Securing your Cloud assets with Fortinet and Lacework FortiCNAPP

George Armeniakos
Cloud Business Development Manager - GRHUCY

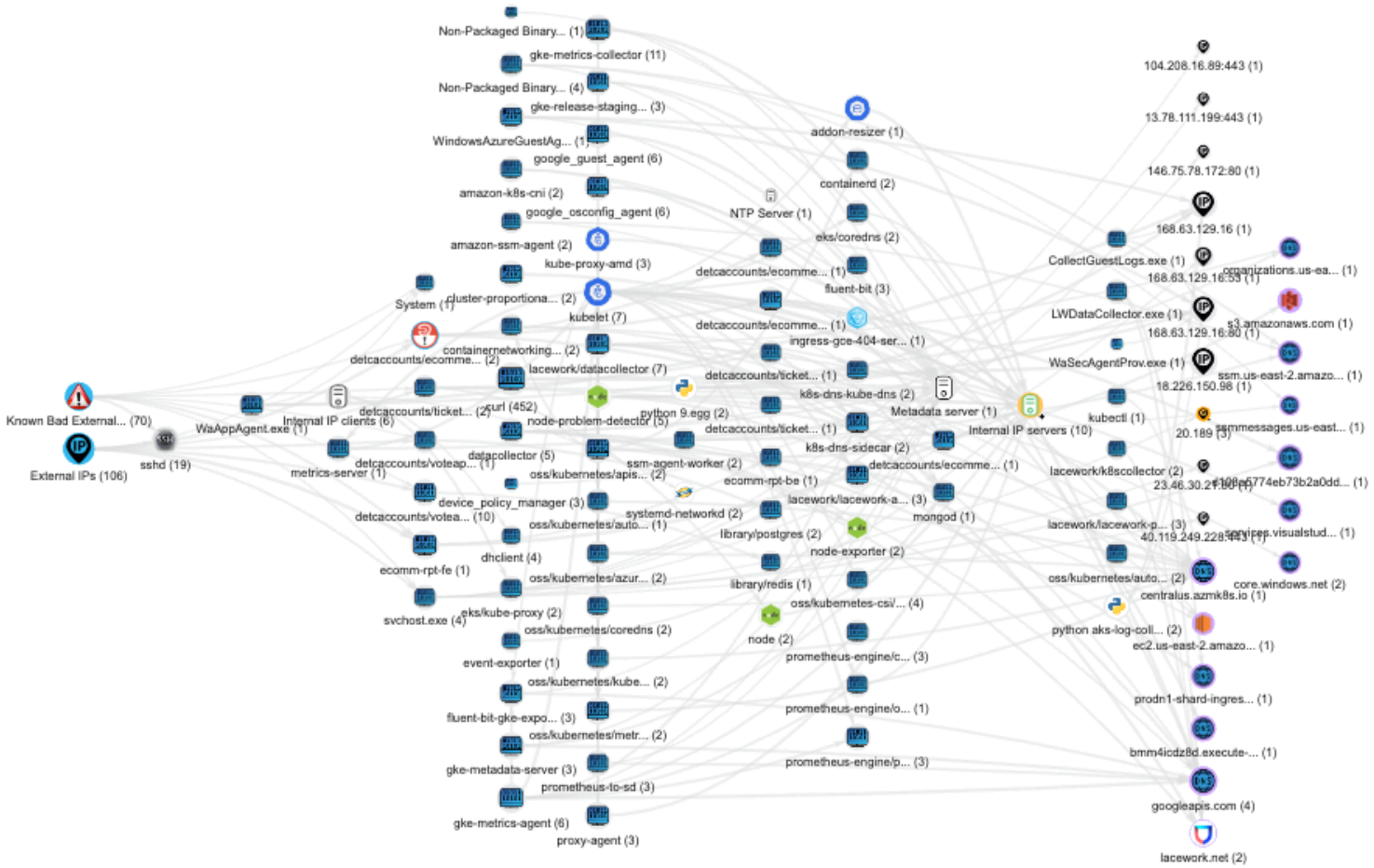
On Premise vs Public Cloud

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

A Simple Cloud Deployment is Very Complex

Cloud is Complex

- 200+ cloud services (AWS only)
- Hundreds of sensitive actions available
- Unlimited public IP space
- Services available to non-expert developers



Fortinet Security Fabric

Broad

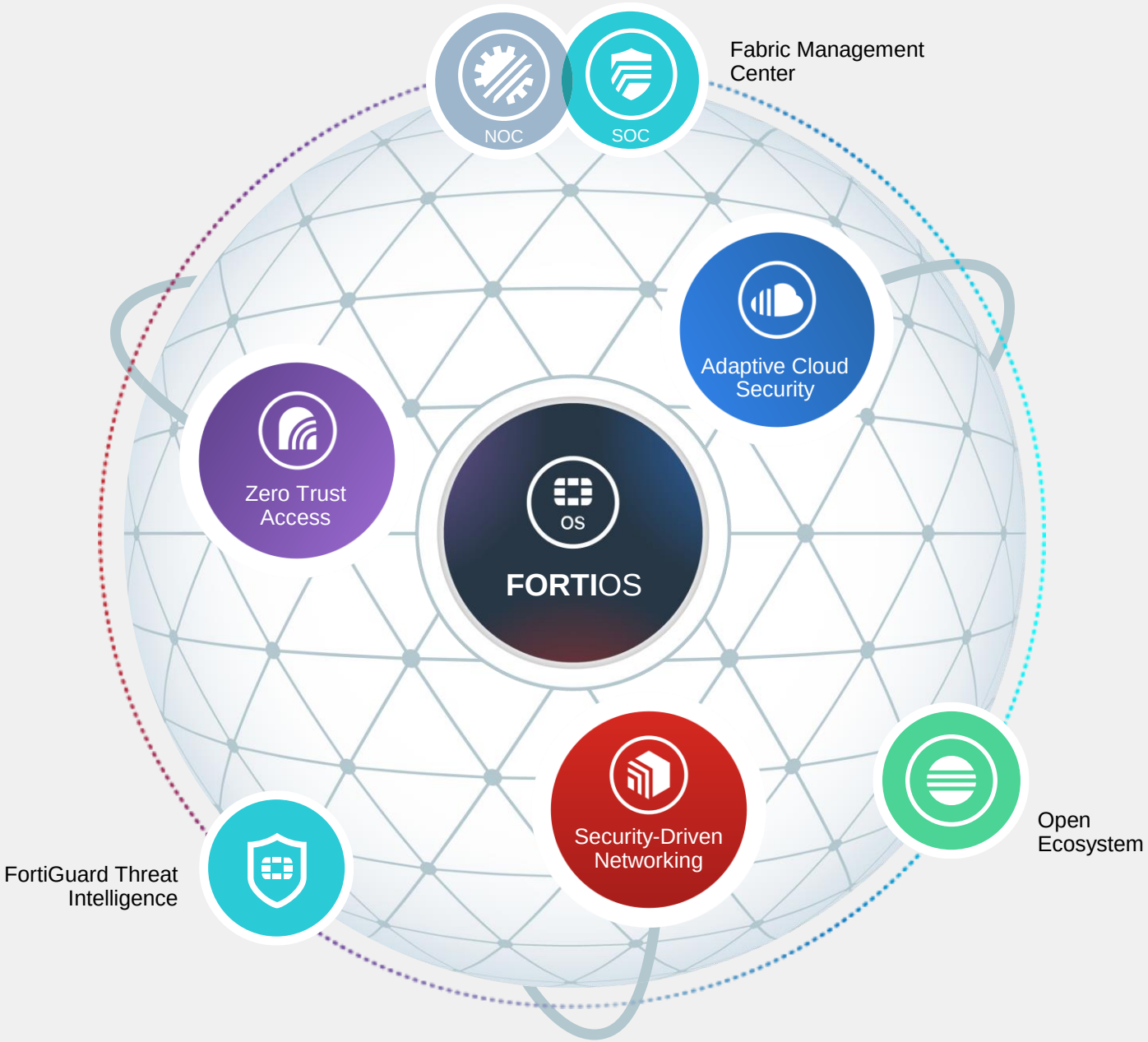
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

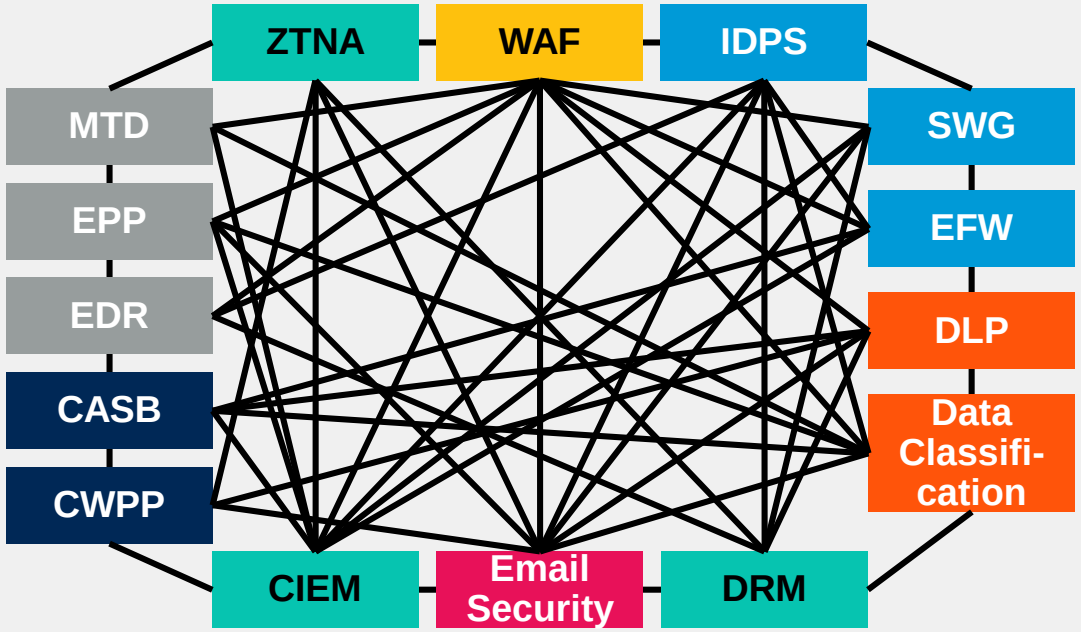
Automated

self-healing networks with AI-driven security for fast and efficient operations



Overview: Gartner Cybersecurity Mesh Architecture

Gartner®



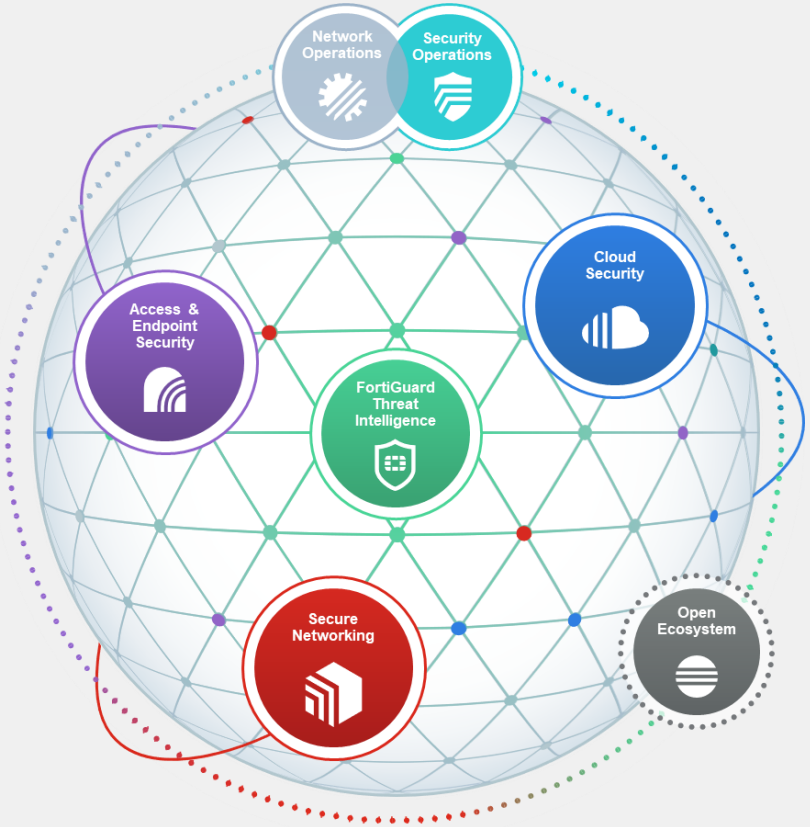
Executive Guide to Cybersecurity Mesh, 2022

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®



The Broadest Platform in Cybersecurity

Secure Networking

FortiGate
NGFW with ASIC acceleration and industry leading Convergence

FortiAP
Protected Wi-Fi connectivity via Secure Networking convergence with FortiGate

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiGate Cloud
SaaS platform offering zero-touch deployment, network management and security analytics

FortiAIOps
AI based insights for rapid analysis and remediation of network issues

FortiVoice
Unified communications with secure voice, chat, conferencing, and fax

FortiRecorder
Secure NVR with smart AI analysis and centralized visibility

FGaaS
Hardware as a service for FortiGate

FortiSwitch
Protected Ethernet connectivity via Secure Networking convergence with FortiGate

FortiManager
Centralized management of your Fortinet security infrastructure

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiEdge Cloud
Cloud management for standalone LAN, WLAN and 5G gateway equipment

FortiFone
Robust IP phones and softclient to stay connected from anywhere

FortiCamera
Physical security with intelligent motion detection in any light condition

FortiConverter
Secure and automated firewall migration from a broad spectrum of vendors

Unified SASE

SASE

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

FortiClient ZTA Agent
Remote access, application access, and risk reduction

FortiProxy
Enforce internet compliance and granular application control

FortiCASB
Prevent misconfigurations of SaaS apps and meet compliance

FortiClient EPP Agent
Endpoint Protection Agent with AV, URL and Sand-box

FortiSASE
Cloud-delivered Security Services Edge

FortiMonitor
SaaS based DEM platform, performance monitoring

CLOUD

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

FortiWeb
Prevent web application attacks against critical web assets

FortiGSLB
Ensure business continuity during unexpected network downtime

FortiFlex
Flexible daily usage-based consumption licensing for a broad catalog of solution

FortiGate CNF
Hosted cloud-native firewall for simplified cloud network security

FortiADC
Application-aware intelligence for distribution of application traffic

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

FortiPoints
Simplified, flexible licensing for annual contracts, renewals, upgrades, and co-terms

Security Operations

FortiAnalyzer
Security Fabric log management, monitoring and response

FortiSIEM
Enterprise-wide monitoring, threat detection, and response

FortiEDR/XDR
Automated endpoint protection and correlated incident response

FortiSOAR
Automated security operations, investigation, and response

FortiNDR
AI-driven analysis to detect and respond to threats

SOCaaS
Continuous security monitoring, incident triage, and escalation

IR Services
Rapid detection, containment, and recovery of cyberattacks

FortiDeceptor
Active deception platform for early in-network attack detection and response

FortiTrust Identity
Identity and Access Management as a Service (IDaaS)

FortiGuest
Access management solution for temporary access to guests and visitors

FortiCNAPP
Secure code to cloud with a single, data-driven platform

FortiNextDLP
Endpoint DLP and Insider Risk management

FortiMail
AI-powered, protection against email-borne threats

FortiSandbox
AI-powered real-time protection against unknown and 0-day threats

FortiToken
Cloud/HW/Mobile MFA provide passwordless adaptive authentication

FortiAuthenticator
Centralized identity and access management solution

FortiGuard MDR Service
Managed threat detection, investigation, and response

FortiRecon
Proactive digital risk protection service and external/internal threat monitoring

FortiPAM
Privileged identity and access management, and session monitoring

FortiTester
Network performance testing and breach attack simulation (BAS)

FortiDevSec
Orchestrated and automated continuous application security testing

FortiDAST
Automated black-box dynamic application security testing

FortiScanner Cloud
Cyber Asset Attack Surface Management Service

FortiAI
Integrated GenAI Assist for SOC and NOC

OT Security Platform

OT Security Service
FortiGuard subscription for FortiGate NGFW enables protection against OT-specific threats

Ruggedized Products
Rugged NGFW, switch, AP, and 5G extenders provide secure connectivity in harsh outdoor environments

FortiSRA
Agentless secure remote access offers robust remote access control, management, session logging, monitoring, and recording

SecOps for OT
Advanced cybersecurity controls bring OT networks into the SOC and incident response plans

Open Ecosystem

FNDN
Advanced tools for Fortinet community to develop custom solutions

Fabric Connectors
Fortinet-developed integrations for automation and security

Fabric API
Partner-developed integrations for end-to-end visibility and protection

DevOps Tools
Community-driven scripts automate network/security tasks

Extended Ecosystem
Integrates with third-party systems and orgs for sharing threat-intel

Resources

Product Matrix
Specifications for top selling models

Free Training
Fortinet is committed to training over 1 million people by 2025

FortiOS
The Heart of the Fortinet Security Fabric

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

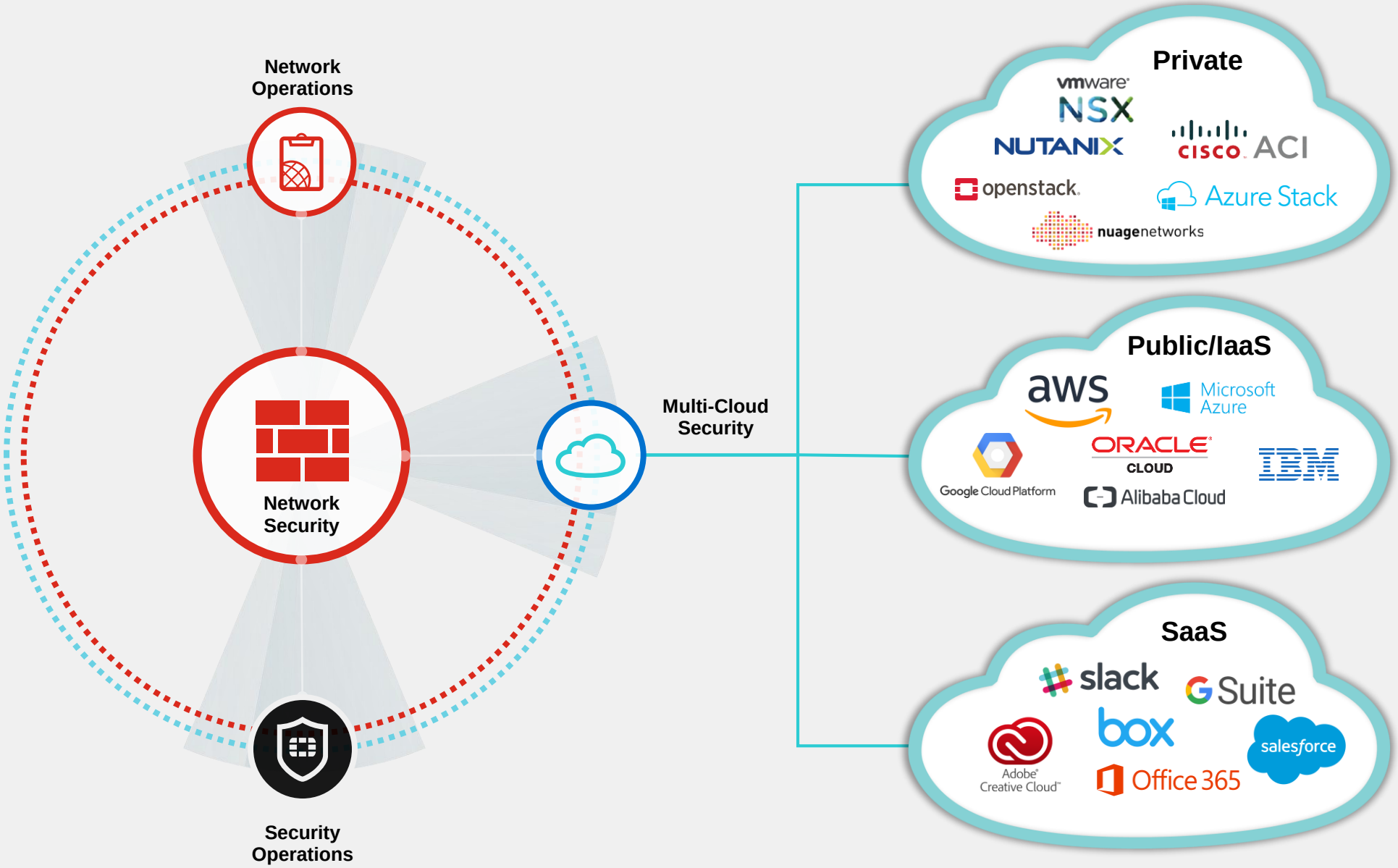
Free Assessment
Perform an assessment in your network to validate your existing controls

FortiCare
Support and mitigation services

AI-Powered FortiGuard Security

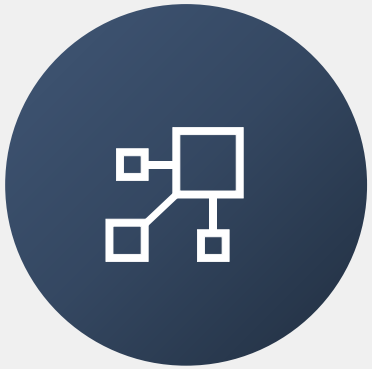
- Web Filtering
- IPS
- AV
- Sandbox
- IL MPS
- Application Control
- Attack Surface
- DLP
- OT Security Services
- IoC
- IL CASB

Private Security Fabric - Cloud



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

Enable Reliable Connectivity with FortiGate NGFW

Reach cloud environments efficiently and securely

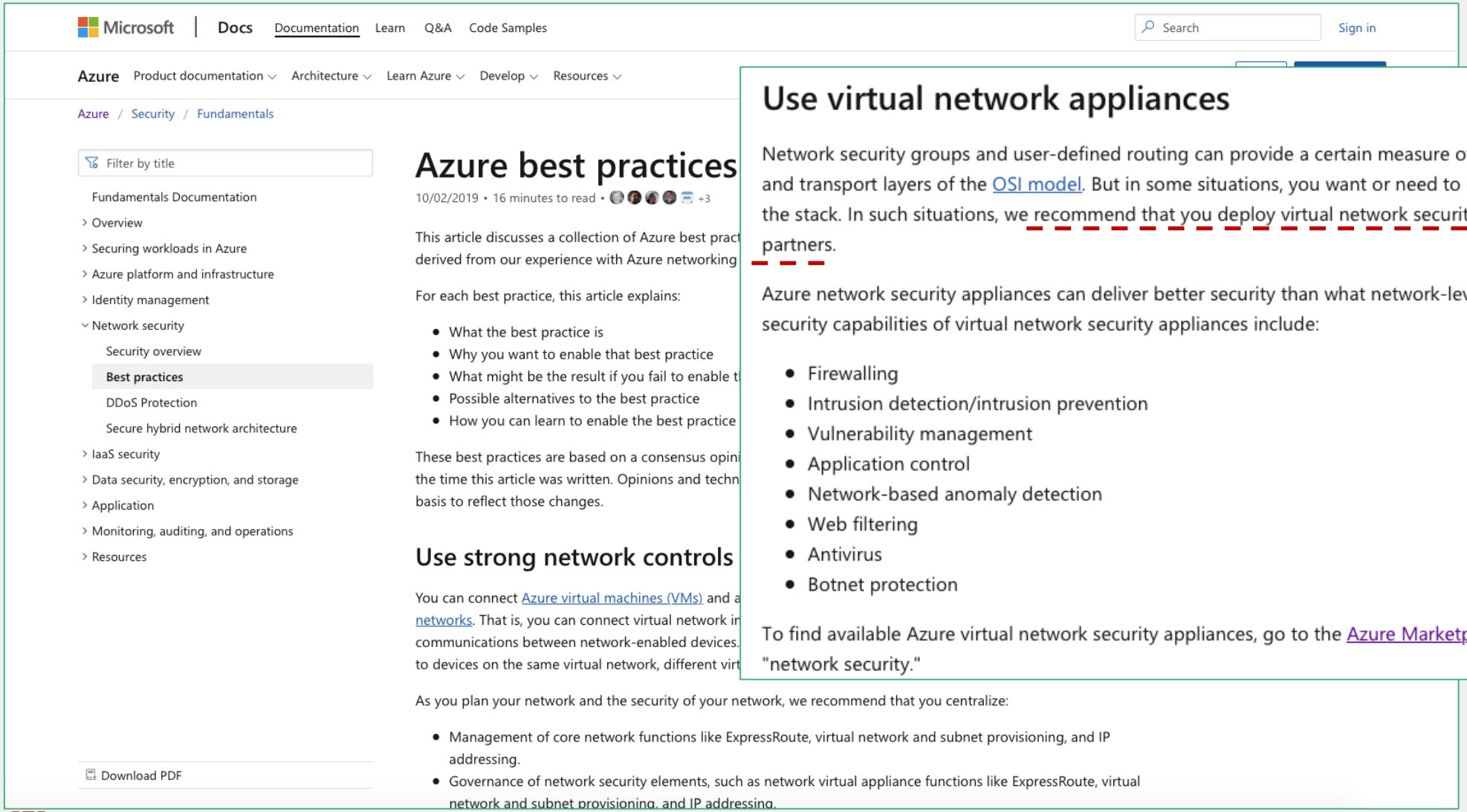
With FortiGate NGFW, organizations can facilitate excellent experiences via a fast SLA and secure connection with integrated SD-WAN.

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



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.

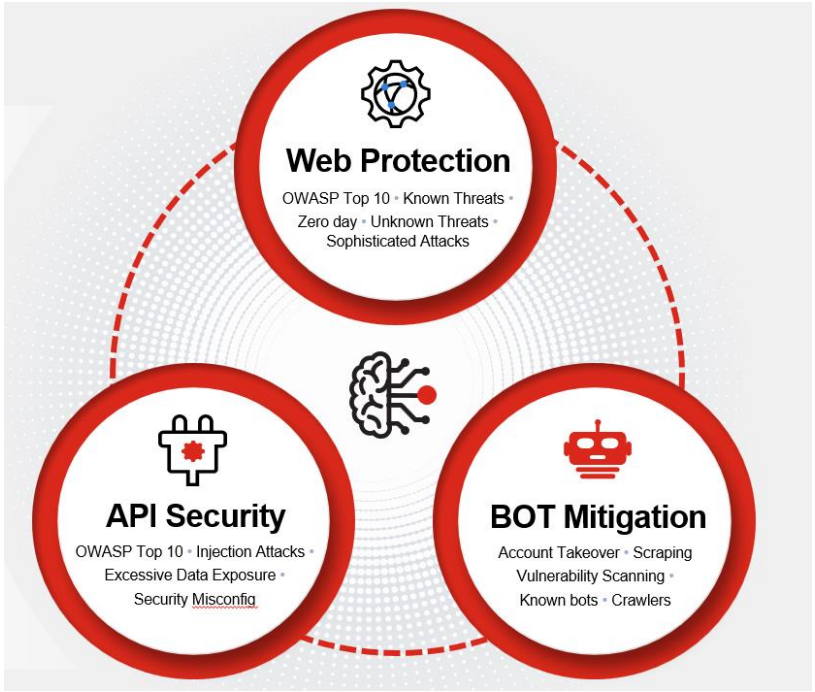
Azure network security appliances can deliver better security than what network-level controls provide. Network security capabilities of virtual network security appliances include:

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

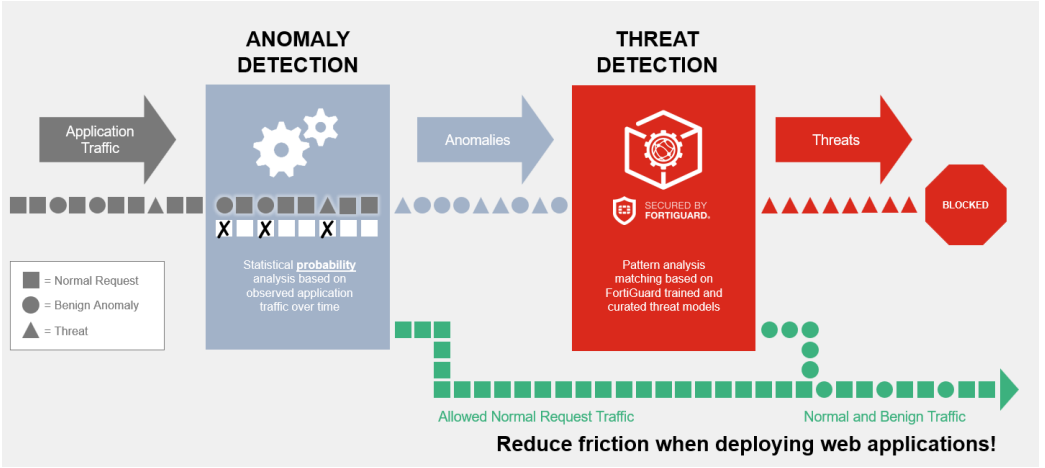
To find available Azure virtual network security appliances, go to the Azure Marketplace and search for "security" and "network security."

https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices

Enhance Security for Applications and APIs with FortiWeb



Machine Learning for Anomaly Detection



Open Web Application Security Project - Top 10

What is Azure Web Application Firewall on Azure Application Gateway?

Article • 01/26/2024 • 15 contributors

Feedback

In this article

- Benefits
- Features
- WAF policy and rules
- Application Gateway WAF SKU pricing

Show 2 more

The Azure Web Application Firewall (WAF) on Azure Application Gateway actively safeguards your web applications against common exploits and vulnerabilities. As web applications become more frequent targets for malicious attacks, these attacks often exploit well-known vulnerabilities such as SQL injection and cross-site scripting.

WAF on Application Gateway is based on the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP).

All of the following WAF features exist inside of a WAF policy. You can create multiple policies, and they can be associated with an Application Gateway, to individual listeners, or to path-based routing rules on

Training

Module

Introduction to Azure We
Training

Describe how Azure Web
Azure web applications fr
including its features, how

Certification

Microsoft Certified: Azur
Certifications

Demonstrate foundationa
concepts, core Azure serv
and governance features

Documentation

Web Application Firewall

Learn about Web Applicat
deployed with Applicatio

Create Web Application F
Application Gateway

Learn how to create Web
for Application Gateway.

Tune Azure Web Application Firewall f Azure Front Door

Article • 07/26/2023 • 14 contributors

Fee

Select the Azure Front Door tier:

Standard/Premium | Classic

In this article

- Understand WAF logs
- Resolve false positives
- Find request fields
- Anomaly scoring rule
- Next steps

The Microsoft-managed default rule set is based on the OWASP Core Rule Set and includes Microsoft

Training

Describe how Azure We
Azure web applications
including its features, ho

Certification

Microsoft Certified: Azu
Certifications

Demonstrate foundatio
concepts, core Azure se
and governance feature

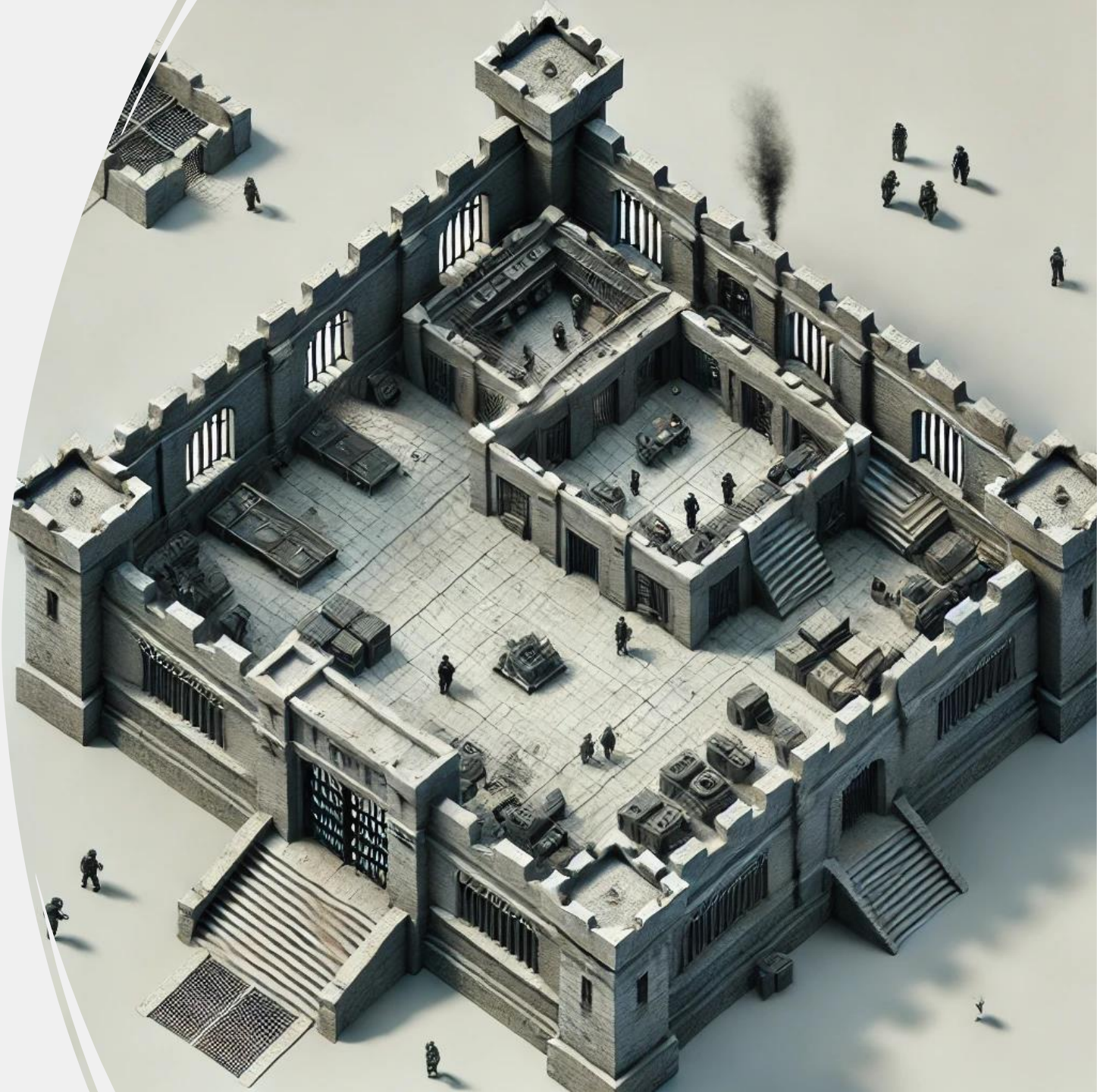
Documentation

Azure Web Application
rules

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



You can't Secure

What you can't See

Cloud-Native Application Protection Platform (CNAPP)

A single platform that secures the entire cloud-native application lifecycle

CODE

- Scan code and APIs in development
- Address vulnerabilities, malware and misconfigurations
- Prevent deployment of non-compliant applications

DEPLOY

- Assess cloud infrastructure configuration
- Evaluate identities and their permissions
- Prioritize risks with attack path analysis

RUN

- Continuously monitor for exposures and sensitive data
- Detect unusual behavior and active threats
- Understand running processes and map network connections

Lacework FortiCNAPP Core Capabilities

A unified platform for code-to-cloud security

CODE

- Scan code and APIs in development
- Address vulnerabilities, malware and misconfigurations
- Prevent deployment of non-compliant applications

CODE SECURITY

Software Composition Analysis (SCA) | Static Application Security Testing (SAST) | Infrastructure as Code (IaC) Security

DEPLOY

- Assess cloud infrastructure configuration
- Evaluate identities and their permissions
- Prioritize risks with attack path analysis

CLOUD CONFIGURATION

Vulnerability Assessment | Security Posture Mgmt (CSPM) | Cloud Infrastructure Entitlement Mgmt (CIEM)

RUN

- Continuously monitor for exposures and sensitive data
- Detect unusual behavior and active threats
- Understand running processes and map network connections

RUNTIME PROTECTION

Cloud Workload Protection (CWP) | Cloud Detection & Response (CDR)


LACEWORK
Hosts
Applications
Files
Machines
Networks
Processes
Users
DISCOVERY
Dashboard
Resource Explorer
THREAT CENTER
Alerts
Cloud logs
Workloads
RISK CENTER
Attack path
Compliance
Identities
Vulnerabilities
Code security
GOVERNANCE
Policies
Frameworks
Reports
Agents
Help
Settings
All filters
Apr 22 05:00 pm - Apr 23 05:00 am (+01:00)
Application
Container
External Hostname
File Hash
File Path
Hostname
IPV4 Address
Port
Machine Tags
Username
Instance ID
Pod Namespace
Pod Name
Pod Type
Pod IP Address
Show more
Reset
Polygraphs
Application communication
Application launch
Insider behavior
vote app
ZOOM
DIFF
Known Bad External... (97)
External IPs (43)
detcaccounts/voteap... (1)
detcaccounts/votea... (10)
library/postgres (3)
library/redis (1)
05 PM
Mon 22 April
06 PM
07 PM
08 PM
09 PM
10 PM
11 PM
12 AM
Tue 23 April
01 AM
02 AM
03 AM
04 AM
*All times local
List of applications
1 - 50 of 125
Application
Machines
Users
amazon-k8s-cni
2
1
containerd
7
1
Active listening ports
1 - 50 of 96
Port number
Machines
Applications
Protocol
111
2
1
UDP
9001
2
4
TCP

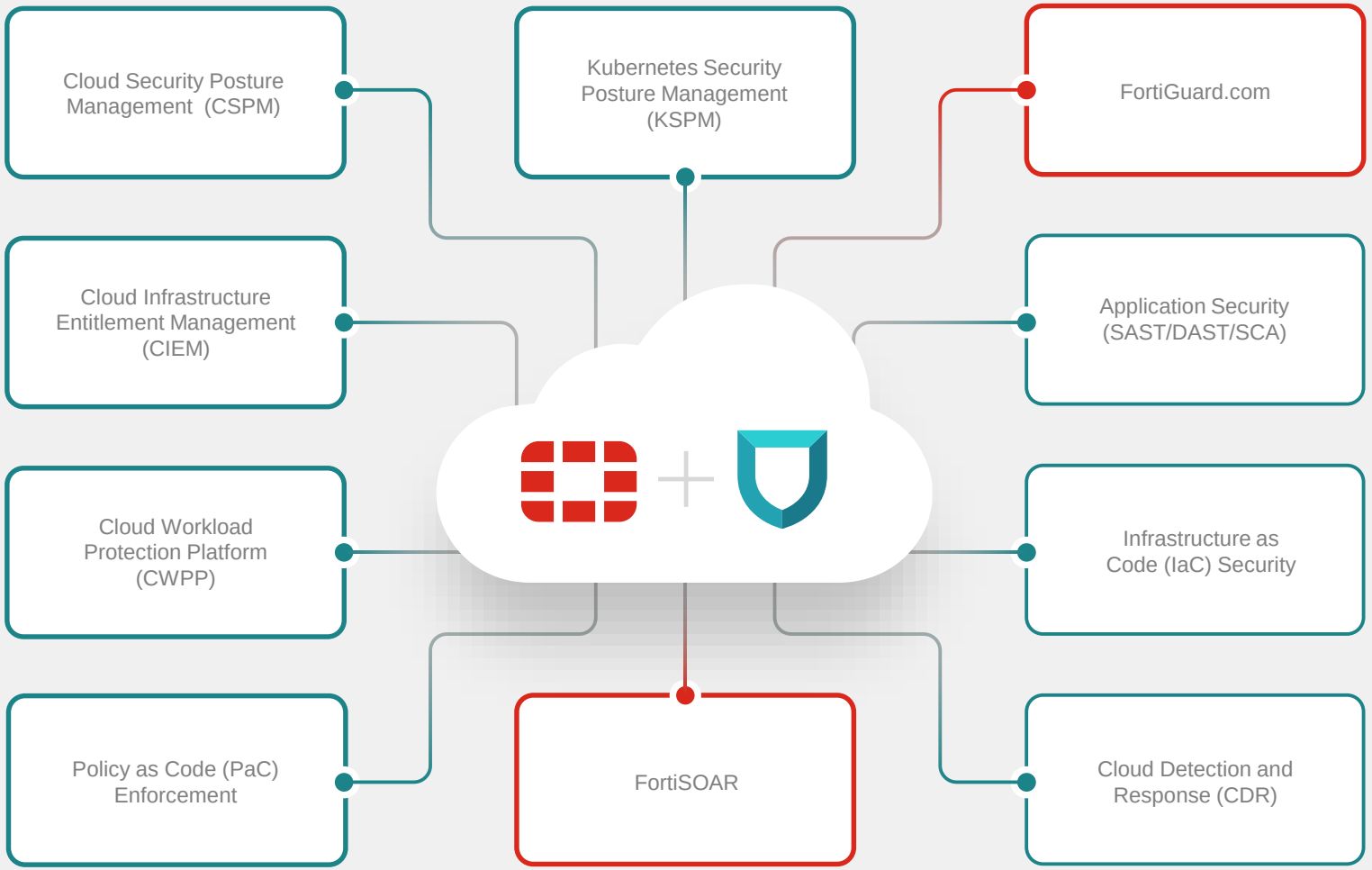
Fortinet + Lacework FortiCNAPP

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.



The ultimate CISO's guide to NIS2 and DORA

You might fall under SEC and NIS2 / DORA

See: ***Materiality Framework***

YES

Are you a publicly traded company in the United States?

NO

Are you a business running IT infrastructure and/or providing digital services?

YES

Is your company located or does it provide a service*‡ in the European Union?

YES

Does your company provide financial services or services to financial institutions?

YES

NO

NO

NO

NIS2 and DORA do not apply

NOTE: There may be less strict requirements for smaller and micro enterprises.

DORA

- Regulation in force since 16th of January 2023.
- Grace period ends 17th of January 2025.

Penalties for noncompliance

CORPORATE FINES

2% of annual turnover

EMPLOY

Standard:

Critical thi

Standard

Risk management

Do you have effective and well-documented procedures for risk assessment, risk prevention, risk detection, and risk response?

Supply chain security

Do you have security oversight over your supply chain, including relationships between each entity and its direct suppliers or service providers?

Secure infrastructure

Have you incorporated:

- security principles into network and information system acquisition, development, and maintenance?
- basic cyber hygiene practices?
- policies around the use of cryptography and encryption?
- multi-factor authentication or continuous authentication solutions?

BCDR & emergency communication

Do you have business continuity and disaster recovery (BCDR) mechanisms in place to stay resilient through a cyber attack and reduce impact to end users?

Do you have secured emergency communication systems in place?

YES

NO

NIS2

- EU member states must localize NIS2 into state law by 17th of October 2024.

Penalties for noncompliance

CORPORATE FINES

Critical sectors*: 10M Euros or

Important sectors‡: 7M Euros or

*High criticality sectors

- Digital infrastructure (internet exchange points; DNS service providers; TLD name registries; cloud computing service providers; data centre service providers; content delivery networks; trust service providers; providers of public electronic communications networks and publicly available electronic communications services)
- ICT service management (managed service providers and managed security service providers)
- Energy
- Transport
- Banking
- Financial market infrastructure
- Health (including manufacture of pharmaceutical products including vaccines
- Drinking water
- Waste water
- Public administration and space

‡Important sectors

- Postal and courier services
- Waste management
- Chemicals
- Food
- Manufacturing of medical devices
- Computers and electronics
- Machinery and equipment
- Motor vehicles
- Trailers and semi-trailers and other transport equipment
- Digital providers (online market places, online search engines, and social networking service platforms)
- Research organizations

Created in collaboration with: Tom Buerbaum, Head of Platform and Security; Craig Tunstal

Lacework FortiCNAPP Pricing & Packaging

Lacework FortiCNAPP packaging and pricing options

STANDARD

$50 per vCPU/year

Start protecting what you build and run in the cloud

Capabilities Include

- Vulnerability Assessment and standard risk score (CVSS, CVE and exploit data)
- Security posture management (CSPM, KSPM)
- Threat Detection: Cloud detection and response (cloud account audit log monitoring)

PRO

$75 per vCPU/year

Gain advanced functionality to prioritize risks, detect threats, and shift security left

Capabilities Include

- All Standard Capabilities plus
- Advanced vulnerability with custom risk score
- Attack path analysis
- Infrastructure as code security
- Threat detection: Cloud detection and response (k8s audit logs (EKS, GKE))
- Cloud infrastructure entitlement management (CIEM)

ENTERPRISE

$100 per vCPU/year

Unlock all capabilities to prioritize risk, prove compliance, find threats, and operationalize security across clouds

Capabilities Include

- All Pro capabilities plus
- Threat Detection: workload security for VMs, containers and Kubernetes
- File integrity monitoring

CODE SECURITY

$1,320 / Developer / Year

Lacework FortiCNAPP Packages	STANDARD	PRO	ENTERPRISE
Security posture management for cloud and Kubernetes (CSPM & KSPM)			
Resource discovery and configuration management, includes custom policies	●	●	●
Secrets detection	●	●	●
Compliance reporting (SOC, ISO, CIS, PCI-DSS, etc.)	●	●	●
Infrastructure as Code scanning		●	●
Cloud vulnerability assessments			
Inline, container, and host scanning	●	●	●
Standard risk-based scoring (CVSS, CVE and exploit data)	●	●	●
Custom risk-based scoring (active vulnerability detection and internet exposure)		●	●
Enforcement for vulnerable images (Kubernetes admission controller)		●	●
Cloud infrastructure entitlement management (CIEM)			
Entitlement discovery and scoping guidance for overly permissive identities		●	●
Attack path analysis			
Top risk dashboard and alerting with Exposure Polygraph visualization		●	●
Threat detection			
Cloud detection and response (audit log monitoring)			
Polygraph behavior-based threat detection for cloud accounts	●	●	●
Polygraph behavior-based threat detection for managed K8s services		●	●
Workload security for virtual machines, containers, and Kubernetes			
Continuous runtime monitoring and snapshots			●
Polygraph behavior-based threat detection			●
Threat detection based on signatures and custom policies			●
File integrity monitoring			●

Lacework FortiCNAPP Case Studies

How Lacework FortiCNAPP helped LendingTree

Learn more here

INDUSTRY

FinTech

CLOUD SERVICE PROVIDERS

AWS, Google Cloud, Azure

Challenge

- Increasingly complex multicloud environment
- Lacked visibility into containerized workloads
- Keeping up with ever-changing regulatory standards

Solution

- Full coverage of multicloud assets with unified platform
- Continuous visibility and threat detection
- Out-of-the-box policies and reports streamline compliance audits

Result

- Saved $200K/yr through tool consolidation
- Reduced investigation time from 10 hours to 5 minutes
- Slashed alert volume by 90%, to less than 5 alerts/day

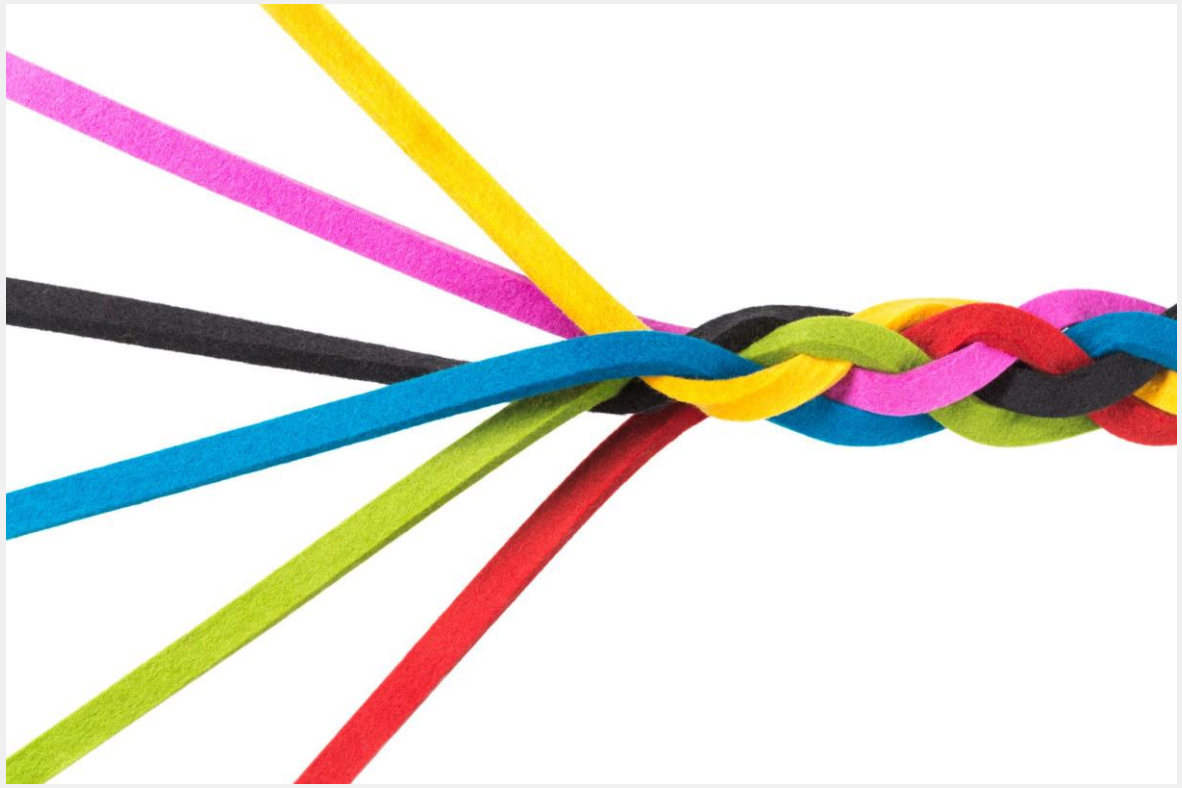
Marketplaces: Product and Solution Availability

aws	PAYG / Private Offer	BYOL
AWS WAF Rules	✓	
Lacework FortiCNAPP	✓	
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	✓	

	PAYG / Private Offer	BYOL
WAF Rules		
Lacework FortiCNAPP		
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	✓	

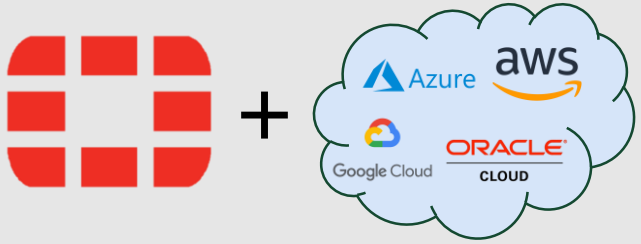
Google Cloud	PAYG / Private Offer	BYOL
WAF Rules		
Lacework FortiCNAPP		
FortiGate-VM*	✓	✓
FortiGate CNF		
FortiManager-VM*		✓
FortiAnalyzer-VM*		✓
FortiWeb-VM*	✓	✓
FortiWeb Cloud	✓	
FortiEDR	✓	
FortiMail-VM		✓
FortiAuthenticator-VM		
FortiADC-VM*	✓	✓
FortiVoice-VM		
FortiRecorderVM		
FortiSandbox-VM		✓
FortiSIEM-VM		
FortiNDR		
FortiProxy-VM		
FortiDevSec	✓	
FortiCASB		✓
Cloud Consulting Services		
FortiFlex program	✓	
FortiPoints program	✓	

ORACLE CLOUD	PAYG / Private Offer	BYOL
WAF Rules		
Lacework FortiCNAPP		
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	✓	



Seamlessly integrate with cloud platforms and ecosystems

Key Takeaways

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


FORTINET