Cloud Security Fabric (2019)

Timo Lohenoja, CISSP

Systems Engineer

Fortinet
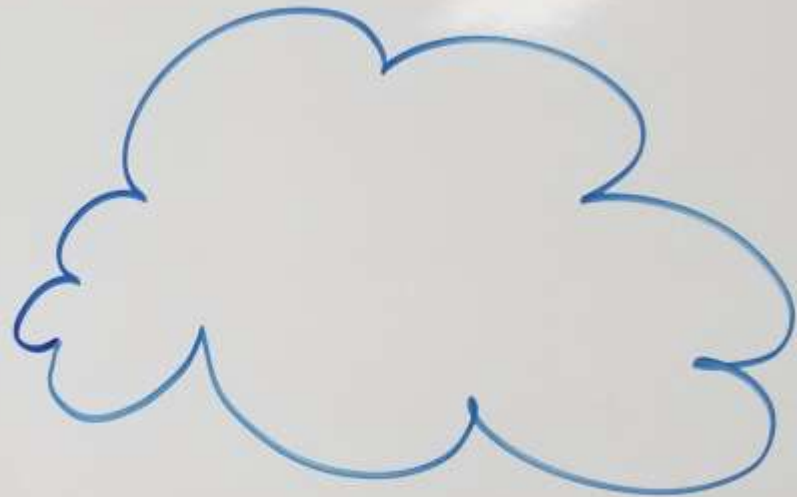
Enterprise Cloud Adoption

- **Fast**
  - » New Cloud services are tried out and used every day
  - » It is much easier to deploy a cloud application than decommission it

- **Decentralized**
  - » New service creation is not funneled through a central IT dept.
  - » Anyone across the organization may source a new cloud service
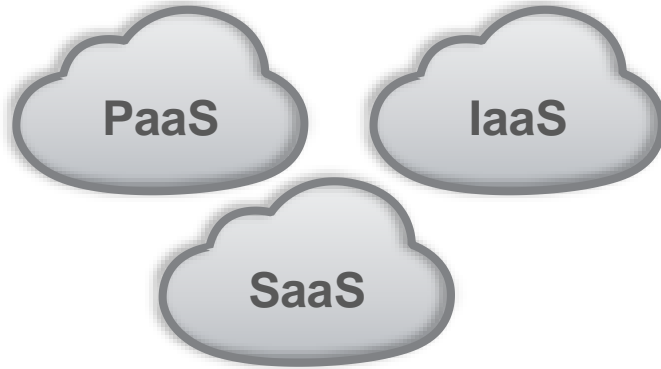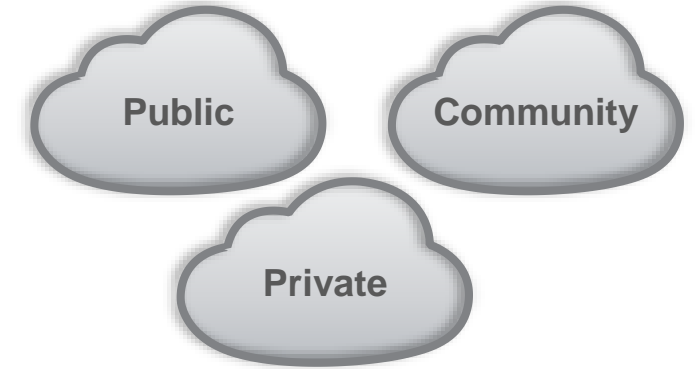
- **Heterogeneous**
  - » Employees will use different cloud services from different providers
  - » Different cloud services offer different security levels

Reality = All of the above

DELIVERY MODEL

PaaS

IaaS

SaaS

DEPLOYMENT MODEL

Public

Community

Private

SERVICE PROVIDERS

aws

Microsoft Azure

IBM

YOURSELF

Google Cloud Platform

ORACLE CLOUD

Alibaba Cloud

Risk = All of the above

DELIVERY MODEL

PaaS

IaaS

SaaS

DEPLOYMENT MODEL

Public

Community

Private

Malicious insiders

Interface and API hacking

Data breaches

DoS and DDoS attacks

APTs

SERVICE PROVIDERS

aws

Microsoft Azure

IBM

YOURSELF

Google Cloud Platform

ORACLE CLOUD

Alibaba Cloud
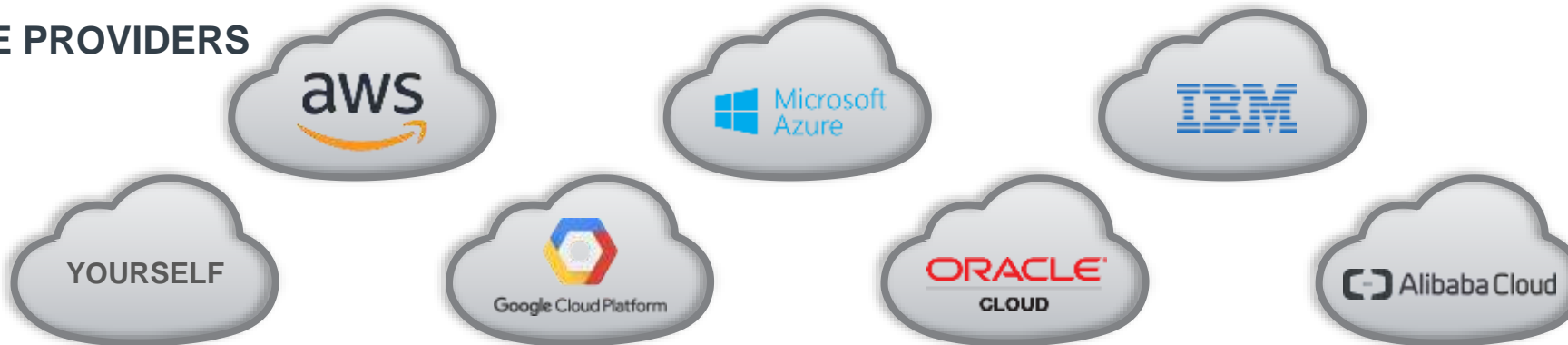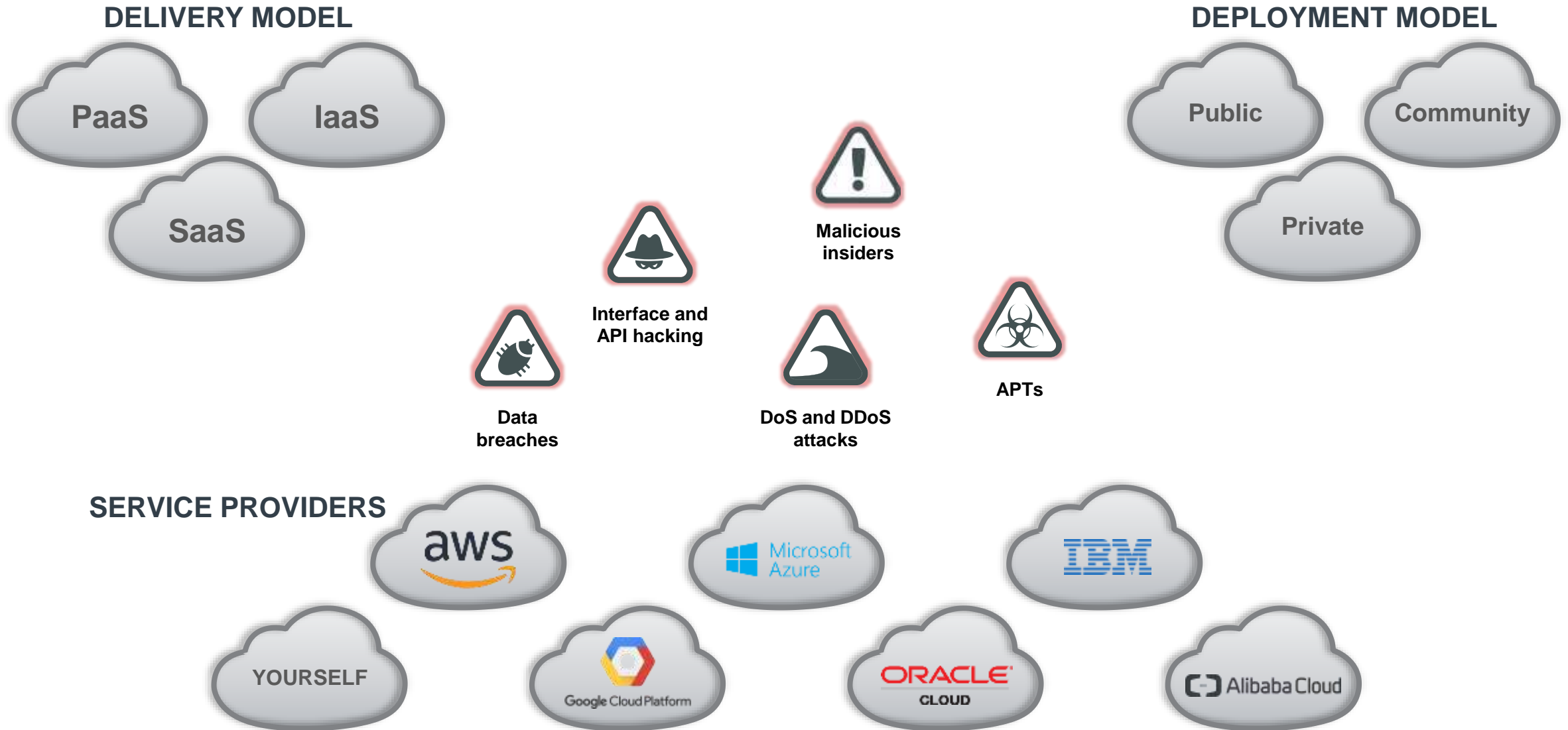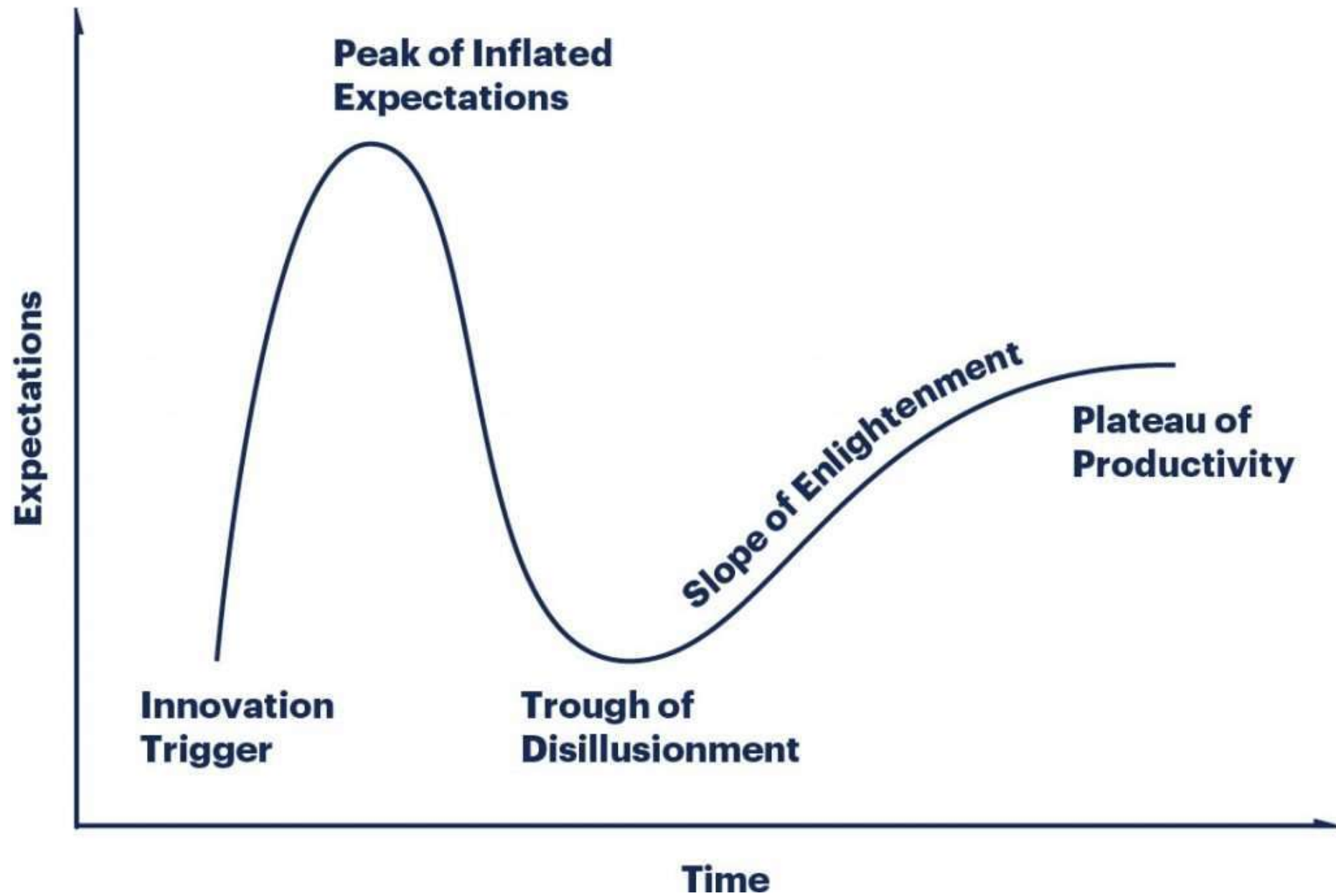
Cloud Adoption Market Breakdown

Laggards

Majority of Customers

Bleeding Edge

Companies

Secure Journey to the Cloud

Mindshare

NGFW

CSPM/CASB

CASB

Cloud Native / CI/CD Integrated

WAF

Security Automation

Container/Serverless Security Orchestration

Cloud Adoption Maturity

FORTINET

7

Security Thinking Evolution

CLOUD

SECURITY

UBIQUITOUS

ON-DEMAND

CONTROLS

POLICIES

PROCESSES

PRODUCTIVITY

Security Thinking Evolution

CLOUD

SECURITY

UBIQUITOUS

ON-DEMAND

CONTROLS

POLICIES

PROCESSES

PRODUCTIVITY

AUTOMATION
- Templates
- Auto-Everything

SECURITY
- Processes
- Policies
- Controls

CLOUD
- On-demand
- Ubiquitous

Shared Responsibility

The majority of the cloud security responsibility is on the user — not the provider

95%

Cloud security failures through 2020 where the customer is at fault[1]

Customer Security responsibility

Data & Content
Applications, Platform & User Management
OS, Firewall & Network Settings & Configuration
Encryption & Network Traffic Protection

Customer builds applications that run IN the Cloud

Public Cloud Infrastructure Services

Storage **Network** **Compute**

Cloud provider secures the infrastructure

Cloud Security Evolution

Virtualization	⟶	Private Cloud	⟷	Hybrid	⟷	Public Cloud

Hypervisor Port   SDN—Orchestration Integration   On-Demand

VM VM VM

Hypervisor

East-West

Connector   API

VMX

North-South

Flow

IaaS Cloud

NGFW   WAF   Management   Reporting   APT

SaaS Cloud

Proxy   Broker
CASI   API
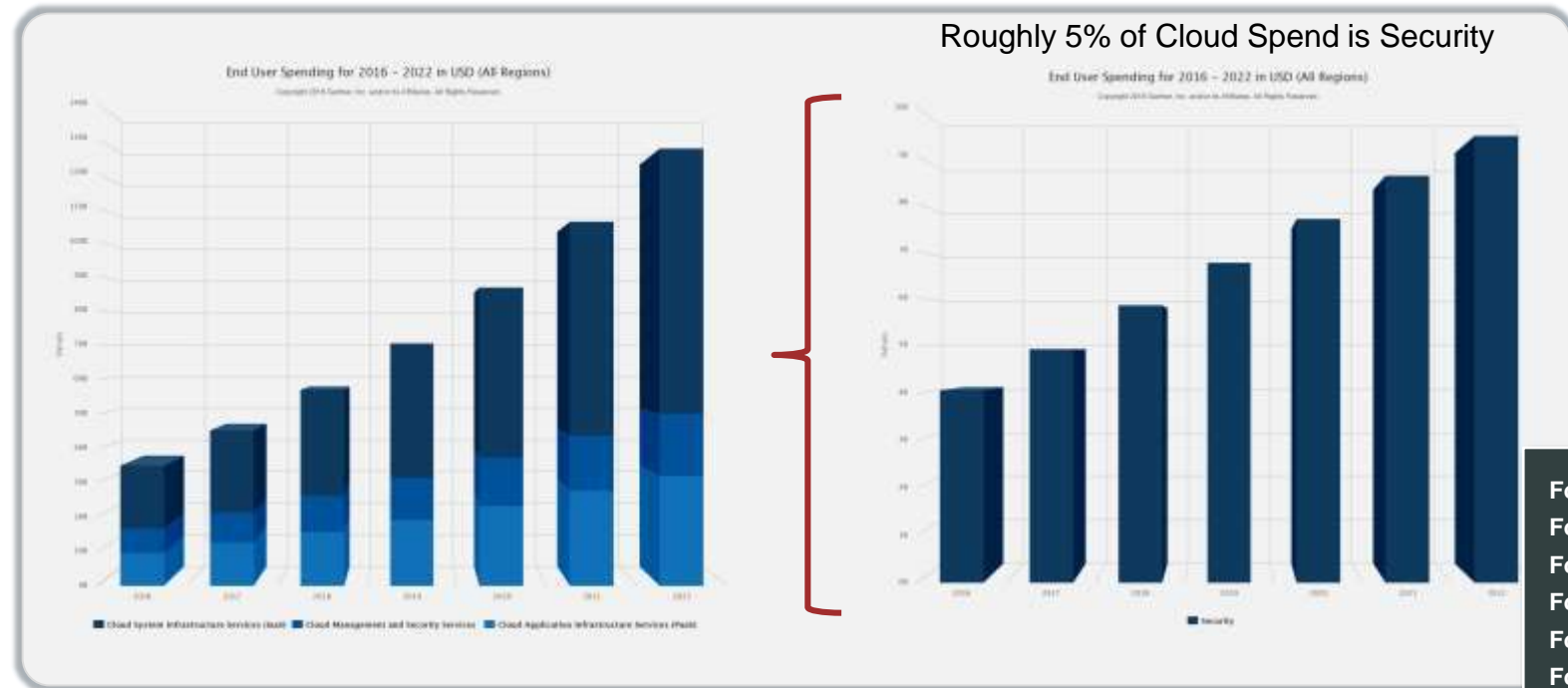
Cloud Market Insights

Information Technology / IT Services / IT Services / Managed Services and Cloud Infrastructure Services

IaaS and Infrastructure Utility Services

Top Vendors	Revenue 2016	Revenue 2017	YOY Growth	2017 Market Share
Amazon	9,775.3	12,220.7	+25%	33.2%
Microsoft	1,579.0	3,130.0	+98.2%	8.5%
Alibaba	670.4	1,090.1	+62.6%	3%
Google	500.2	780.0	+55.9%	2.1%
IBM	646.7	734.2	+13.5%	2%
Atos	504.7	586.5	+16.2%	1.6%
CGI	449.0	568.9	+26.7%	1.5%
Wipro	509.0	549.3	+7.9%	1.5%
Capgemini	458.6	526.3	+14.8%	1.4%
DXC	152.2	413.2	+171.4%	1.1%
Other Vendors	14,327.7	16,255.4	+13.5%	44.1%
Total	**29,572.9**	**36,854.6**	**24.6%**	**100%**

Source: Gartner (July 2018)   Revenue (Millions of U.S. Dollars)

Roughly 5% of Cloud Spend is Security

FortiGate-VM
FortiWeb
FortiMail
FortiSandbox
FortiManager
FortiAnalyzer
FortiAuthenticator
FortiSIEM

Fortinet has offerings and partial offerings for only part of the cloud security market

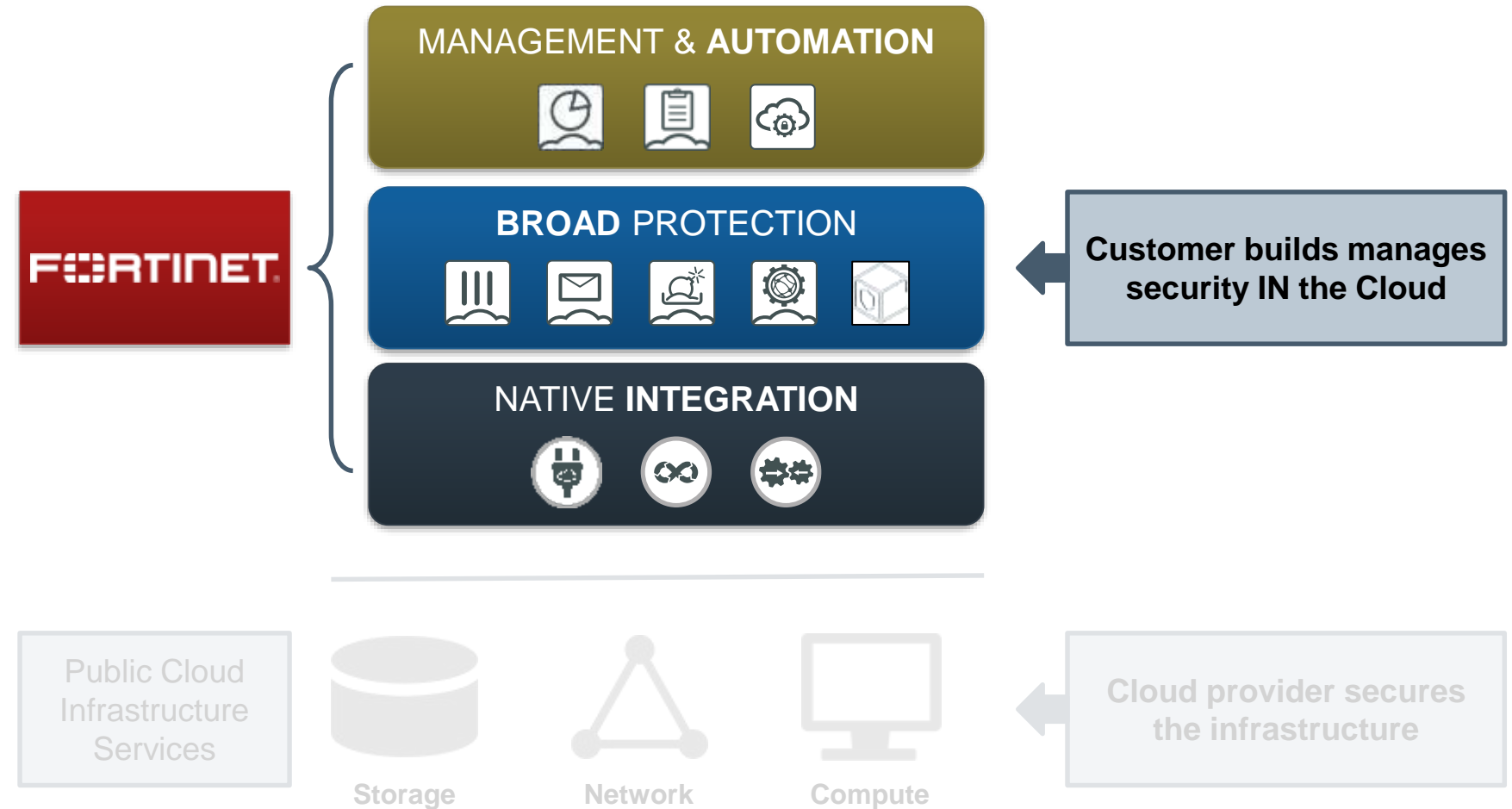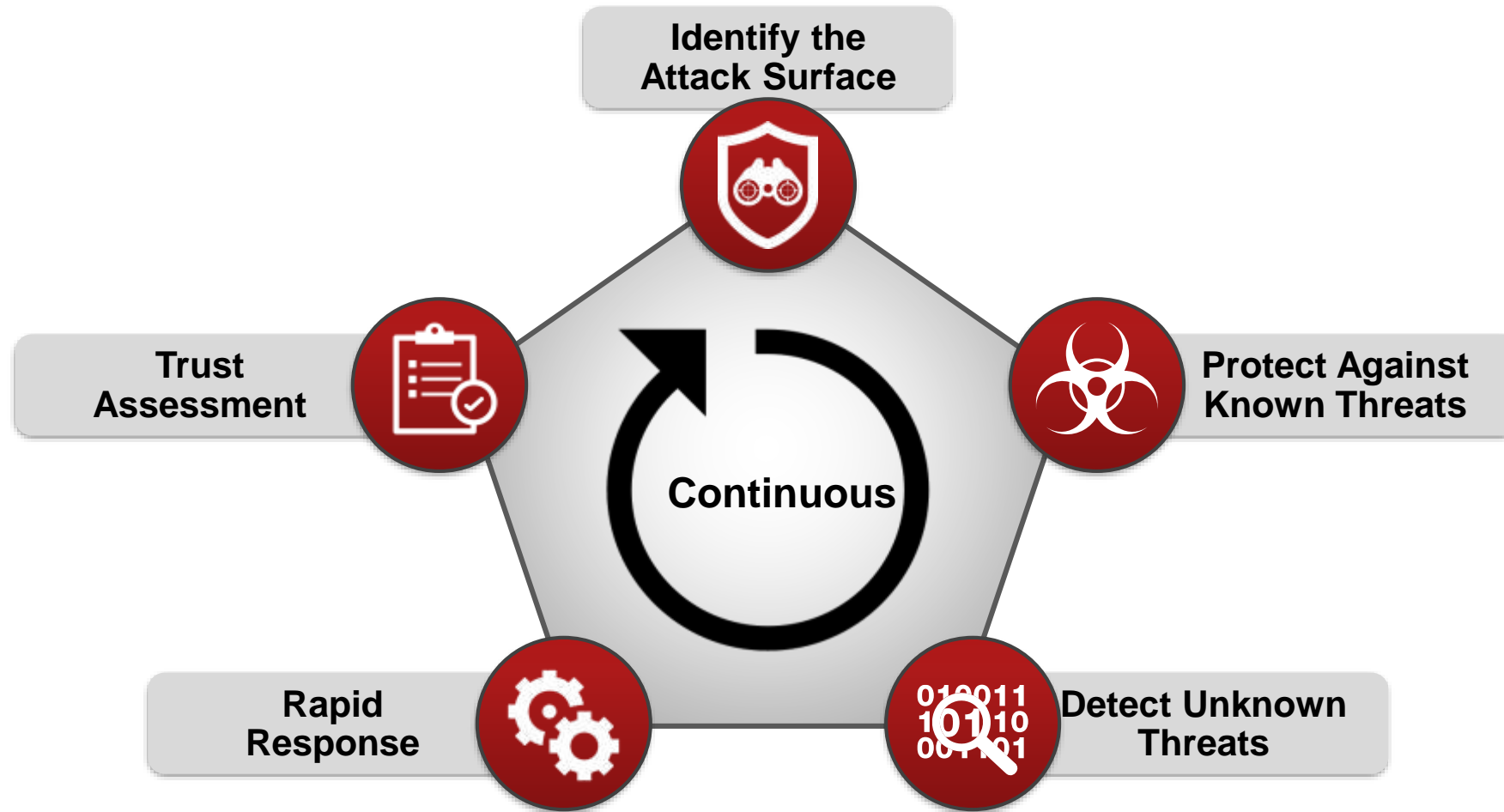CASB | CSPM | NGFW | Micro Segmentation | Security Analytics | Security Management | WAF | Security Automation | Fabric Products

Customer Responsibility

Fortinet builds cloud security solutions to help the customer secure the cloud

FORTINET

MANAGEMENT & AUTOMATION

BROAD PROTECTION

Customer builds manages security IN the Cloud

NATIVE INTEGRATION

Public Cloud Infrastructure Services

Storage

Network

Compute

Cloud provider secures the infrastructure

Security Framework for Digital Security

NIST Model

Identify the Attack Surface

Trust Assessment

Protect Against Known Threats

Continuous

Rapid Response

Detect Unknown Threats

Fortinet Security Fabric for the Cloud

DELIVERY MODEL

PaaS

IaaS

SaaS

DEPLOYMENT MODEL

Public

Community

Private

MANAGEMENT & **AUTOMATION**

BROAD PROTECTION

NATIVE **INTEGRATION**

SERVICE PROVIDERS

aws

Microsoft Azure

IBM

YOURSELF

Google Cloud Platform

ORACLE CLOUD

Alibaba Cloud
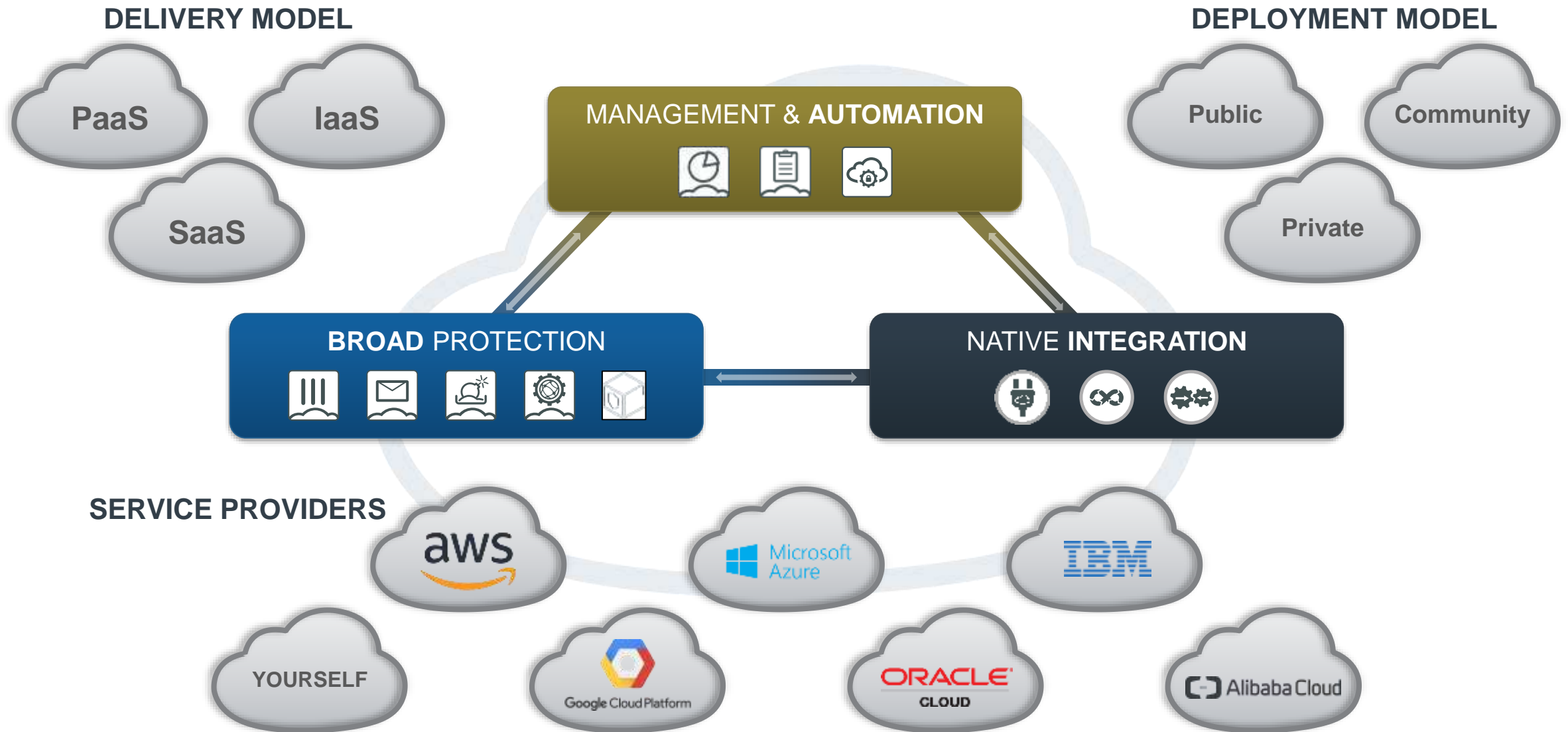
What's Needed? - Multi-Cloud Security

Single Console

Multiple Clouds   **Multiple Integrations**   **Multiple Applications**
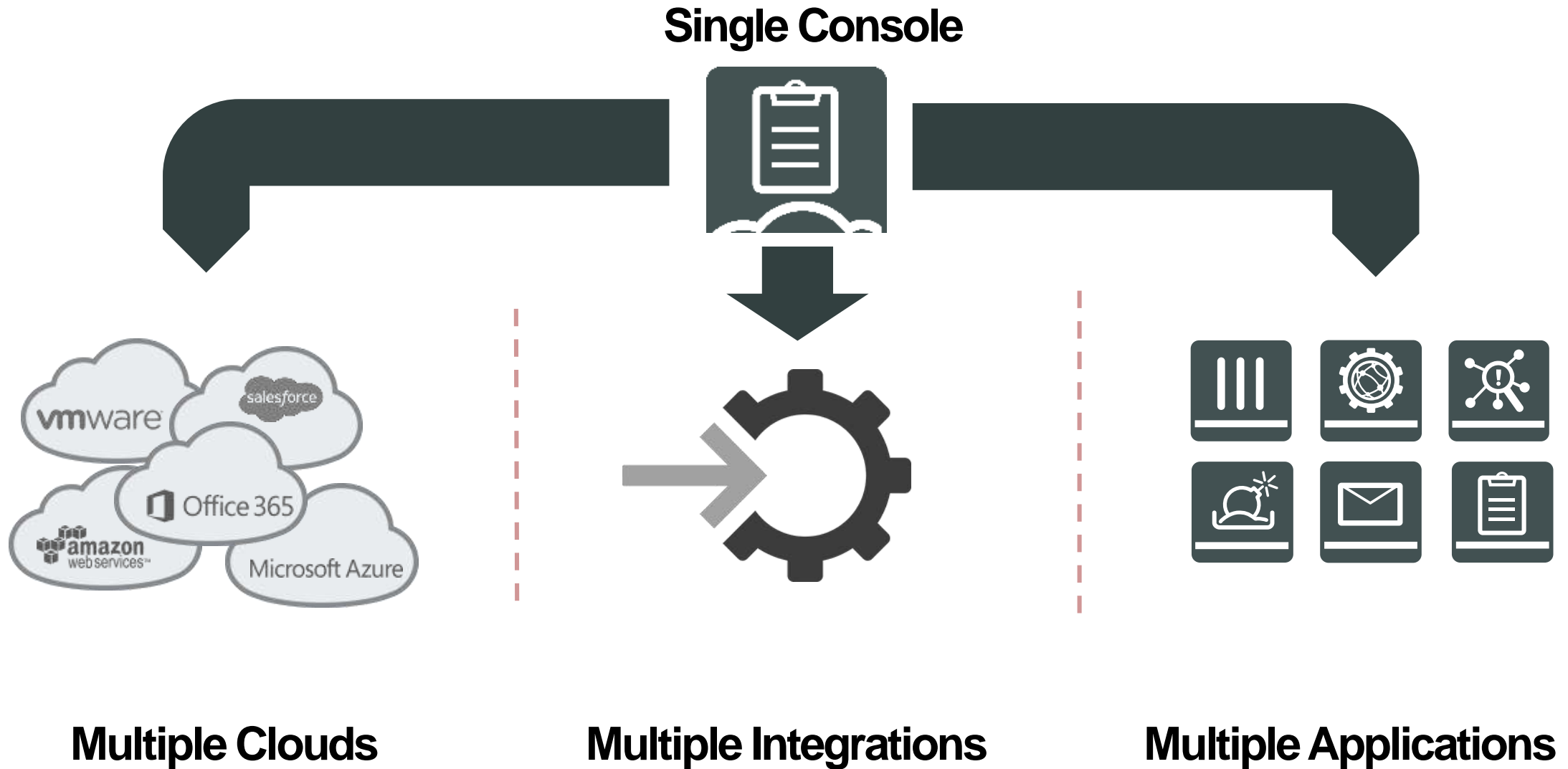
Cloud Adoption Initiatives

| Migrating/Extending Applications to the Cloud | Building Cloud Native Applications | Consuming SaaS Applications |
| Datacenter transformation to the Cloud | | |

| MIGRATE | BUILD | CONSUME |
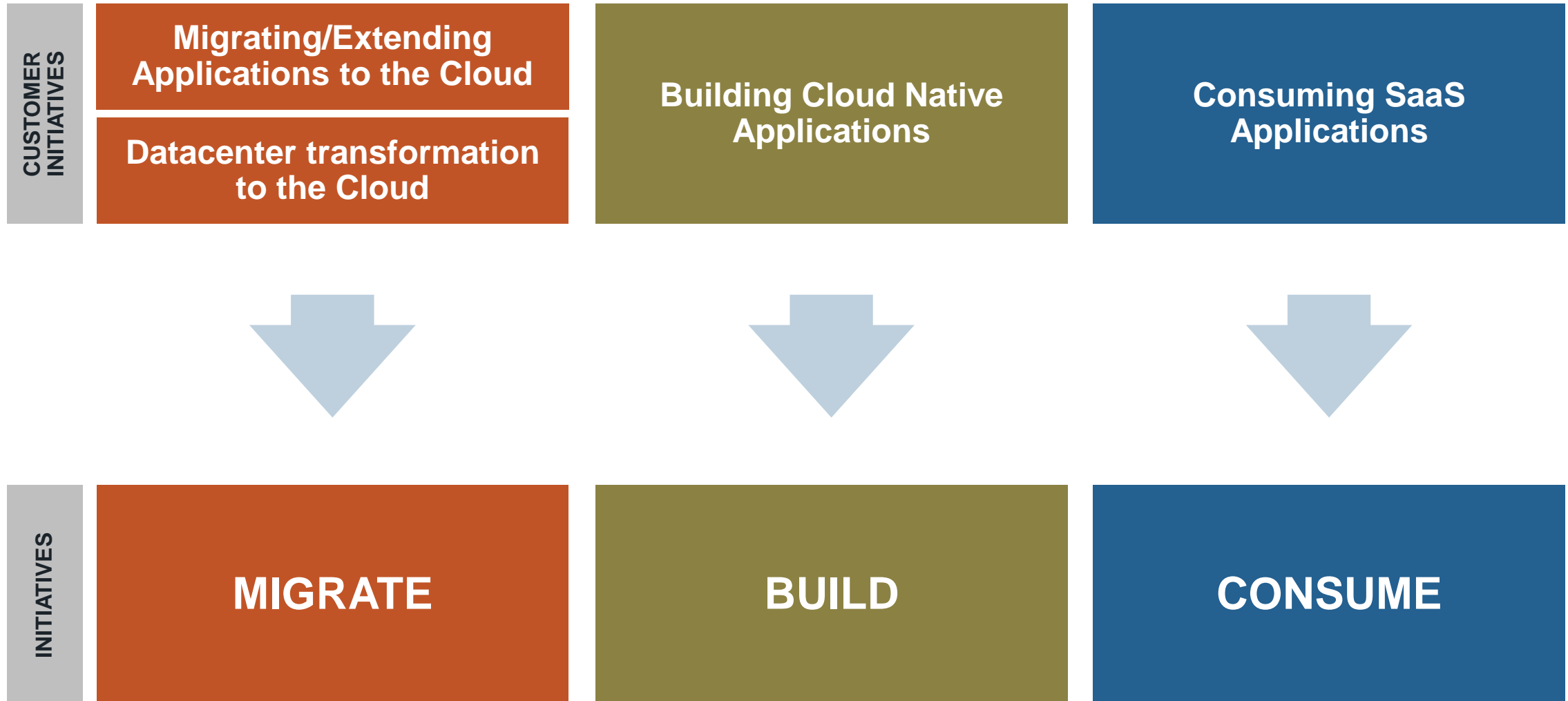
Fortinet Secures the Cloud Migration Journey

INITIATIVES

| MIGRATE | BUILD | CONSUME |

SOLUTIONS

Visibility and Control

Application Security

Secure Connectivity

PRODUCTS

FortiGate   FortiWeb   FortiManager   FortiAnalyzer

FortiCASB-Cloud   FortiSandbox   FortiClient

FortiGate   FortiWeb   FortiSandbox

FortiCASB-Cloud

FortiMail

FortiCASB
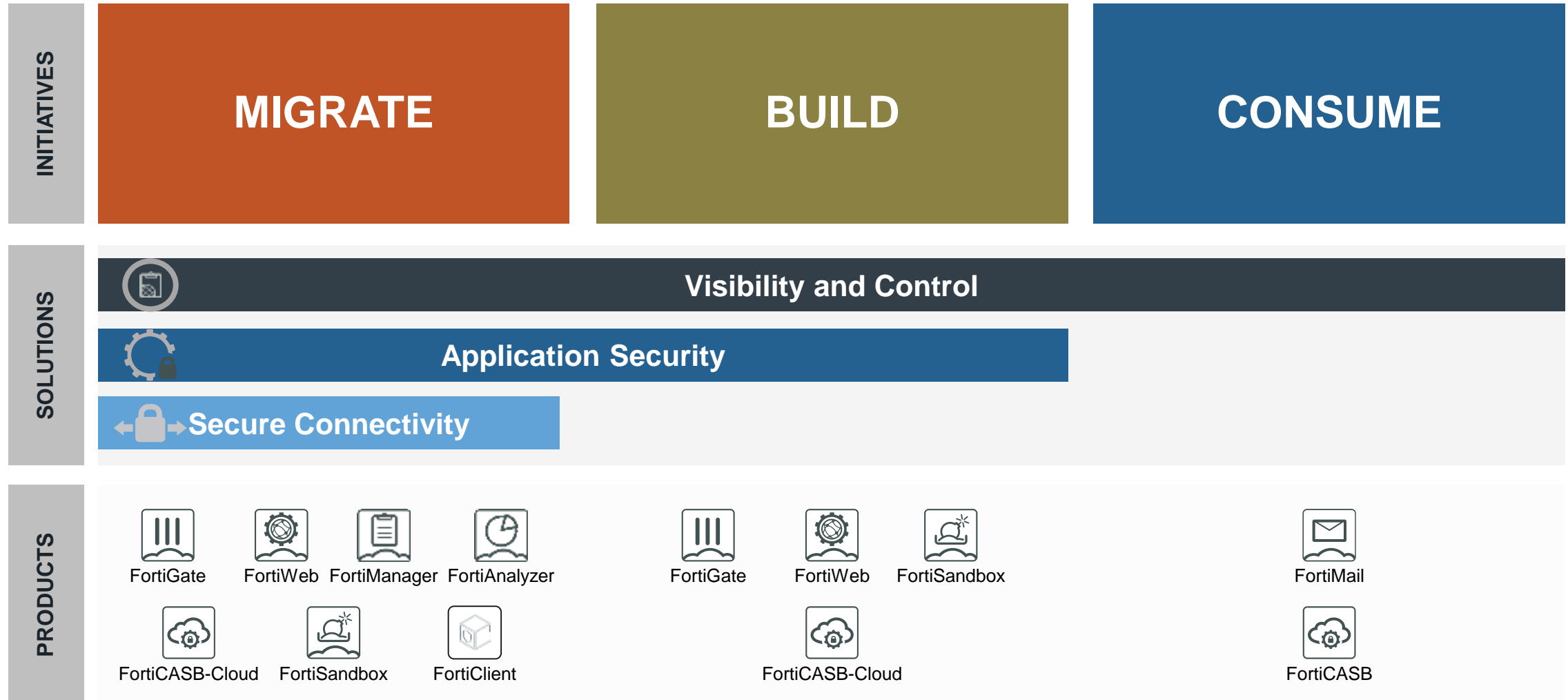
Cloud Security Services Hub

Customer Challenge

As organizations grow, and their consumption of the cloud increases and expands, the need to separate security management from application development increases. Different organizational units tent to build applications in different virtual networks and even different clouds and datacenters. Securing all disperse locations becomes challenging.

SD-WAN

Cloud Network

Cloud Network

Cloud VPN Gateway

Cloud Security Services Hub

Cloud Network
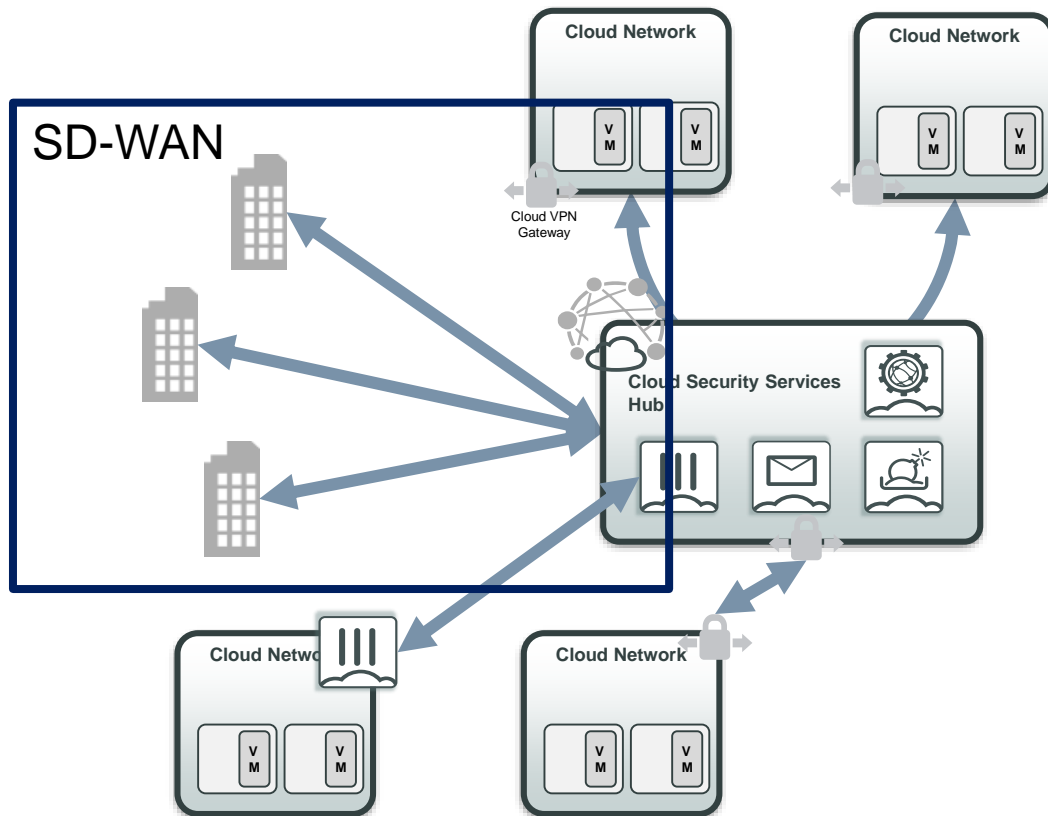
Cloud Network

Solution

By building a central hub (transit network) for security functionality, that securely interconnects all disperse networks, locations, clouds and datacenters and can effectively enforce security policies between the different virtual networks and locations as well as offer central security filtering for traffic between these networks and the internet, organizations can effectively split the role of security management from application development.
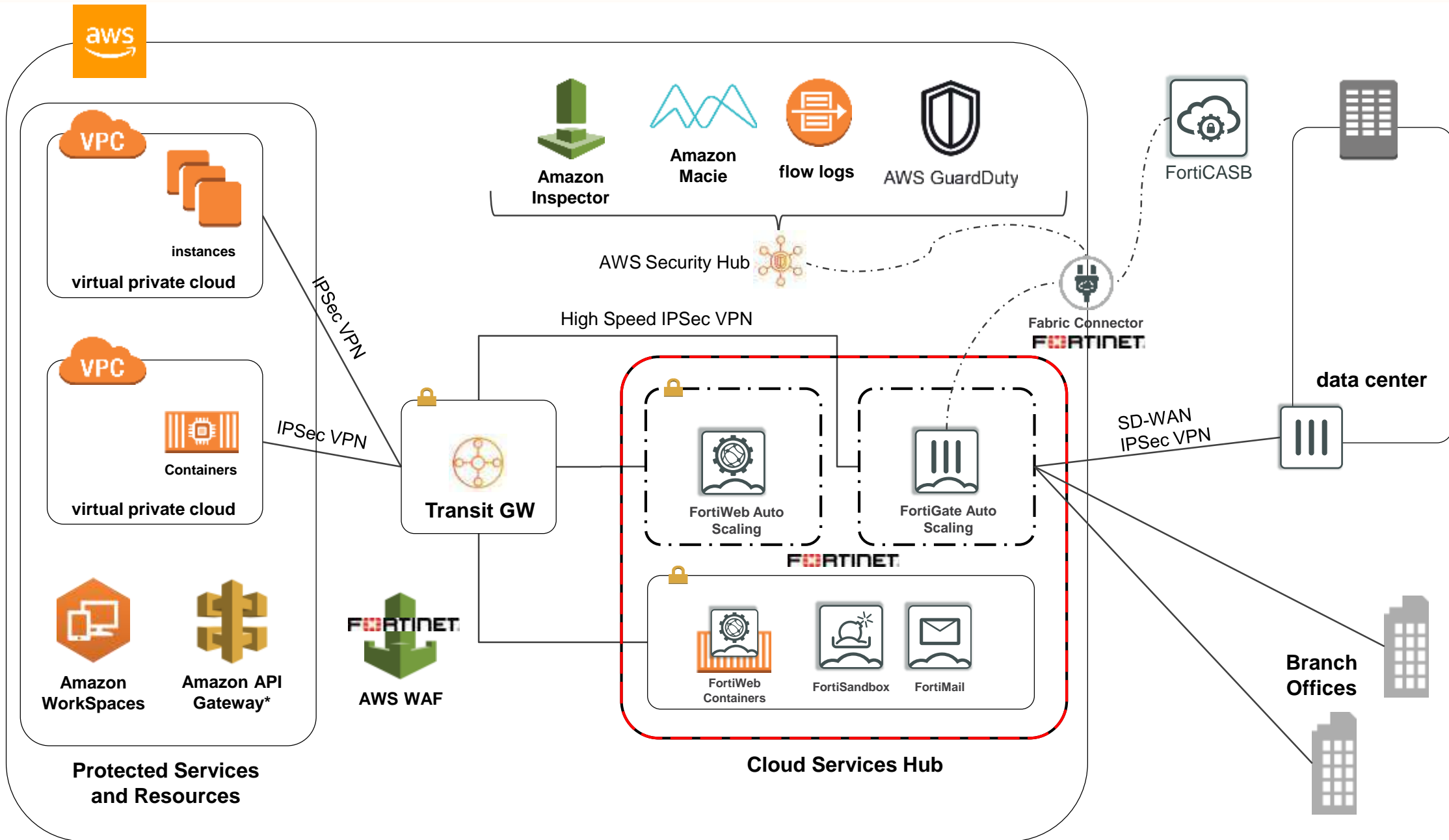
Benefits

- The key benefits of this approach are the ability to enforce consistent security across the entire set of networks
- Additionally, organizational units can continue to develop security solutions autonomously without needing to wait for security policies to be applies and without exposing the organization to unwanted risk.
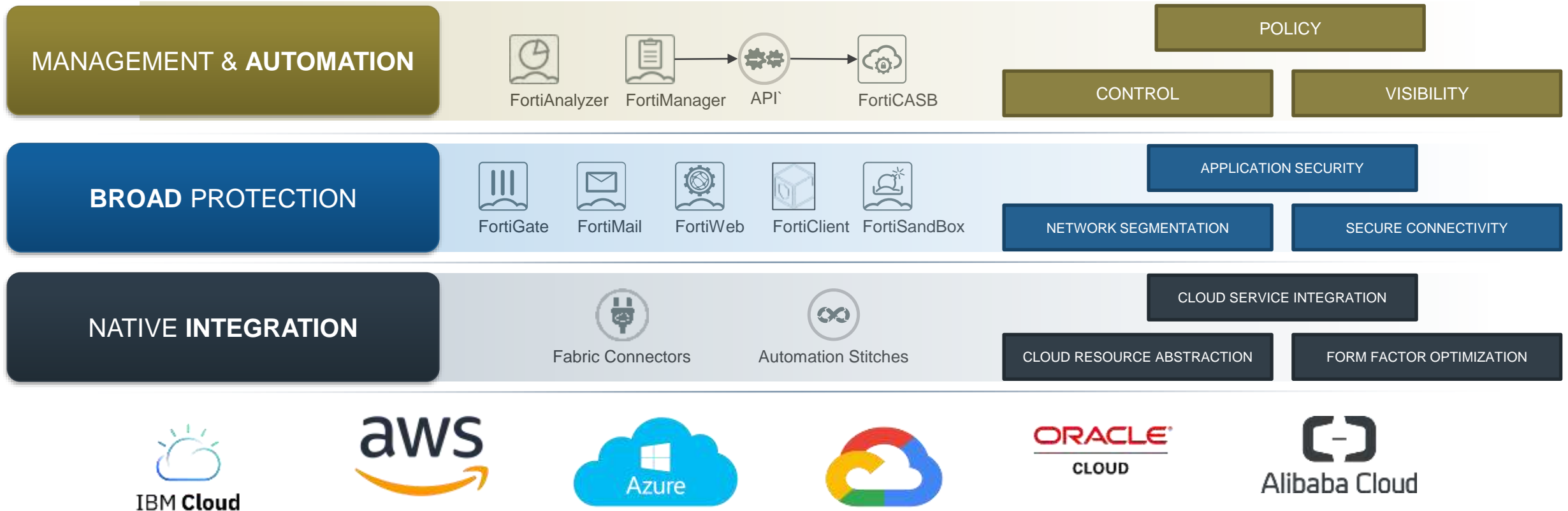
Unique Selling Points

- High Speed VPN Connectivity with Scale-out and Scale-Up options
- Flexible network connectivity and advanced routing capabilities
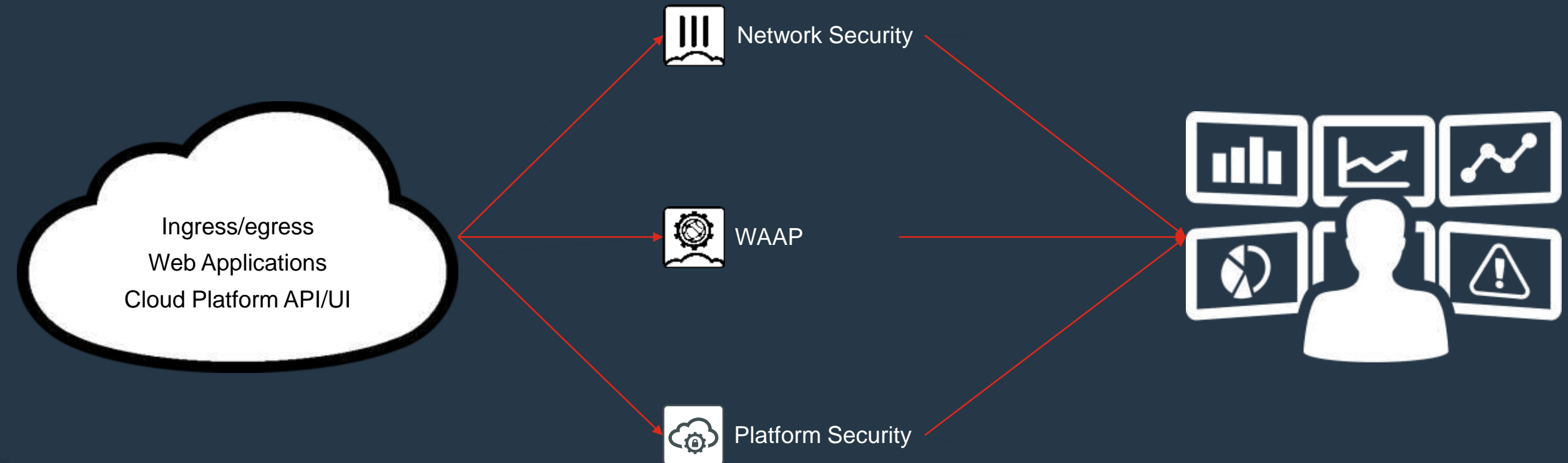
Related Topics

FortiGate-VM Datasheets
AWS Transit VPC & Transit Gateway functionality
GCP Shared VPC

Fortinet Cloud Security Strategy – 3 Pillars

MANAGEMENT & AUTOMATION

FortiAnalyzer FortiManager API` FortiCASB

POLICY

CONTROL

VISIBILITY

BROAD PROTECTION

FortiGate FortiMail FortiWeb FortiClient FortiSandBox

APPLICATION SECURITY

NETWORK SEGMENTATION

SECURE CONNECTIVITY

NATIVE INTEGRATION

Fabric Connectors Automation Stitches

CLOUD SERVICE INTEGRATION

CLOUD RESOURCE ABSTRACTION

FORM FACTOR OPTIMIZATION

IBM Cloud aws Azure ORACLE CLOUD Alibaba Cloud

Cloud Security - Technology Fundamentals

Ingress/egress
Web Applications
Cloud Platform API/UI

Network Security

WAAP

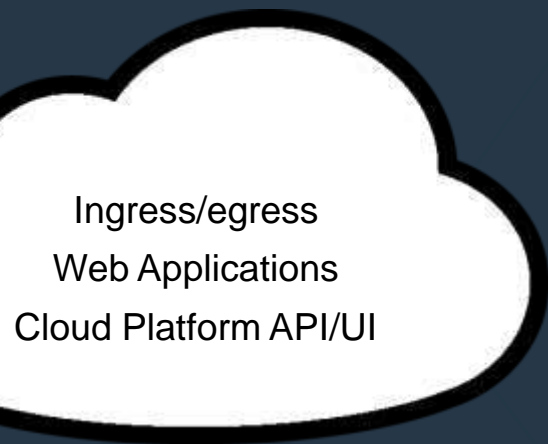Platform Security

What Built in Cloud Network Security Lacks

- Management
  - The Human Factor
  - Operational Model
  - DevOps vs. SecOps
- Application Awareness
- Multi-Cloud

Comparison of Network Security Features and Terminology

Network Security	AWS	Azure	GCP
VPN Gateway	VPC-to-Site IPsec	Azure VPN Gateway	Cloud VPN
Dedicated Network	Amazon Virtual Private Cloud (VPC)	Azure VNet	Cloud VPC
Transit Network	Requires Cisco Cloud Service Router (CSR)	Transit VNet	
User-Defined Routes	VPC Route Tables	Part of VNet Functionality	Cloud Router
Cloud Security Groups at Subnet Level		Azure Network Security Groups (NSGs)	Firewall Rules
Cloud Security Groups at VNIC Level	AWS Security Groups	NSGs	
IPv6 Security Groups	AWS Security Groups		
Attribute-Based Cloud Security Groups		Application Security Groups	Source and Target Tags
Subnet Access Lists	Network ACLs	Endpoint ACLs	
Dedicated DDOS-Free Connection	AWS Direct Connect	Azure Express Route	Dedicated Interconnect
DDOS Protection	AWS Shield, AWS Shield Advanced	Azure DDOS Protection (in Preview)	CloudArmor (Not Scrubbing)
Traffic Tracking	Flow Logs	Flow Logs	
WAF (OWASP Top 10 Core)	AWS WAF	Azure Application Gateway	
WAF (Managed Third-Party Rules)	AWS WAF		
WAF Policy Language (Bespoke Rules)	AWS WAF		

ID: 343562

© 2018 Gartner, Inc.

23

Cloud Security – Fortinet Differentiators

Ingress/egress
Web Applications
Cloud Platform API/UI

FortiGate NGFW

Most Scalable (out and up) – VPN, IPS, App Control

Multiple Connectors – Multi-Cloud, Multi-Org, Cloud Services
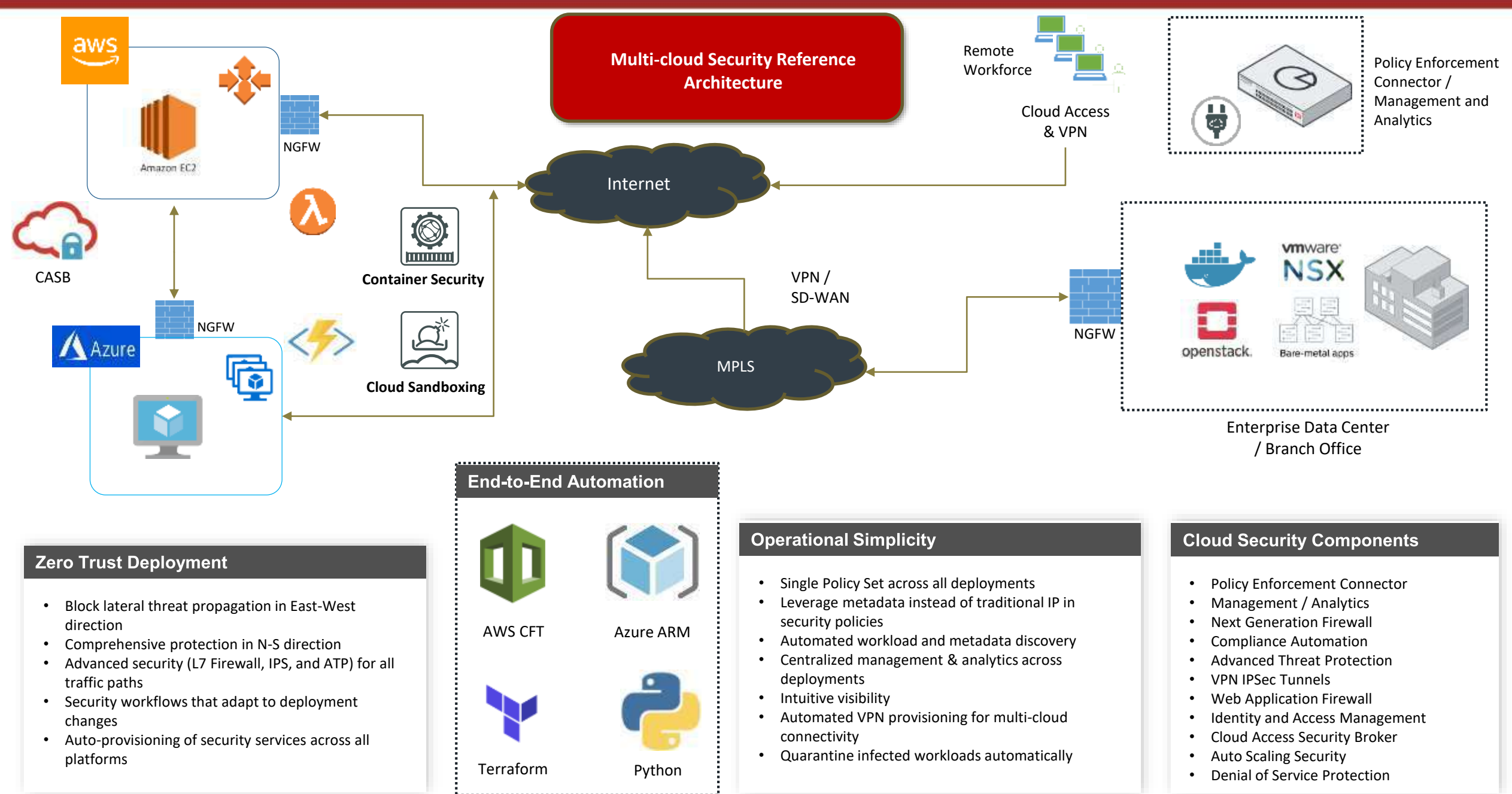
HA Failover (Unicast)

FortiWeb WAF

Form factor flexibility – Docker for CI/CD, SaaS

ML simplicity and Accuracy – WAAP for All

Fabric Integration – SOC Integration

FortiCASB-Cloud Platform Security

Multi-Cloud Dashboards - Consistency

FortiGuard Labs integration – Advanced Threat Protection

Fabric Integration – SOC Integration

Multi-cloud Security Reference Architecture

Zero Trust Deployment

- Block lateral threat propagation in East-West direction
- Comprehensive protection in N-S 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

AWS CFT   Azure ARM

Terraform   Python

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

Realizing the Vision of:
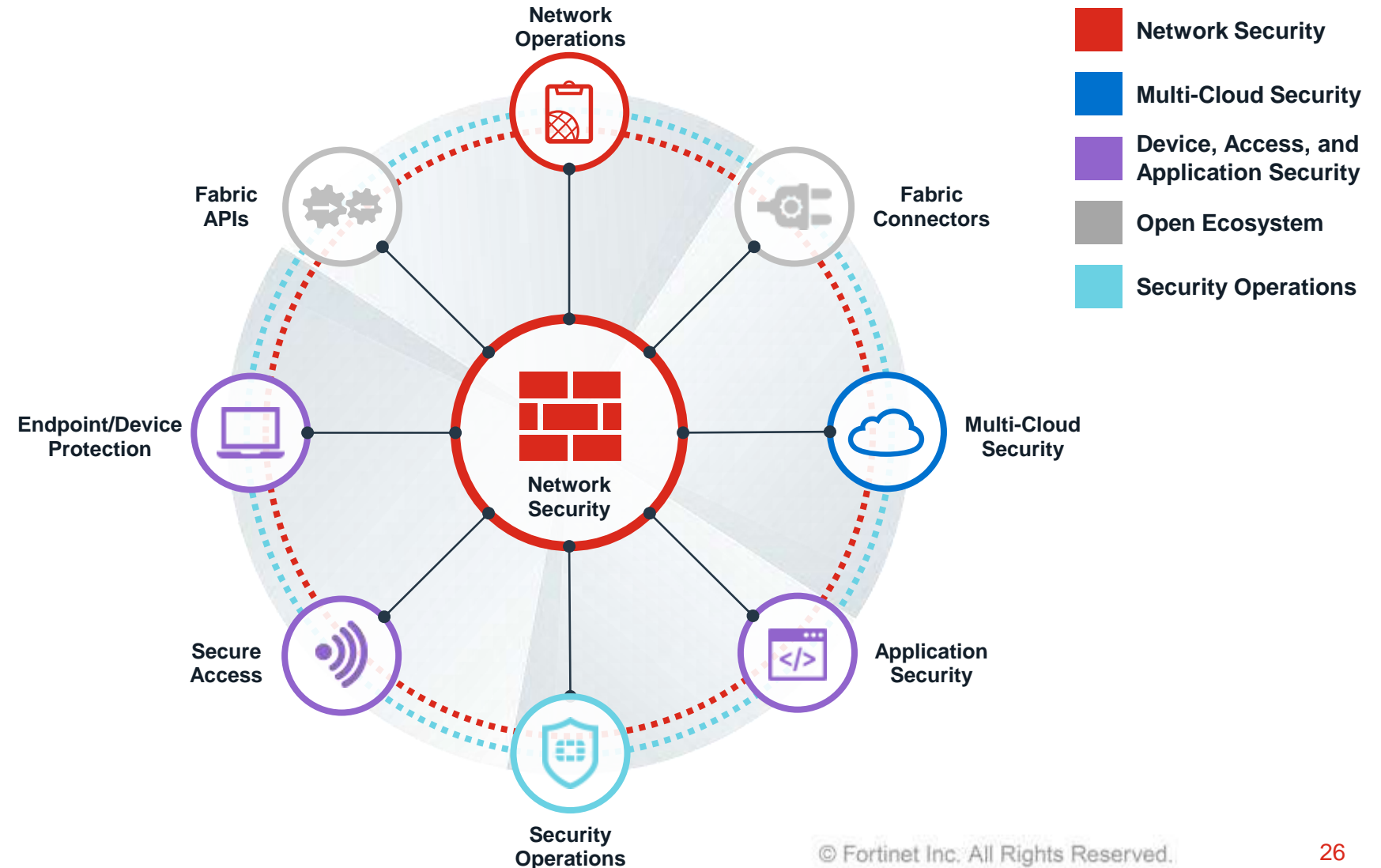# Security Driven Networking

BROAD

Visibility of the entire digital attack surface

INTEGRATED

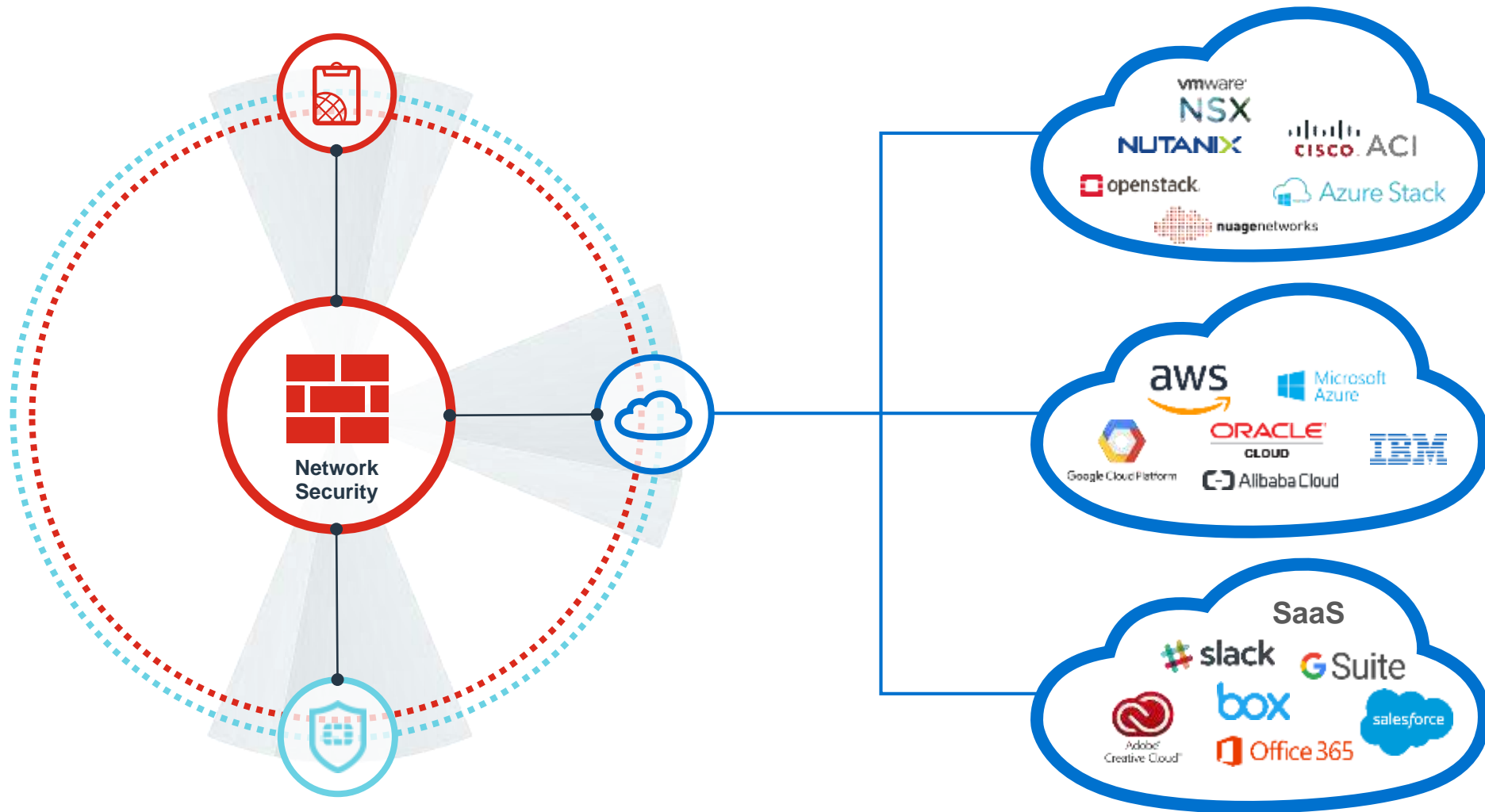**Protection across all devices, networks, and applications**
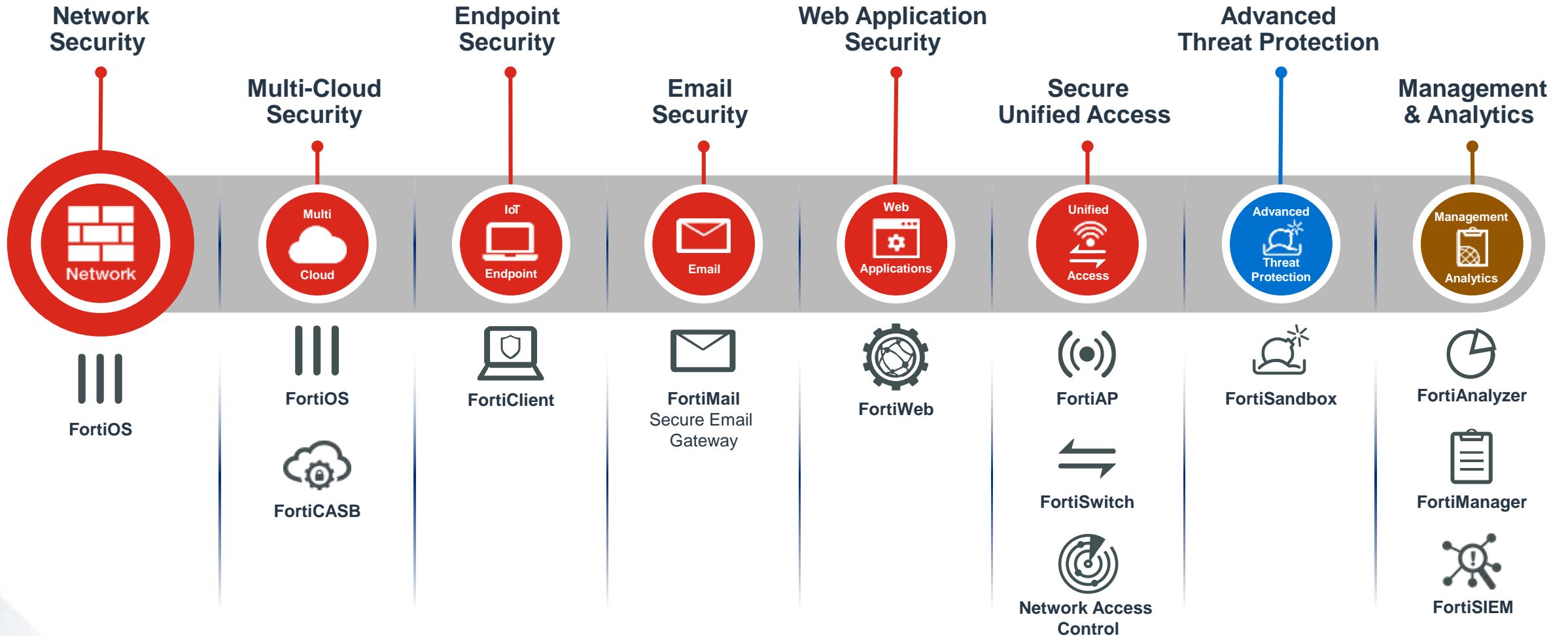
AUTOMATED

Operations and response driven by Machine Learning

Network Operations

Fabric APIs

Fabric Connectors

Endpoint/Device Protection

Network Security

Multi-Cloud Security

Secure Access

Application Security

Security Operations

Legend:
- Network Security
- Multi-Cloud Security
- Device, Access, and Application Security
- Open Ecosystem
- Security Operations

FERTINET

Fortinet Security Fabric—Cloud

The Broadest Security Portfolio in the Industry

Built from the ground up to deliver true integration end-to-end

Network Security	Multi-Cloud Security	Endpoint Security	Email Security	Web Application Security	Secure Unified Access	Advanced Threat Protection	Management & Analytics
Network	Multi Cloud	IoT Endpoint	Email	Web Applications	Unified Access	Advanced Threat Protection	Management Analytics
FortiOS	FortiOS	FortiClient	FortiMail Secure Email Gateway	FortiWeb	FortiAP	FortiSandbox	FortiAnalyzer
	FortiCASB				FortiSwitch		FortiManager
					Network Access Control		FortiSIEM

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			

The Integration of Security Automation Into the Application Lifecycle

DevSecOps
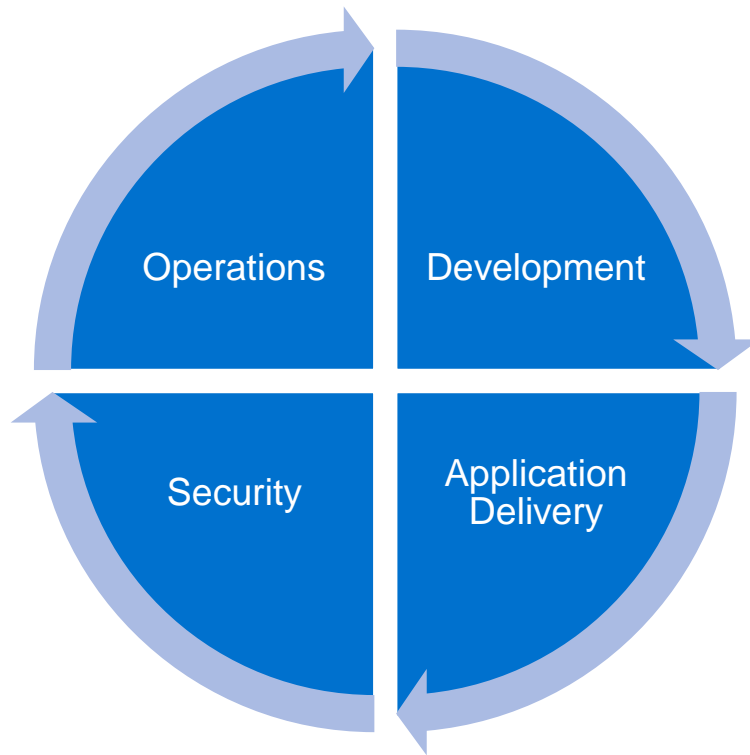
DevOps
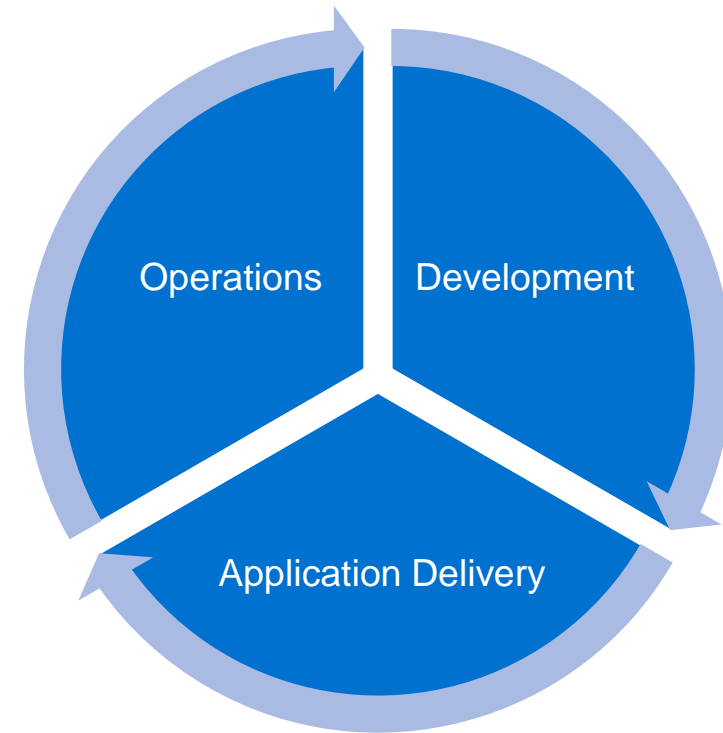
Protection for the Layer 7 Perimeter
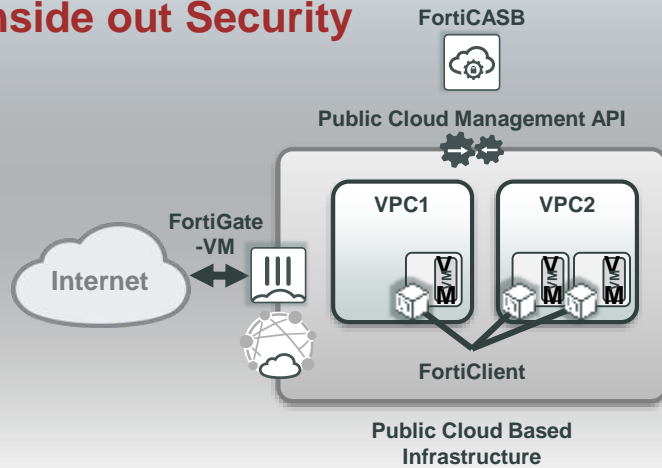

Web Protection

API Protection

Bot Protection

Cloud Security Use Cases

VISIBILITY AND CONTROL
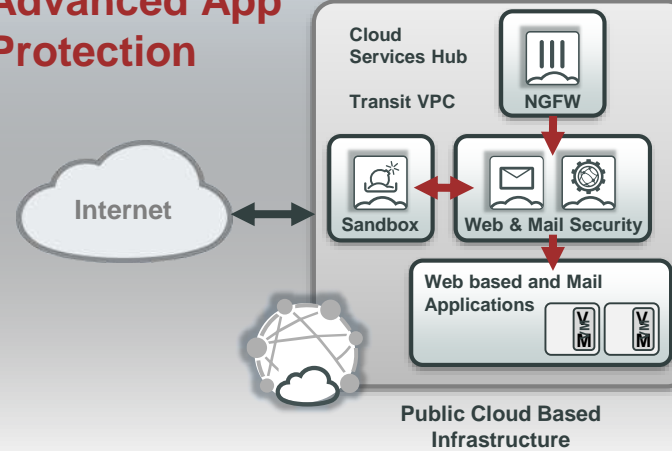
APPLICATION SECURITY

SECURE CONNECTIVITY

- SaaS Visibility and Control
- Cloud Infrastructure Visibility and Control
- Compliance in the Cloud
- Cloud Based Security management and analytics
- Web Application Security
- Intent Based Segmentation
- Container Security
- Cloud Workload Protection
- Secure Hybrid Cloud
- Cloud Security Services Hub
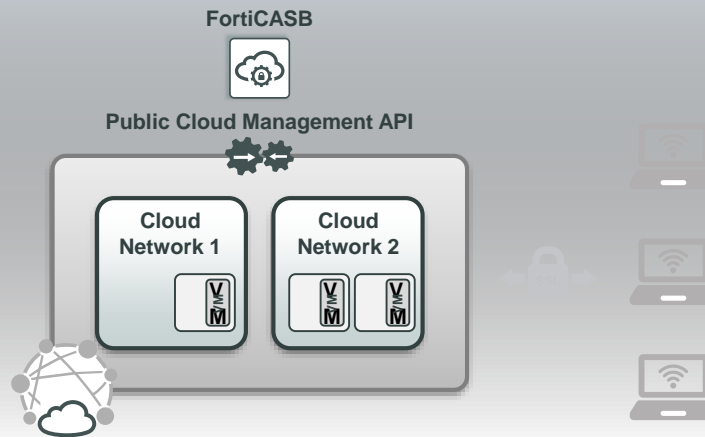- Secure Remote Access
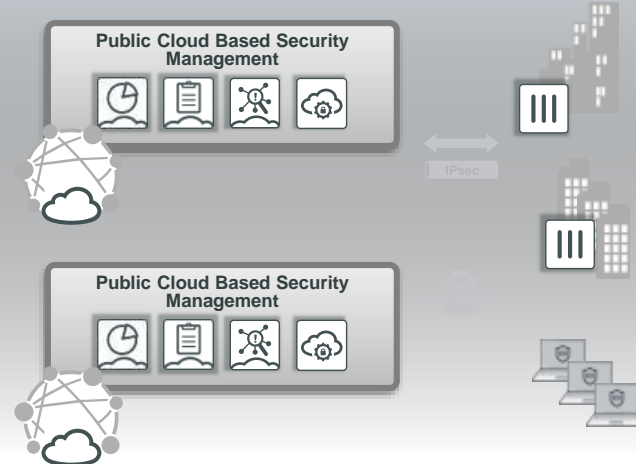
Top Uses Cases

Inside out Security

FortiCASB

Public Cloud Management API

FortiGate -VM

Internet

VPC1 VPC2

FortiClient

Public Cloud Based Infrastructure

Advanced App Protection

Cloud Services Hub

Transit VPC

NGFW

Internet

Sandbox

Web & Mail Security

Web based and Mail Applications

Public Cloud Based Infrastructure

Cloud Services Hub

Internet

Cloud Services Hub

Transit VPC

IPsec

VPC1 VPC2

Public Cloud Based Infrastructure

IaaS and SaaS

FortiCASB

Public Cloud Management API

Cloud Network 1 Cloud Network 2

Security Management

Public Cloud Based Security Management

IPsec

Public Cloud Based Security Management

Remote Access VPN

FortiGate-VM

SSL

IPsec

FortiGate-VM

Cloud Remote Access Points
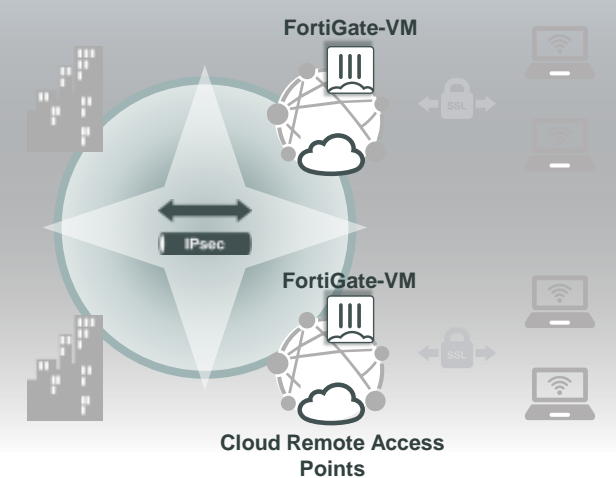
BRACE YOURSELVES

PERFORMANCE IS COMING

Performance Testing

FortiTester includes a wide range of testing functionalities, such:

- » Connection per Second
- » Request per Second
- » Concurrent Connection
- » Throughput
- » HTTP Transaction
- » Packet per Second
- » Payload Throughput
- » Latency
- » Loss Rate
- » Back to Back and more...

Performance Testing

FortiTester includes a wide range of protocols and applications

HTTP	HTTPS	SSL	IPSEC	SSL-VPN	UDP
TCP	RFC Benchmark	DNS	NTP	RADIUS	SIP
TFTP	BitTorrent	CIFP/SMB	FIX	FTP	IMAP
LDAP	NFS	POP3	PSQL	RDP	SMTP
YouTube	SSH	DHCP	WhatsApp	IGMP	RTSP/RTP

Deception is Widely Used in

Natural world

Human warfare

vs

Honeypot
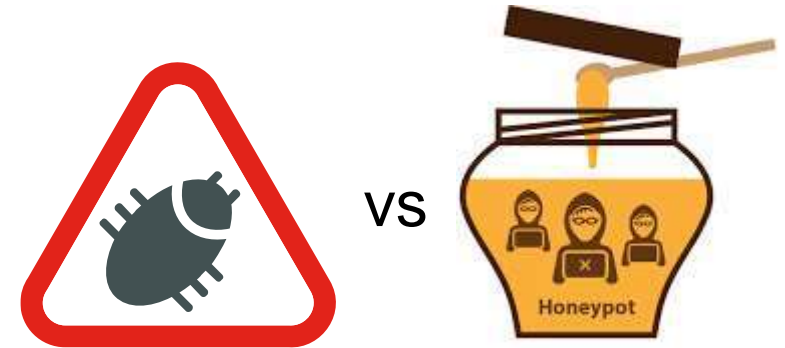
Cybersecurity warfare

(attack vs defend)

FortiDeceptor: Flexible

DEPLOYMENT
- On-Premise
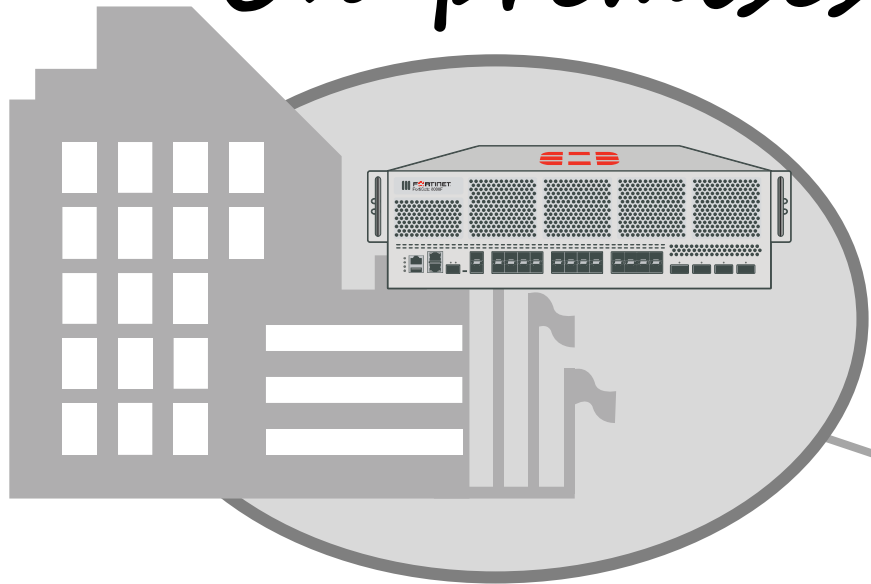- Public Cloud

DECOYS
- Branch
- Campus
- Data Center/Public Cloud

DECEPTION VMs
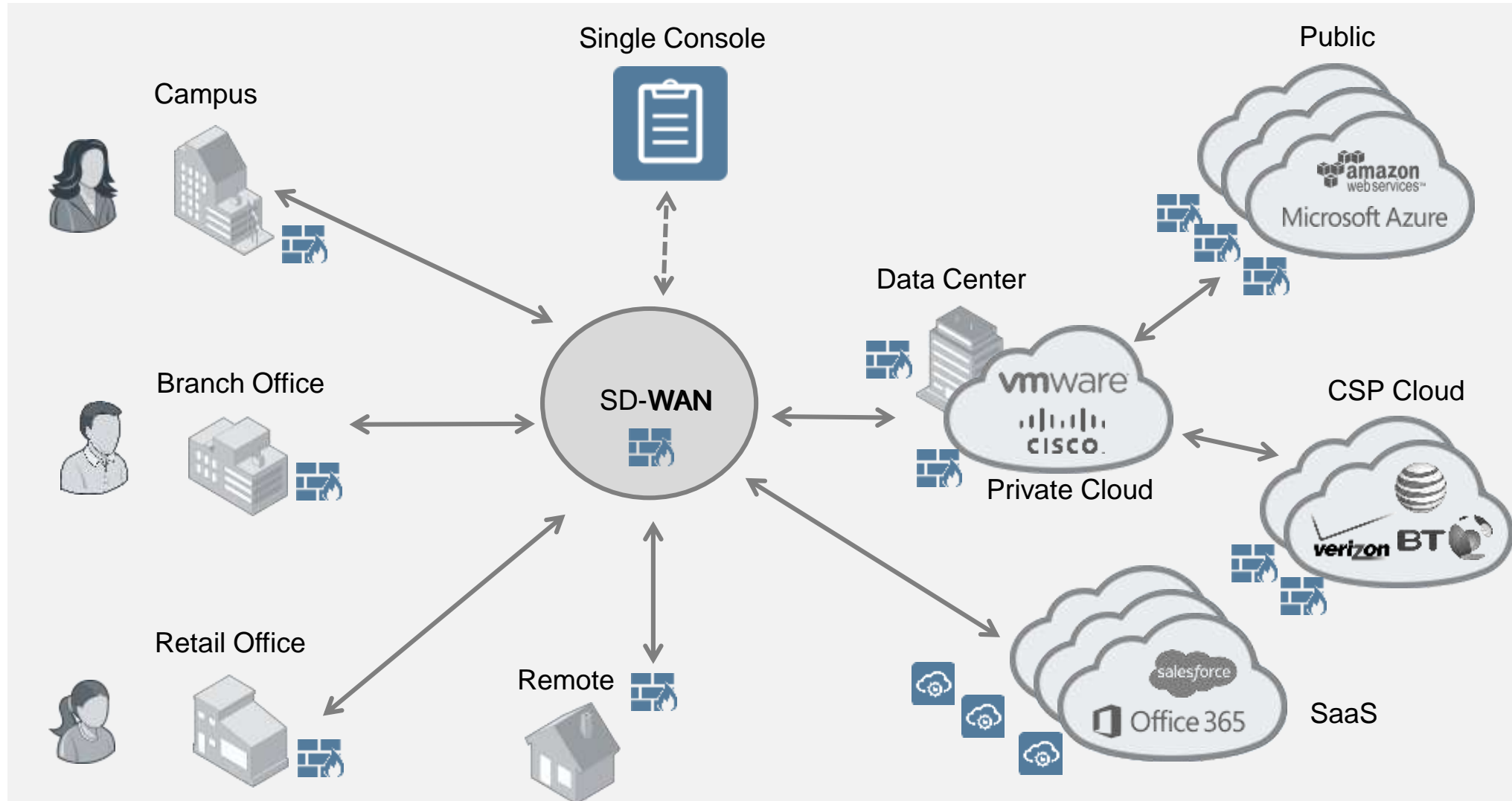- Windows
- Linux
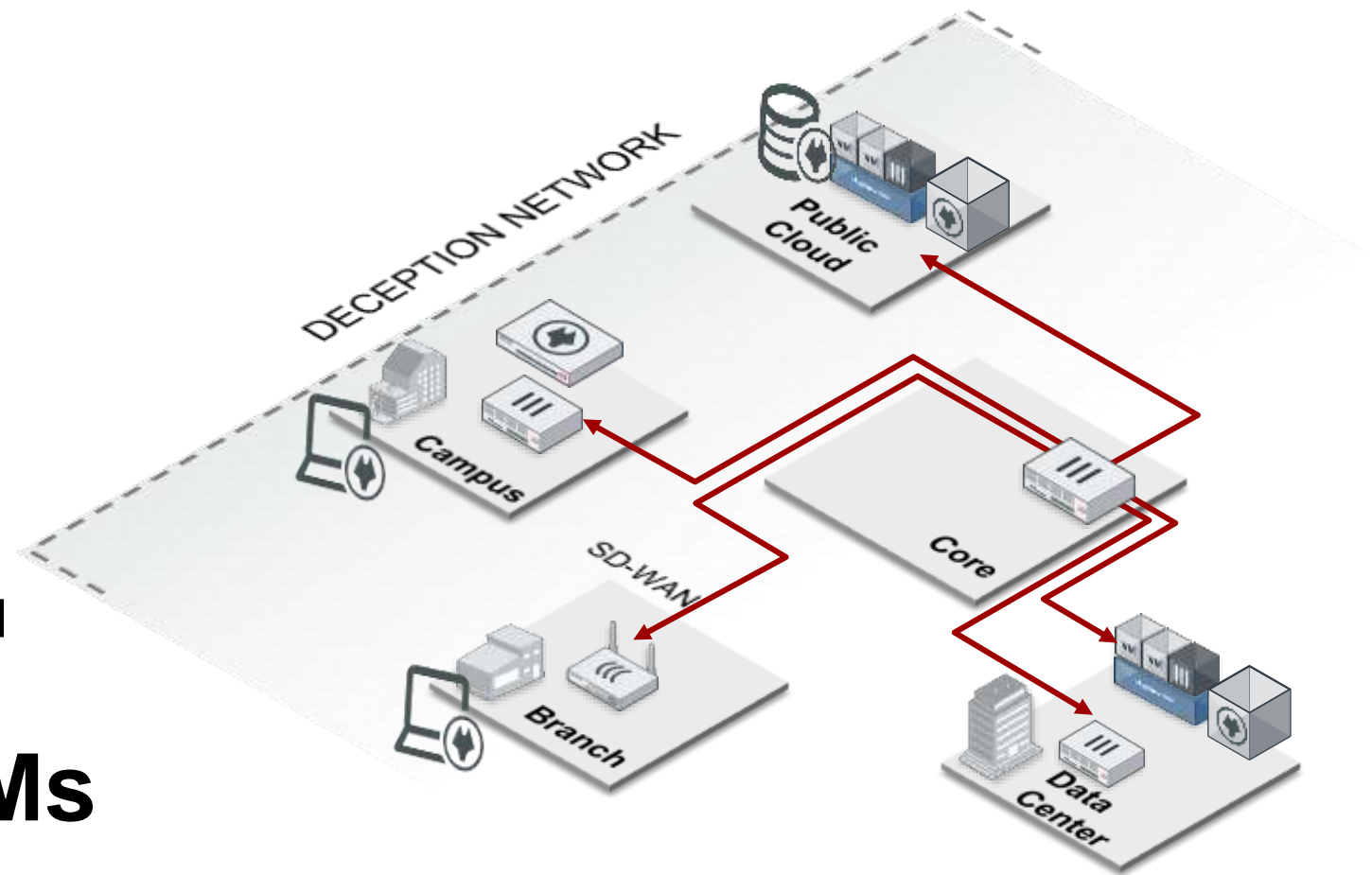
On-premises

SD-WAN

Cloud

Multi-Cloud Expansion has Expanded the Attack Surface

The leader in Multi-Cloud Security

- Industry's **most cloud security offerings** (Dozens)
- **Maximum flexibility** with global availability on all 6 cloud platforms
- **Simplified** <u>solution deployment</u> *and* <u>security operations</u> with A full suite of API's, Automation Templates, and Integrations
- **Mitigates on-going cloud security risks** via over 3 million global threat feeds providing advanced security telemetry.
- **Helping over 340,000 customers secure their journey to the cloud**
- Leader in **helping customers *design*, *implement*, and *operate*** true Multi-Cloud Security with Dedicated Cloud Security Architect team

Summary

Business Aligned & Consistent Visibility, Control & Automation of Cloud Security

timo@fortinet.com
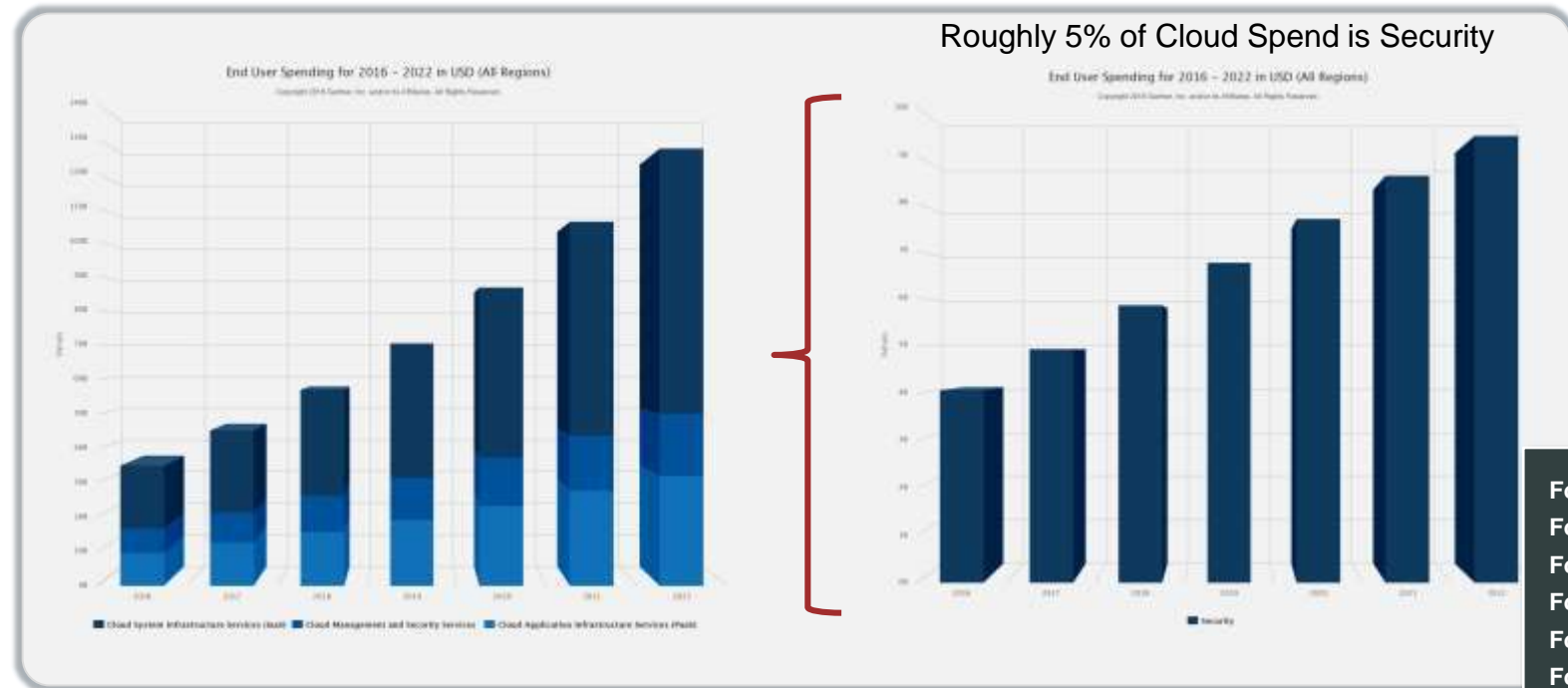
Cloud Market Insights

Information Technology / IT Services / IT Services / Managed Services and Cloud Infrastructure Services

IaaS and Infrastructure Utility Services

Top Vendors	Revenue 2016	Revenue 2017	YOY Growth	2017 Market Share
Amazon	9,775.3	12,220.7	+25%	33.2%
Microsoft	1,579.0	3,130.0	+98.2%	8.5%
Alibaba	670.4	1,090.1	+62.6%	3%
Google	500.2	780.0	+55.9%	2.1%
IBM	646.7	734.2	+13.5%	2%
Atos	504.7	586.5	+16.2%	1.6%
CGI	449.0	568.9	+26.7%	1.5%
Wipro	509.0	549.3	+7.9%	1.5%
Capgemini	458.6	526.3	+14.8%	1.4%
DXC	152.2	413.2	+171.4%	1.1%
Other Vendors	14,327.7	16,255.4	+13.5%	44.1%
Total	**29,572.9**	**36,854.6**	**24.6%**	**100%**

Source: Gartner (July 2018) Revenue (Millions of U.S. Dollars)

Roughly 5% of Cloud Spend is Security

FortiGate-VM
FortiWeb
FortiMail
FortiSandbox
FortiManager
FortiAnalyzer
FortiAuthenticator
FortiSIEM

Fortinet has offerings and partial offerings for only part of the cloud security market

CASB CSPM NGFW Micro Segmentation Security Analytics Security Management WAF Security Automation Fabric Products