

FORTINET SMB SUMMIT

Security First on Cloud

Securing your Cloud assets with Fortinet and Lacework FortiCNAPP

Nov 7th 2024 | Athens, Greece



Konstantinos Diplas, IDEAL Technology Presales Security Engineer





Digital Innovation

is disrupting
all industries



Retail



Healthcare



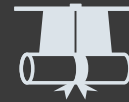
Finance



Manufacturing



Industrial



Higher Ed



Insurance



Consumer



Transport



Utilities



Government



Oil & Gas



Science



Auto



CSP

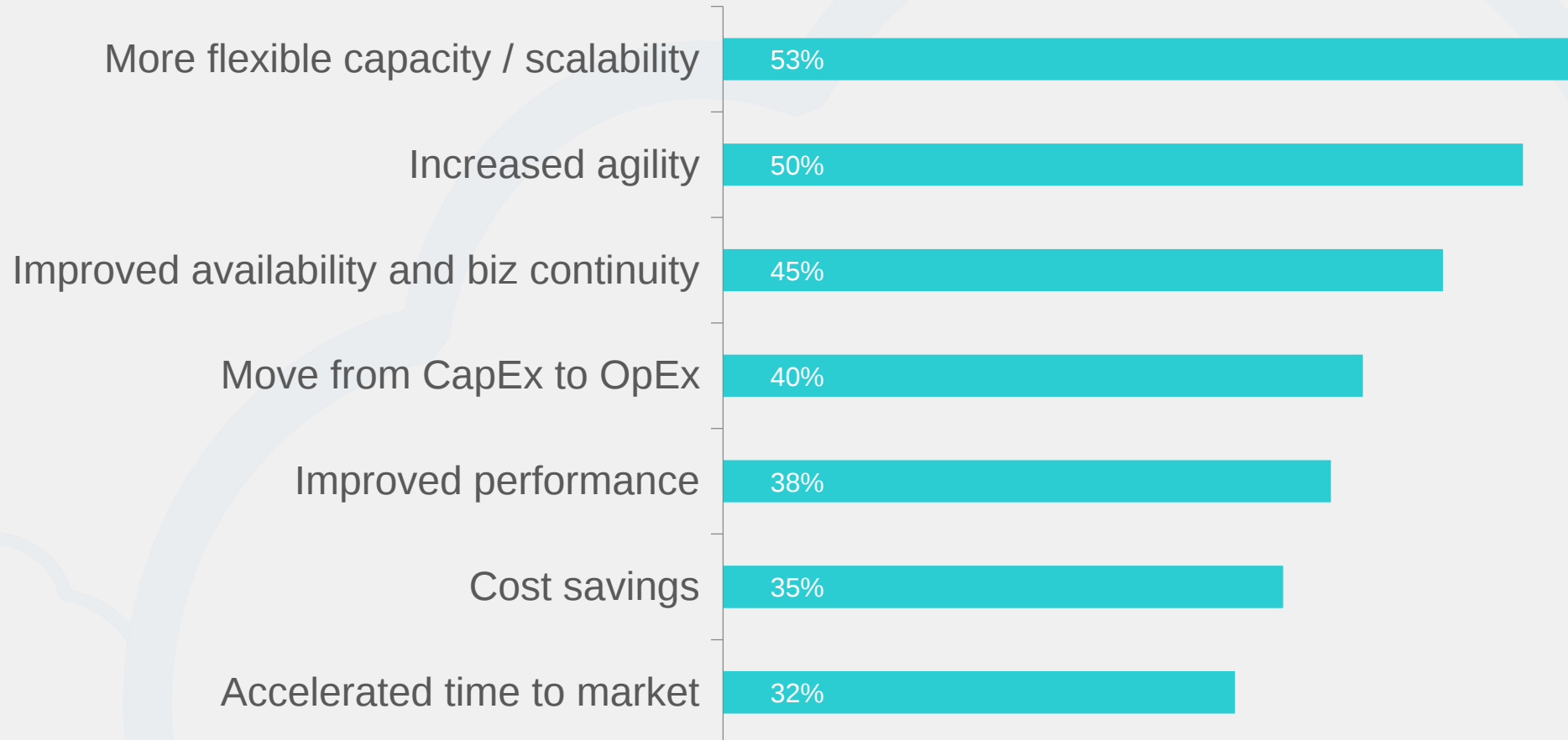


K12

Why are Customers Adopting Cloud?

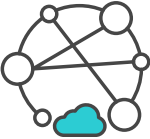
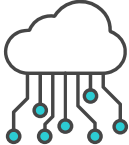
Key Business Drivers

Key benefits for moving to the Cloud

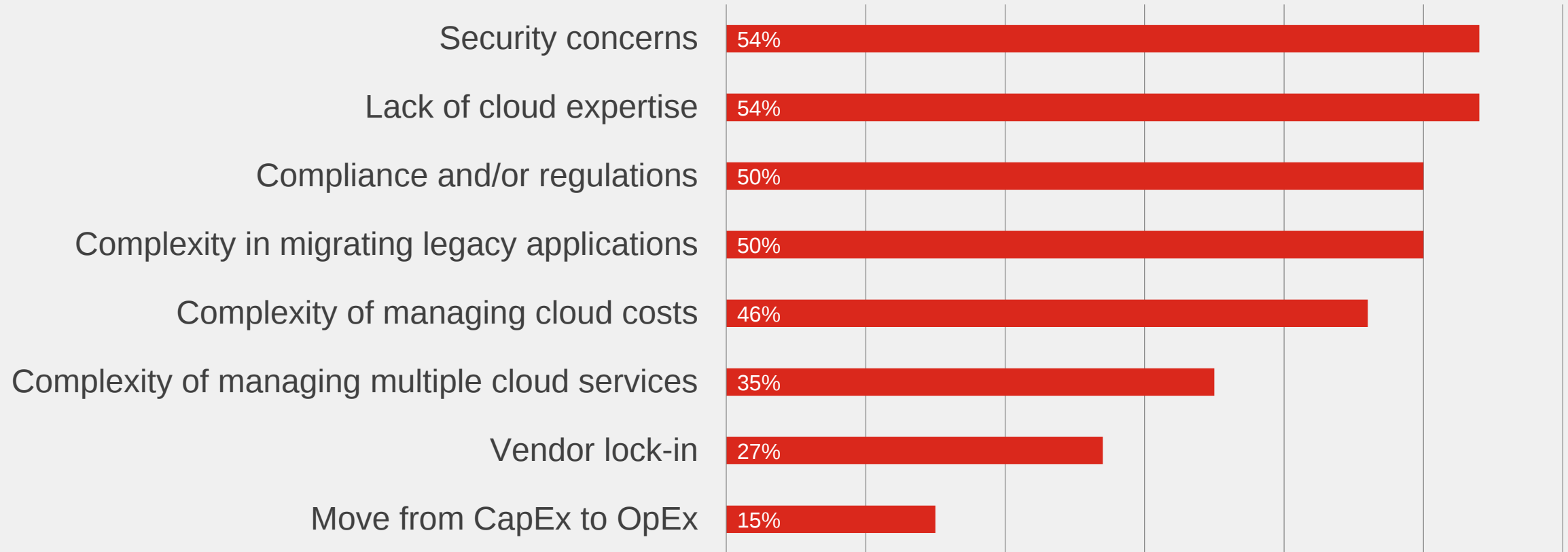




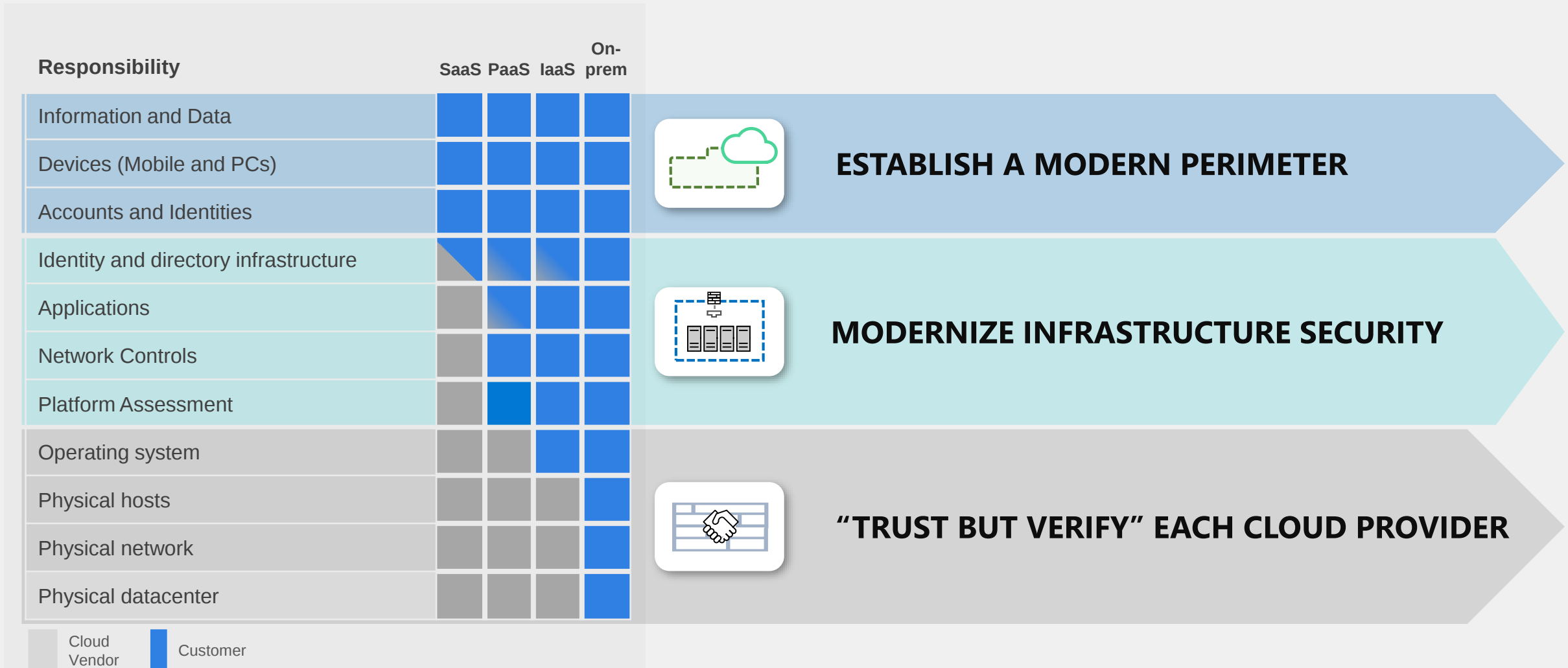
On Premise v Public Cloud

	 On-Premise	 Public Cloud
Perimeter	 CLEAR, DEFINED	 NONEXISTENT
Change	 SLOW, STATIC	 FAST, DYNAMIC
Infrastructure	 ENDPOINTS, PHYSICAL SERVERS	 APIs, MICROSERVICES
Security & Risk	 SOLE RESPONSIBILITY, SECURITY	 SHARED RESPONSIBILITY, DEVSECOPS
Access	 CONFINED TO LOGICAL NETWORK	 DECENTRALIZED FROM ANYWHERE

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®

Recognized As a Leader in the 2024 Gartner® Magic Quadrant™ for SD-WAN, 2022 Gartner Magic Quadrant for Network Firewalls, and in the 2024 Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure



2024 Gartner® Magic Quadrant™ for SD-WAN



2022 Gartner® Magic Quadrant™ for Network Firewalls



2024 Gartner® Magic Quadrant™ for Enterprise Wired and Wireless LAN Infrastructure



All Gartner recognitions here

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



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

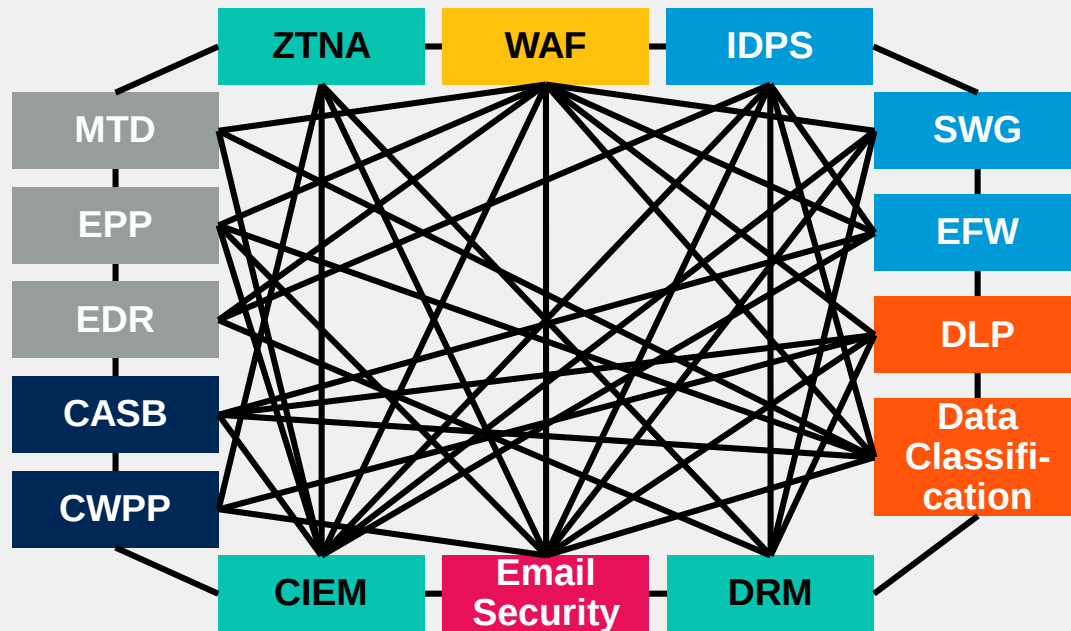


IBM Cloud



Overview: Gartner Cybersecurity Mesh Architecture

Gartner®



Executive Guide to Cybersecurity Mesh, 2022

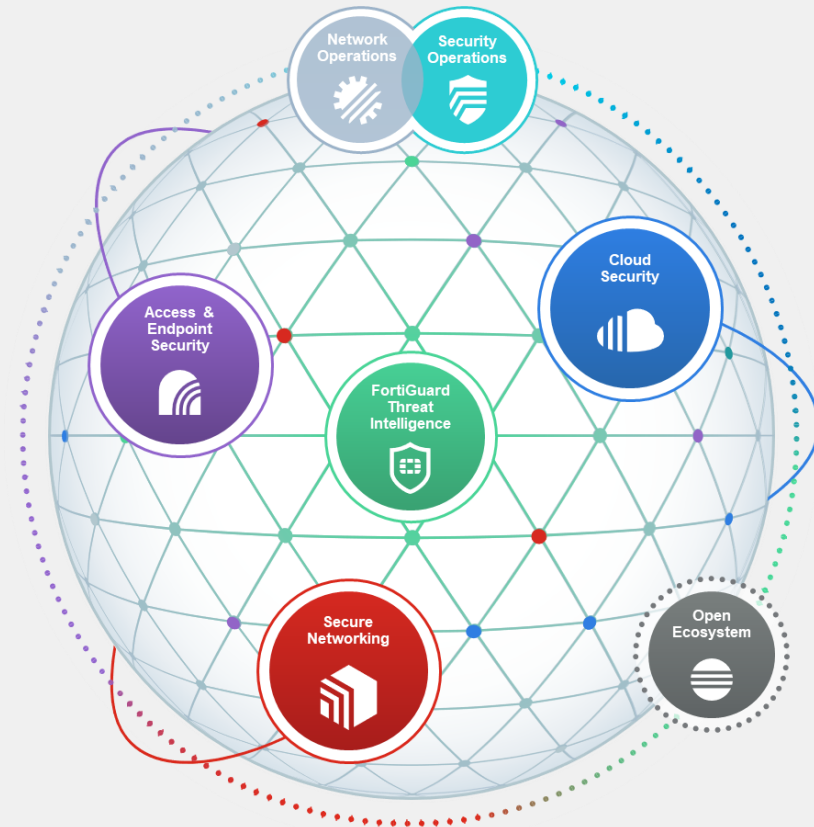
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

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 +1 Strategies – Securing Hybrid Cloud and Multicloud



Simplify and Strengthen Network Security by



Securing Connectivity



Protecting Perimeters

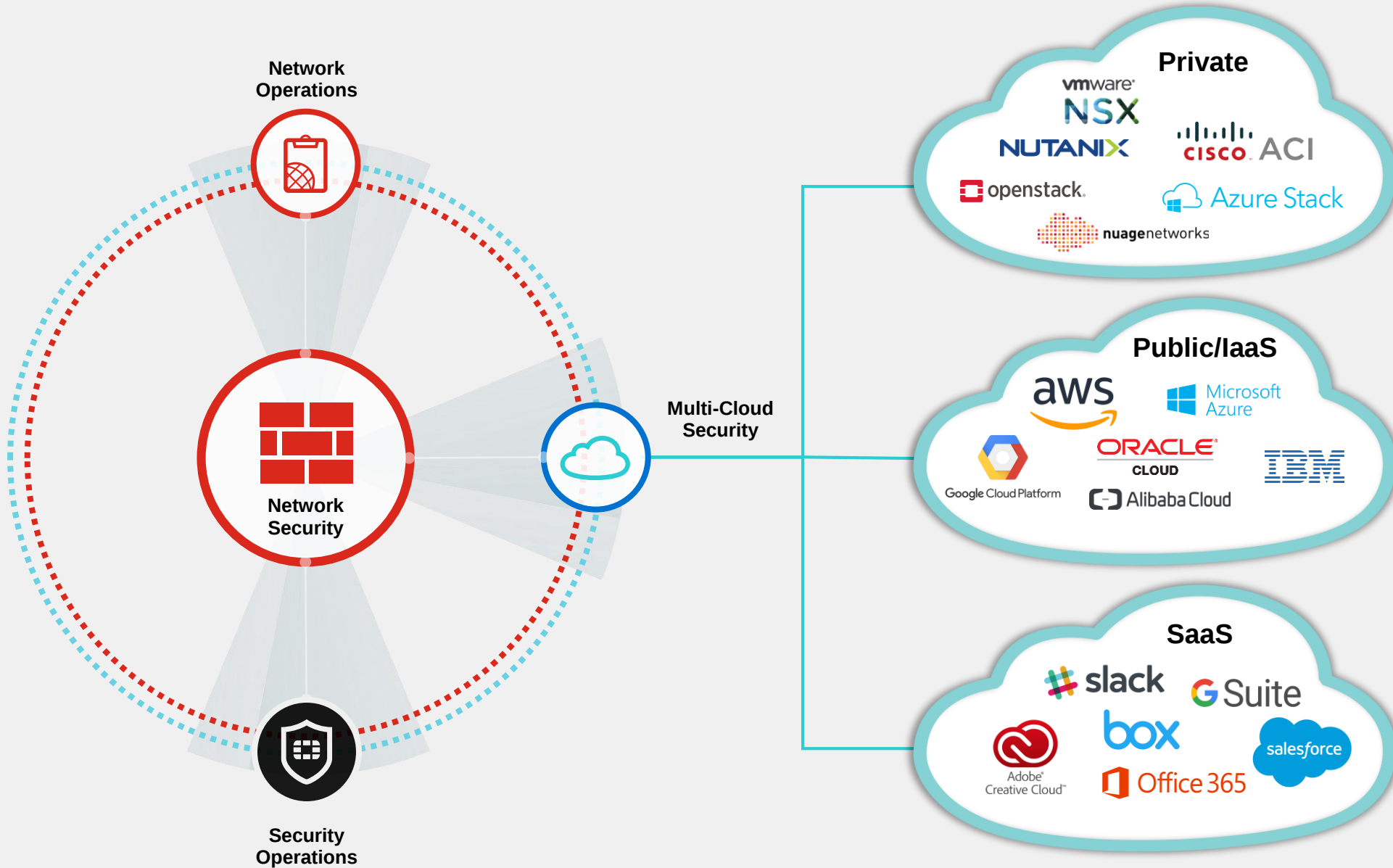


Centralizing Operations

Cloud Native Application Protection Platform



Fortinet Security Fabric - Cloud



Enable Reliable Connectivity with FortiGate NGFW



Reach cloud environments efficiently and securely

With FortiGate NGFW, organizations can facilitate excellent experiences via a fast SLA and secure connection with integrated SD-WAN.



Simplify and improve connections across distributed sites, Cloud workloads, and applications

Existing customers can easily transition to FortiGate NGFW and manage the migration with FortiManager

Azure Network Security Best Practices

Protect your workloads beyond native Azure security options

 Microsoft

Docs

Documentation

Learn

Q&A

Code Samples

Search

Sign in

Azure

Product documentation

Architecture

Learn Azure

Develop

Resources

Azure / Security / Fundamentals

Filter by title

Fundamentals Documentation

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.

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 that 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 at the time this article was written. Opinions and technical details are subject to change on a regular basis to reflect those changes.

Use strong network controls

You can connect [Azure virtual machines \(VMs\)](#) and [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.

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."

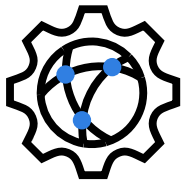
Download PDF

Enhance Security for Applications and APIs with FortiWeb



Enable communication between applications, e-commerce, and infrastructure with FortiWeb

Unlock new levels of reliability and scalability for customer-facing solutions on the Cloud. Leverage Fortinet's built in AI/ML for enhanced security.



Machine Learning for Anomaly Detection

Machine Learning-based anomaly detection learns how your users interact with your application, delivering both improved threat detection and reducing the false positives that drive administrative overhead.

Your castle: Your critical infrastructure

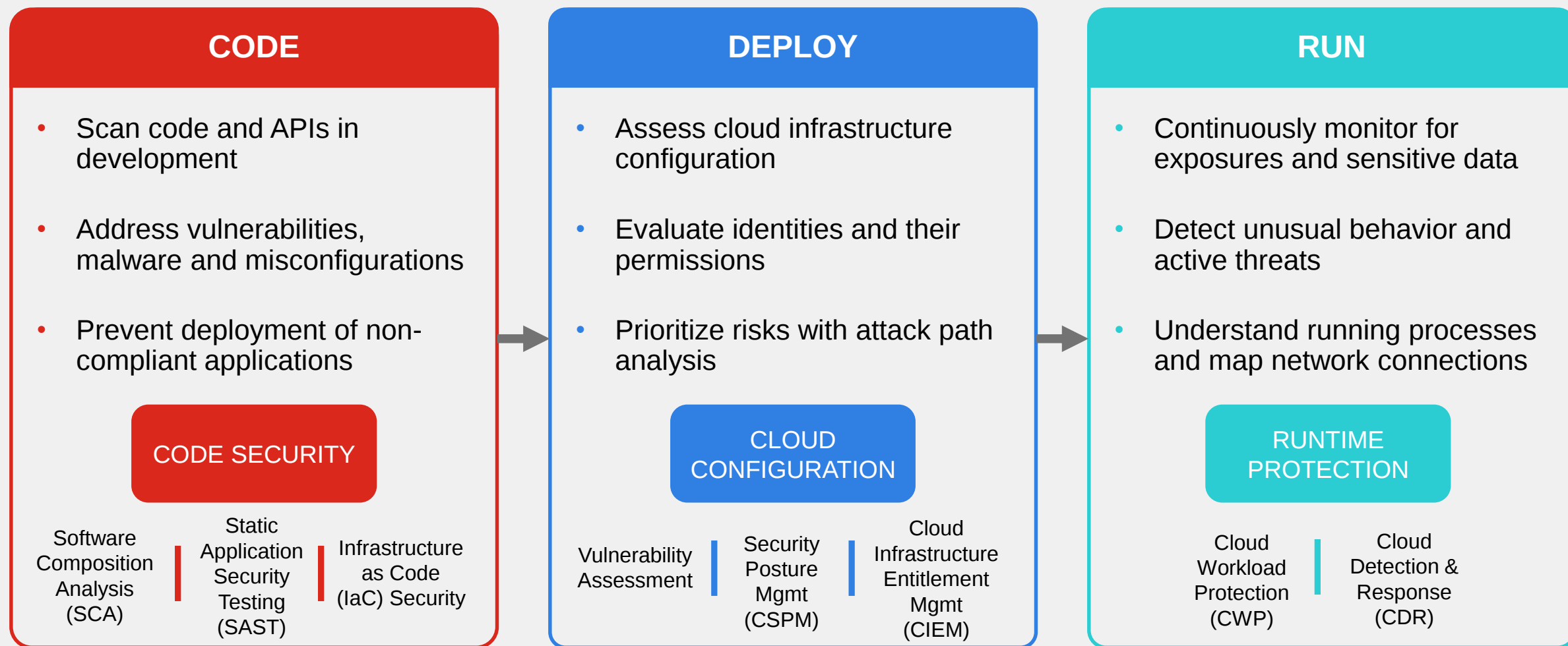
Gartner predicts that by 2029, “**60%** of enterprises that do not deploy a unified CNAPP solution within their cloud architecture **will lack extensive visibility into the cloud attack surface and consequently fail to achieve their desired zero-trust goals.**”

Read Insights from Gartner® on CNAPPs



Lacework FortiCNAPP – Cloud Native Application Security Platform

A unified platform for code-to-cloud security





Fortinet + Lacework FortiCNAPP

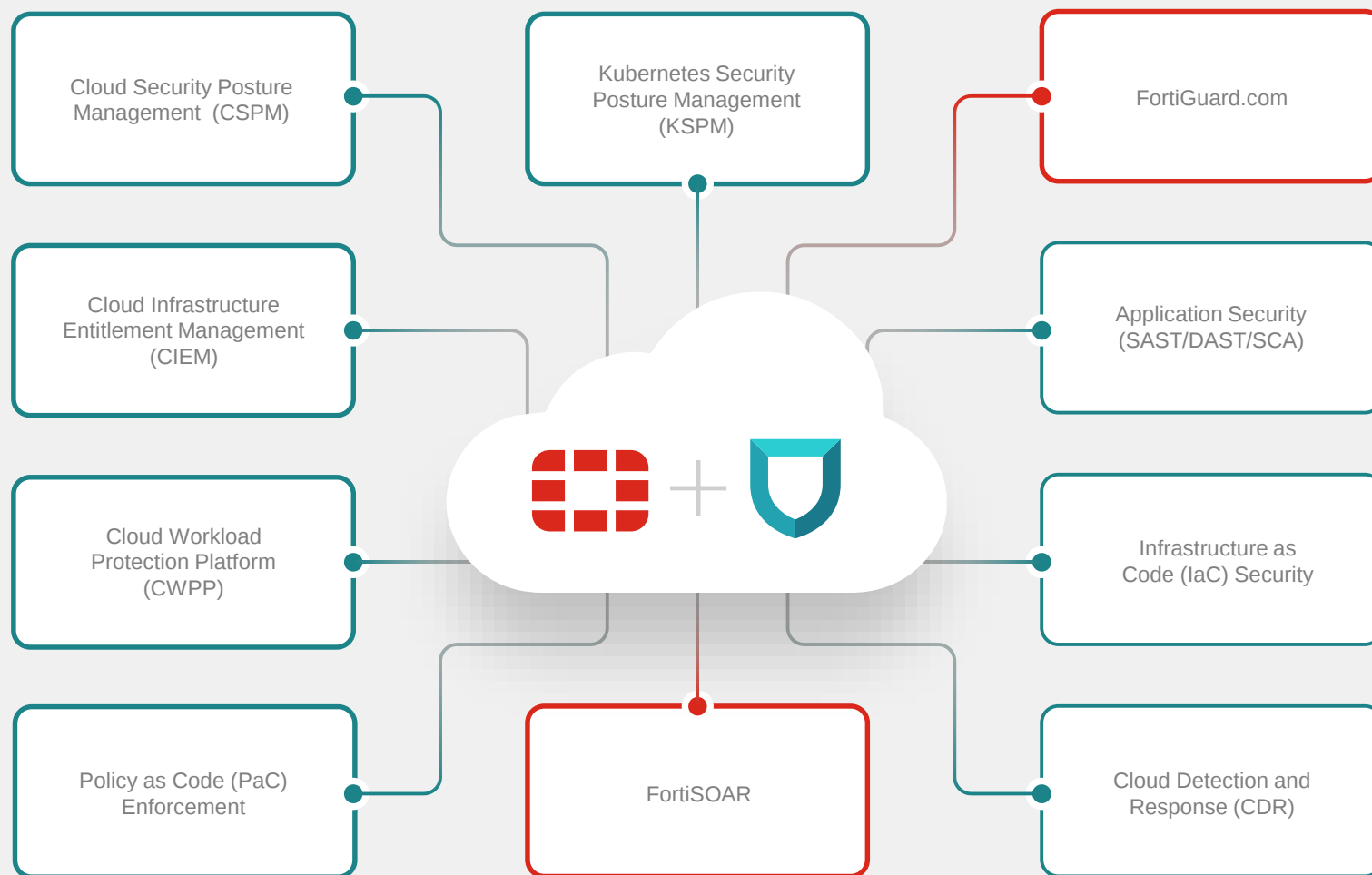
The Most Complete AI-driven Cloud-Native Application Protection Platform



Single vendor for all cloud security and secure CI/CD application development needs.

See AND protect everything from coding, deploying, and running applications across hybrid and multi-clouds.

Simplify security with AI-driven platforms from both Lacework FortiCNAPP and Fortinet.



Marketplaces: Product and Solution Availability

aws	PAYG	BYOL
AWS WAF Rules	✓	
FortiCNP	✓	
FortiGate-VM*	✓	✓
FortiGate CNF	✓	
FortiManager-VM*	✓	✓
FortiAnalyzer-VM*	✓	✓
FortiWeb-VM*	✓	✓
FortiWeb Cloud	✓	
FortiEDR		
FortiMail-VM		✓
FortiAuthenticator-VM		✓
FortiADC-VM*	✓	✓
FortiVoice-VM		✓
FortiRecorder-VM	✓	
FortiSandbox-VM	✓	✓
FortiSIEM-VM		✓
FortiNDR		
FortiProxy-VM		✓
FortiSOAR		✓
Zero Trust App Gateway		✓
FortiTester		✓
FortiPortal		✓
Cloud Consulting Services	✓	
FortiFlex program	✓	
FortiPoints program	✓	

A	PAYG	BYOL
WAF Rules		
FortiCNP		
FortiGate-VM*	✓	✓
FortiGate CNF		
FortiManager-VM*		✓
FortiAnalyzer-VM*		✓
FortiWeb-VM*	✓	✓
FortiWeb Cloud	✓	
FortiEDR		
FortiMail-VM		✓
FortiAuthenticator-VM		✓
FortiADC-VM*	✓	✓
FortiVoice-VM		✓
FortiRecorder-VM		✓
FortiSandbox-VM	✓	✓
FortiSIEM-VM		✓
FortiNDR		
FortiProxy-VM		✓
FortiGate for Azure vWAN		✓
Zero Trust Gateway		✓
FortiPAM		✓
FortiTester		✓
FortiPortal		✓
Cloud Consulting Services		
FortiFlex program	✓	

Google Cloud	PAYG	BYOL
WAF Rules		
FortiCNP		
FortiGate-VM*	✓	✓
FortiGate CNF		
FortiManager-VM*		✓
FortiAnalyzer-VM*		✓
FortiWeb-VM*	✓	✓
FortiWeb Cloud	✓	
FortiEDR	✓	
FortiMail-VM		✓
FortiAuthenticator-VM		
FortiADC-VM*	✓	✓
FortiVoice-VM		
FortiRecorder-VM		
FortiSandbox-VM		✓
FortiSIEM-VM		
FortiNDR		
FortiProxy-VM		
FortiDevSec	✓	
FortiCASB		✓
Cloud Consulting Services		
FortiFlex program	✓	
FortiPoints program	✓	

ORACLE CLOUD	PAYG	BYOL
WAF Rules		
FortiCNP		
FortiGate-VM*	✓	✓
FortiGate CNF		
FortiManager-VM*		✓
FortiAnalyzer-VM*		✓
FortiWeb-VM*		✓
FortiWeb Cloud		✓
FortiEDR		
FortiMail-VM		✓
FortiAuthenticator-VM		✓
FortiADC-VM*		✓
FortiVoice-VM		
FortiRecorder-VM		
FortiSandbox-VM		✓
FortiSIEM-VM		
FortiNDR		
FortiProxy-VM		
Zero Trust App Gateway		
Cloud Consulting Services		
FortiFlex program	✓	

Licensing \ Fortinet Cloud Consumption Models

Flexible procurement options to fit customer needs

Marketplace Transactable				
	BYOL (Bring Your Own License)	PAYGO (Pay As You Go)	FortiFlex (Points-based, similar to EA)	Private Offers (Custom Contracts)
Who it's for?	Pre-existing customers who already own their licenses and want to run solutions in the cloud	Ideal for development and testing, temporary projects, or workloads with inconsistent traffic	Ideal for dynamic environments where flexibility in consumption is desired	Ideal for high-value or complex transactions where custom terms and pricing are desired
Use Case	Customers use existing product licenses they bought through channel but pay for cloud infrastructure to run the product in the cloud.	Customer pays for software and compute capacity by the hour with no long-term commitments. Annualized contracts available at a discounted rate	Customers buy points that provide the flexibility for customers to scale their solutions up or down, in or out as needed without extra procurement.	Customers negotiate a custom price with Fortinet for guaranteed consumption volume or term length for listings we offer in through cloud marketplaces
License Portability	Licenses can be used on any cloud	Usable only on the cloud where subscribed	Licenses can be used on any cloud	Usable only on the cloud where subscribed, unless FortiFlex

Key Takeaways

 Security – A Holistic Approach	 What MSFT and 3rd party analyst have to Say?
 +  = Better Together	 More Economical, and options to “count” towards Cloud commitment



FORTINET®

Contact us
security@ideal.gr