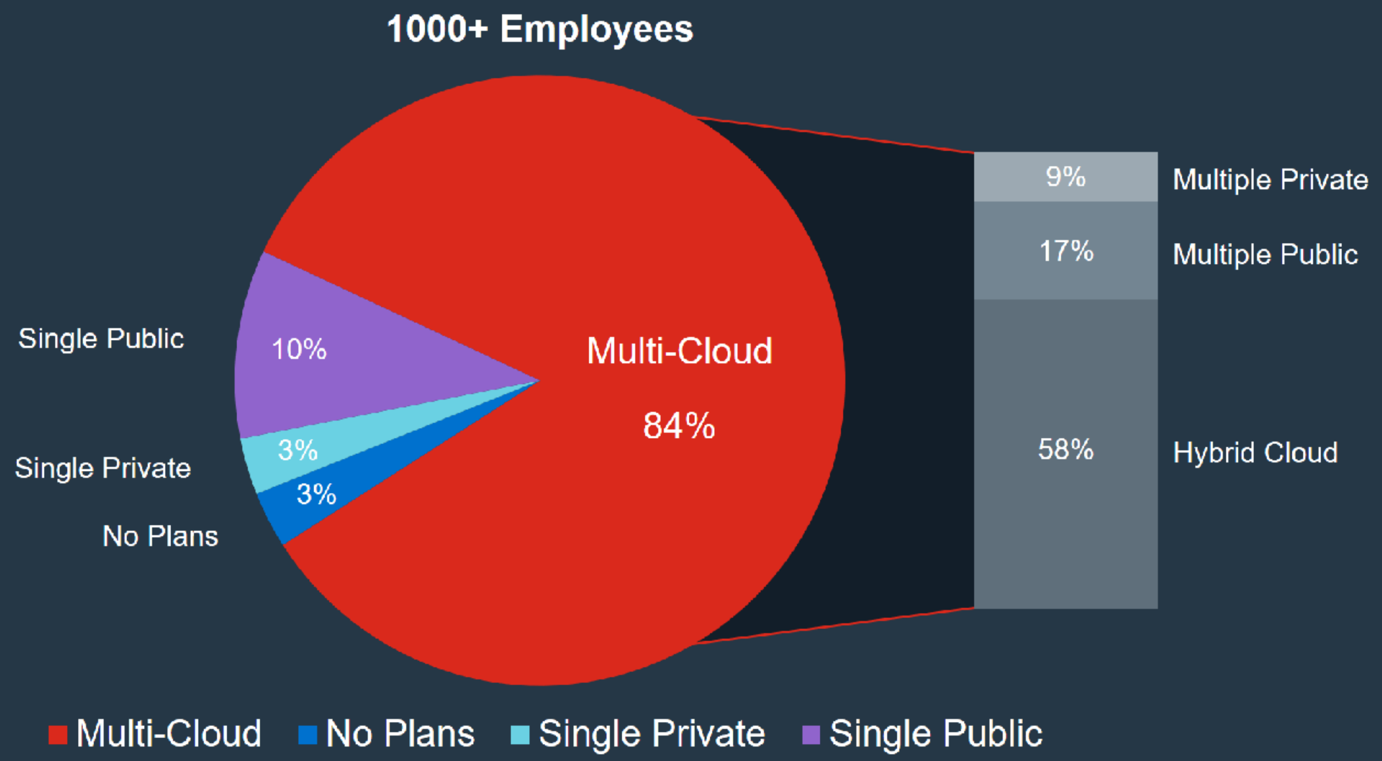
FORTINET MULTI-CLOUD SOLUTION

USE CASE

SUMMARY

Today Multi-Cloud Challenge

Dynamic Multi-Cloud



Source: RightScale 2019 State of the Cloud Report from Flexera

COMPLEXITY DRIVEN HUMAN ERROR

PLATFORM VISIBILITY

REGULATORY COMPLIANCE

EXPLOSION OF DATA

Cloud adoption Increases Attack Surface

“By 2021, 90% of web-enabled applications will have more surface area for attack in the form of exposed APIs rather than the UI, up from 40% in 2019.” –

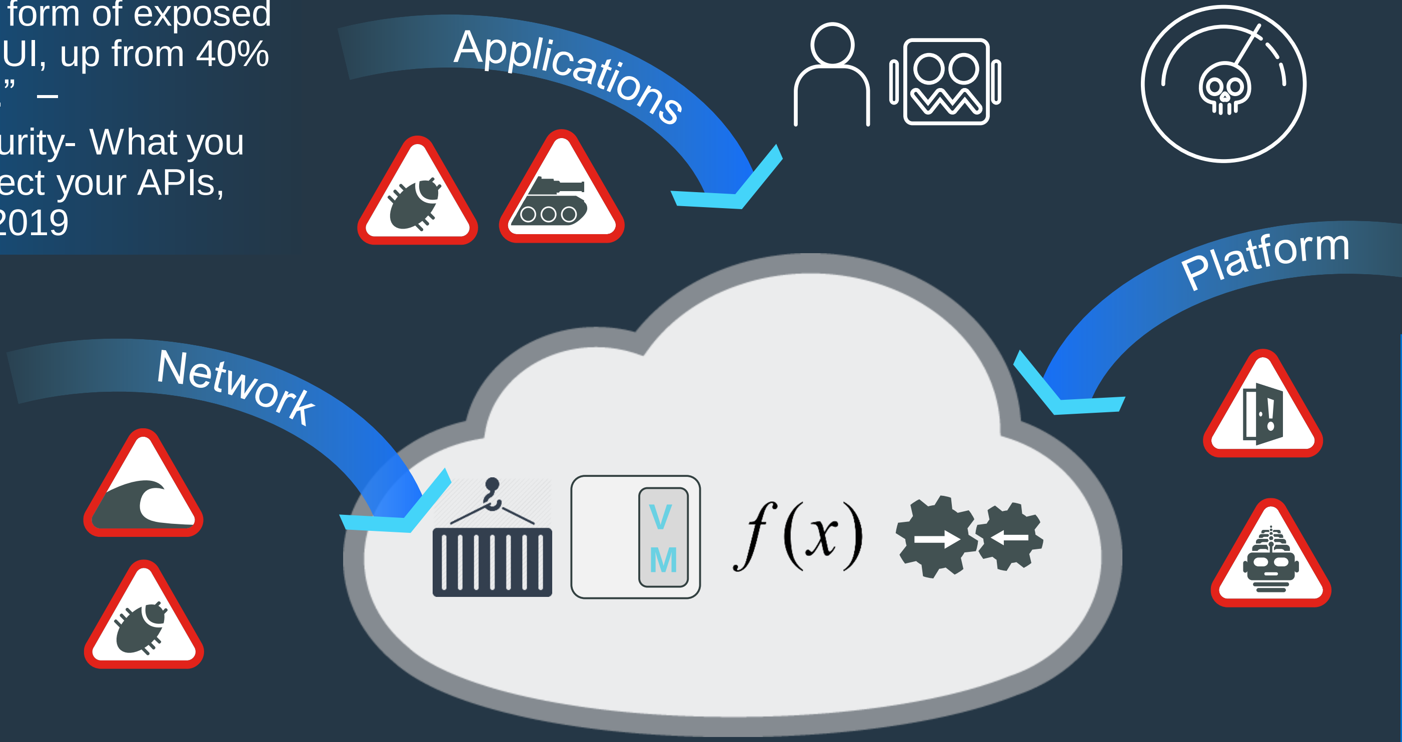
Gartner – API Security- What you need to do to protect your APIs, August 2019

THE RISE OF BOTS AND ATTACK FRAMEWORKS

MULTI-LAYERED ATTACK STRATEGIES

ATTACKS HIDDEN IN ENCRYPTED TRAFFIC

ENDLESS STREAM OF ZERO-DAY VULNERABILITIES



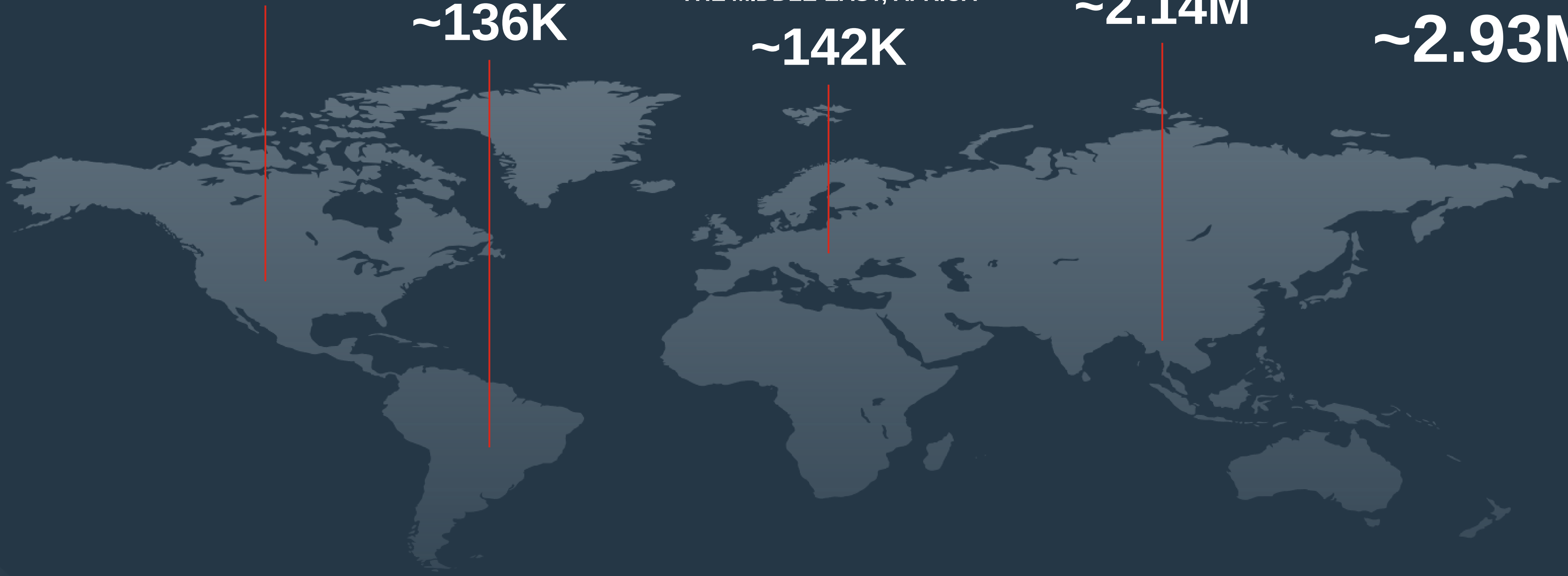
Multi Cloud

“Through 2025, 99% of cloud security failures will be the customer’s fault.”

Gartner – A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic, 25, February 2019

Global Shortage of Skilled Security Professionals

Gap in Cybersecurity Professionals By Region



NORTH AMERICA
~498K

LATIN AMERICA
~136K

EUROPE,
THE MIDDLE EAST, AFRICA
~142K

ASIA PACIFIC
~2.14M

GLOBAL
~2.93M

Unlocking Business Agility with Security

Dynamic Multi Cloud Reality

Private Public SaaS

Security for any platform

Cloud Increases Attack Surface

Multi Layer Cloud Security

Shortage in Skilled Security Professionals

Single Pane of Glass Management

Shared Responsibility Model

■ **Customer management of risk**

Data classification and data accountability

◩ **Shared management of risk**

Identity & access management | End point devices

□ **Provider management of risk**

Physical | Networking

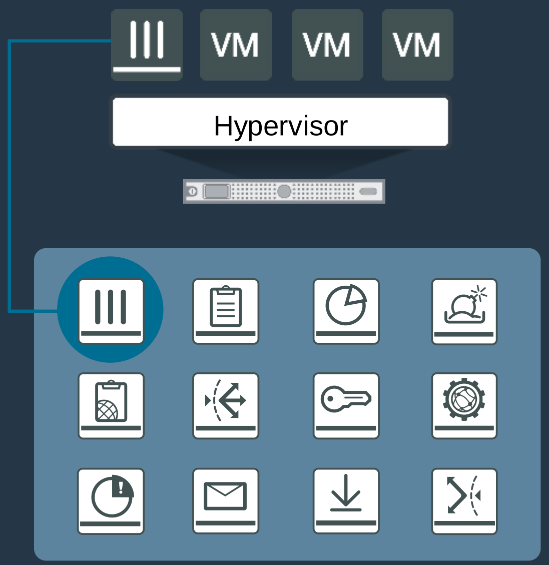
Responsibility	On-Prem	IaaS	SaaS
Platform Control	■	■	■
Visibility	■	■	■
Access Control	■	■	◩
Data Classification	■	■	◩
Application Protection	■	■	□
Libraries/Containers	■	■	□
End Point Protection	■	◩	□
Configuration	■	◩	□
Network Protection	■	◩	□
Physical Security	■	□	□

Fortinet Multi-Cloud Solution

Cloud Security Evolution

Virtualization → Private Cloud ↔ Hybrid ↔ Public Cloud

Hypervisor Port



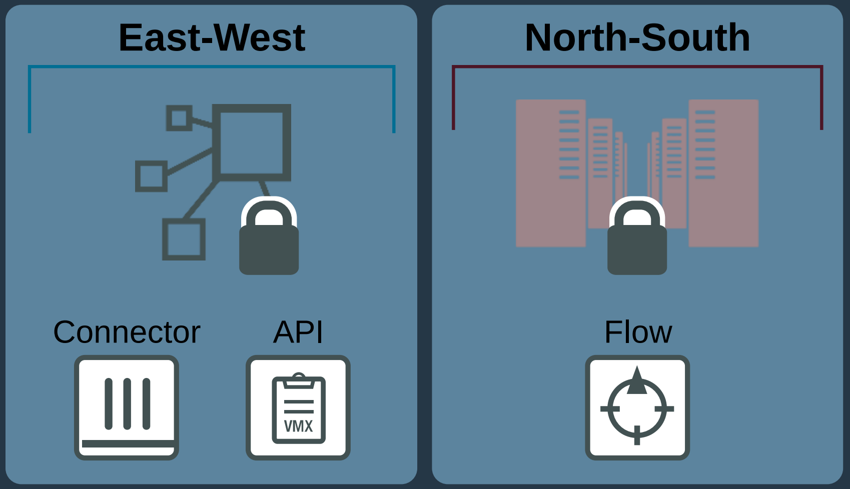
VM

VM

VM

Hypervisor

SDN - Orchestration Integration



East-West

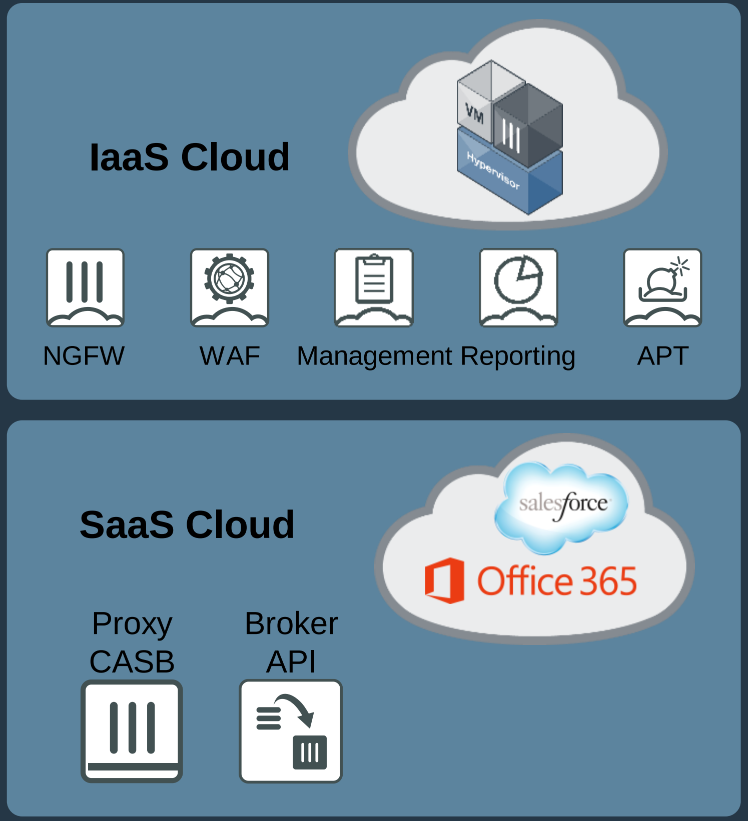
Connector

API

North-South

Flow

On-Demand



IaaS Cloud

NGFW

WAF

Management

Reporting

APT

SaaS Cloud

Proxy CASB

Broker API

Cloud Security 3 Pillars

Network Security

NGFW
Segmentation
VPN
IPS
App Control

Application Security

Compliance
Web Applications
Vulnerabilities
Bot Security
API Security

Platform Visibility & Control

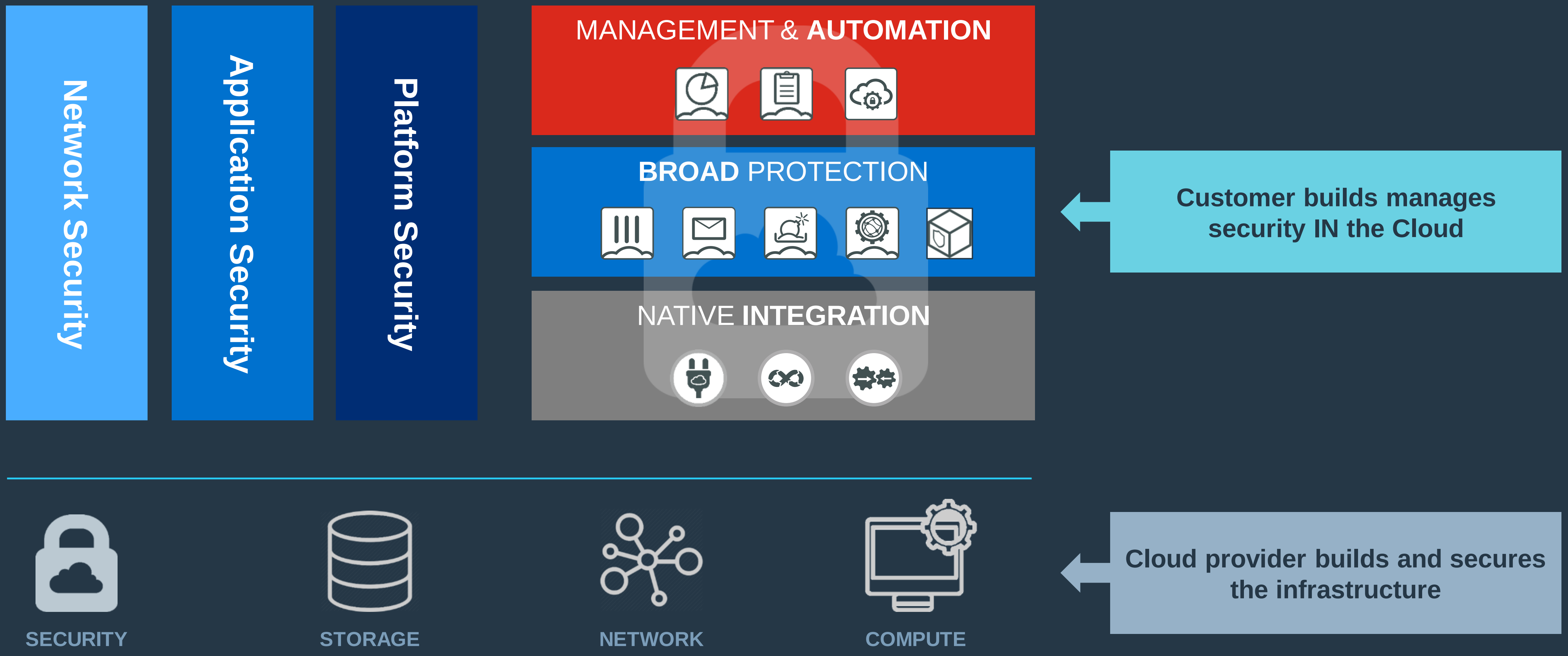
Configurations
Account Activity
Traffic Analysis
Data Security
Compliance

Virtual Machine

Security as a Service

Private — Public — SaaS

FORTINET



Network Security

Application Security

Platform Security

MANAGEMENT & **AUTOMATION**

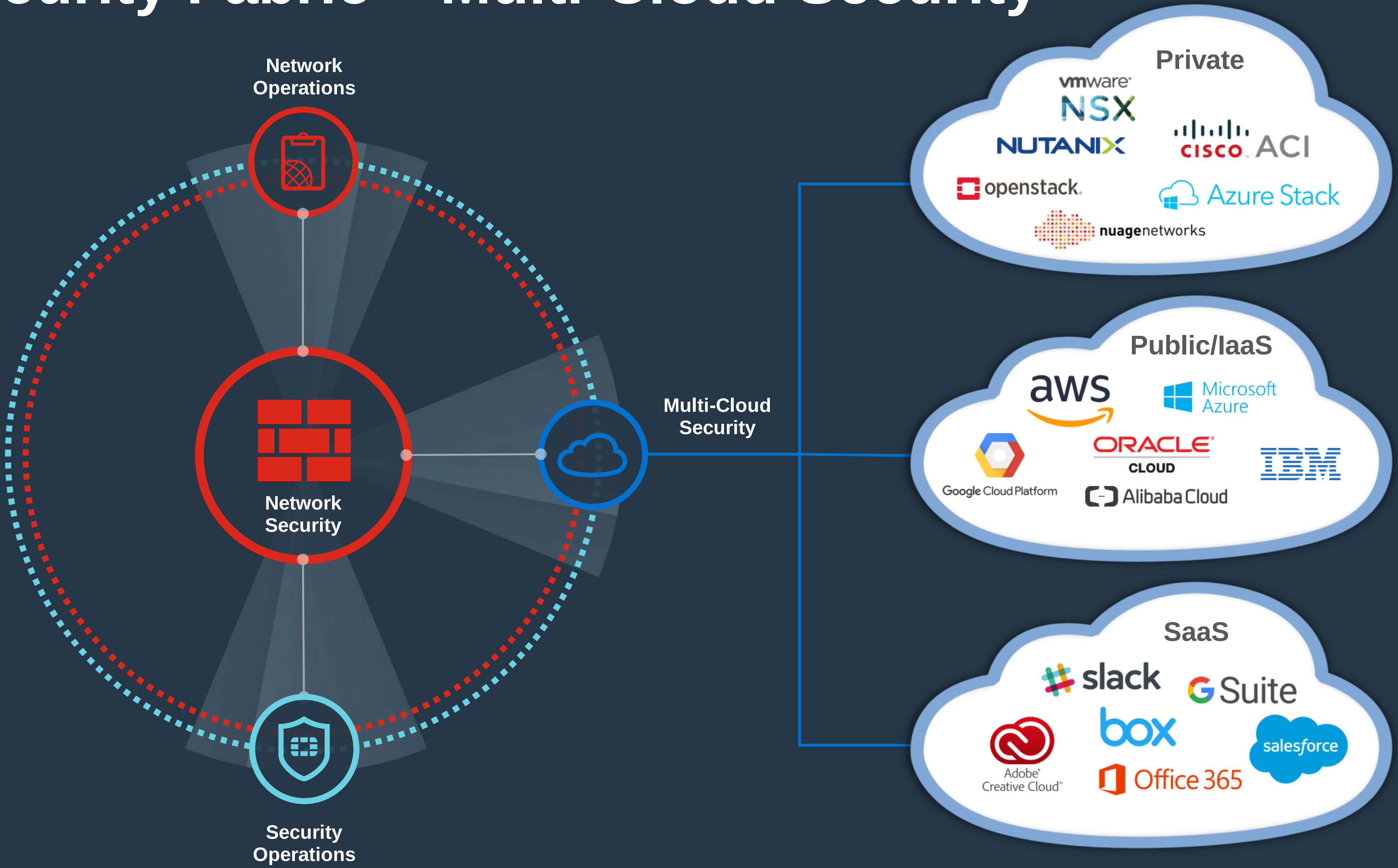
BROAD PROTECTION

NATIVE **INTEGRATION**

Customer builds manages security IN the Cloud

Cloud provider builds and secures the infrastructure

Security Fabric – Multi-Cloud Security



FORTINET

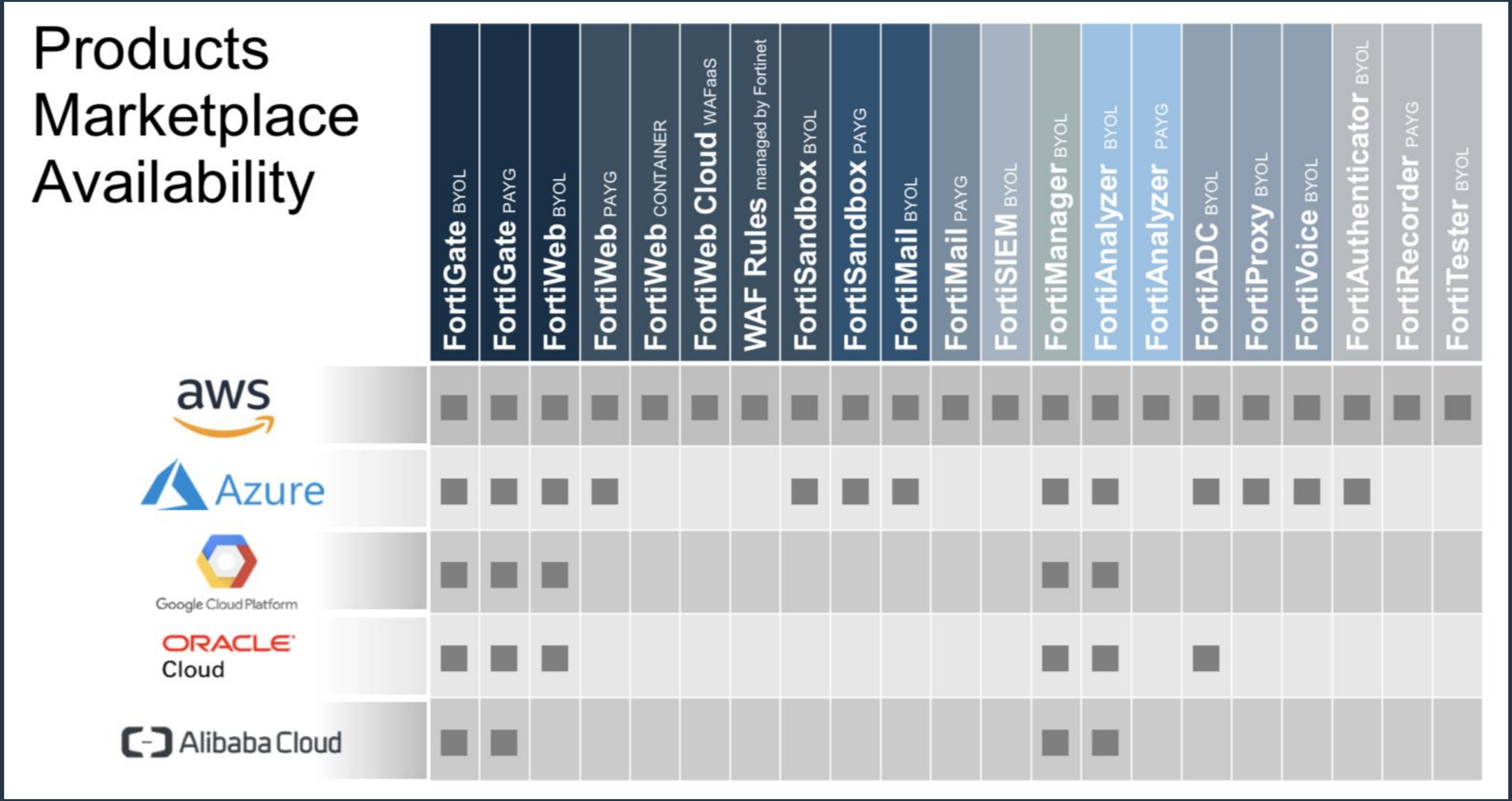
NATIVE INTEGRATION

	aws	Azure		ORACLE CLOUD	Alibaba Cloud
Service Integration	WAF Rules Guard Duty				
Config Templates	Cloud Formation, Quick Start Guides	ARM Template		OCI Terraform	
Auto-Scaling	Config Sync	Config Sync	Config Sync		Config Sync
High Availability	Session and Config Sync	Config Sync	Config Sync	Config Sync	Session and Config Sync
Container Security	EKS	AKS	GKE	OKE	
Automation Scripts	Lambda, Cloud-init	Azure Functions, Cloud-Init	Cloud Functions, Cloud Init	Cloud Init	Cloud Init
Optimization	SR-IOV on C5n	SR-IOV		Native Mode support	
Connectors	Topology, Meta-Data	Meta-Data	Meta-Data	Meta-Data	Meta-Data

NATIVE **INTEGRATION**

	VM	VM	VM	VM	VM	VM	VM	VM
Fabric Connectors	🟩	🟩	🟩	🟩	🟩	🟩		
Automation Scripts	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Service Insertion					🟩	🟩	🟩	🟩
High Availability	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	vmware ESX/ESXi	Microsoft Hyper-V	KVM	CITRIX XenServer	CISCO Cisco ACI	vmware NSX	NUTANIX	vmware NSX-T 2.2.0

BROAD PROTECTION



Products Marketplace Availability

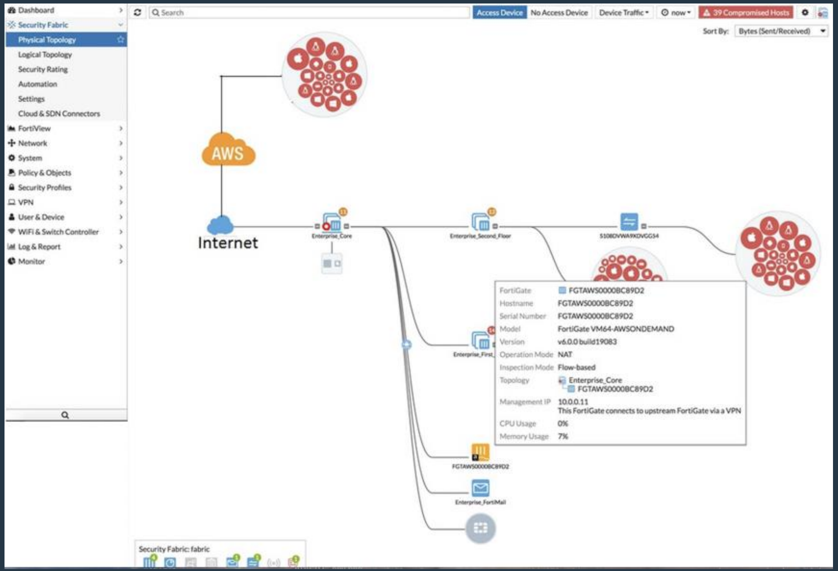
	FortiGate BYOL	FortiGate PAYG	FortiWeb BYOL	FortiWeb PAYG	FortiWeb CONTAINER	FortiWeb Cloud WAFaaS	WAF Rules managed by Fortinet	FortiSandbox BYOL	FortiSandbox PAYG	FortiMail BYOL	FortiMail PAYG	FortiSIEM BYOL	FortiManager BYOL	FortiAnalyzer BYOL	FortiAnalyzer PAYG	FortiADC BYOL	FortiProxy BYOL	FortiVoice BYOL	FortiAuthenticator BYOL	FortiRecorder PAYG	FortiTester BYOL
aws	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Azure	■	■	■	■				■	■	■			■	■		■	■	■	■		
Google Cloud Platform	■	■	■										■	■							
ORACLE Cloud	■	■	■										■	■		■					
Alibaba Cloud	■	■											■	■							

BROAD PROTECTION

	VM	VM	VM	VM	VM	VM	VM	VM
Fabric Connectors	🟩	🟩	🟩	🟩	🟩	🟩		
Automation Scripts	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Service Insertion					🟩	🟩	🟩	🟩
High Availability	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	vmware™ ESX/ESXi	Microsoft Hyper-V	KVM	CiTRiX® XenServer	CISCO Cisco ACI	vmware® NSX	NUTANIX	vmware® NSX-T 2.2.0

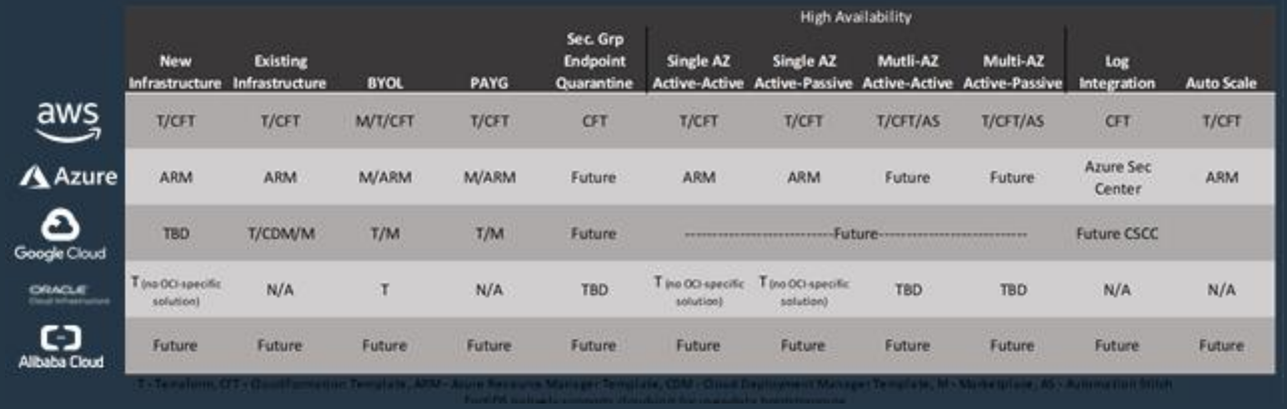
MANAGEMENT & AUTOMATION

AWS Fabric Integration View



FortiGate FGTAWS0000BC89D2
Hostname FGTAWS0000BC89D2
Serial Number FGTAWS0000BC89D2
Model FortiGate VM64-AWSONDEMAND
Version v6.0.0 build19083
Operation Mode NAT
Inspection Mode Flow-based
Topology Enterprise_Core
FGTAWS0000BC89D2
Management IP 10.0.0.11
This FortiGate connects to upstream FortiGate via a VPN
CPU Usage 0%
Memory Usage 7%

Public Cloud Automation & Deployment Templates

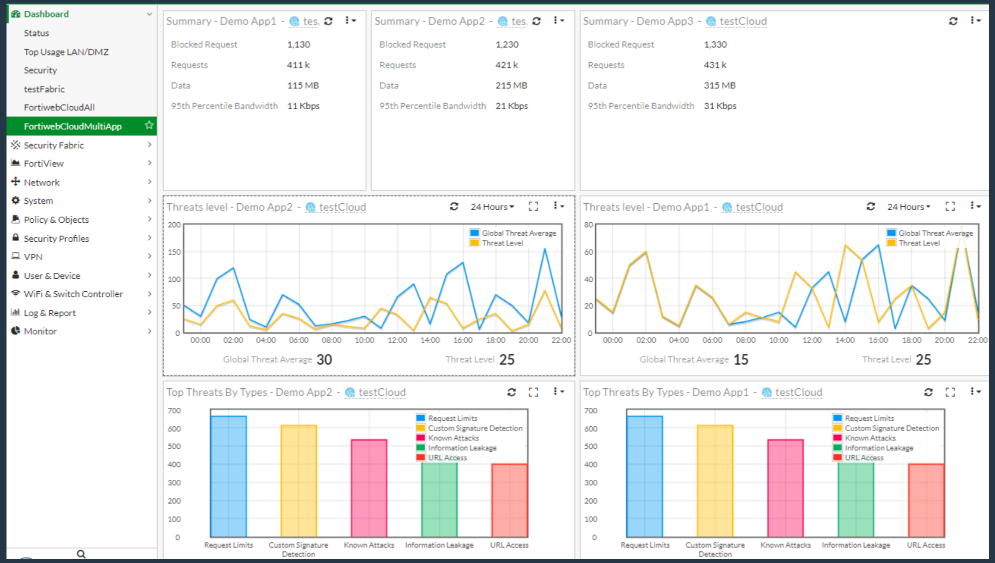


						High Availability					
	New Infrastructure	Existing Infrastructure	BYOL	PAYG	Sec. Grp Endpoint Quarantine	Single AZ Active-Active	Single AZ Active-Passive	Mutli-AZ Active-Active	Multi-AZ Active-Passive	Log Integration	Auto Scale
aws	T/CFT	T/CFT	M/T/CFT	T/CFT	CFT	T/CFT	T/CFT	T/CFT/AS	T/CFT/AS	CFT	T/CFT
Azure	ARM	ARM	M/ARM	M/ARM	Future	ARM	ARM	Future	Future	Azure Sec Center	ARM
Google Cloud	TBD	T/CDM/M	T/M	T/M	Future	---------------------------Future---------------------------				Future CSCC	
ORACLE	T (no OCI-specific solution)	N/A	T	N/A	TBD	T (no OCI-specific solution)	T (no OCI-specific solution)	TBD	TBD	N/A	N/A
Alibaba Cloud	Future	Future	Future	Future	Future	Future	Future	Future	Future	Future	Future

T - Terraform, CFT - CloudFormation Template, ARM - Azure Resource Manager Template, CDM - Cloud Deployment Manager Template, M - Marketplace, AS - Automation Stitch

[illegible]

FortiWeb Cloud Fabric Integration View



Summary - Demo App1 - tes.

Blocked Request	1,130
Requests	411 k
Data	115 MB
95th Percentile Bandwidth	11 Kbps

Summary - Demo App2 - tes.

Blocked Request	1,230
Requests	421 k
Data	215 MB
95th Percentile Bandwidth	21 Kbps

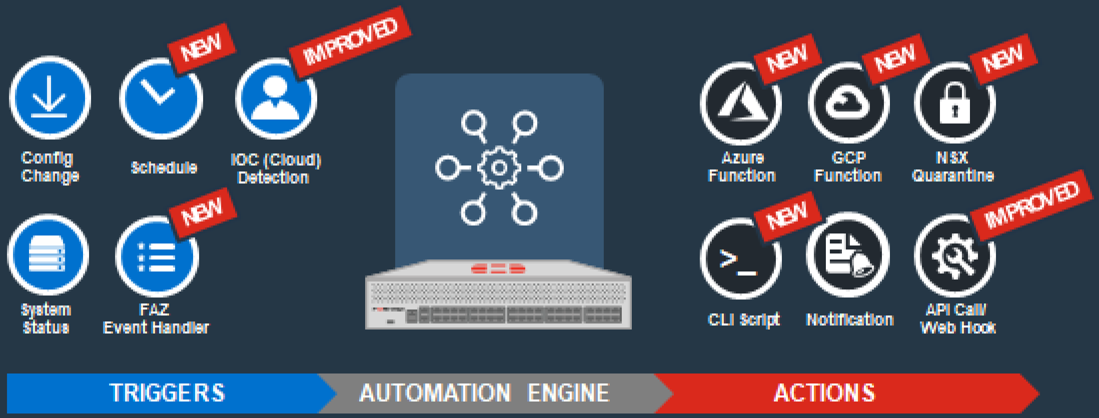
Summary - Demo App3 - testCloud

Blocked Request	1,330
Requests	431 k
Data	315 MB
95th Percentile Bandwidth	31 Kbps

Threats level - Demo App2: Global Threat Average 30, Threat Level 25

Threats level - Demo App1: Global Threat Average 15, Threat Level 25

Automation & Dev-Ops



Config Change

NEW Schedule

IMPROVED IOC (Cloud) Detection

System Status

NEW FAZ Event Handler

NEW Azure Function

NEW GCP Function

NEW NSX Quarantine

NEW CLI Script

Notification

IMPROVED API Call/ Web Hook

TRIGGERS → AUTOMATION ENGINE → ACTIONS

Multi-Cloud Use Case

Securing the Cloud Use Cases

PLATFORM SECURITY	▪ SaaS Visibility and Control ▪ Cloud Infrastructure Visibility and Control ▪ Compliance in the Cloud ▪ Cloud Based Security management and analytics
APPLICATION SECURITY	▪ Web Application Security ▪ Container Security ▪ Secure Productivity
NETWORK SECURITY	▪ Secure Hybrid Cloud ▪ Cloud Security Services Hub ▪ Logical (Intent Based) Segmentation ▪ Secure Remote Access

Network Security: Cloud Security Services Hub

- Branch Connectivity/On-Ramp

  SD-WAN

- Hybrid Cloud

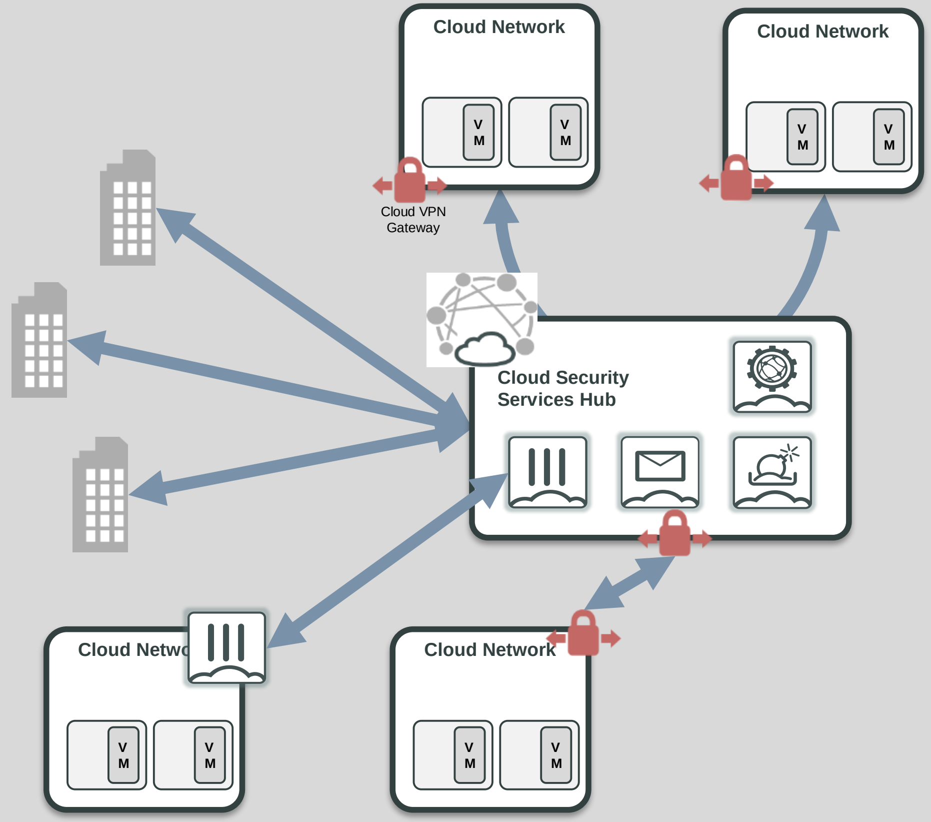
  High Speed Site-to-Site or Site-to-Cloud connectivity

- VPC to VPC segmentation

  Intent-Based Segmentation

- Remote Access

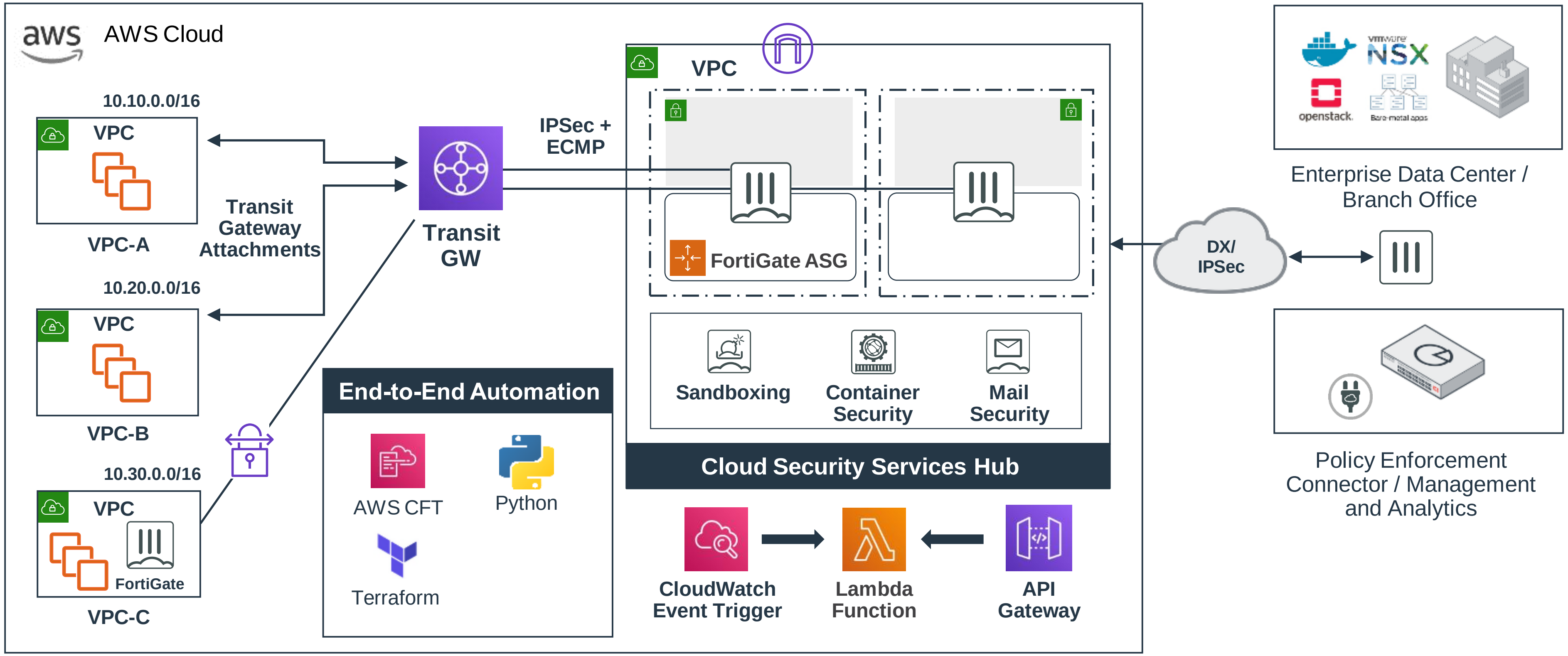
  Terminate connectivity in the Hub



Cloud Security Services Hub with Autoscaling and AWS Transit Gateway

Operational Simplicity

- Single Policy Set across all deployments
- Dynamically scalable security services
- 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



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
- Container Security
- Denial of Service Protection

Return

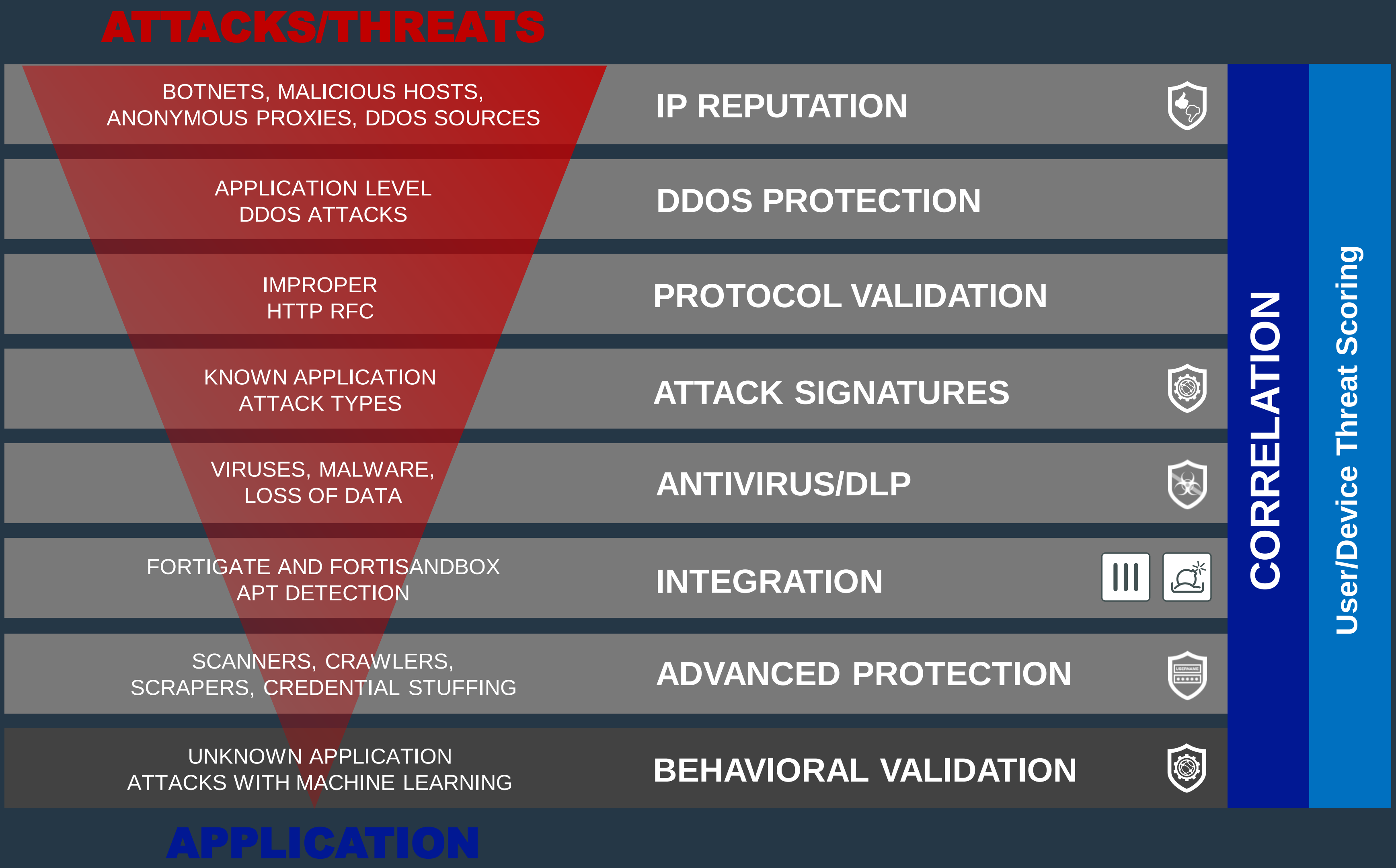
Application Security: Web Applications and Containers

- Digital Innovation drives Increased adoption Web Services and APIs
- Micro Services and Serverless API gateways common delivery platform
- Web Servers and API servers exposed to the internet
- Web Server Vulnerabilities affect the entire stack
- Botnets on the rise

docker

kubernetes

FortiWeb - Application Security



ATTACKS/THREATS

BOTNETS, MALICIOUS HOSTS, ANONYMOUS PROXIES, DDOS SOURCES	IP REPUTATION
APPLICATION LEVEL DDOS ATTACKS	DDOS PROTECTION
IMPROPER HTTP RFC	PROTOCOL VALIDATION
KNOWN APPLICATION ATTACK TYPES	ATTACK SIGNATURES
VIRUSES, MALWARE, LOSS OF DATA	ANTIVIRUS/DLP
FORTIGATE AND FORTISANDBOX APT DETECTION	INTEGRATION
SCANNERS, CRAWLERS, SCRAPERS, CREDENTIAL STUFFING	ADVANCED PROTECTION
UNKNOWN APPLICATION ATTACKS WITH MACHINE LEARNING	BEHAVIORAL VALIDATION

CORRELATION

User/Device Threat Scoring

APPLICATION

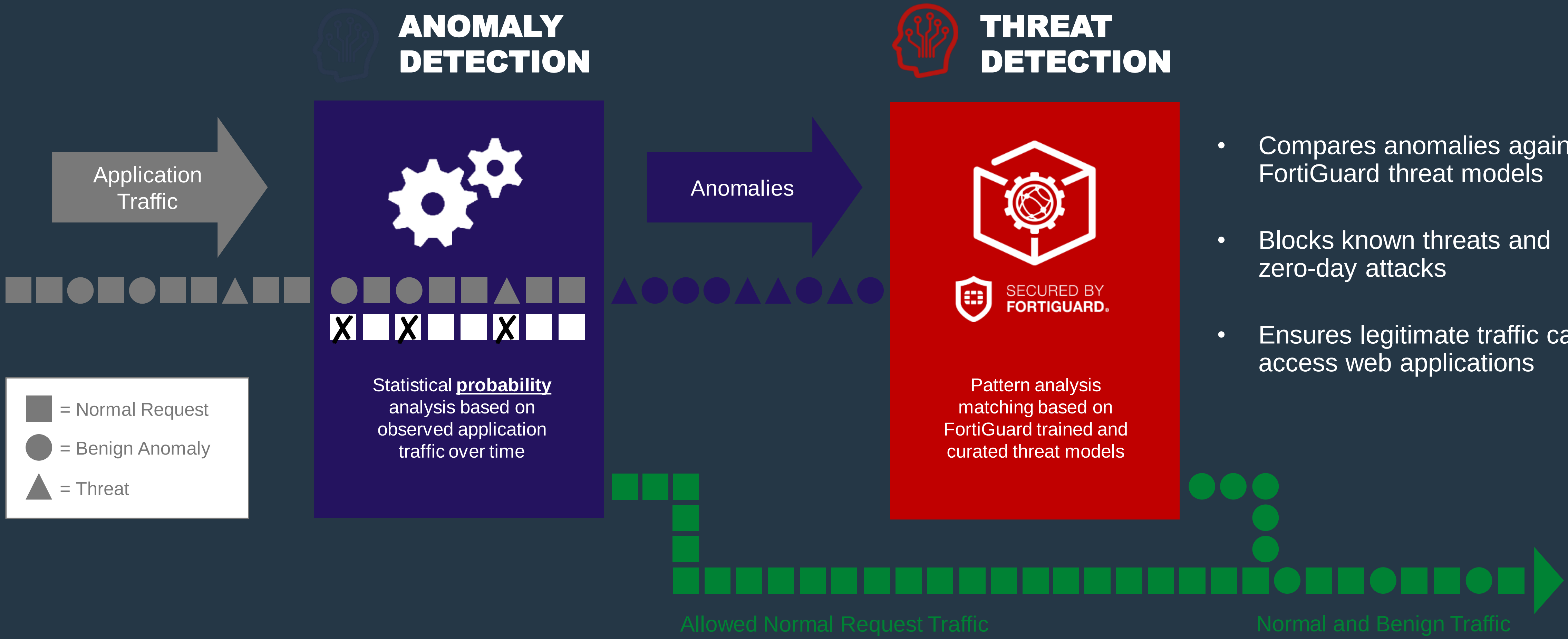
FortiWeb Application Security

Fortinet uniquely leverages Machine Learning (ML) to address key challenges organizations face when deploying Internet-facing web services:

- Web App Protection
- Bot Mitigation
- API Protection

Machine Learning-based Web App Protection

How it works



■ = Normal Request
● = Benign Anomaly
▲ = Threat

Statistical **probability** analysis based on observed application traffic over time

Pattern analysis matching based on FortiGuard trained and curated threat models

- Compares anomalies against FortiGuard threat models
- Blocks known threats and zero-day attacks
- Ensures legitimate traffic can access web applications

Fortinet Web Application and API Security Solutions

Multiple options for maximum deployment flexibility

aws AWS Cloud

Public Cloud VM

- Multiple VM models
- Web Apps, Botnets and API Security covering OWASP top 1 and more
- BYOL and PAYG
- AWS, Azure, Google Cloud, Oracle Cloud

SaaS

- Dynamically AWS region closest to app
- ML Enabled
- Data or Bandwidth Based
- PAYG and BYOL

Container

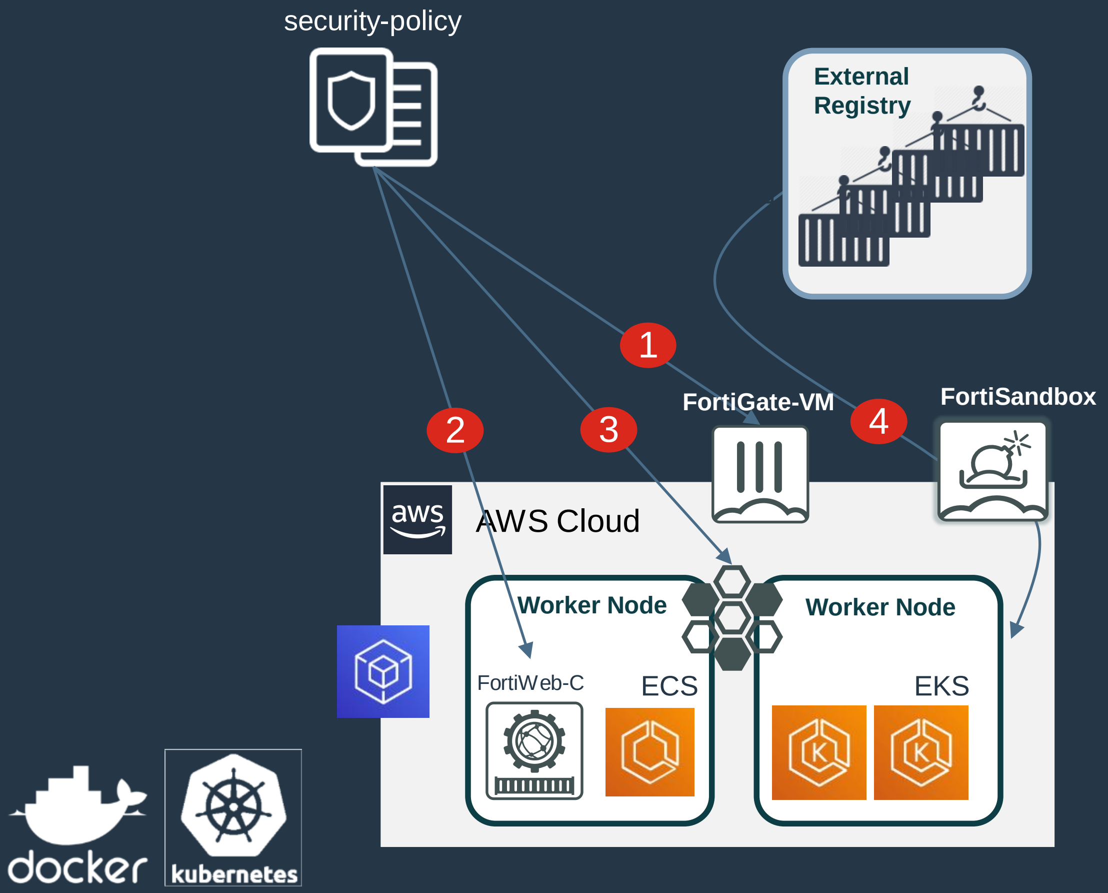
- AWS ECS Service
- ML Enabled for Web Apps
- Web Apps, Botnets and API Security covering OWASP top 1 and more

aws WAF

Partner Rules

- WAFv1 & WAFv2 Support
- ALB & API Gateway Support
- Basic to complete OWASP Top 10 protection

Container Security



SOLUTION

1 **Aware -** Aware to Container meta-data / north-south
2 **Enabled -** Delivered as a Container
3 **Integrated -** Service mesh integration / east-west
4 **Registry -** Container image Security Scanning

BENEFITS

- **Security for all stages of container lifecycle**
- **Faster development with security built-in**

UNIQUE SELLING POINTS

- **WebAppSec integrated with Container App lifecycle**
- **Joint solutions enable container-integrated Security**

Products

FortiGate-VM, FortiSandbox-VM/Cloud, FortiCWP, FortiWeb-CE

Platform Security: Cloud Visibility and Compliance

→ Risk Management

→ Data Security

→ Threat Detection and Response

→ Compliance

→ Traffic Analysis and Investigation

FortiCWP/CASB

Key Functions

Visibility

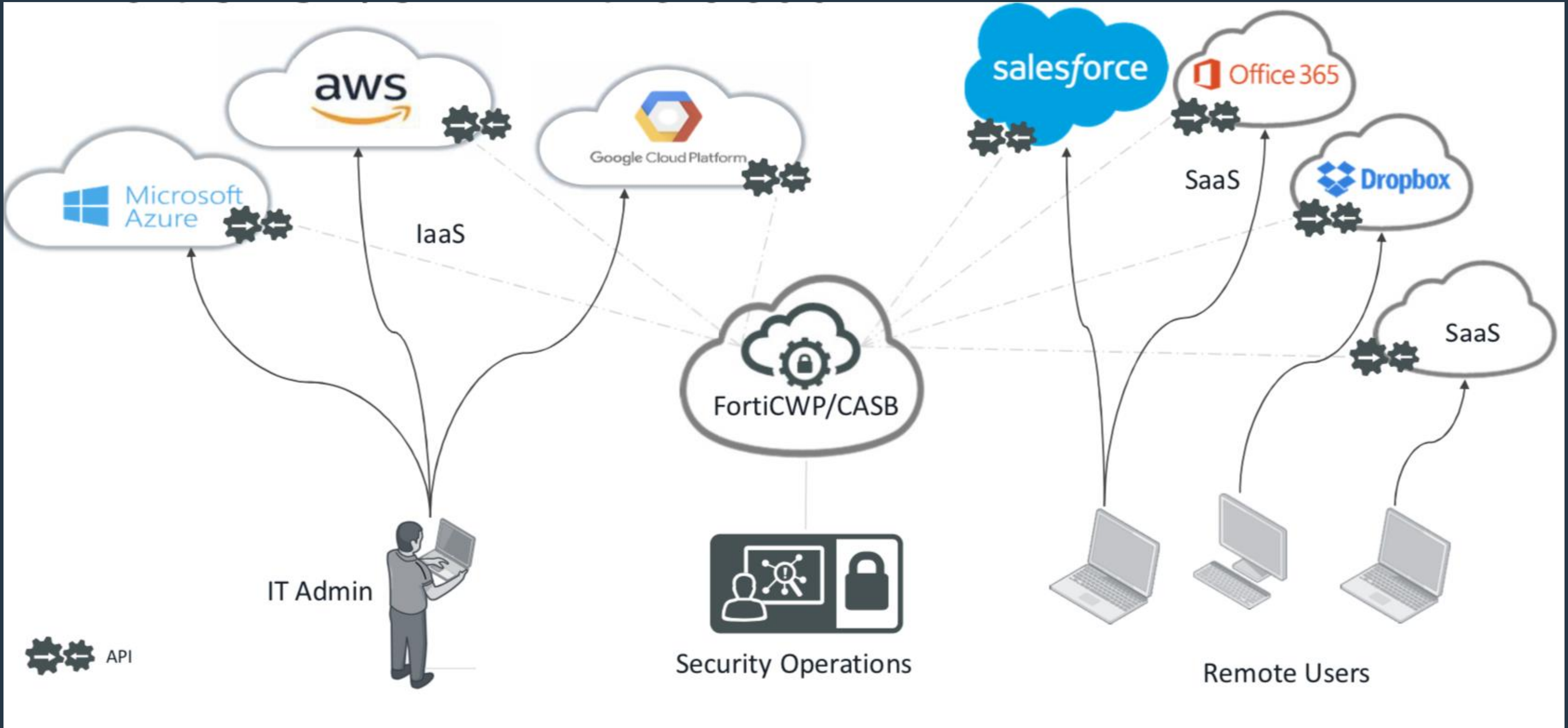
Security posture, configuration, and activity across clouds

Automation & Remediation

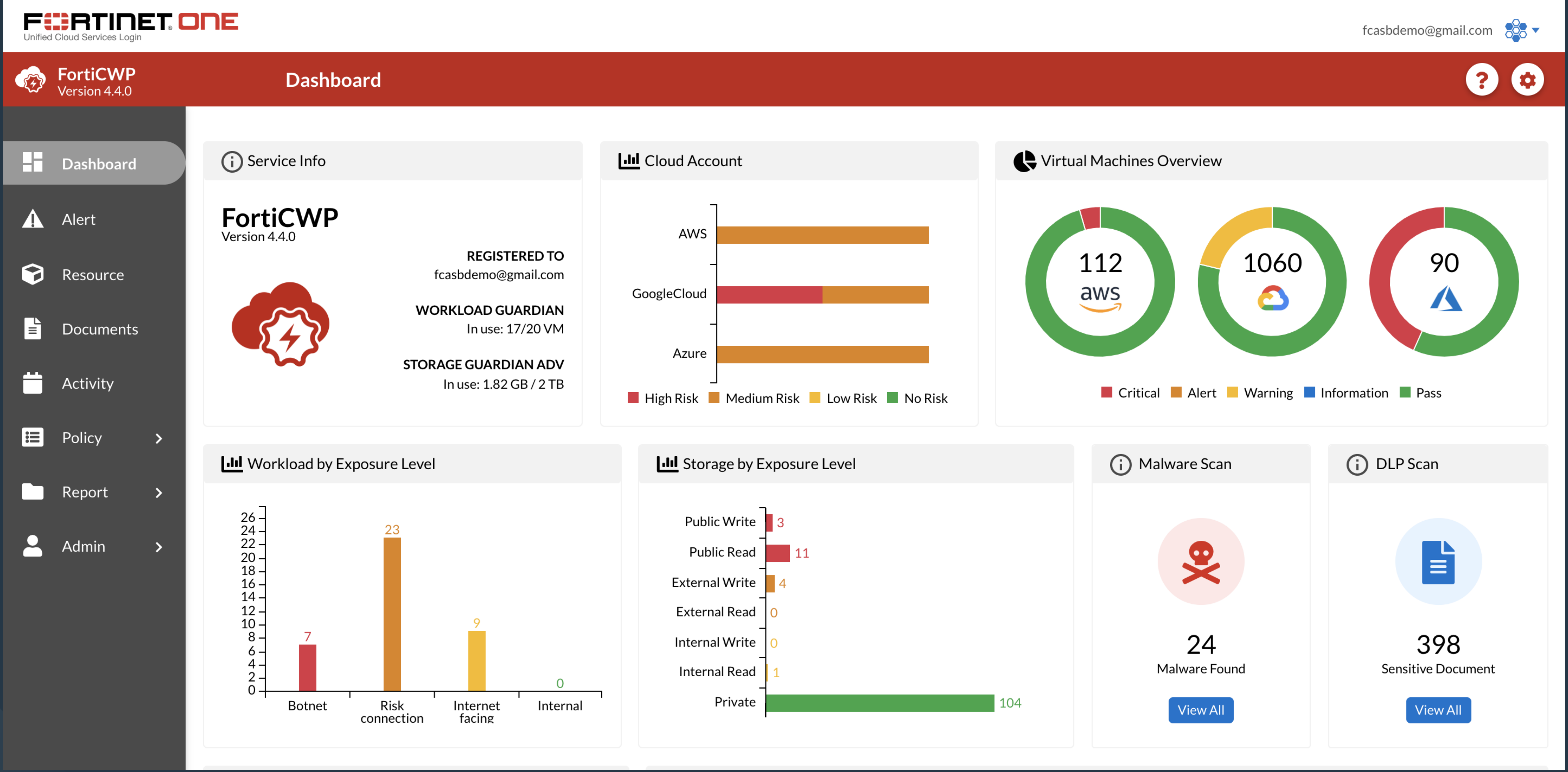
Policies to automate alerts and trigger actions based on security events

Compliance Discovery and Reporting

Security Visibility FortiCWP/CASB



FortiCWP – IaaS Visibility



FORTINET ONE
Unified Cloud Services Login

fcasbdemo@gmail.com

FortiCWP
Version 4.4.0

Dashboard

- Dashboard
- Alert
- Resource
- Documents
- Activity
- Policy >
- Report >
- Admin >

Service Info

FortiCWP
Version 4.4.0

REGISTERED TO
fcasbdemo@gmail.com

WORKLOAD GUARDIAN
In use: 17/20 VM

STORAGE GUARDIAN ADV
In use: 1.82 GB / 2 TB

Cloud Account

Virtual Machines Overview

Workload by Exposure Level

Storage by Exposure Level

Malware Scan

24
Malware Found

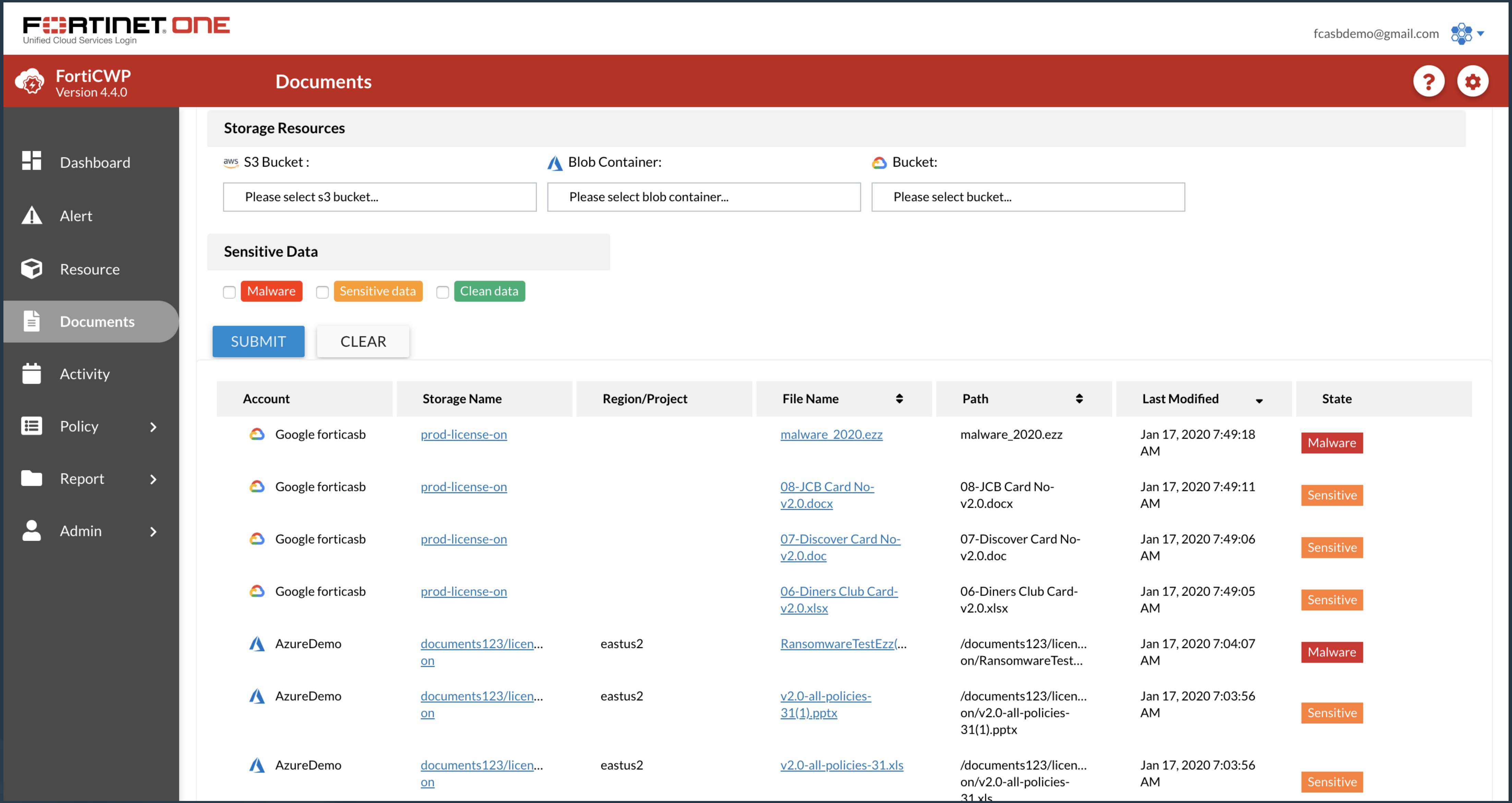
View All

DLP Scan

398
Sensitive Document

View All

FortiCWP – IaaS Visibility



Storage Resources

S3 Bucket : Please select s3 bucket...

Blob Container: Please select blob container...

Bucket: Please select bucket...

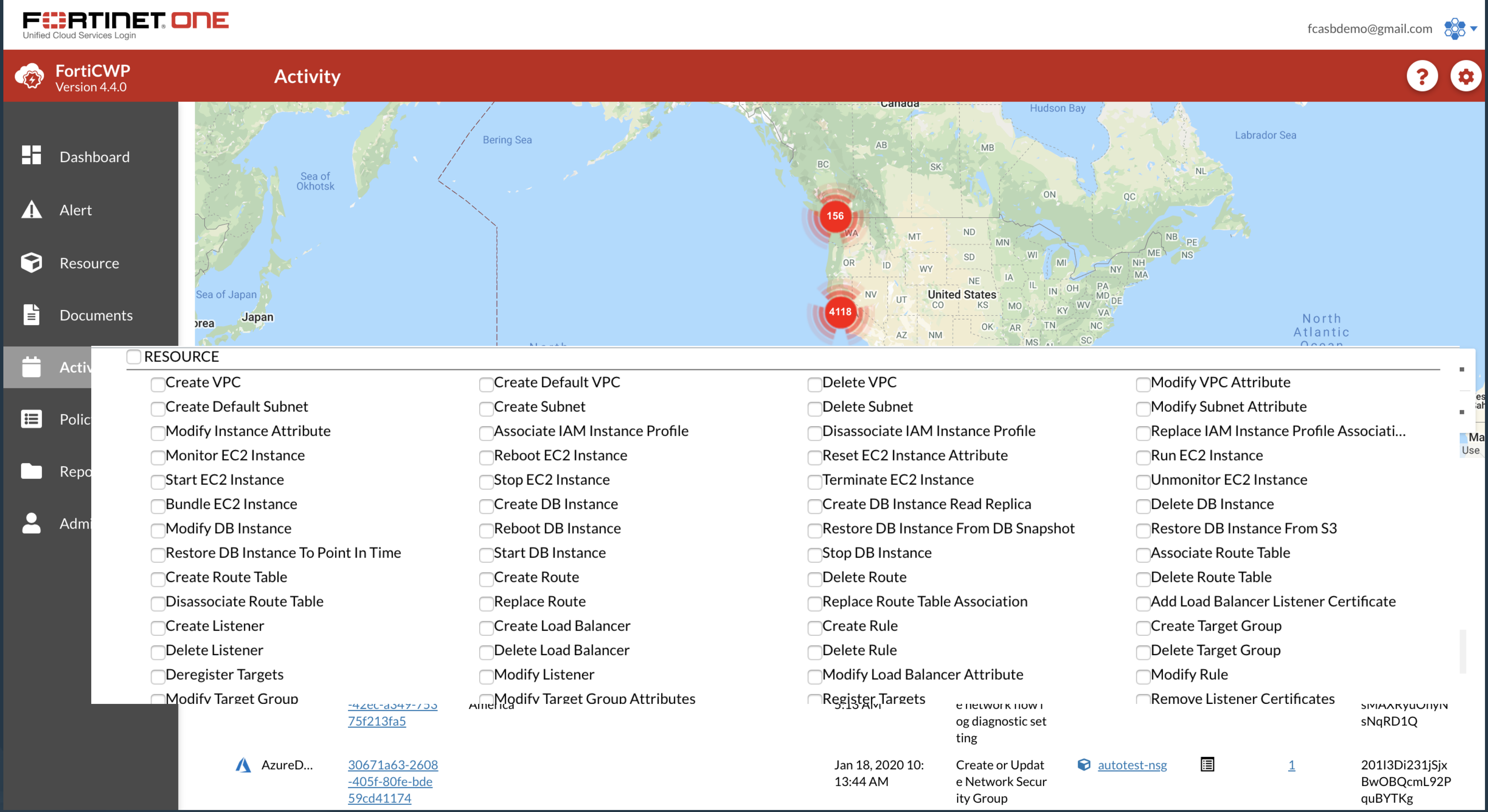
Sensitive Data

□ Malware □ Sensitive data □ Clean data

SUBMIT CLEAR

Account	Storage Name	Region/Project	File Name	Path	Last Modified	State
Google forticasb	prod-license-on		malware_2020.ezz	malware_2020.ezz	Jan 17, 2020 7:49:18 AM	Malware
Google forticasb	prod-license-on		08-JCB Card No-v2.0.docx	08-JCB Card No-v2.0.docx	Jan 17, 2020 7:49:11 AM	Sensitive
Google forticasb	prod-license-on		07-Discover Card No-v2.0.doc	07-Discover Card No-v2.0.doc	Jan 17, 2020 7:49:06 AM	Sensitive
Google forticasb	prod-license-on		06-Diners Club Card-v2.0.xlsx	06-Diners Club Card-v2.0.xlsx	Jan 17, 2020 7:49:05 AM	Sensitive
AzureDemo	documents123/licen...on	eastus2	RansomwareTestEzz(...	/documents123/licen...on/RansomwareTest...	Jan 17, 2020 7:04:07 AM	Malware
AzureDemo	documents123/licen...on	eastus2	v2.0-all-policies-31(1).pptx	/documents123/licen...on/v2.0-all-policies-31(1).pptx	Jan 17, 2020 7:03:56 AM	Sensitive
AzureDemo	documents123/licen...on	eastus2	v2.0-all-policies-31.xls	/documents123/licen...on/v2.0-all-policies-31.xls	Jan 17, 2020 7:03:56 AM	Sensitive

FortiCWP – IaaS Visibility

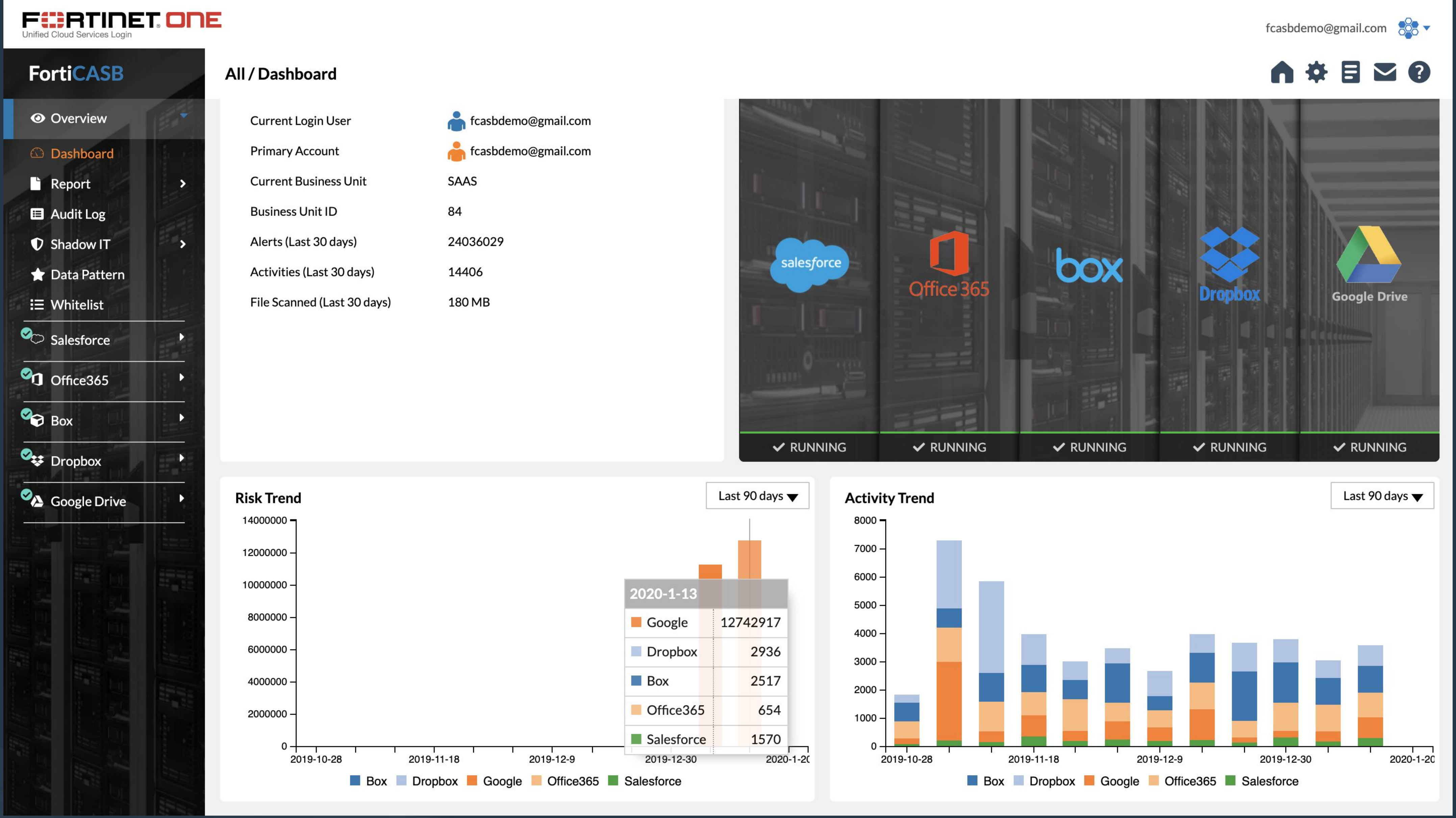


☐ RESOURCE

☐ Create VPC ☐ Create Default VPC ☐ Delete VPC ☐ Modify VPC Attribute
☐ Create Default Subnet ☐ Create Subnet ☐ Delete Subnet ☐ Modify Subnet Attribute
☐ Modify Instance Attribute ☐ Associate IAM Instance Profile ☐ Disassociate IAM Instance Profile ☐ Replace IAM Instance Profile Associati...
☐ Monitor EC2 Instance ☐ Reboot EC2 Instance ☐ Reset EC2 Instance Attribute ☐ Run EC2 Instance
☐ Start EC2 Instance ☐ Stop EC2 Instance ☐ Terminate EC2 Instance ☐ Unmonitor EC2 Instance
☐ Bundle EC2 Instance ☐ Create DB Instance ☐ Create DB Instance Read Replica ☐ Delete DB Instance
☐ Modify DB Instance ☐ Reboot DB Instance ☐ Restore DB Instance From DB Snapshot ☐ Restore DB Instance From S3
☐ Restore DB Instance To Point In Time ☐ Start DB Instance ☐ Stop DB Instance ☐ Associate Route Table
☐ Create Route Table ☐ Create Route ☐ Delete Route ☐ Delete Route Table
☐ Disassociate Route Table ☐ Replace Route ☐ Replace Route Table Association ☐ Add Load Balancer Listener Certificate
☐ Create Listener ☐ Create Load Balancer ☐ Create Rule ☐ Create Target Group
☐ Delete Listener ☐ Delete Load Balancer ☐ Delete Rule ☐ Delete Target Group
☐ Deregister Targets ☐ Modify Listener ☐ Modify Load Balancer Attribute ☐ Modify Rule
☐ Modify Target Group ☐ Modify Target Group Attributes ☐ Register Targets ☐ Remove Listener Certificates

	-42ec-a349-753 75f213fa5	America	5:13 AM	e network flow l og diagnostic set ting				sMAXRyuOnyN sNqRD1Q
AzureD...	30671a63-2608 -405f-80fe-bde 59cd41174		Jan 18, 2020 10: 13:44 AM	Create or Updat e Network Secur ity Group	autotest-nsg		1	20113Di231jSjx BwOBQcmL92P quBYTKg

FortiCASB – SaaS Visibility



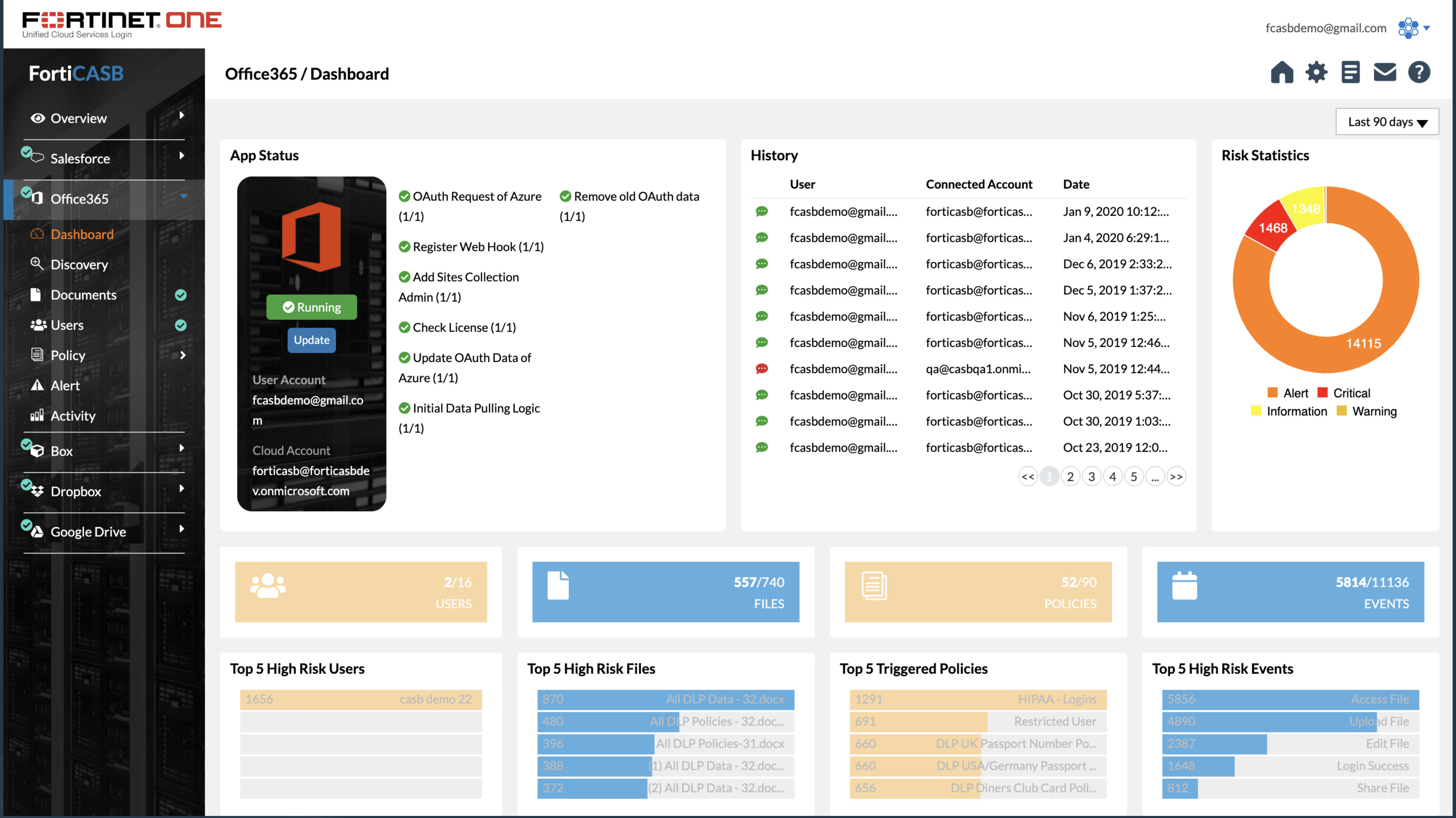
Current Login User	fcasbdemo@gmail.com
Primary Account	fcasbdemo@gmail.com
Current Business Unit	SAAS
Business Unit ID	84
Alerts (Last 30 days)	24036029
Activities (Last 30 days)	14406
File Scanned (Last 30 days)	180 MB

Risk Trend

2020-1-13	
Google	12742917
Dropbox	2936
Box	2517
Office365	654
Salesforce	1570

Activity Trend

FortiCASB – SaaS Visibility



Office365 / Dashboard

App Status

User Account
fcasbdemo@gmail.com

Cloud Account
forticasb@forticasbdev.onmicrosoft.com

- ✓ OAuth Request of Azure (1/1)
- ✓ Remove old OAuth data (1/1)
- ✓ Register Web Hook (1/1)
- ✓ Add Sites Collection Admin (1/1)
- ✓ Check License (1/1)
- ✓ Update OAuth Data of Azure (1/1)
- ✓ Initial Data Pulling Logic (1/1)

History

User	Connected Account	Date
fcasbdemo@gmail....	forticasb@forticas...	Jan 9, 2020 10:12:...
fcasbdemo@gmail....	forticasb@forticas...	Jan 4, 2020 6:29:1...
fcasbdemo@gmail....	forticasb@forticas...	Dec 6, 2019 2:33:2...
fcasbdemo@gmail....	forticasb@forticas...	Dec 5, 2019 1:37:2...
fcasbdemo@gmail....	forticasb@forticas...	Nov 6, 2019 1:25:...
fcasbdemo@gmail....	forticasb@forticas...	Nov 5, 2019 12:46...
fcasbdemo@gmail....	qa@casbqa1.onmi...	Nov 5, 2019 12:44...
fcasbdemo@gmail....	forticasb@forticas...	Oct 30, 2019 5:37:...
fcasbdemo@gmail....	forticasb@forticas...	Oct 30, 2019 1:03:...
fcasbdemo@gmail....	forticasb@forticas...	Oct 23, 2019 12:0...

Risk Statistics

🟧 Alert 🟥 Critical 🟨 Information 🟨 Warning

2/16 USERS

557/740 FILES

52/90 POLICIES

5814/11136 EVENTS

Top 5 High Risk Users

1656	casb demo 22

Top 5 High Risk Files

870	All DLP Data - 32.docx
480	All DLP Policies - 32.doc...
396	All DLP Policies-31.docx
388	(1) All DLP Data - 32.doc...
372	(2) All DLP Data - 32.doc...

Top 5 Triggered Policies

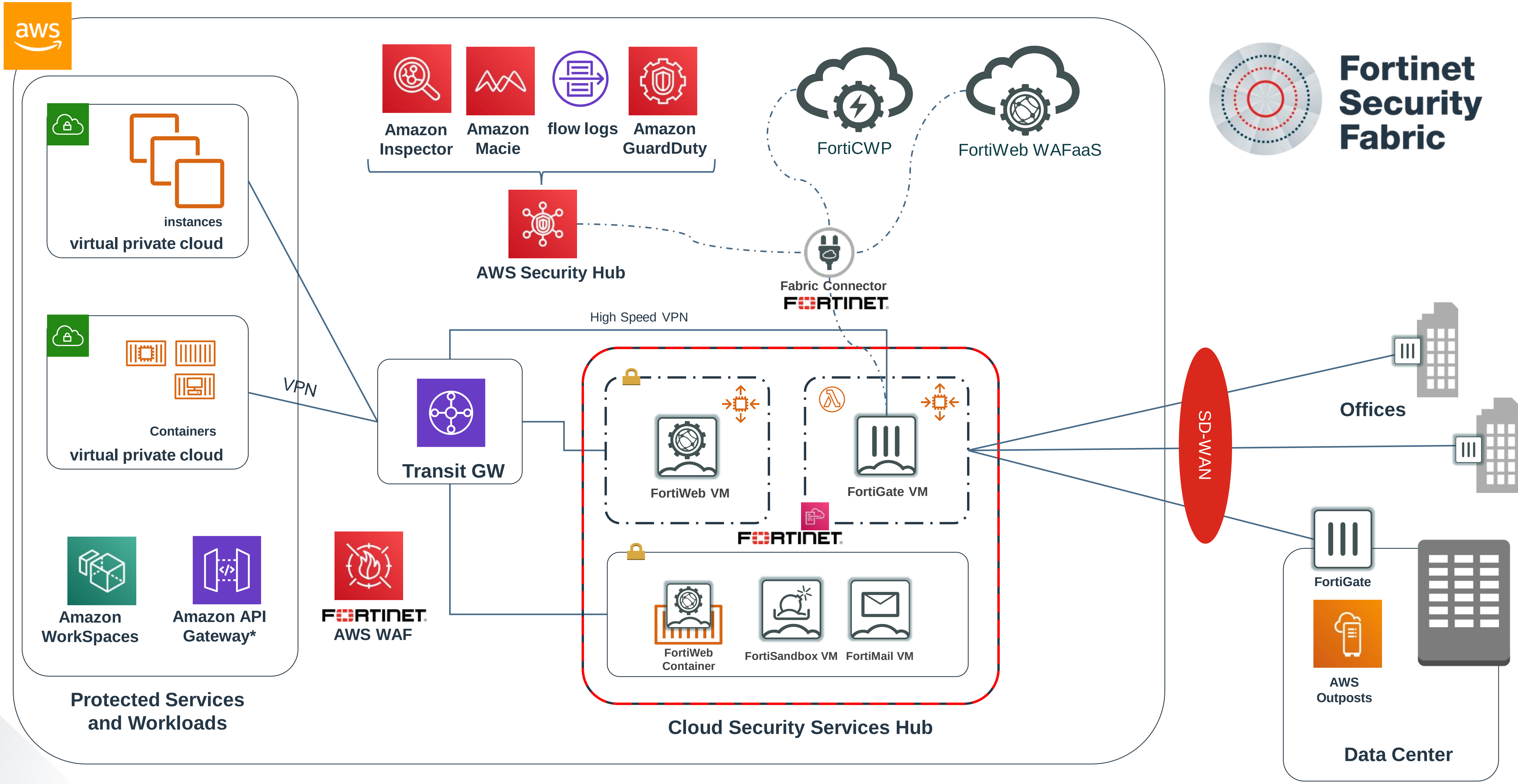
1291	HIPAA - Logins
691	Restricted User
660	DLP UK Passport Number Po...
660	DLP USA/Germany Passport ...
656	DLP Diners Club Card Poli...

Top 5 High Risk Events

5856	Access File
4890	Upload File
2387	Edit File
1648	Login Success
812	Share File

Summary

Fortinet Security Fabric



Amazon Inspector
Amazon Macie
flow logs
Amazon GuardDuty
AWS Security Hub
FortiCWP
FortiWeb WAFaaS
Fabric Connector
FORTINET
High Speed VPN
instances
virtual private cloud
Containers
virtual private cloud
VPN
Transit GW
FortiWeb VM
FortiGate VM
FORTINET
FortiWeb Container
FortiSandbox VM
FortiMail VM
Amazon WorkSpaces
Amazon API Gateway*
FORTINET AWS WAF
SD-WAN
Offices
FortiGate
AWS Outposts
Data Center
Protected Services and Workloads
Cloud Security Services Hub

FORTINET

Return

Fortinet Security Fabric : Complete Cloud Security

FortiGate

Application Controls

Anti-Virus, IPS, VPN

Web Filtering, Threat Intel

FortiWeb

Protect over SQL Injection, cross site scripting, etc.

FortiManager

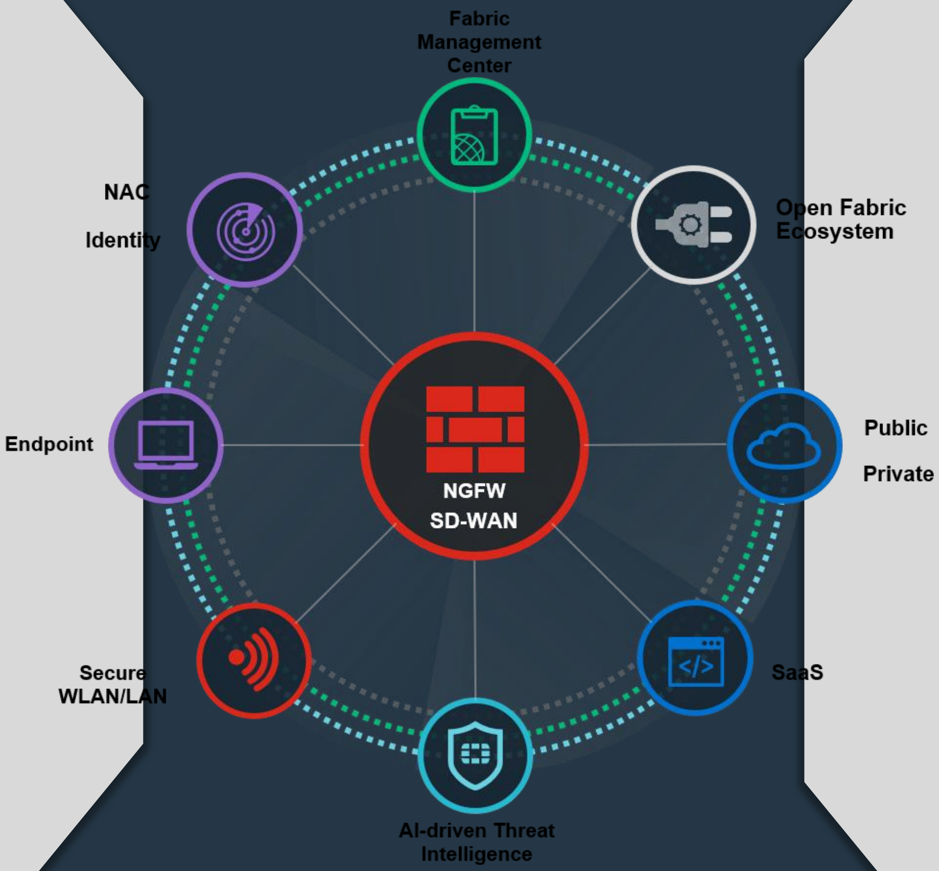
Consistency and control

FortiMail

Location (IP Range)

FortiAnalyzer

Compliance and visibility



FortiCWP

Configuration Management

User Behavior Analysis

Malware and Sensitive Data

Compliance Reporting

FortiCASB

Configuration Management

Sensitive Data Scan

Audit Log

Compliance Reporting

Shadow IT Discovery

FORTINET®