



Securing Applications and Data
in the Cloud



George Armeniakos
Business Development Manager

Agenda

Topic	Speaker
The Challenge of Cloud Security	
Fortinet Cloud Security Vision	
Fortinet / Microsoft / AWS Relationship	
Fortinet Solutions in the Cloud	
Why Customers Choose Fortinet	





Digital Innovation

is disrupting
all industries



Retail



Healthcare



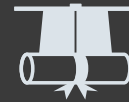
Finance



Manufacturing



Industrial



Higher Ed



Insurance



Consumer



Transport



Utilities



Government



Oil & Gas



Science



Auto



CSP



K12



What is the “Cloud”?

Cloud computing is the **on-demand** availability of computer system resources (O/S, storage, etc), or applications over network (LAN, Internet)

- Traditional datacenter staffing and maintenance
- Expensive

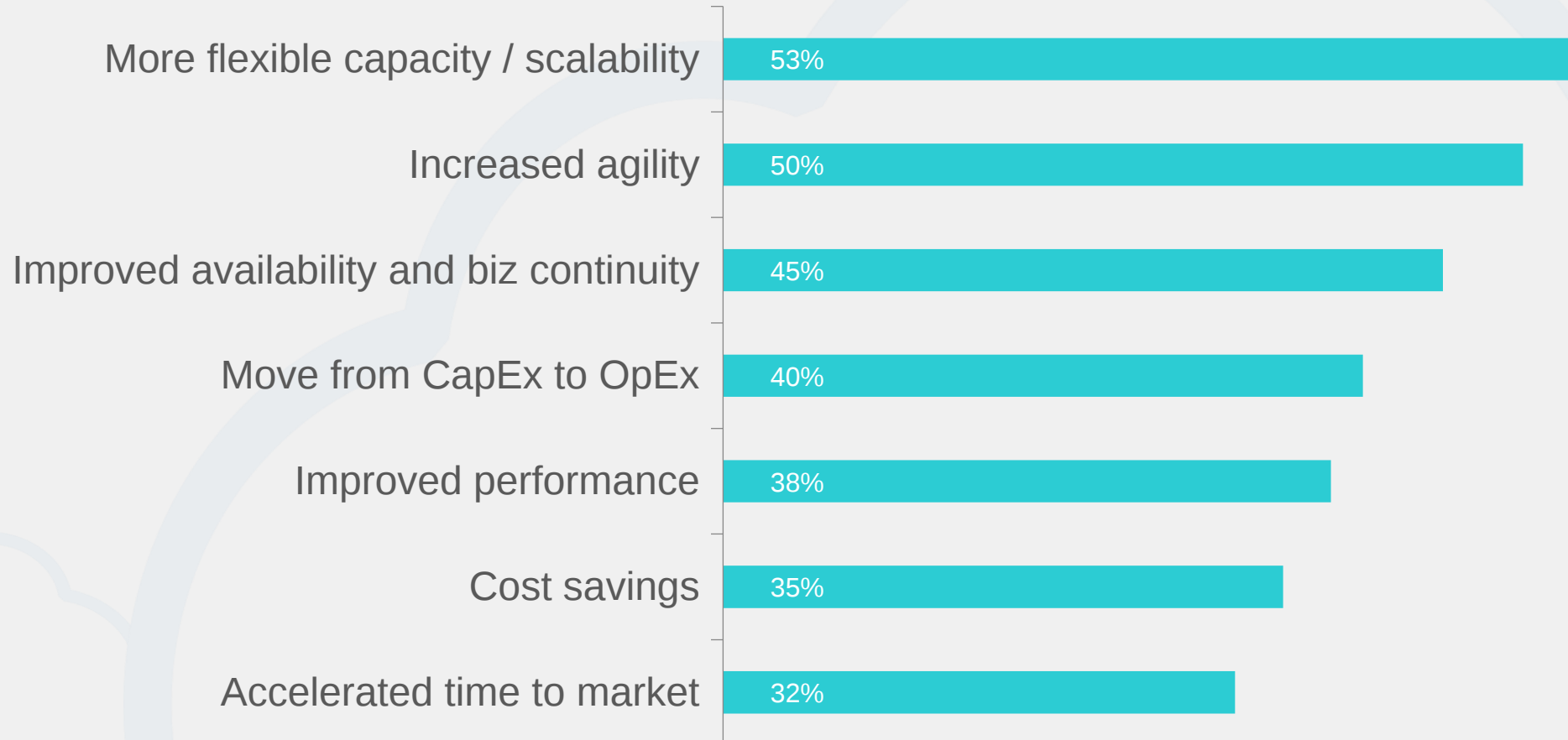


- Available to anyone over public internet
- Scales quickly and convenient

Why are Customers Adopting Cloud?

Key Business Drivers

Key benefits for moving to the Cloud



Why Public Cloud now?

[Google - Announces Region in GR](#)

New cloud regions coming to a country near you

October 11, 2022

New cloud regions coming to a country near you



Sachin Gupta
Vice President and GM, Infrastructure

Our global network of [Google Cloud](#) regions underpins all of the important work we do for our customers. With 35 regions, 106 zones, 173 network edge locations and 22 submarine cables available to

[Microsoft announces datacenter in GR](#)

Regions	Greece Central
	Coming soon
LOCATION	Athens
YEAR OPENED	Coming soon
AVAILABILITY ZONES PRESENCE	Coming soon
Compliance	Azure compliance offerings
DATA RESIDENCY	Stored at rest in Greece Learn more
DISASTER RECOVERY	Coming soon
PRODUCTS BY REGION	Coming soon
AVAILABLE TO	Coming soon

[AWS – Edge location in GR](#)

Europe

Europe (Ireland) Region Availability Zones: 3 <i>Launched 2007</i>	Europe (Frankfurt) Region Availability Zones: 3 <i>Launched 2014</i>	Europe (London) Region Availability Zones: 3 <i>Launched 2016</i>
Europe (Stockholm) Region Availability Zones: 3 <i>Launched 2018</i>	Europe (Milan) Region Availability Zones: 3 <i>Launched 2020</i>	Europe (Zurich) Region Availability Zones: 3 <i>Launched 2022</i>

AWS Edge Locations

Edge locations - Amsterdam, The Netherlands; Athens, Greece; Berlin, Germany; Brussels, Belgium; Bucharest, Romania; Dusseldorf, Germany; Frankfurt, Germany; Hamburg, Germany; Helsinki, Finland; Lisbon, Portugal; London, England; Munich, Germany; Oslo, Norway; Palermo, Italy; Paris, France; Prague, Czech Republic; Rome, Italy; Sofia, Bulgaria; Zurich, Switzerland

Regional Edge Caches - Dublin, Ireland; Frankfurt, Germany; London, England

[Learn more about the Global Edge Network »](#)

Europe (Ireland) Region is located in the Republic of Ireland.

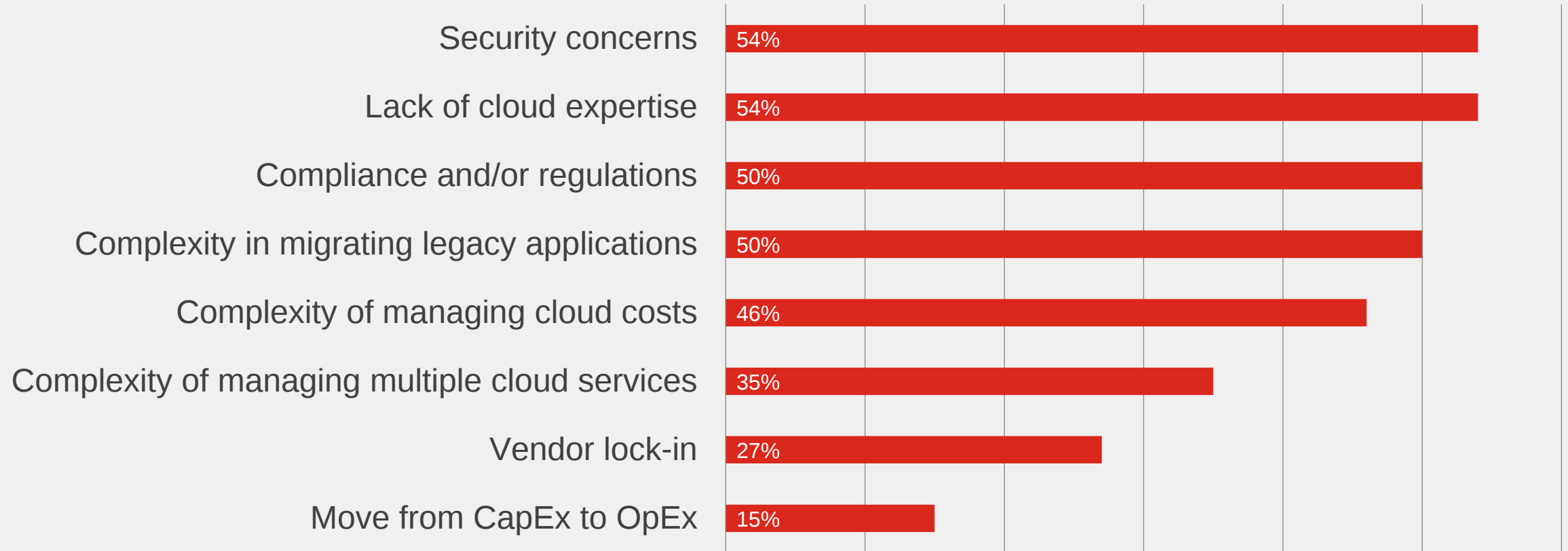
[See detailed list of offerings at all AWS locations](#)

Triple effect of region launch:

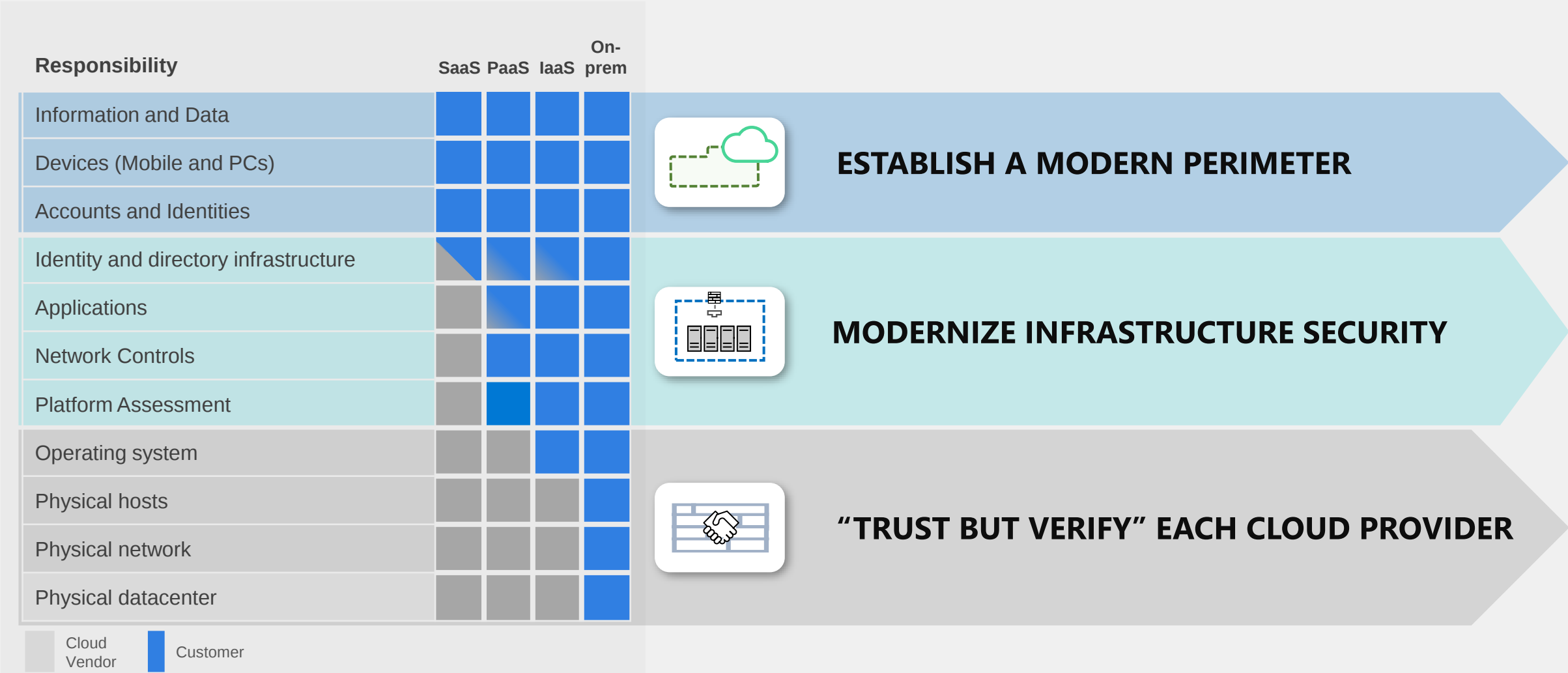
- Improved user experience
- Regulatory impact
- Cloud provider sales teams developing the market



Key business challenges for moving to the Cloud



Shared Responsibility and Key Strategies





But...

My cloud has security

**It is not the same security as
used on prem...**

**It's not the same security used
in other clouds**

**It's not the state-of-the-art in
security technology**

FORTINET®



One OS for Networking and Security

Only vendor recognized as a leader across both SD-WAN and Network Firewall

Sept. 2022 Magic Quadrant for WAN Edge Infrastructure
Fortinet Recognized as a Leader for 3rd Consecutive Year



Nov. 2022 Magic Quadrant for Network Firewalls
Fortinet Recognized as a Leader for 13th Consecutive Year

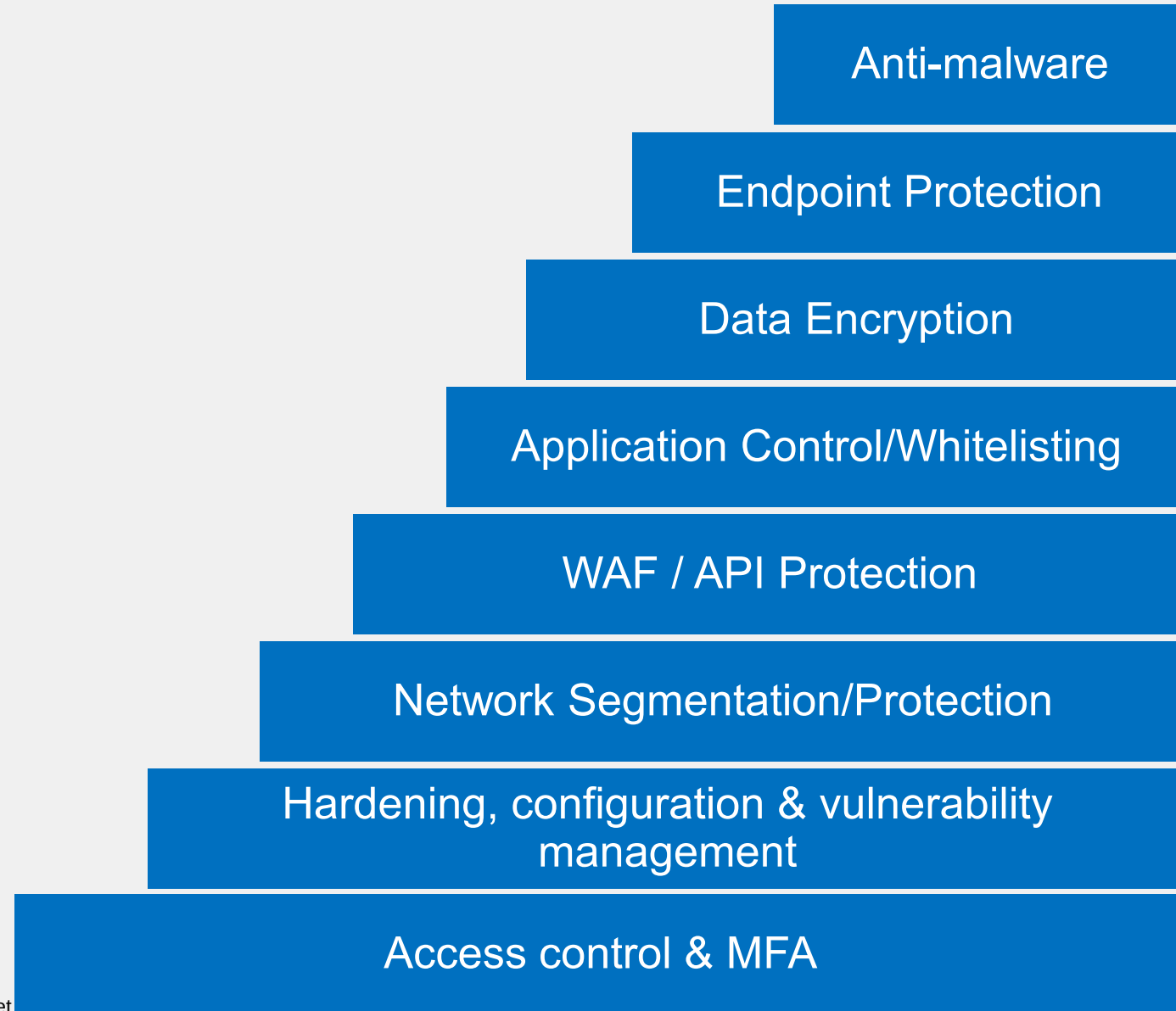


This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



Effective
Security
requires layered
security woven
into a Fabric

Security Strategy



Fortinet Cloud Security Vision

A Seamless Security Fabric

A seamless security fabric that extends across clouds and data centers.

Driven by Peerless Threat Intelligence

Best-in-class security backed by the leading security threat feeds and research.

Security that is Software Defined and Automated

Agile security, automated, DevOps ready, and container aware.

**Complete
cybersecurity
protection,
everywhere you
need it.**



Google Cloud



Alibaba Cloud



IBM Cloud





Fortinet Security Fabric The
industry's highest-performing integrated
cybersecurity mesh platform



Product Matrix



Click on icons in this
document for additional
information



Fortinet Brochure

Highlighting our broad, integrated,
and automated solutions, quarterly



Free Training

Fortinet is committed to training
over 1 million people by 2025



FortiOS

The Heart of the Fortinet
Security Fabric



Secure Networking



FortiGate

NGFW w/ SOC acceleration and
industry-leading secure SD-WAN



FortiGate SD-WAN

Application-centric, scalable, and
Secure SD-WAN with NGFW



FortiExtender

Extend scalable and resilient LTE
and LAN connectivity



FortiAP

Protected LAN Edge deployments
with wireless connectivity



FortiSwitch

Deliver security, performance,
and manageable access to data



Linksys HomeWRK

Secure Work-from-Home solution
for remote and hybrid workers



FortiNAC

Visibility, access control and
automated responses for all
networked devices



FortiProxy

Enforce internet, compliance and
granular application control



Fortisolator

Maintain an "air-gap" between
browser and web content



Cloud Security



FortiGate VM

NGFW w/ SOC acceleration and
industry-leading secure SD-WAN



FortiDDOS

Machine-learning quickly inspects
traffic at layers 3, 4, and 7



FortiCNP

Manage risk and compliance
through multi-cloud infrastructures



FortiDevSec

Continuous application security
testing in CI/CD pipelines



FortiWeb

Prevent web application attacks
against critical web assets



FortiADC

Application-aware intelligence for
distribution of application traffic



FortiGSLB Cloud

Ensure business continuity during
Unexpected network downtime



FortiMail

Secure mail gateway to protect
against SPAM and virus attacks



FortiCASB

Prevent misconfigurations of SaaS
applications and meet compliance



Zero Trust Access



FortiSASE

Enforce dynamic network access
control and network segmentation



ZTNA Agent

Remote access, application
access, and risk reduction



FortiAuthenticator

Identify users wherever they are
and enforce strong authentication



FortiToken

One-time password application
with push notification



FortiClient Fabric Agent

IPSec and SSL VPN tunnel,
endpoint telemetry and more



FortiConnect

Simplified guest access, BYOD,
and policy management



**Fabric Management
Center: NOC**



FortiManager

Centralized management of your
Fortinet security infrastructure



FortiGate Cloud

SaaS w/ zero touch deployment,
configuration, and management



FortiMonitor

Analysis tool to provide NOC and
SOC monitoring capabilities



FortiAIOps

Network inspection to rapidly
analyze, enable, and correlate



FortiExtender Cloud

Deploy, manage and customize
LTE internet access



FNDN

Exclusive developer community for
access to advanced tools & scripts



**Fabric Management
Center: SOC**



FortiDeceptor

Discover active attackers inside
with decoy assets



FortiNDR

Accelerate mitigation of evolving
threats and threat investigation



FortiEDR

Automated protection and
orchestrated incident response



FortiSandbox / FortiAI

Secure virtual runtime environment
to expose unknown threats



FortiAnalyzer

Correlation, reporting, and log
management in Security Fabric



FortiSIEM

Integrated security, performance,
and availability monitoring



FortiSOAR

Automated security operations,
analytics, and response



FortiTester

Network performance testing and
breach attack simulation (BAS)



SOC-as-a-Service

Continuous awareness and control
of events, alerts, and threats



**Incident Response
Service**

Digital forensic analysis, response,
containment, and guidance



**Support & Mitigation
Services**



FortiCare Essentials*

15% of hardware, FG-80 & below



FortiCare Premium*

20% of hardware



FortiCare Elite**

25% of hardware



FortiConverter

25% of hardware

* FortiCare Premium is formerly 24x7
Support. Lower support price for Switches
and APs

** Response time for High Priority tickets.
Available for FortiGate, FortiManager,
FortiAnalyzer, FortiSwitch, and FortiAP



**FortiGuard Threat
Intelligence**

Powered by FortiGuard Labs



Open Ecosystem

The industry's most extensive
ecosystem of integrated solutions



Fabric Connectors

Fortinet-developed



DevOp Tools & Script

Fortinet & community-driven



Fabric API Integration

Partner-led



Extended Ecosystem

Threat sharing w/ tech vendors

**Communication and
Surveillance**



FortiFone

Application-centric, scalable, and
Secure SD-WAN with NGFW



FortiVoice

Extend scalable and resilient LTE
and LAN connectivity



FortiCamera

NGFW w/ SOC acceleration and
industry-leading secure SD-WAN



FortiRecorder

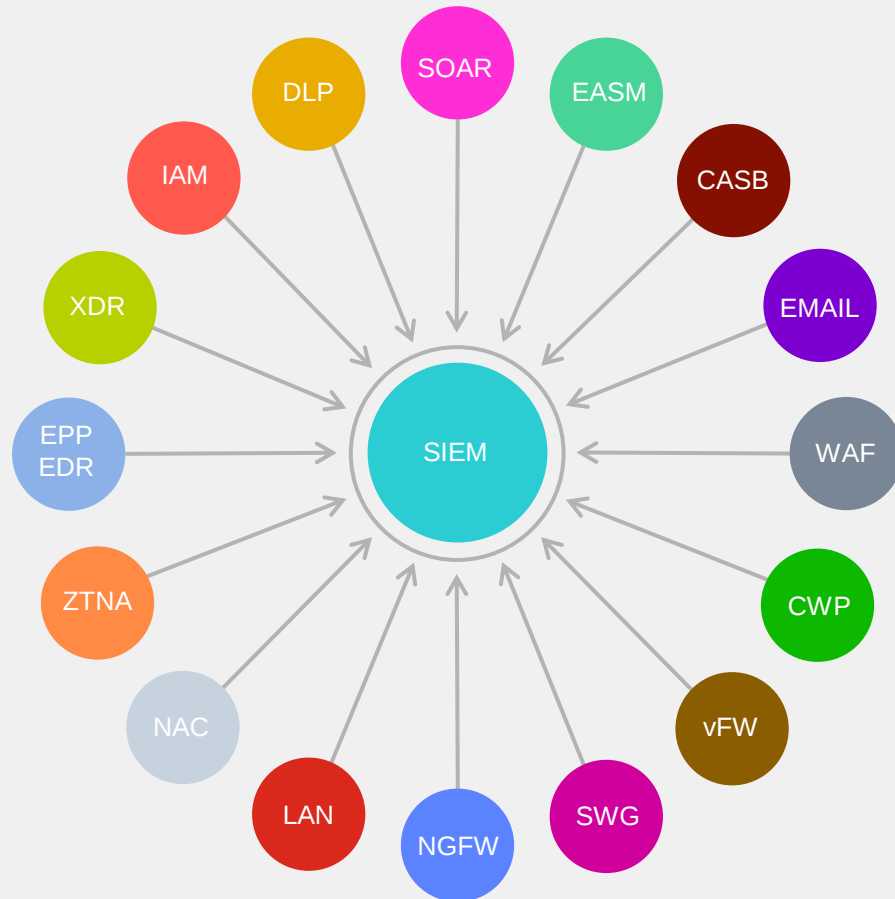
Protected LAN Edge deployments
with wireless connectivity



Product Integrations vs a Security Fabric

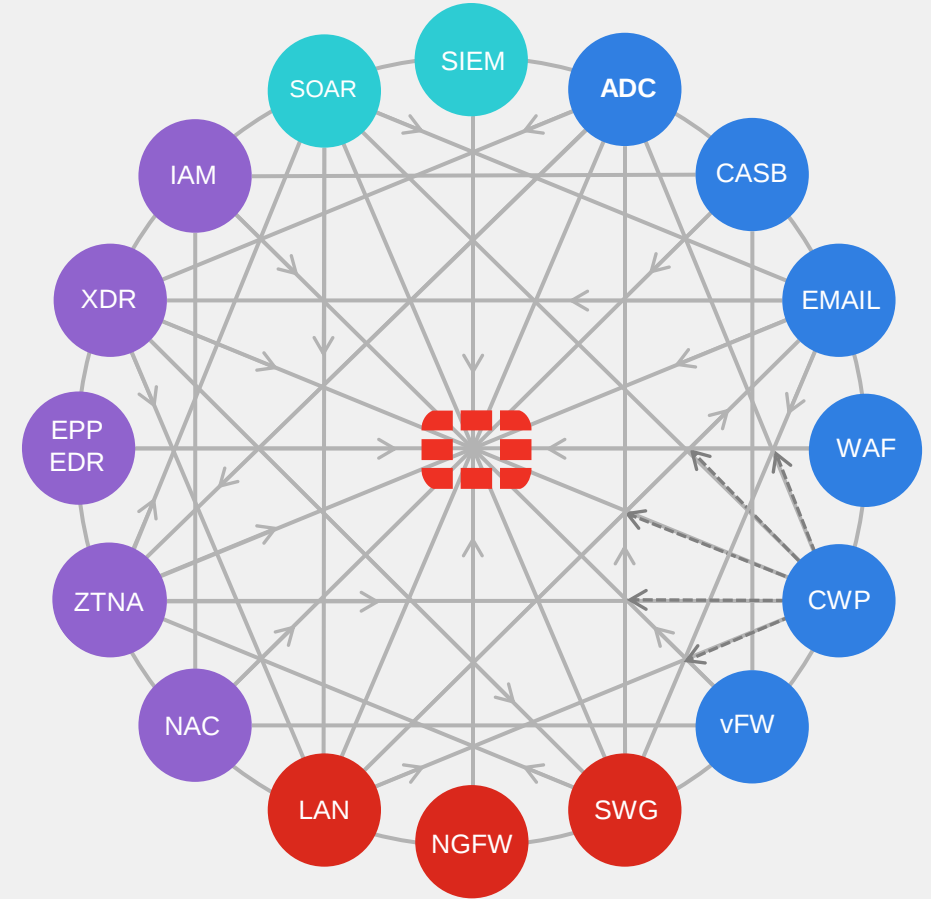
A SIEM is not a Mesh

Cybersecurity Point Products



Most Vendors

Cybersecurity Platform Approach

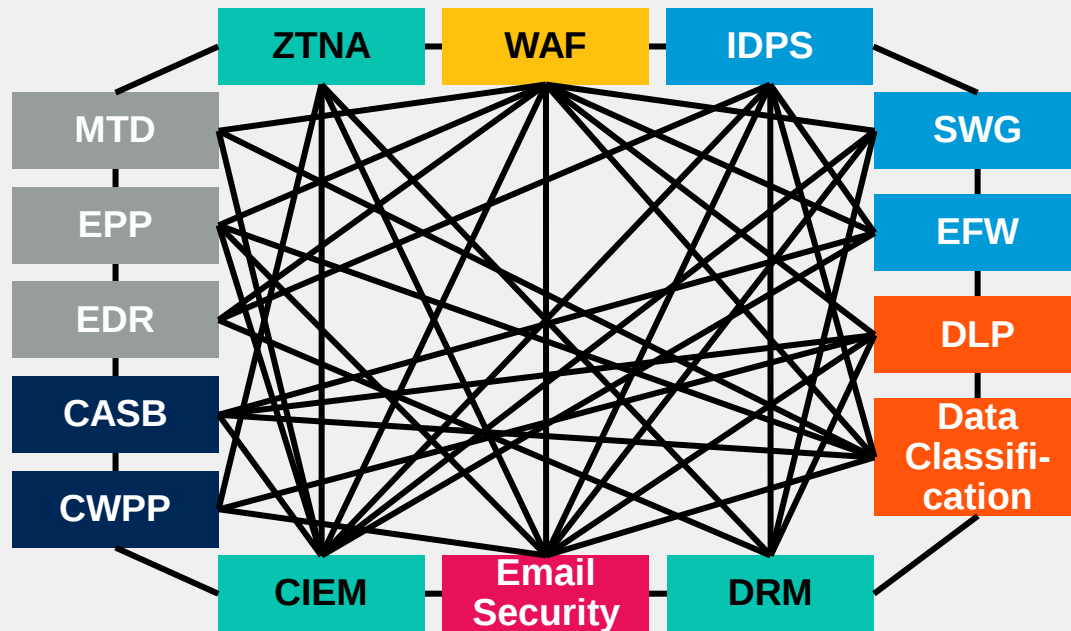


Fortinet Security Fabric



Overview: Gartner Cybersecurity Mesh Architecture

Gartner®



Executive Guide to Cybersecurity Mesh, 2022

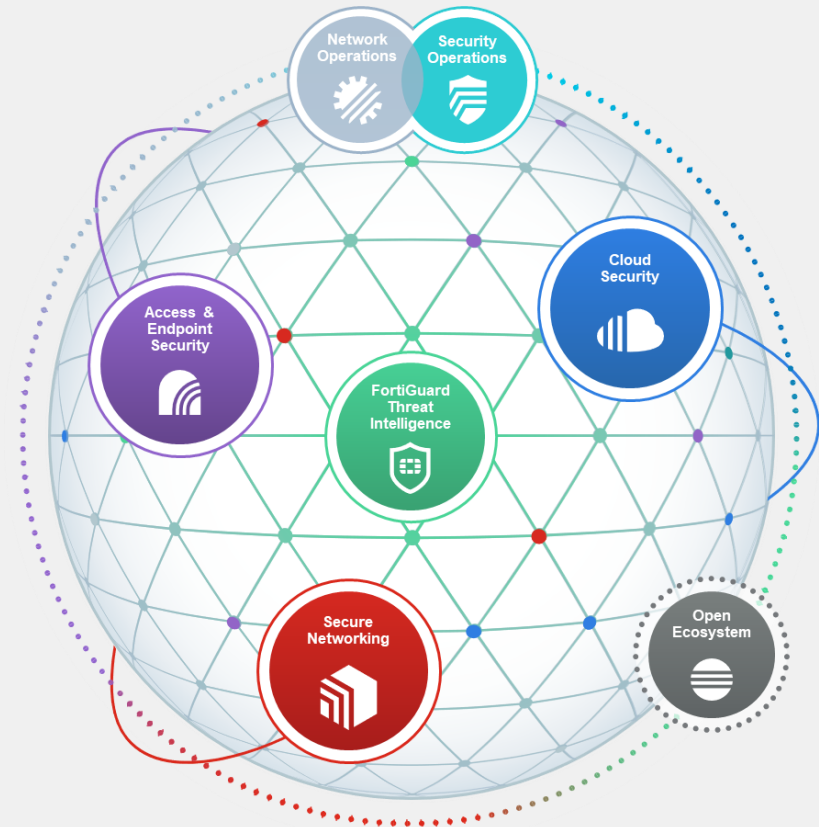
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Fortinet.



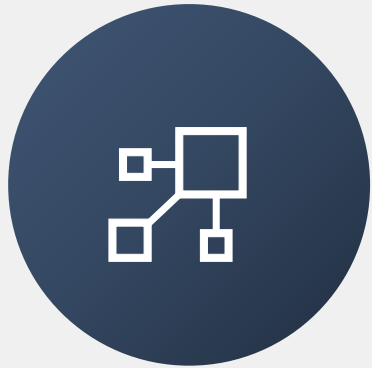
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORTINET®



Top 3 Strategies – Securing Hybrid Cloud and Multicloud

Simplify and Strengthen Network Security by



Securing Connectivity



**Protecting
Perimeters**



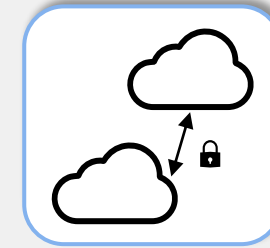
**Centralizing
Operations**

Top 3 Strategies – Securing Connectivity



Hybrid Cloud Connectivity

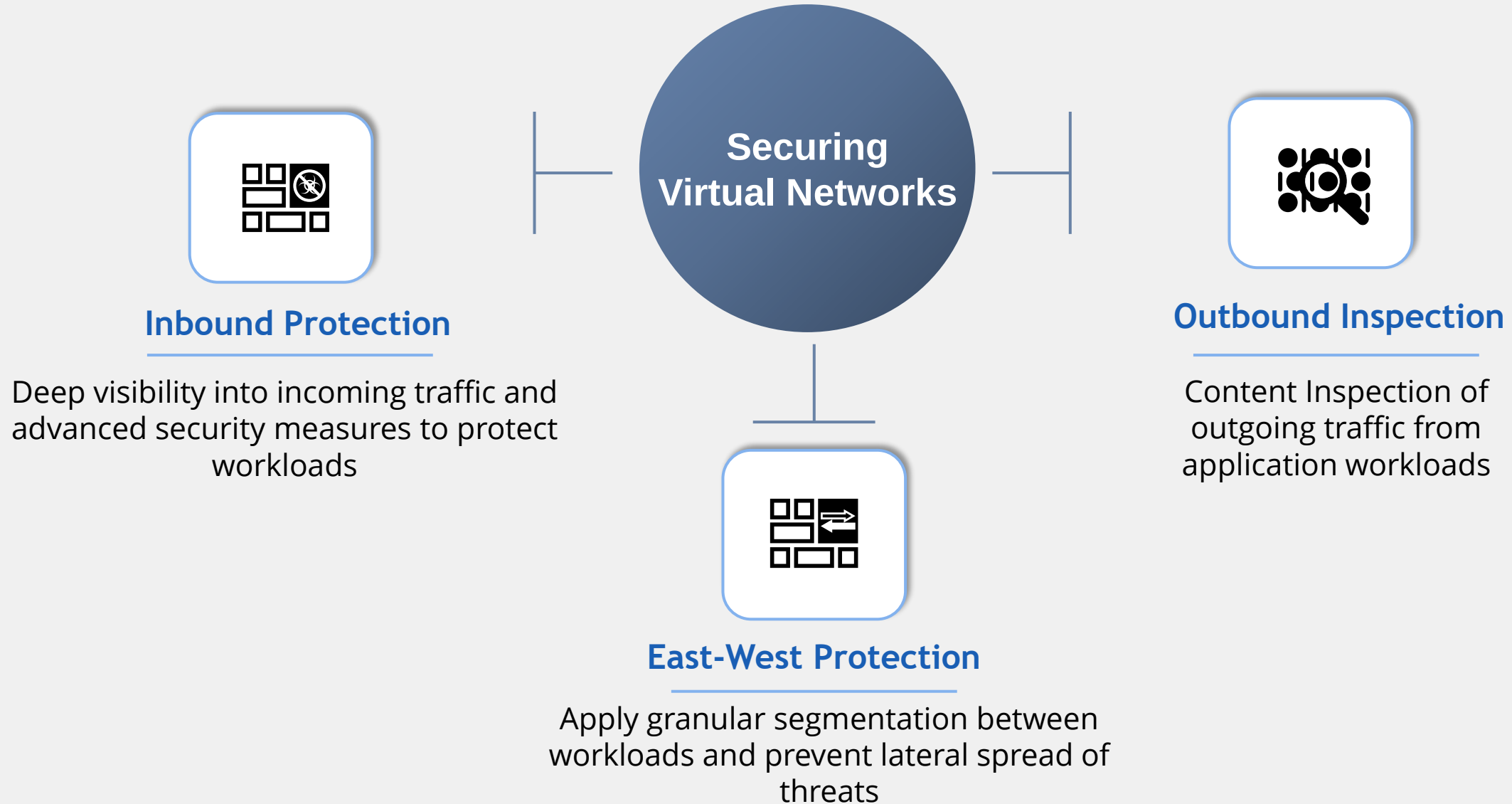
Connect users to applications in public cloud and Virtual datacenters



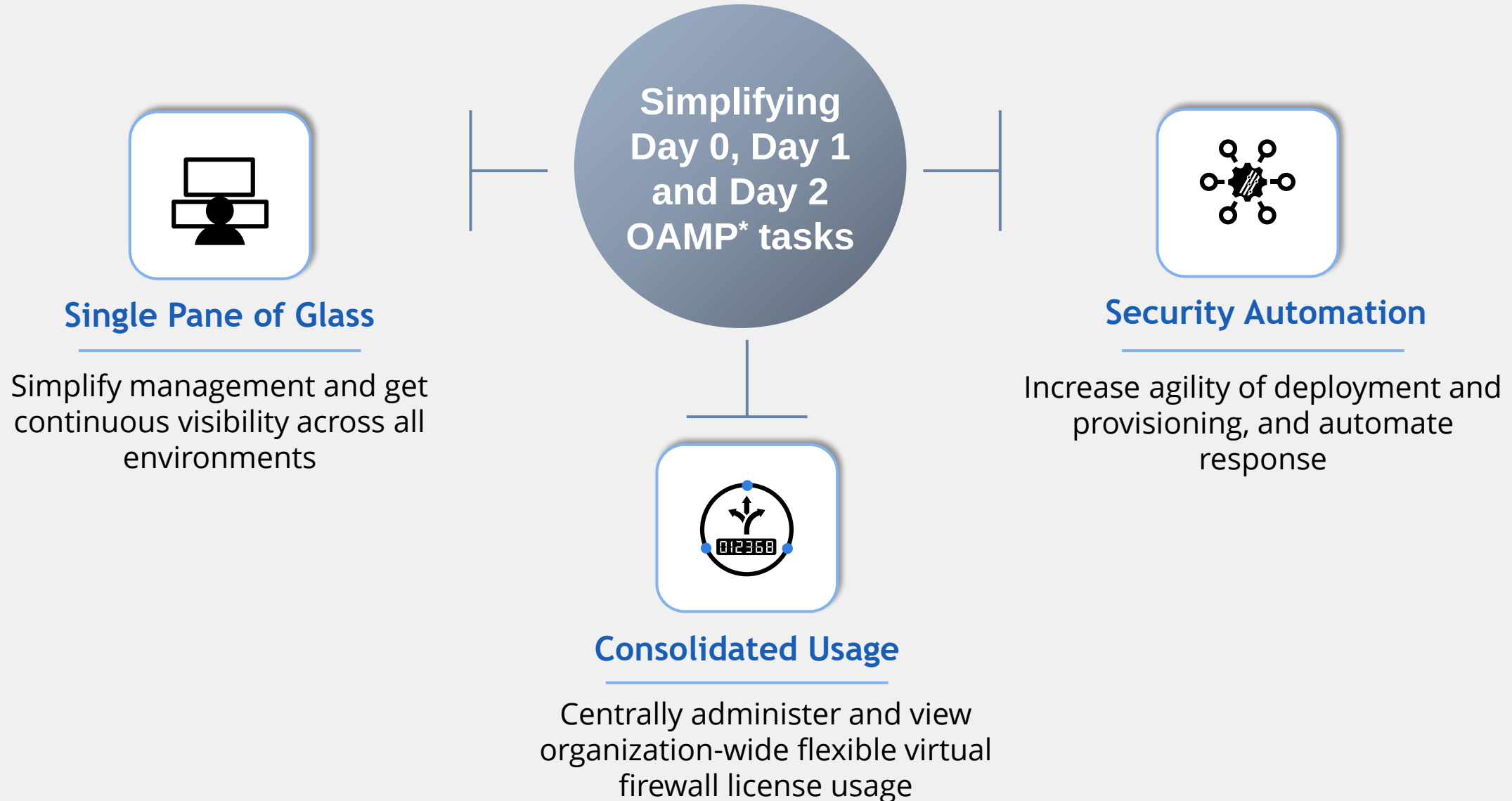
Multicloud Connectivity

Connect applications across clouds including public and private clouds

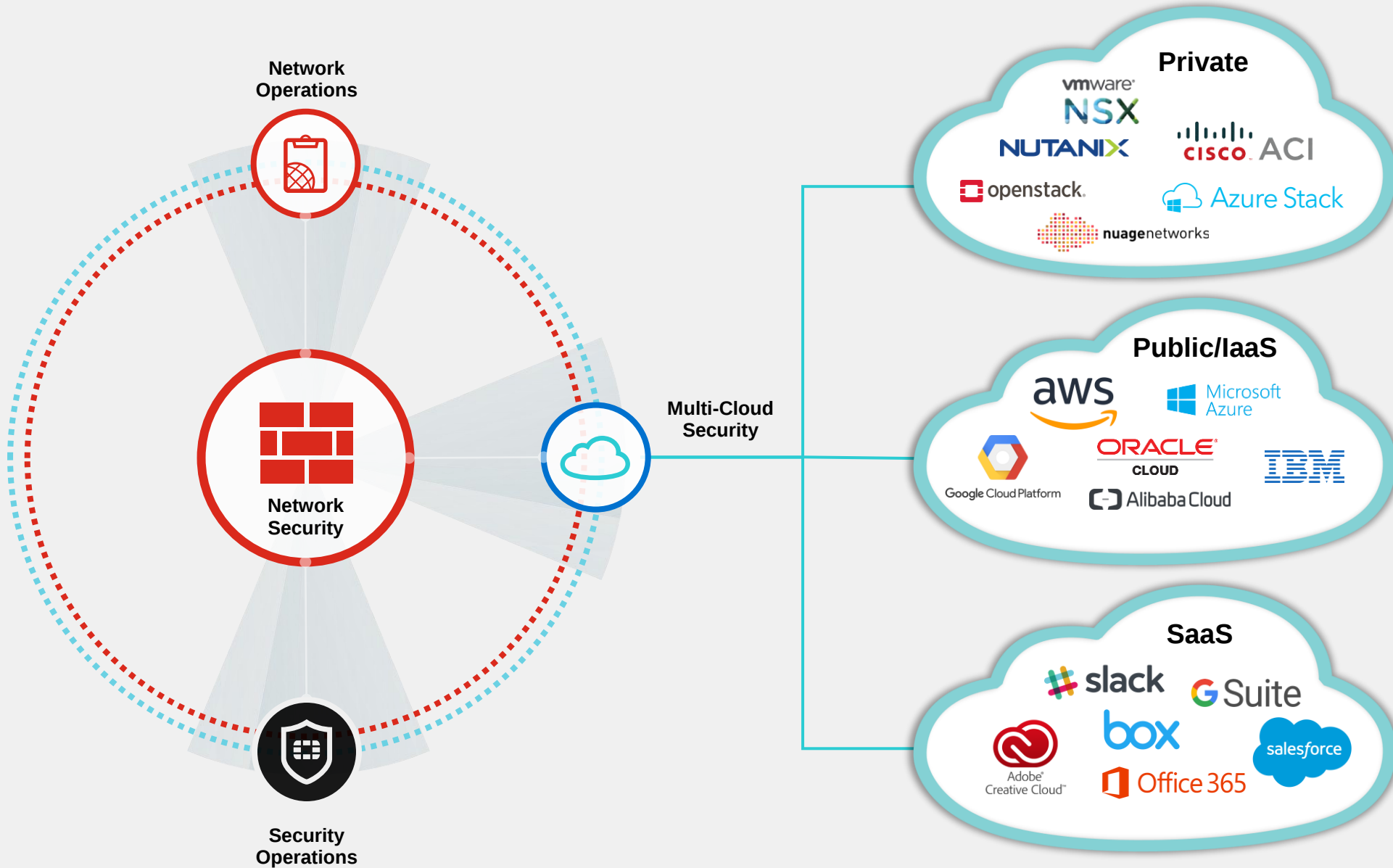
Top 3 Strategies – Protecting Perimeters



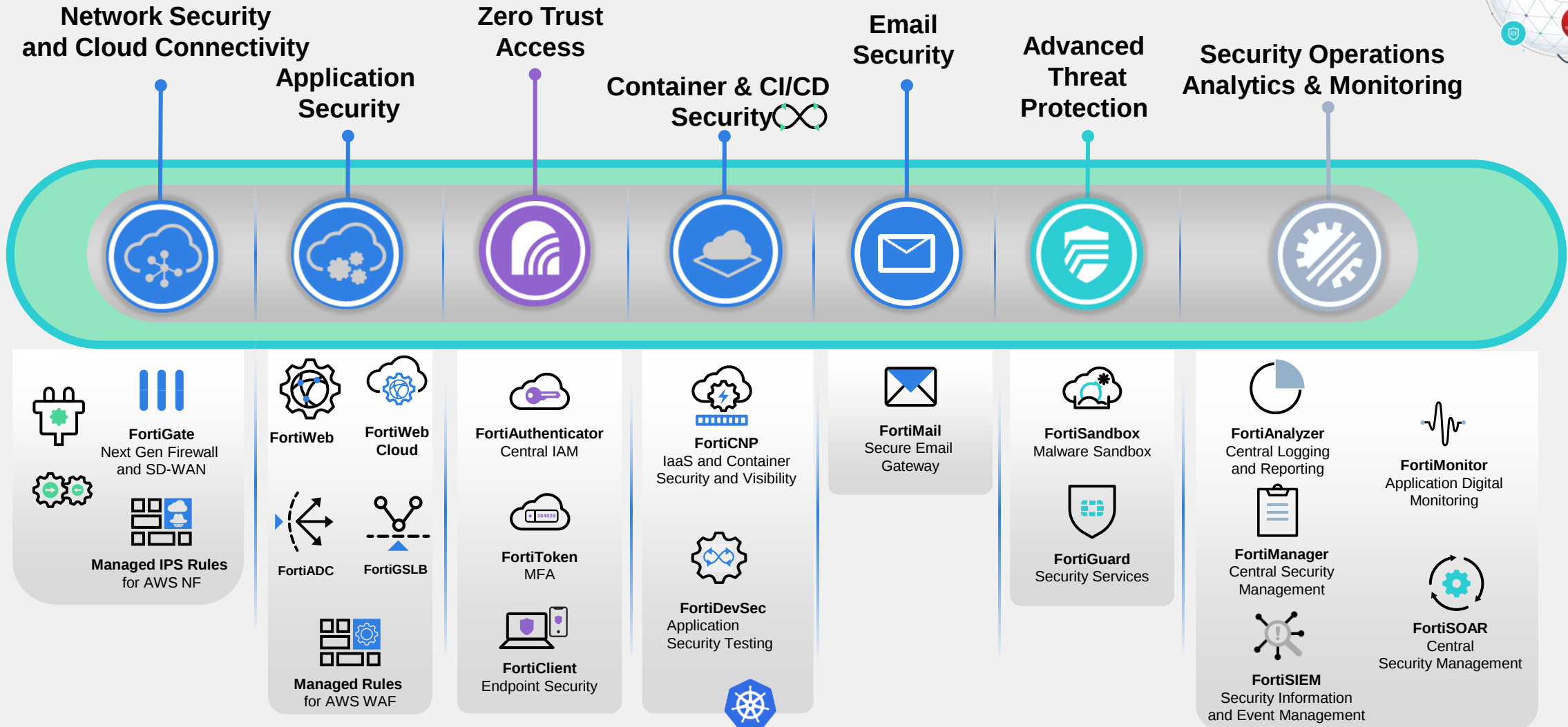
Top 3 Strategies – Centralize Operations



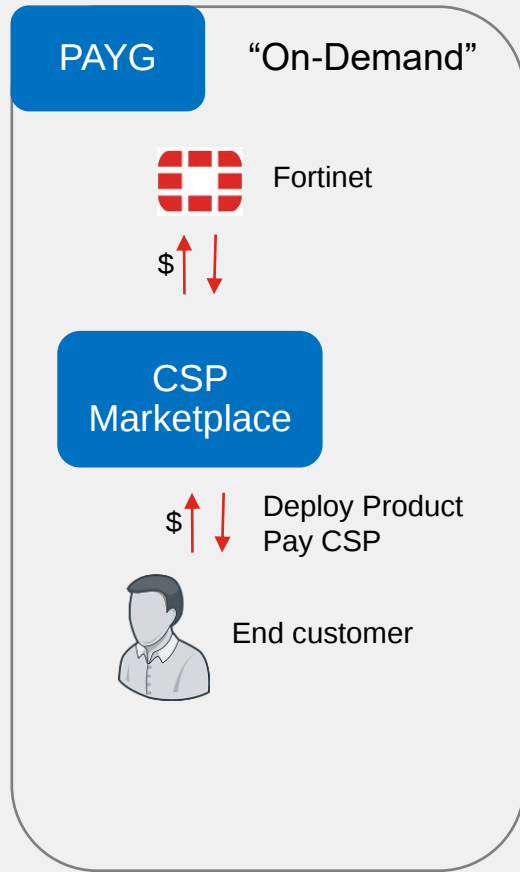
Fortinet Security Fabric - Cloud



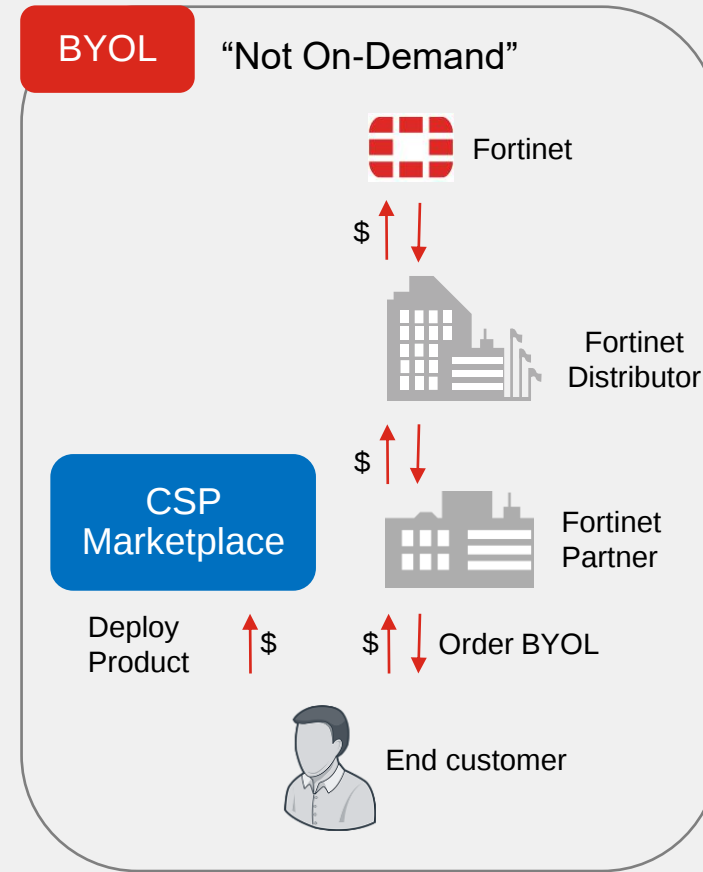
Fortinet Security Fabric for Cloud Environments



Purchasing Model – BYOL vs. PAYG



- Post-paid, on-demand, direct
- No commitment/contract
- Mostly SMB, Startups



- Pre-paid
- Traditional GTM via partners



Partnering with Microsoft

Fortinet and Microsoft working together for security and compliance



The Fortinet / Microsoft Partnership

Partnering to secure mission critical workloads

Sharing a common vision extending security across clouds and data centers with network, application, and platform security.

Working together to support Enterprise and Government accounts

Business and technical engagements at all levels. Fortinet is the only security vendor on Microsoft's SAP WW Partner Advisory Board



Business Level Engagement

- Over **10,000** Azure Customers
- Microsoft Marketplace Partner of the Year
- Top Security ISV Consumption Partner
- Fortinet on Microsoft SAP Advisory Board
- Fortinet is an Azure top ISV Consumption Partner
- Fortinet helps secure Microsoft Technology Centers (MTCs)

Deep 2-Way Technical Integrations

Over 101 points of integration including Azure Virtual WAN, Azure Stack, Edgewise, automation technology, Sentinel and more. Meanwhile, Microsoft has achieved "Fabric Ready"





INDUSTRY TRENDS

Choose Your Cloud Firewall Wisely



- Cloud vendors entering the NGFW space
- Microsoft shipping their first NGFW
- Been described as “Good Enough” security



Azure Network Security Best Practices

Protect your workloads beyond native Azure security options

Microsoft | Docs Documentation Learn Q&A Code Samples

Azure Product documentation Architecture Learn Azure Develop Resources

Azure / Security / Fundamentals

Filter by title

Overview

Securing workloads in Azure

Azure platform and infrastructure

Identity management

Network security

Security overview

Best practices

DDoS Protection

Secure hybrid network architecture

IaaS security

Data security, encryption, and storage

Application

Monitoring, auditing, and operations

Resources

Azure best practices

10/02/2019 • 16 minutes to read • 3

This article discusses a collection of Azure best practices derived from our experience with Azure networking and security.

For each best practice, this article explains:

- What the best practice is
- Why you want to enable that best practice
- What might be the result if you fail to enable the best practice
- Possible alternatives to the best practice
- How you can learn to enable the best practice

These best practices are based on a consensus opinion of the time this article was written. Opinions and technology change on a regular basis to reflect those changes.

Use strong network controls

You can connect [Azure virtual machines \(VMs\)](#) and [Azure virtual networks](#). That is, you can connect virtual network interfaces to devices on the same virtual network, different virtual networks, or to devices on the same virtual network, different virtual networks.

As you plan your network and the security of your network, we recommend that you centralize:

- Management of core network functions like ExpressRoute, virtual network and subnet provisioning, and IP addressing.
- Governance of network security elements, such as network virtual appliance functions like ExpressRoute, virtual network and subnet provisioning, and IP addressing.

Download PDF

Use virtual network appliances

Network security groups and user-defined routing can provide a certain measure of network security at the network and transport layers of the [OSI model](#). But in some situations, you want or need to enable security at high levels of the stack. In such situations, we recommend that you deploy virtual network security appliances provided by Azure partners.

Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include:

- Firewalling
- Intrusion detection/intrusion prevention
- Vulnerability management
- Application control
- Network-based anomaly detection
- Web filtering
- Antivirus
- Botnet protection

To find available Azure virtual network security appliances, go to the [Azure Marketplace](#) and search for "security" and "network security."

Gartner - 2022 vs 2021

- Azure Network Firewall downgraded Challenger -> Niche Player
- FortiGate for 13th time Leader and with greater “Ability to execute” related to PAN and Checkpoint
- SDWAN Leader 2020/2021/2022 (no Azure presence)

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (November 2021)



Fortinet is Co-Sell Ready Now - and in the Future

Fortinet- Fortigate Next Generation Firewall (with Solution Template)

Fortinet (Global)

FortiGate for Azure brings the security agility needed to support today's elastic cloud application workloads. FortiGate on Azure is based on the same FortiOS™ that runs over 3 million devices protecting leading Service Provider, Enterprise & Commercial customers. Backed by FortiGuard™, Fortinet's in-house threat research team, FortiGate on Azure is the solution that delivers industry leading next generation security protection to your cloud application & data.

Readiness: Co-Sell Prioritized

Total 12-mo Partner Revenue (Avg Azure Deal): 70000

GTM Offer Tier: CoSell Ready (FY17)

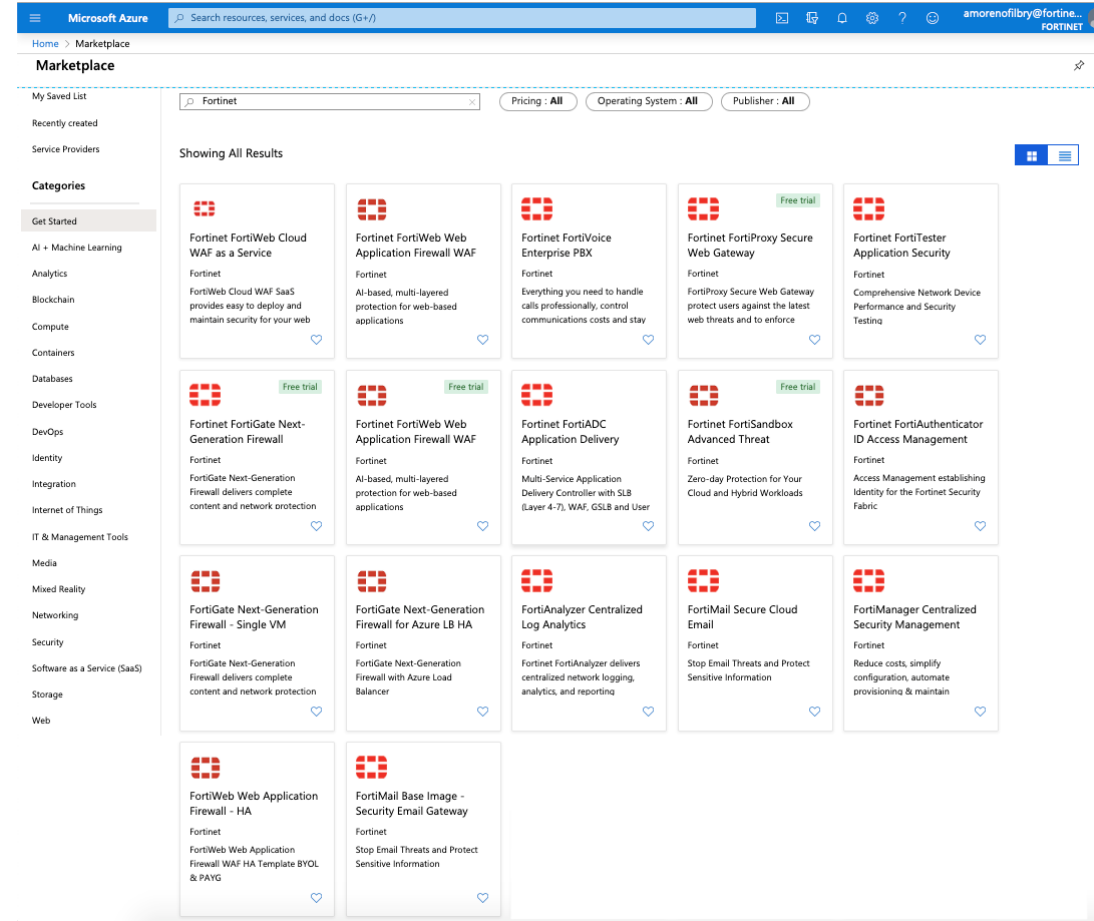
Azure License: Unbundled

Shared Opportunities: 430

Sourced Deals: 54 registered, 27 approved



- Solutions approved as Co-sell worldwide



Microsoft Security 20/20

W I N N E R

Microsoft Security Customer Impact

Fortinet



FORTINET®



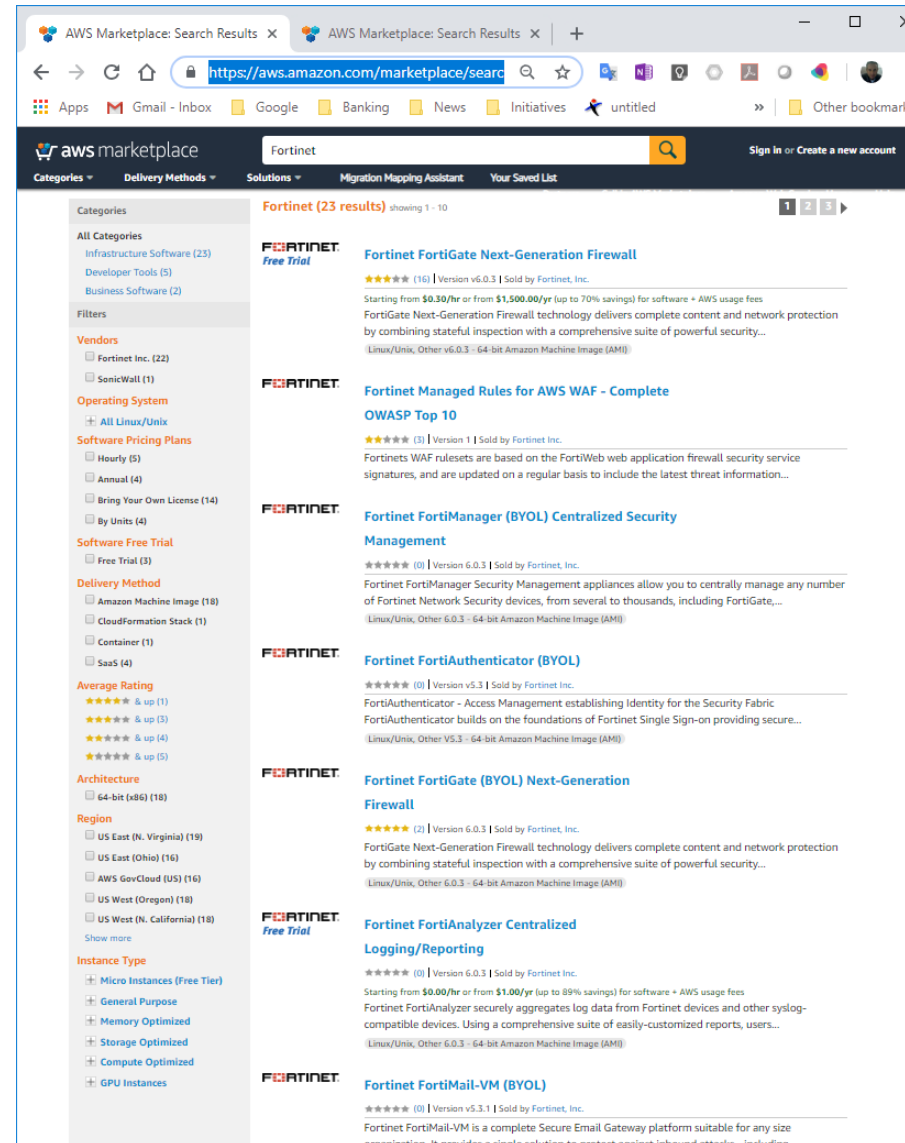
Winner Microsoft Partner of the Year - 2020

Azure
Commercial
Marketplace

https://aws.amazon.com/marketplace



- 35 Products in AWS Marketplace



Delivery Method

- ☐ Amazon Machine Image (18)
- ☐ CloudFormation Stack (1)
- ☐ Container (1)
- ☐ SaaS (4)

Fortinet GitHub (Cloud Templates)



fortinet-azure-solutions Public

A set of Azure Templates for getting you started in Azure with Fortinet solutions. This repository is a place for beta releases and work on the latest templates to be published on [github.com/fortin...](https://github.com/fortinet/azure-solutions)

● HCL ☆ 33 🔗 49

fortinet-aws-solutions Public

☆ 9 🔗 11

fortinet-gcp-solutions Public

GCP Deployment Manager templates for easy and automated deployments of various Fortigate architectures in Google Compute.

● Jinja ☆ 6 🔗 9

fortinet-oci-solutions Public

A set of OCI Terraform Templates for getting you started in Oracle with Fortinet solutions.

● HCL ☆ 4 🔗 5

<https://github.com/40net-cloud>

Top 4 - What should we consider a hot customer?

Uses Native Firewall / WAF

- We are much better than native
- More Economical

Exchange Online with plans <= E3

- Microsoft Defender P2 for EXO is included in E5
- [O365 License Suites](#)

On AWS (CNP)

- Only on AWS Marketplace
- Azure Security Posture is direct competition

Starts now their cloud journey

- Alignment with CAF and Landing Zones



Partner with Fortinet for Greater Trust & Opportunity



100% Channel

Fortinet is a 'Channel-Only' organization and has been for 20+ years.



Revenue Streams

Quickly unlock new revenue streams with Fortinet's breadth of products and free of charge training. Integrated into one platform, use tools to easily connect with adjacent technologies.



Market Leader

Fortinet is a Market Leader in 2 Gartner Magic Quadrants, represented in 4 more, and are recommended by IDC, Forrester, and Frost and Sullivan.



Trusted by Customers

Fortinet has been recognized as a 'Customers Choice' in the latest Gartner Peer Insights 'Voice of the Customer', achieving 4.8 out of 5.0, three years running.



FORTINET®