Wiki Webinar

by inetum. realdolmen

Fortinet security fabric Fast Track en demo lab

23 juni 2021

FORTINET

Partnerships to enable business innovation

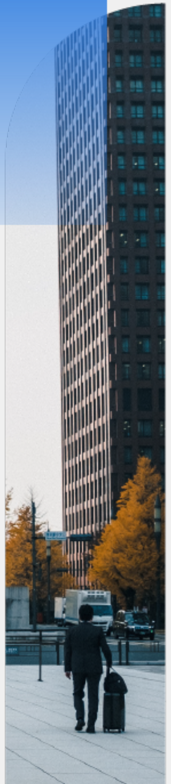
inetum
realdolmen
Positive digital flow

ENGAGE
FORTINET ADVANCED PARTNER
Integrator

Inetum-Realdolmen is Fortinet Advanced Partner of the Year 2021

FORTINET

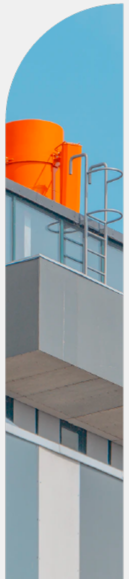
NSE Training Institute



Creating a Comprehensive Security Fabric

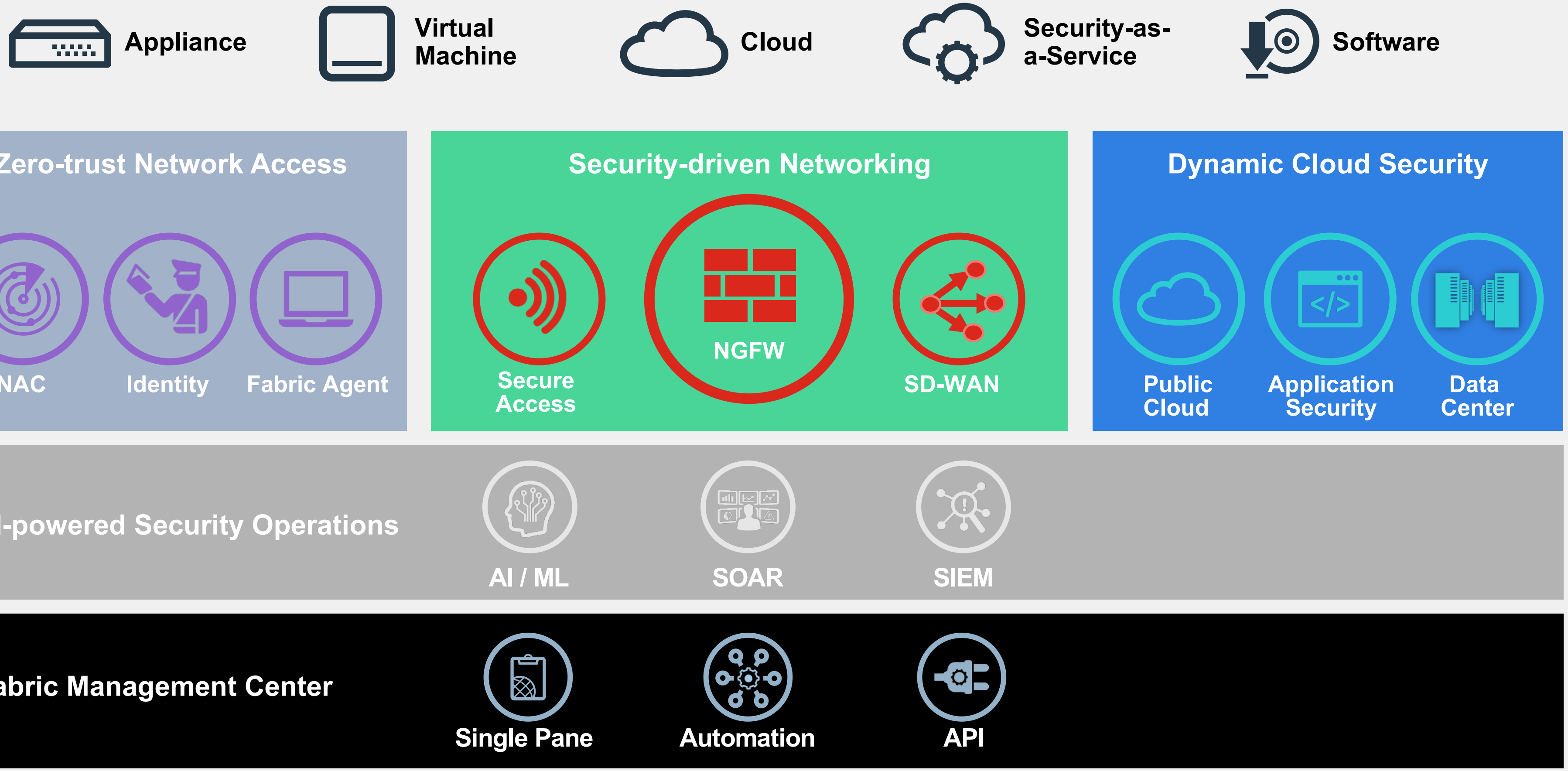
Lars Putteneers

System Engineer



Fortinet Security Fabric Enables Digital Innovation

Protecting every edge in the infrastructure



Appliance

Virtual Machine

Cloud

Security-as-a-Service

Software

Zero-trust Network Access

NAC

Identity

Fabric Agent

Security-driven Networking

Secure Access

NGFW

SD-WAN

Dynamic Cloud Security

Public Cloud

Application Security

Data Center

AI-powered Security Operations

AI / ML

SOAR

SIEM

Fabric Management Center

Single Pane

Automation

API

Fortinet Security Fabric

Broad

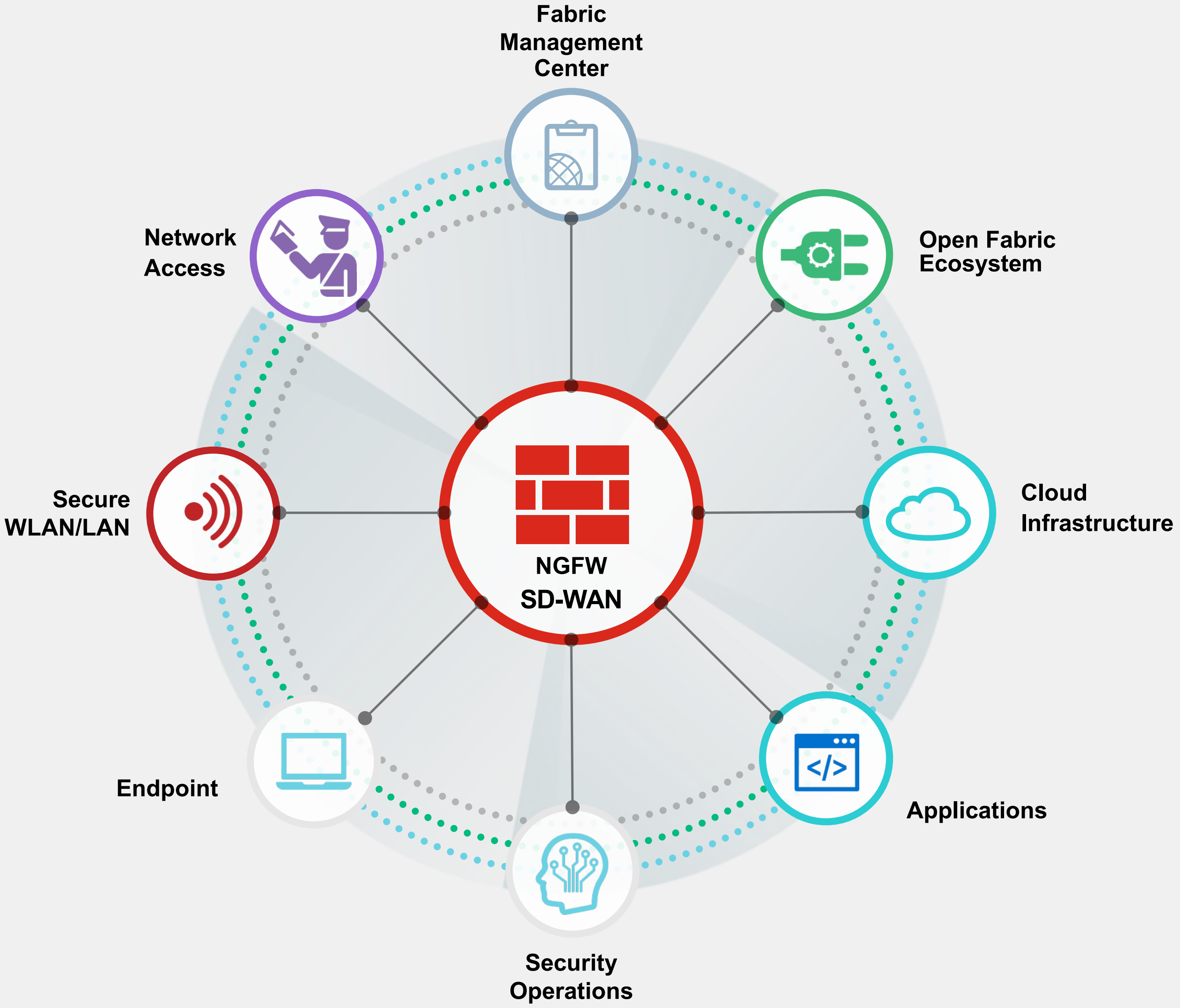
visibility of the entire digital attack surface to better manage risk

Integrated

solution that reduces the complexity of supporting multiple point products

Automated

workflows to increase speed of operations and response



Security Fabric Products

Different consumption models available

Appliance

Virtual Machine

Cloud

Security-as-a-Service

Software

FortiNAC	FortiAP	FortiGate	FortiGate VM	FortiWeb	FortiClient	FortiAnalyzer	FortiManager
FortiClient Fabric Agent	FortiSwitch		FortiCWP	FortiMail	FortiEDR	FortiSIEM	FortiGate Cloud
FortiAuthenticator	FortiExtender			FortiCASB		FortiSandbox	FortiCloud
				FortiADC		FortiSOAR	

FortiGuard Services

Network Security

Next-generation Firewall

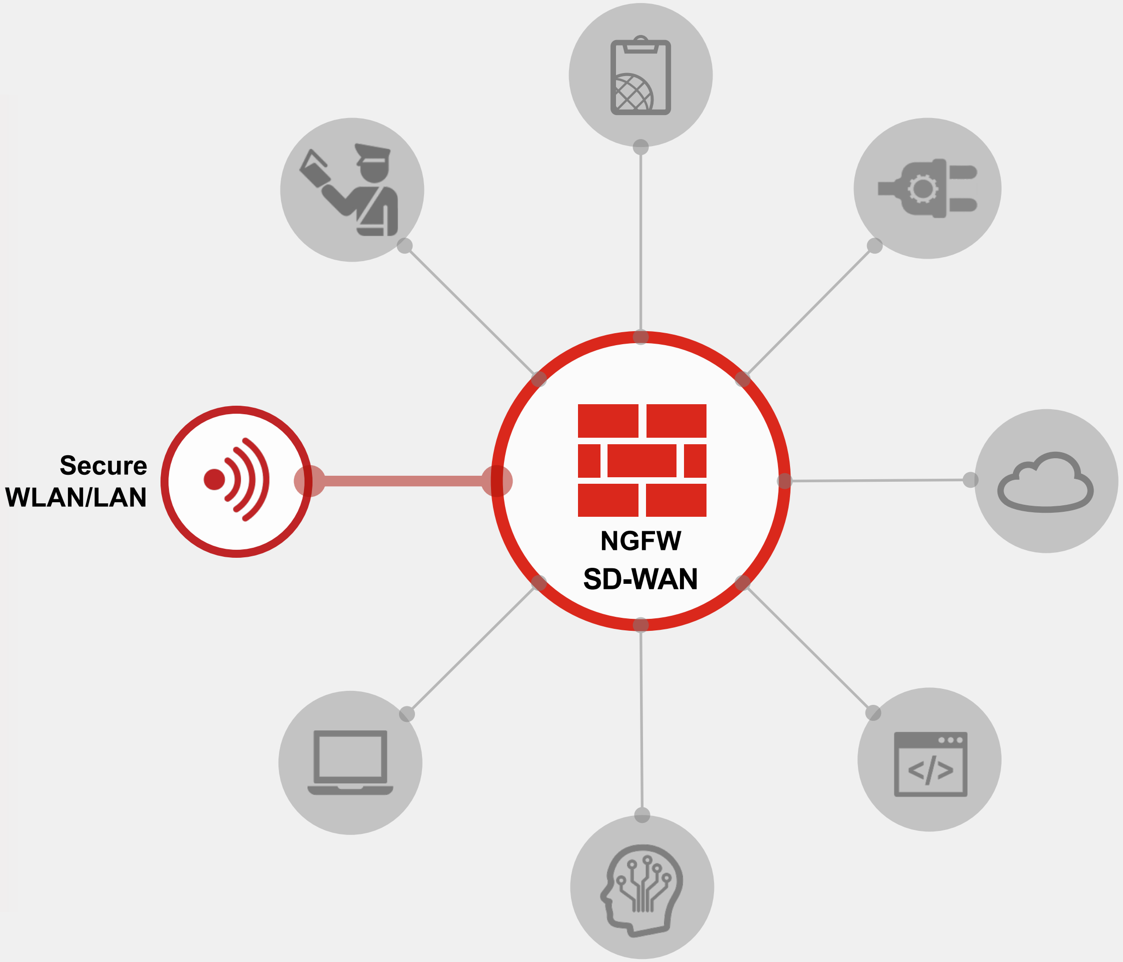
Manage all security risks & protect hyperscale

SD-WAN

Improve user/application experience

Secure Web Gateway

Block threats



Network Security

NGFW

Cybersecurity attacks are originating externally and from within internal networks. They can disrupt business services. Managing security risks at very high scale and performance is required for business continuity.

FortiGate

NGFW

Segmentation

- Manage external and internal risks
- Remove blind spots with SSL inspection
- Protect hyperscale infrastructure

NGFW

Network Security

SD-WAN

Rapidly increasing bandwidth consumption and cloud adoption lead to poor user experience and increased WAN costs. Businesses need to simplify operations, reduce cost and enable secure cloud transformation.

FortiGate

SD-WAN

- Reduce WAN cost
- Improve application experience
- Enable cloud-ready branch

SD-WAN

Network Security

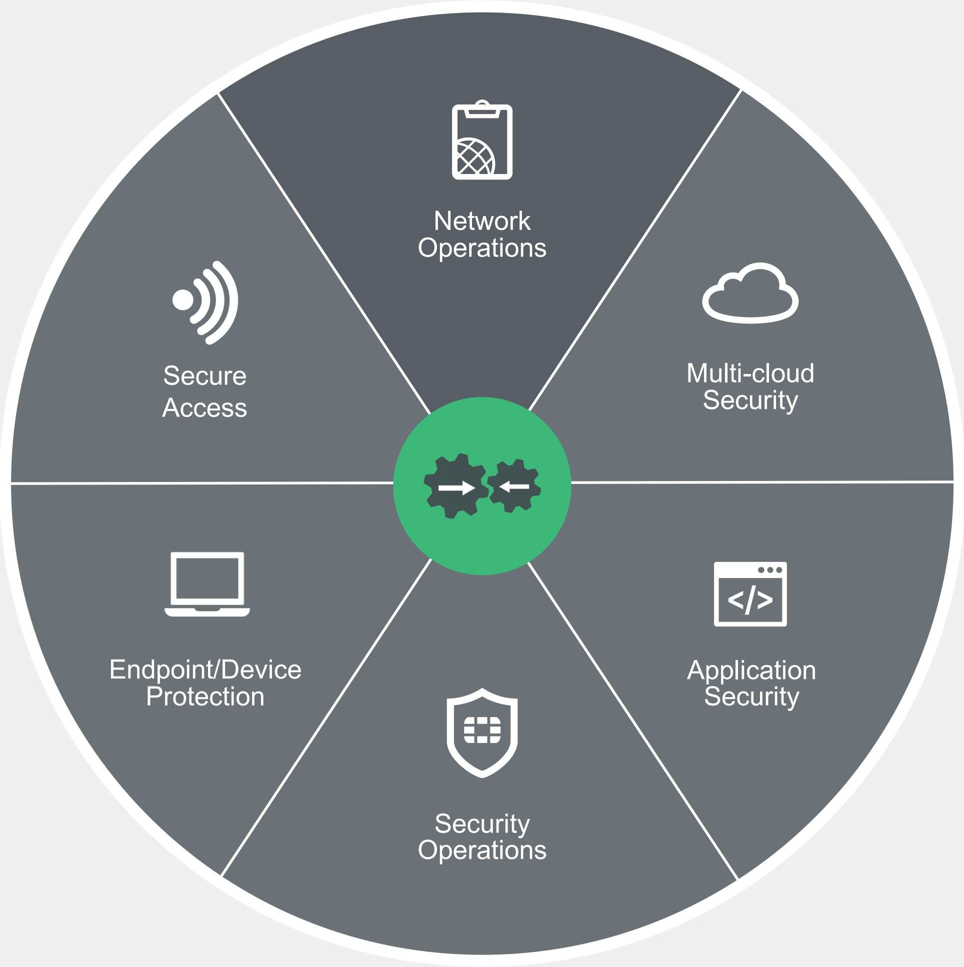
Secure Web Gateway (SWG)

Malicious URLs are home to threats that can result in malware infections and stolen data. With 70%+ traffic encrypted, there are more blind spots in the network. Web filtering is natively integrated in NGFW to protect growing internet-borne threats.

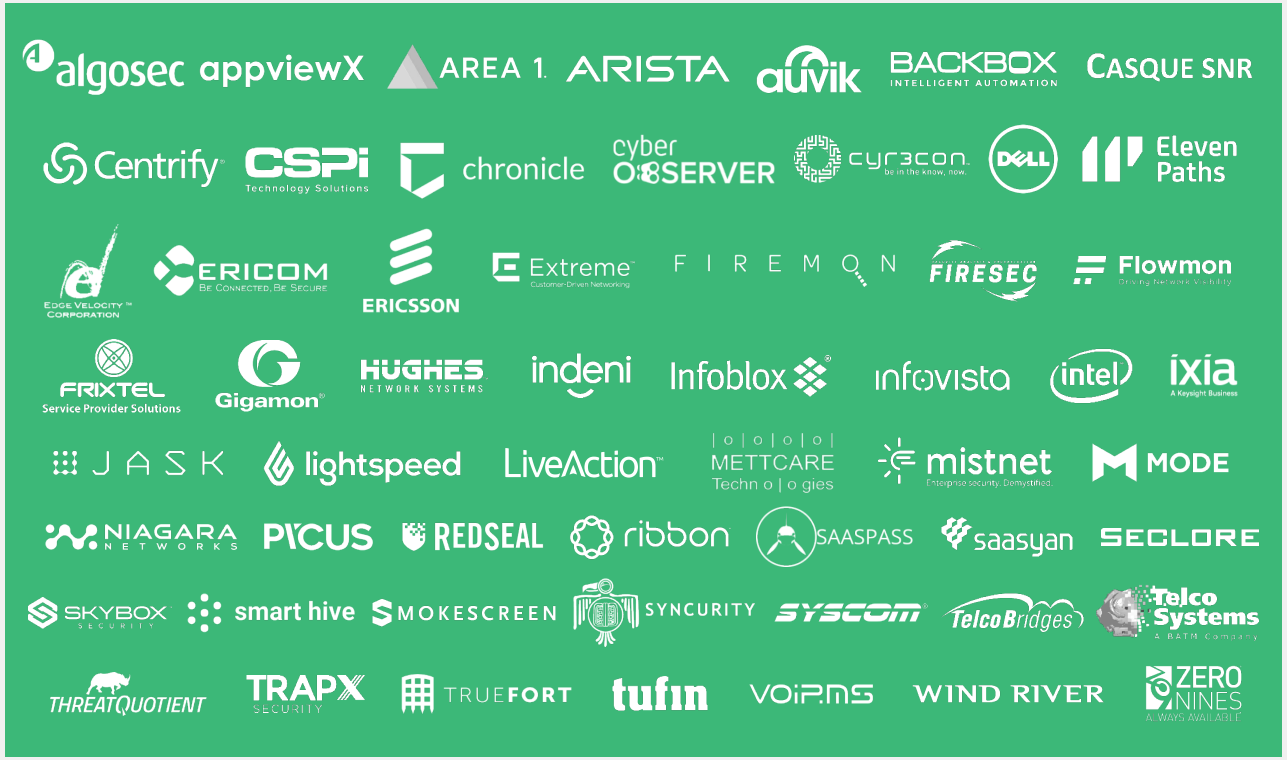
- Protect users from malicious URL
- Remove blind spots with SSL inspection
- Reduce point products and complexity

Network Operations Ecosystem

Fabric API Partnerships with FortiGate & FortiManager



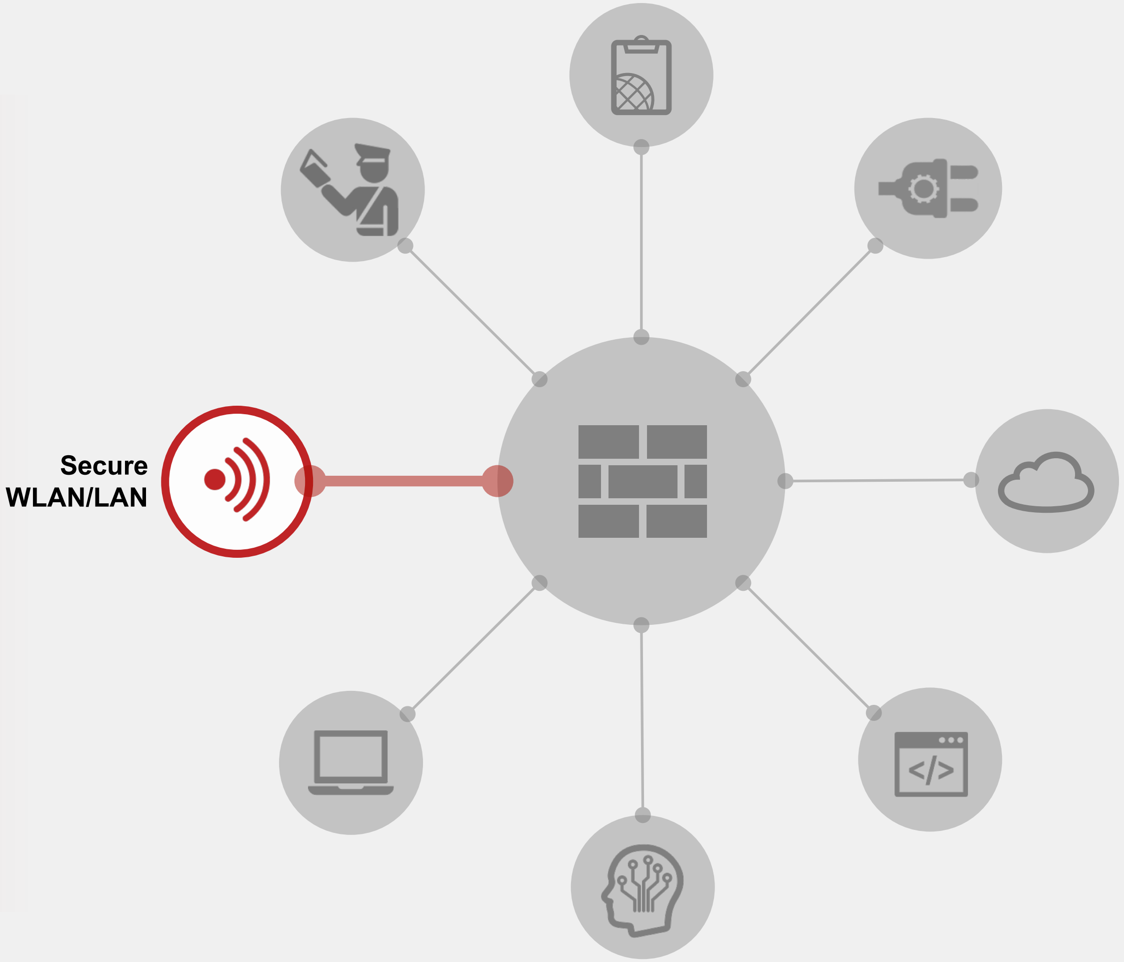
Fabric API



Secure Infrastructure

Secure WLAN/LAN

Extend Security to Access Layer



Secure Infrastructure

Extend security to access layer

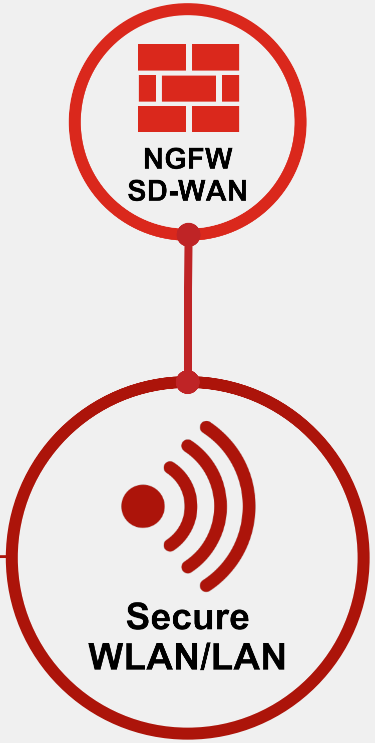
Most access edge products lack integration with security and management. FortiGate protection can be extended to the access network to enable deeper integration and consistent security.

FortiGate

FortiAP

FortiSwitch

- Extend security to access layer
- Simplify operations
- Enable SD-Branch solution



NGFW
SD-WAN

Secure
WLAN/LAN

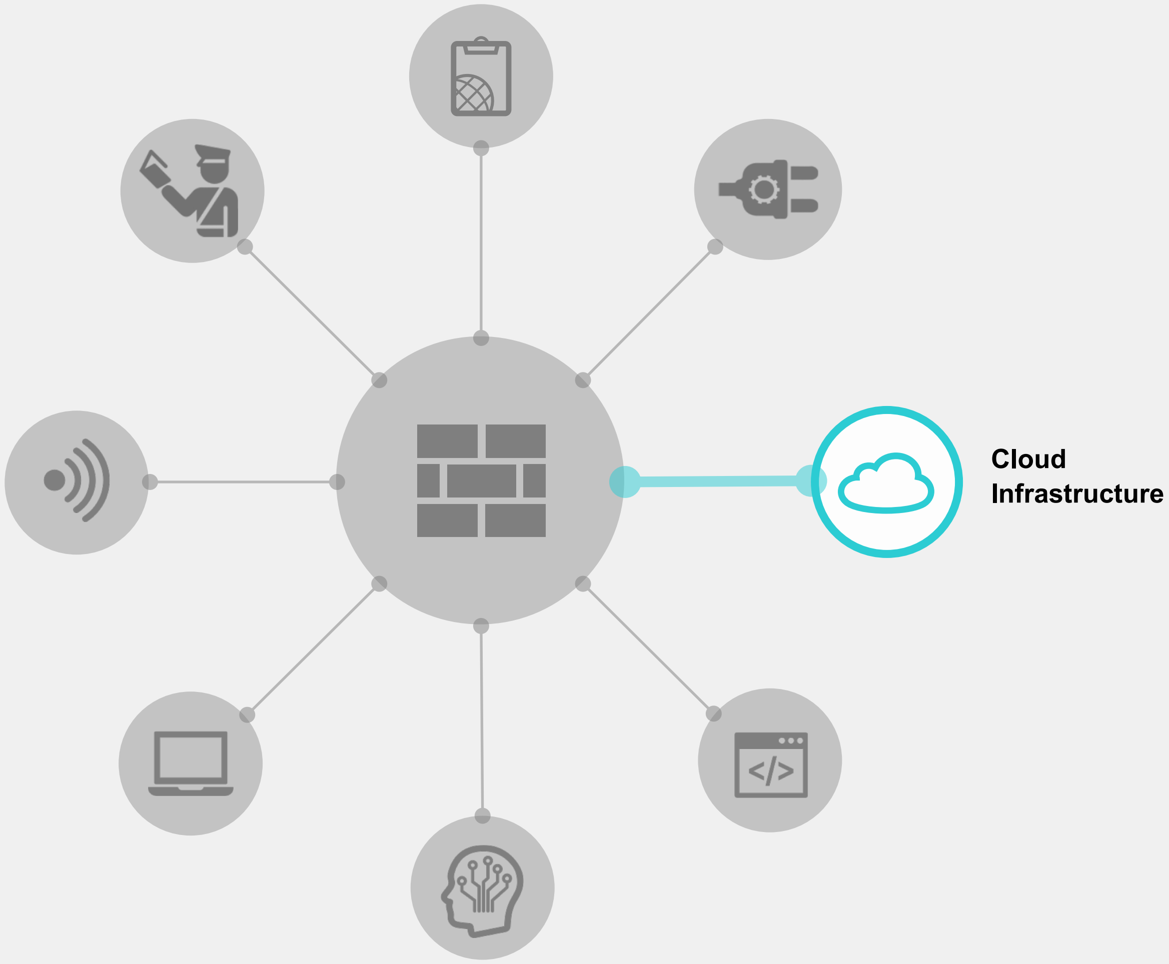
Dynamic Cloud Security

Public Cloud Infrastructure

Security for Compute & Applications Built in the Cloud

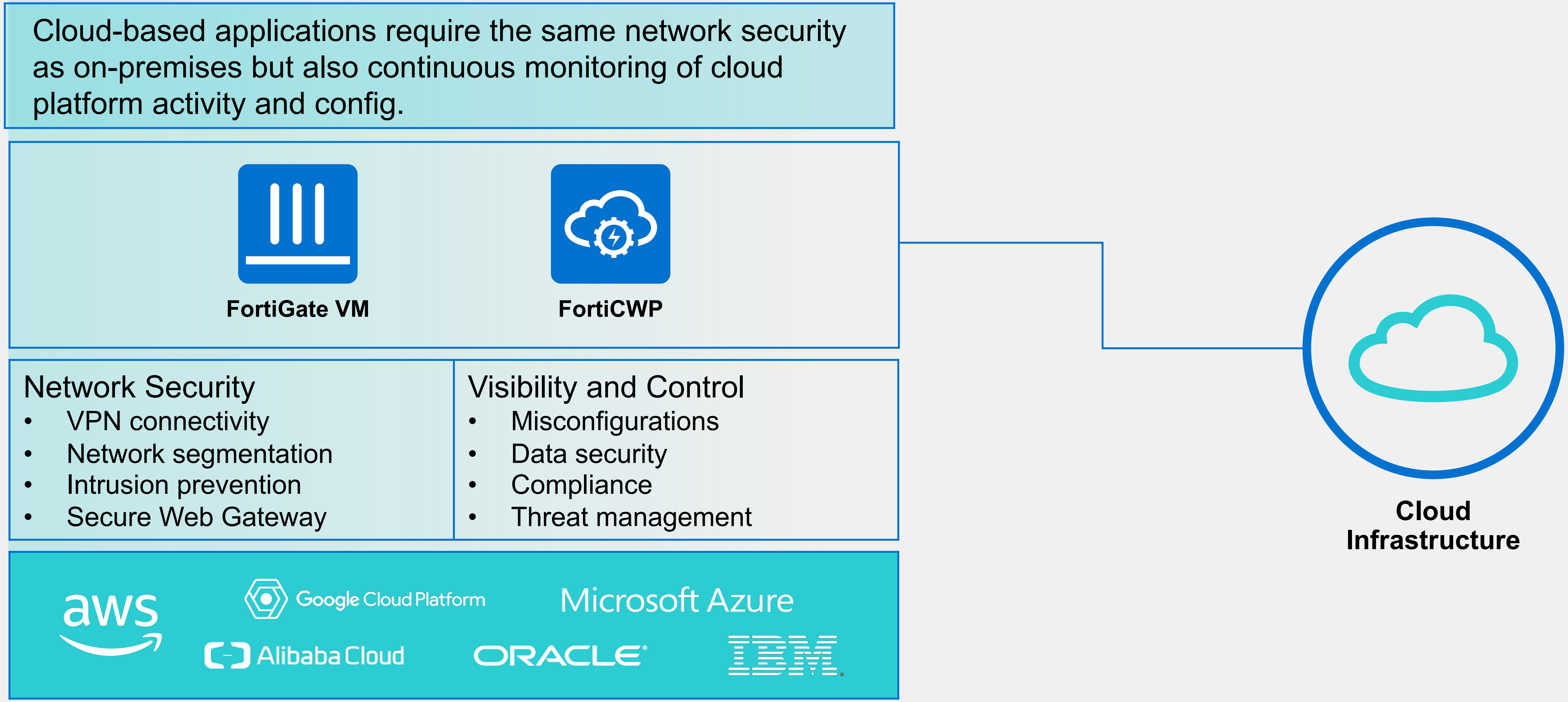
Private Cloud & SDN

Security Automation & Integration for Private Clouds



Dynamic Cloud Security

Public cloud infrastructure



Cloud-based applications require the same network security as on-premises but also continuous monitoring of cloud platform activity and config.

Network Security

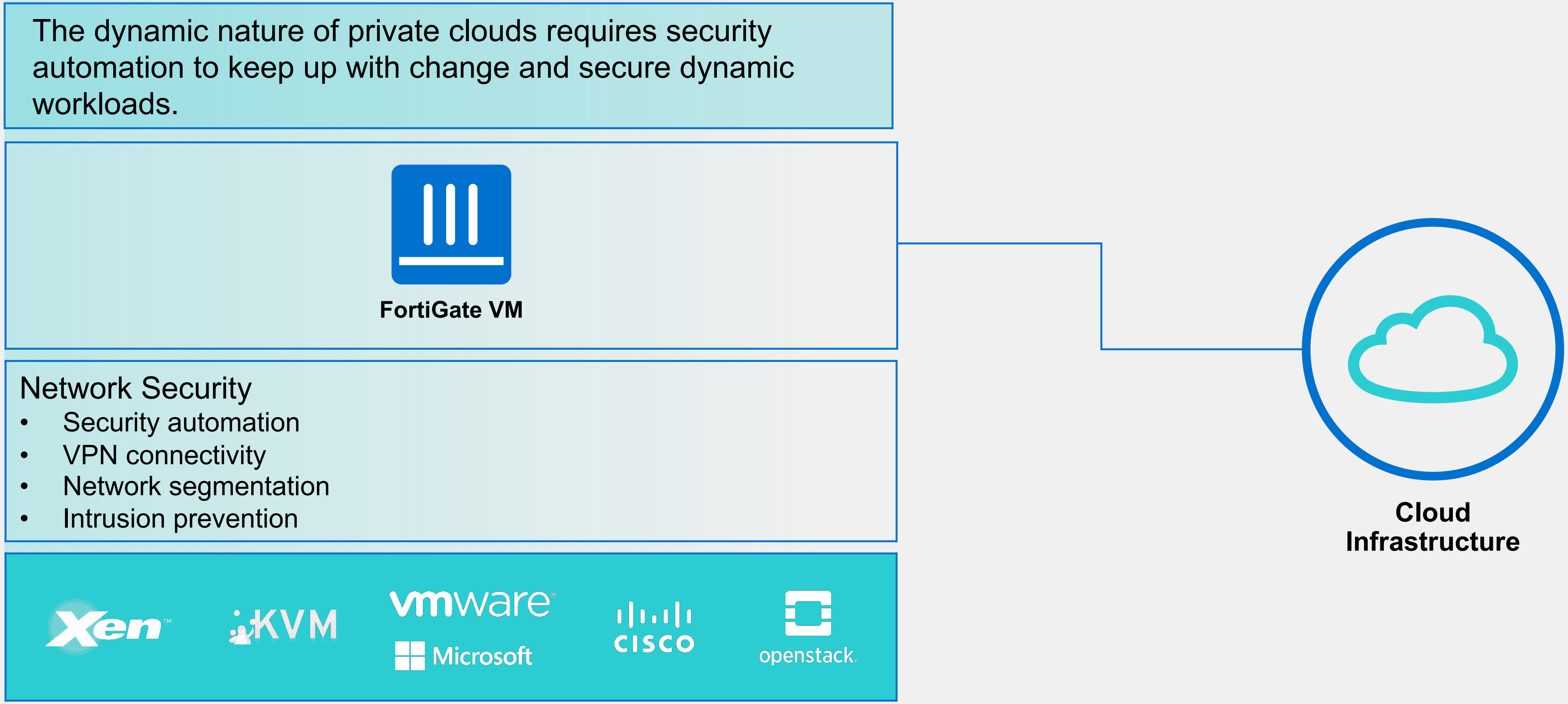
- VPN connectivity
- Network segmentation
- Intrusion prevention
- Secure Web Gateway

Visibility and Control

- Misconfigurations
- Data security
- Compliance
- Threat management

Dynamic Cloud Security

Private cloud & SDN

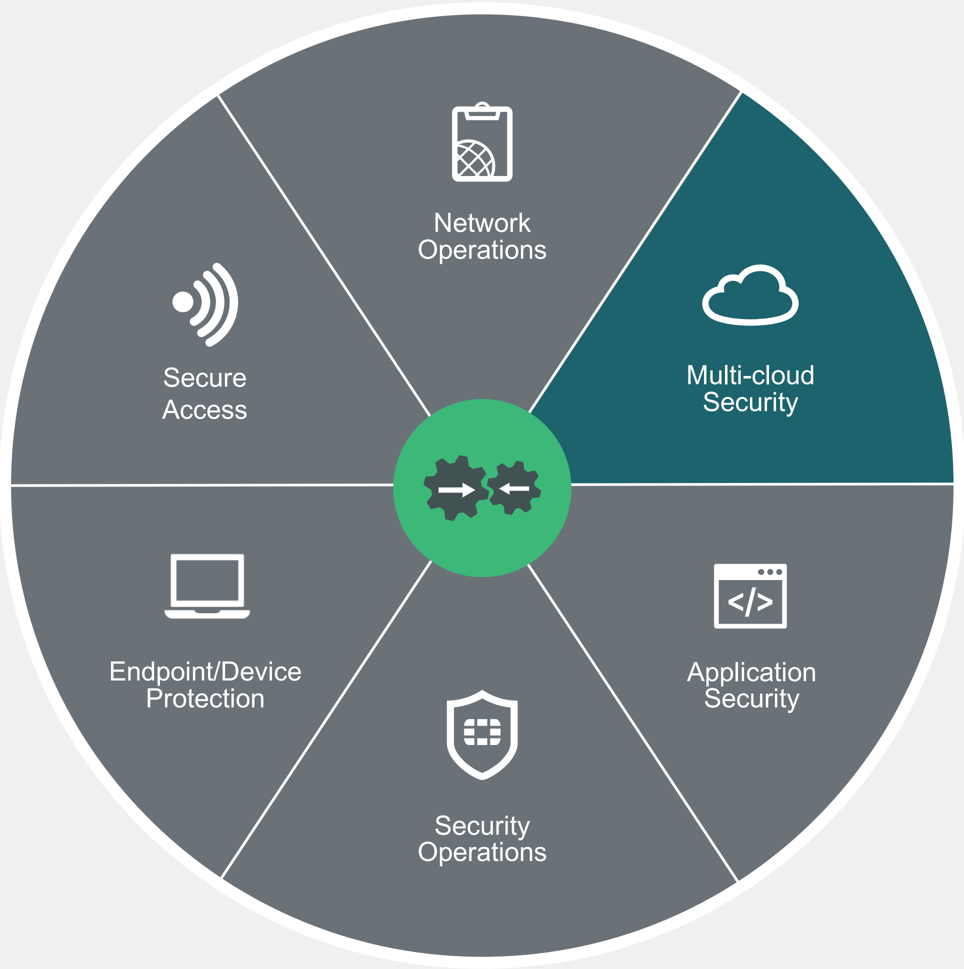


The dynamic nature of private clouds requires security automation to keep up with change and secure dynamic workloads.

Network Security
- Security automation
- VPN connectivity
- Network segmentation
- Intrusion prevention

Multi-cloud Security Ecosystem

Public & private cloud partnerships



Fabric Connector

Alibaba Cloud · aws · cisco · Google Cloud · Azure · nuagenetworks From Nokia · openstack. · ORACLE · vmware

Fabric API

ADVA Optical Networking · alcide · amdocs · aviatrix · big switch networks · CLOUDIFY · corsa · ENEA · HYTRUST · IBM · Lenovo · NEC · NOKIA Alcatel·Lucent · NoviFlow · NUTANIX · Pluribus NETWORKS · StackRox · TIGERA · tufin · Ubiqube

Fabric DevOps

Alibaba Cloud · aws · Google Cloud · Azure · nuagenetworks From Nokia · openstack. · ORACLE · RED HAT ANSIBLE Tower · HashiCorp Terraform · vmware

Dynamic Cloud Security

Web Application & API Security

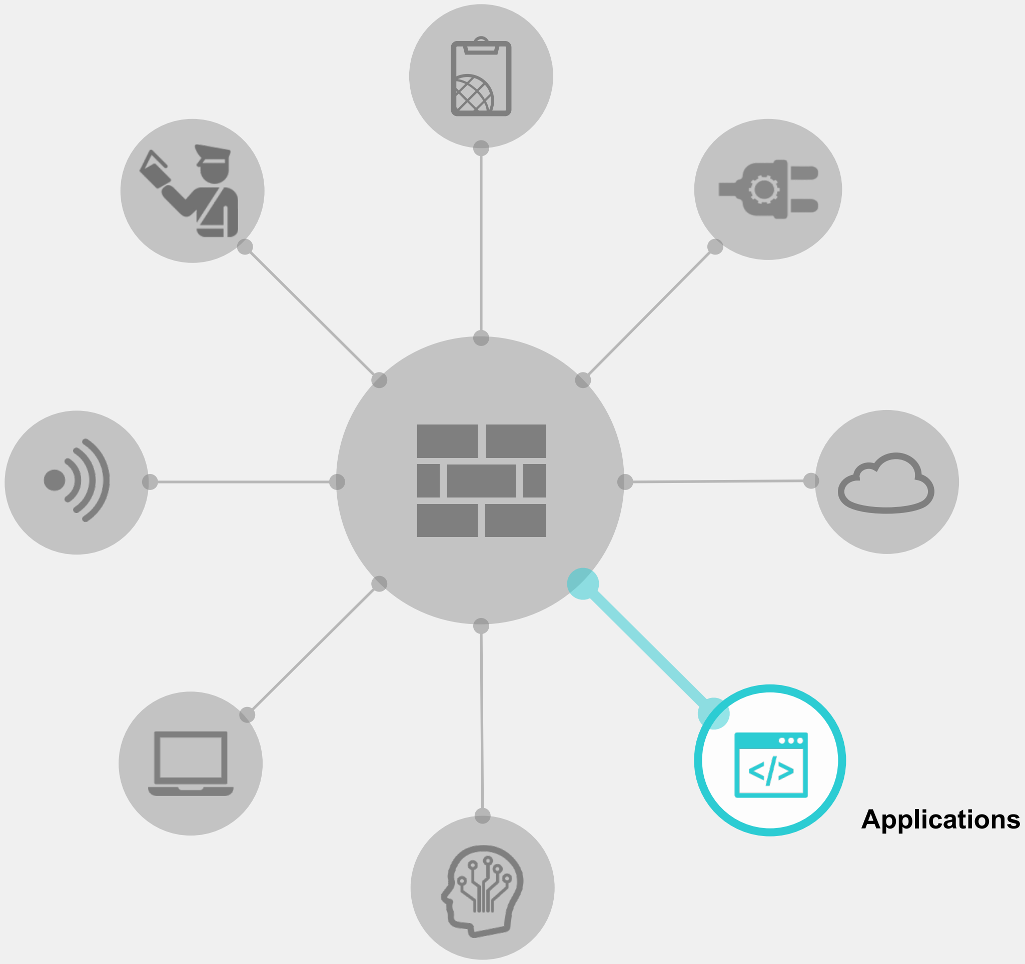
Securing web applications and APIs from application layer attacks

Email Security

Ensuring safe and appropriate cloud-based and on-premises email communications

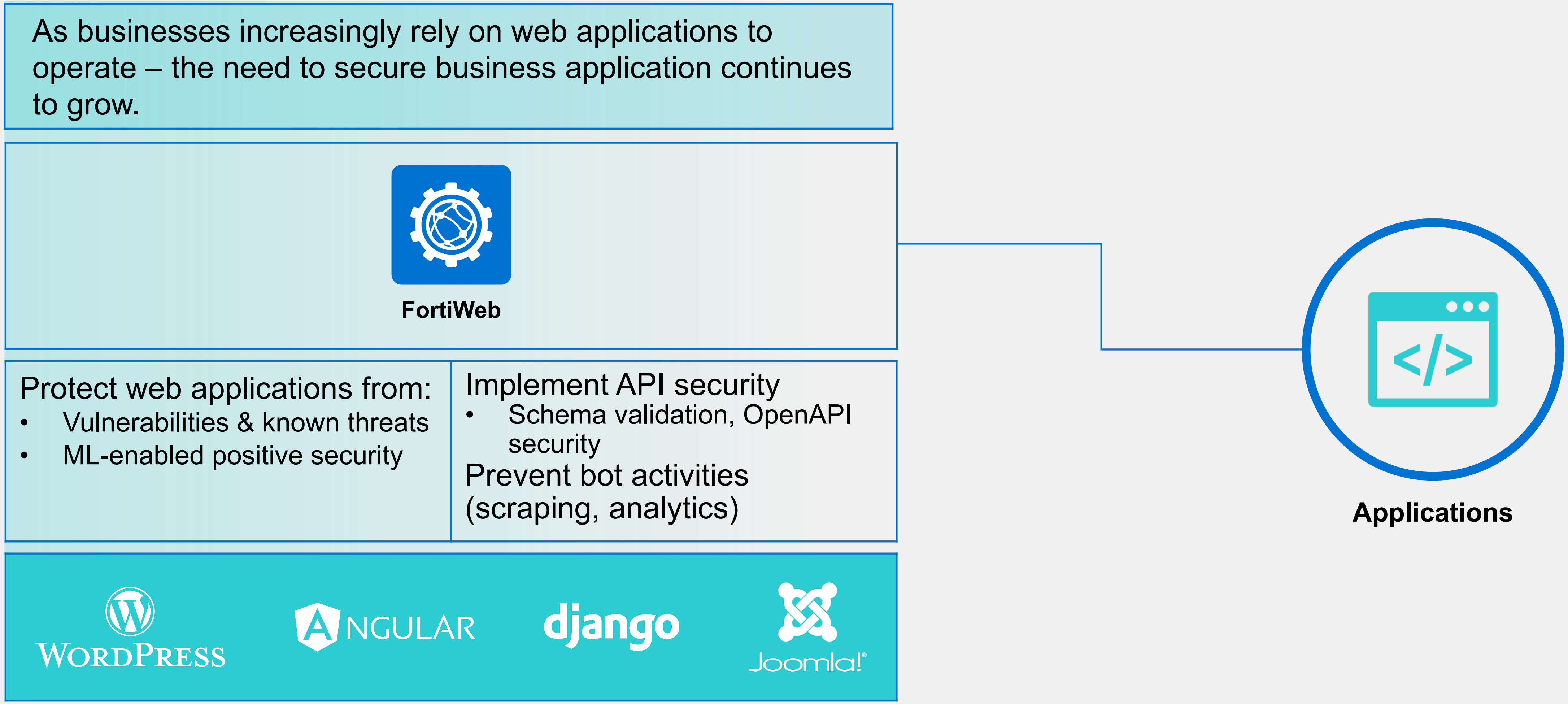
SaaS Security

Securing SaaS applications from threats and risk



Dynamic Cloud Security

Web application and API Security



As businesses increasingly rely on web applications to operate – the need to secure business application continues to grow.

FortiWeb

Protect web applications from:

- Vulnerabilities & known threats
- ML-enabled positive security

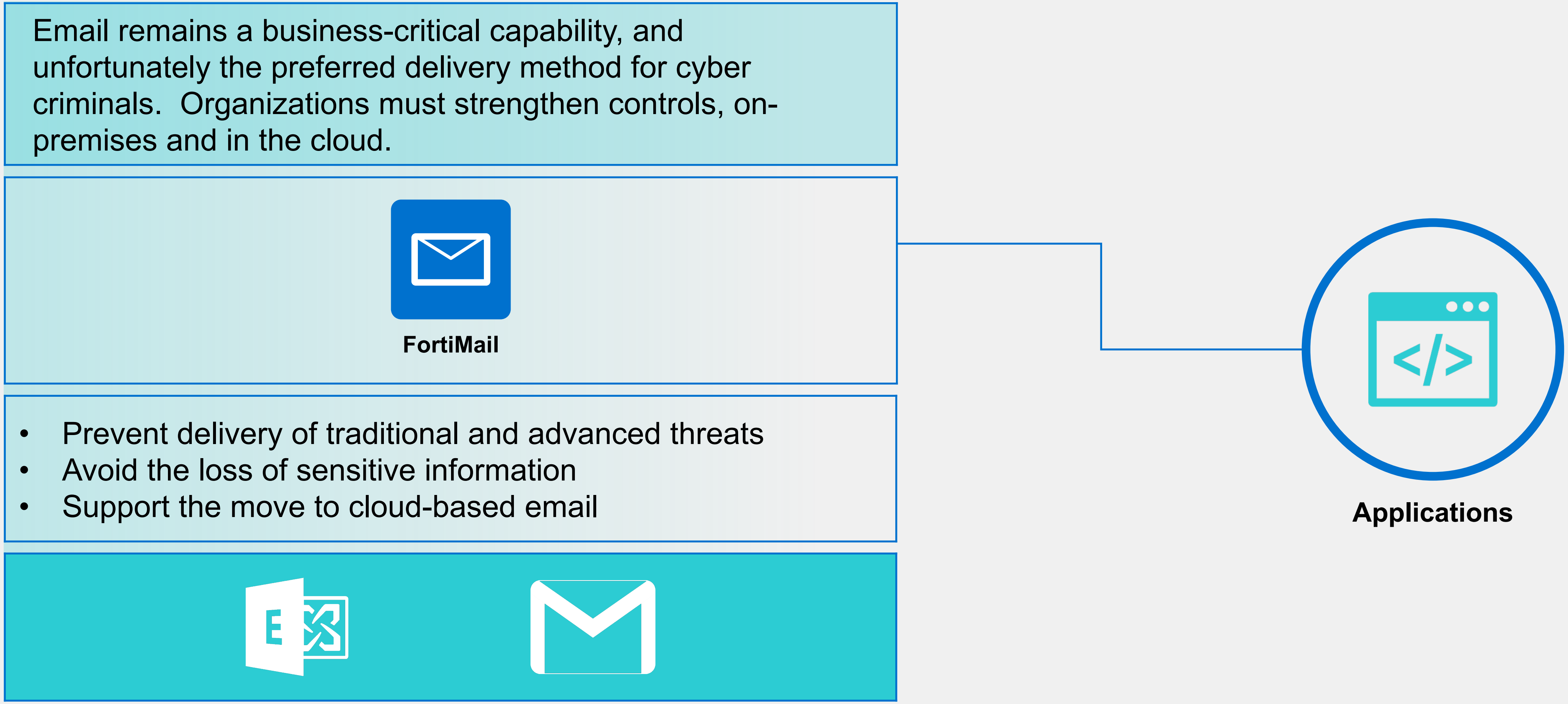
Implement API security

- Schema validation, OpenAPI security

Prevent bot activities (scraping, analytics)

Dynamic Cloud Security

Email security



Email remains a business-critical capability, and unfortunately the preferred delivery method for cyber criminals. Organizations must strengthen controls, on-premises and in the cloud.

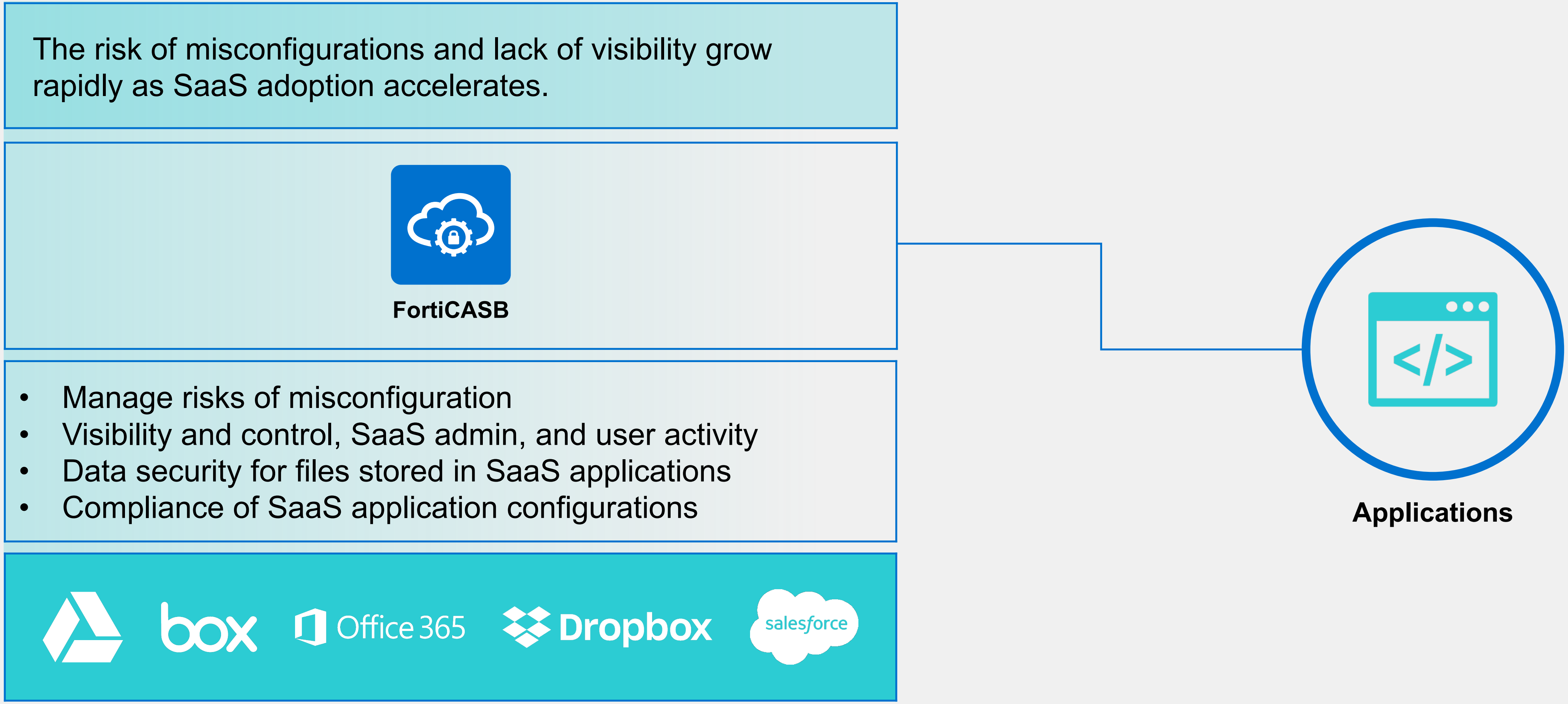
FortiMail

- Prevent delivery of traditional and advanced threats
- Avoid the loss of sensitive information
- Support the move to cloud-based email

Applications

Dynamic Cloud Security

SaaS security

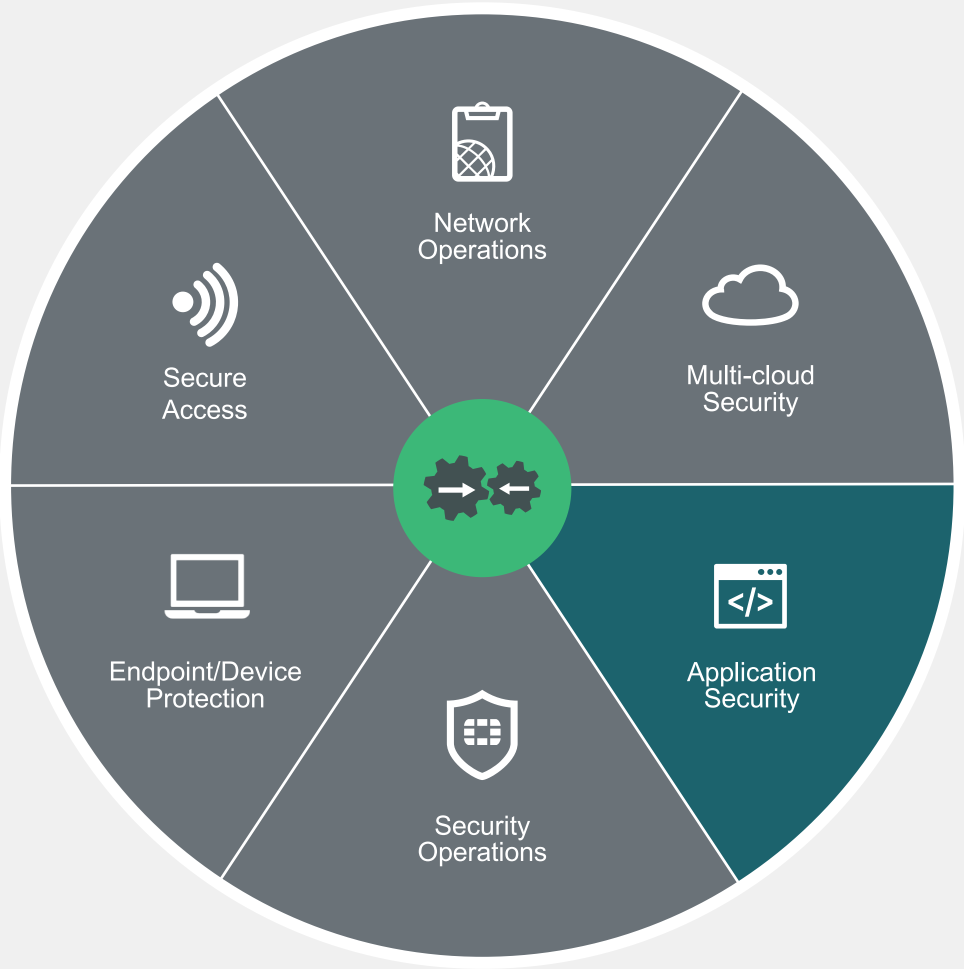


The risk of misconfigurations and lack of visibility grow rapidly as SaaS adoption accelerates.

- Manage risks of misconfiguration
- Visibility and control, SaaS admin, and user activity
- Data security for files stored in SaaS applications
- Compliance of SaaS application configurations

Application Security Ecosystem

Fabric API Partnerships with FortiWeb and FortiMail



Fabric API

atarlabs
CYBERSPONSE ADAPTIVE SECURITY
DefendEdge
DFLABS CYBER INCIDENTS UNDER CONTROL
gemalto security to be free
illapa cloud power
IMAGE ANALYZER
ImmuniWeb® AI for Application Security
MICRO FOCUS®
Qualys.
Restorepoint
WhiteHat SECURITY.

Zero-trust Network Access

NAC

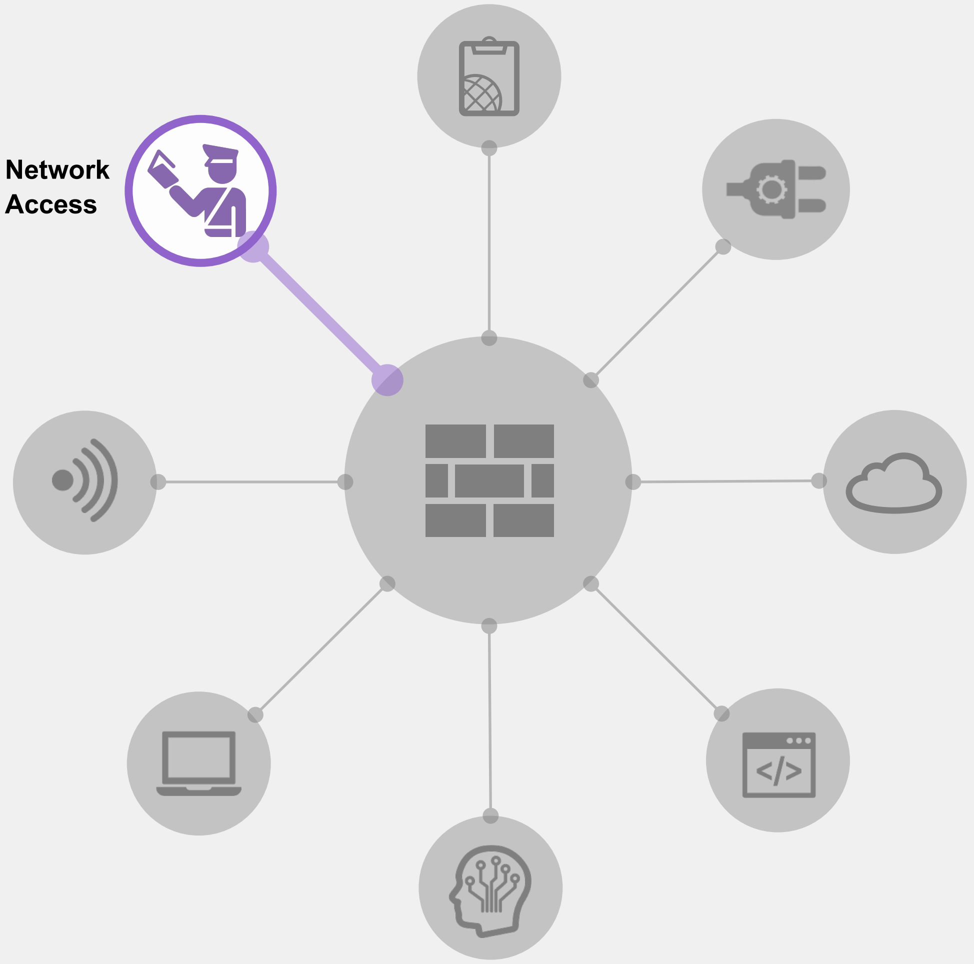
Know and control what is on your network

Identity

Know and control who is on your network

Endpoint

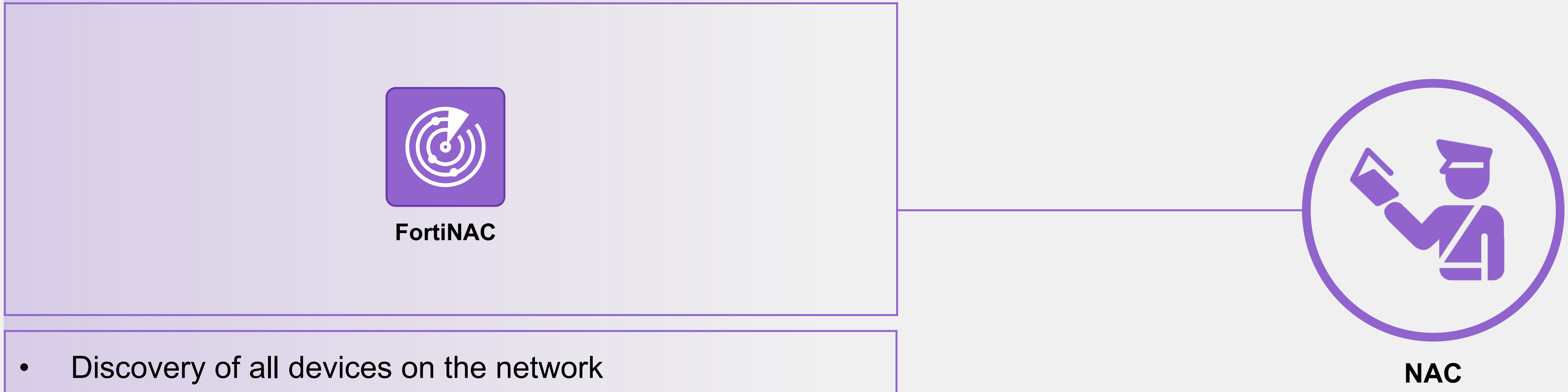
Track users and devices on-net, off-net



Zero-trust Network Access

Identify *What* is on your network

Explosion of devices and IoT ushers in threats.
Organizations are deploying NAC to regain visibility.



FortiNAC

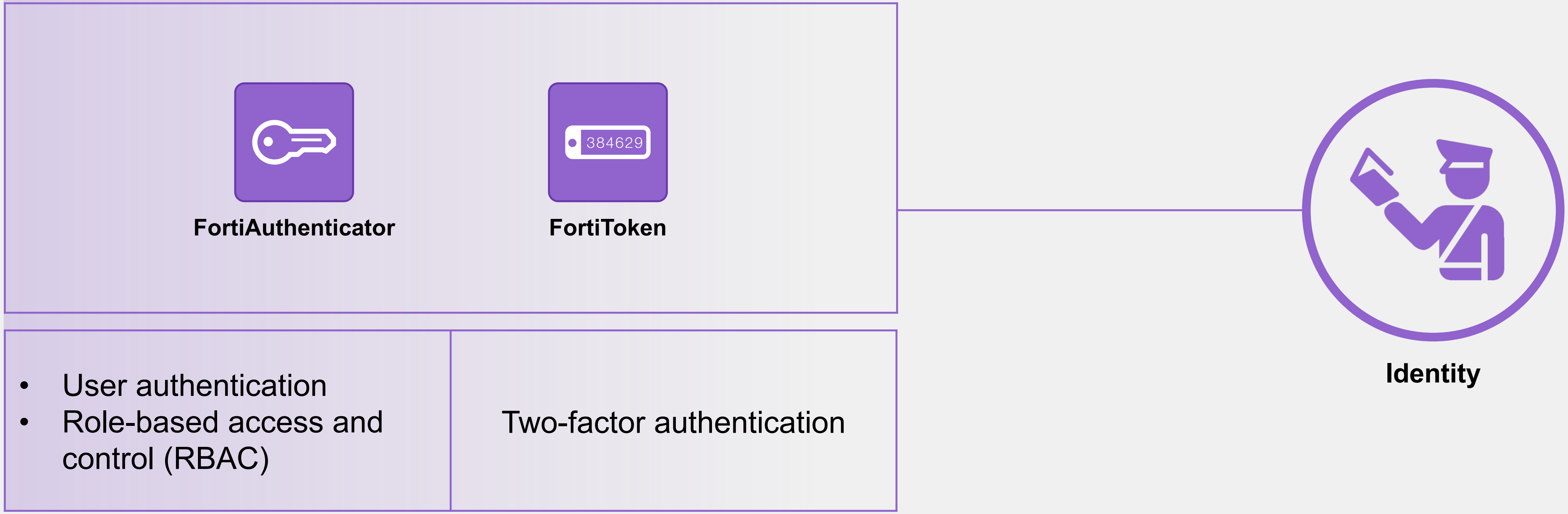
NAC

- Discovery of all devices on the network
- Identification of devices
- Policy-based control
- Continuous monitoring and anomaly detection

Zero-trust Network Access

Identify *Who* is on your network

Weak passwords and stolen credentials leave networks vulnerable. Strong authentication and role-based access are required.



FortiAuthenticator

FortiToken

- User authentication
- Role-based access and control (RBAC)

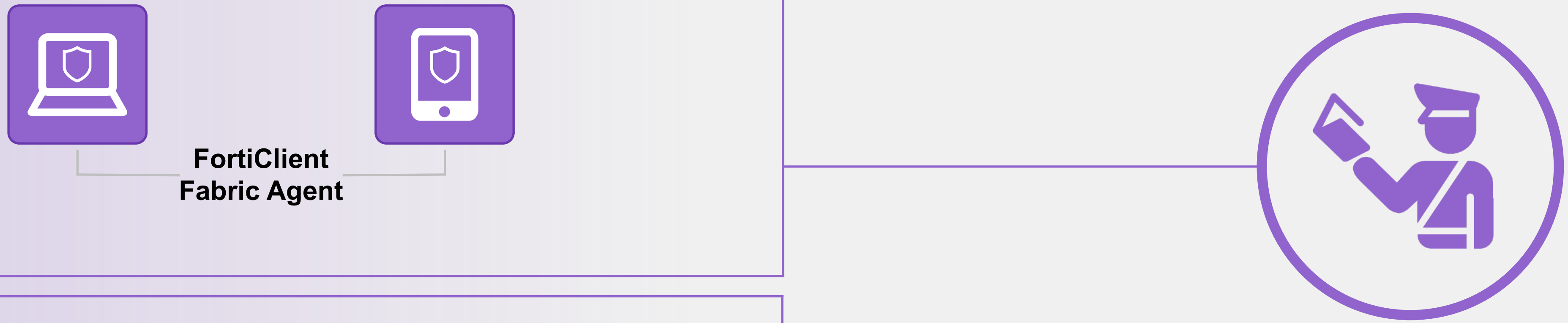
Two-factor authentication

Identity

Zero-trust Network Access

Track users & devices on-net, off-net

Today's digital business requires that employees work anytime, anywhere, on most any device. Endpoint agent must provide visibility and control.

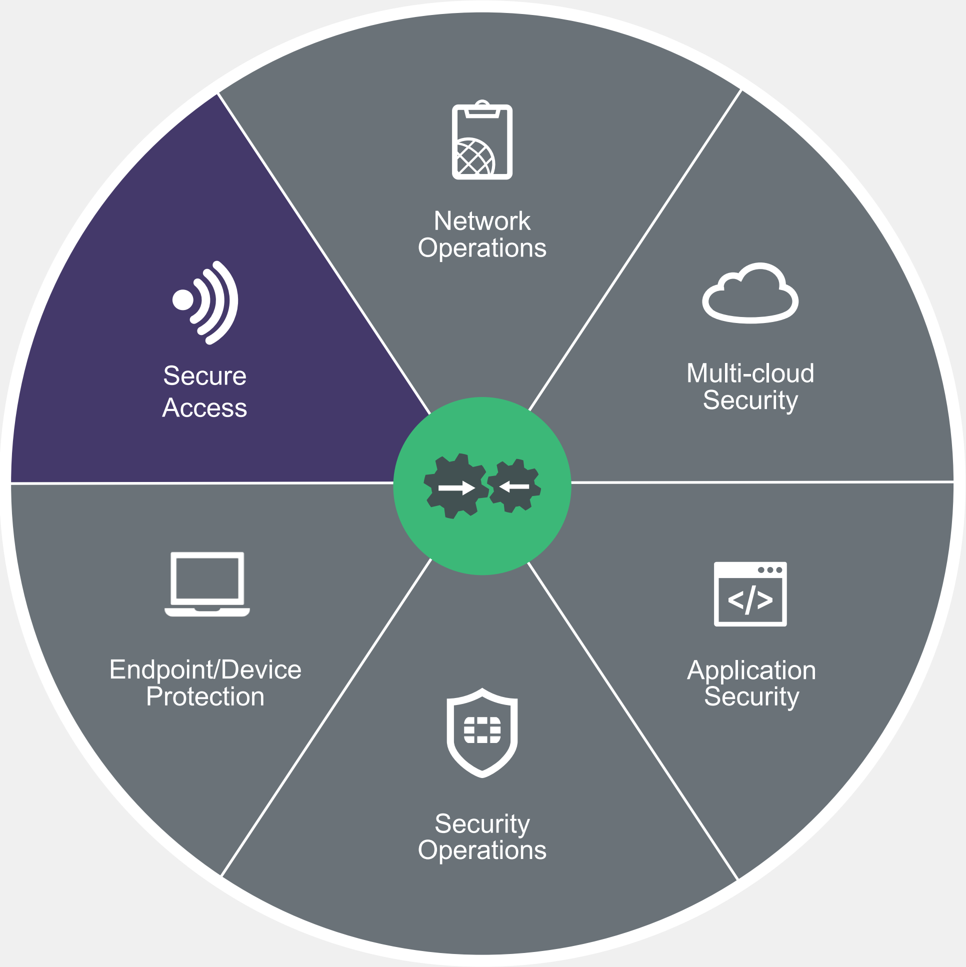


FortiClient
Fabric Agent

- Endpoint visibility
- Dynamic access control

Secure Access Ecosystem

Fabric API Partnerships with FortiNAC and FortiAuthenticator



Fabric Connector

aruba a Hewlett Packard Enterprise company

cisco

Fabric API

CYBER MDX

cyglass

Extreme networks

FORESCOUT

Gigamon®

Infocyte®

intel

METTCARE Technologies

MEDIGATE

ordr

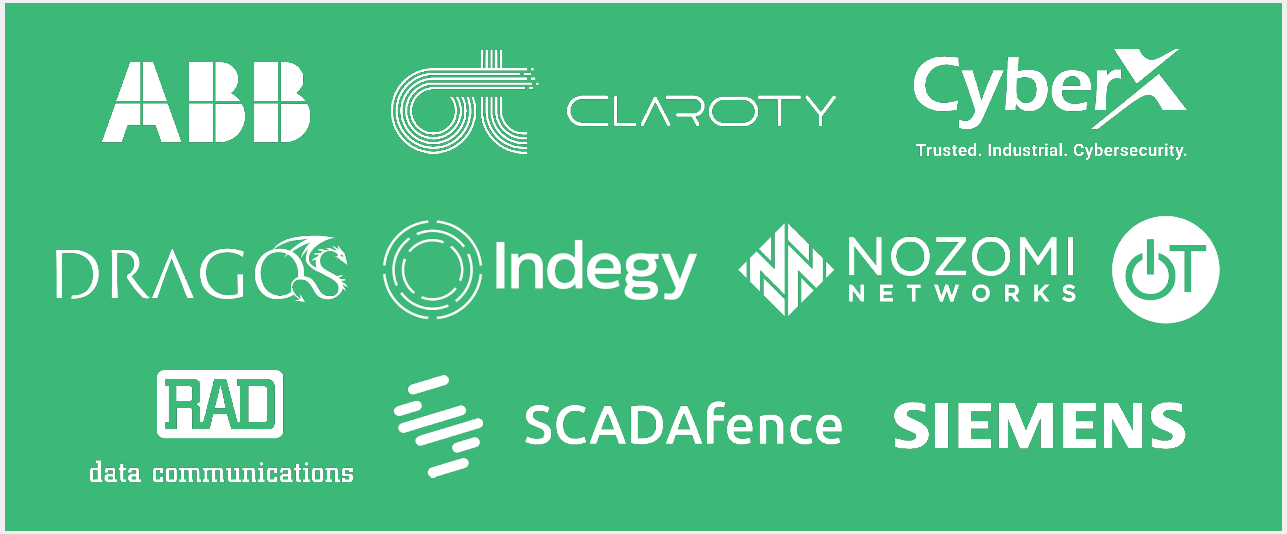
Pulse Secure

zentera® Connect · Protect · Shield

SCADA/Industrial Control

Fabric API Partnerships in OT vertical

Fabric API

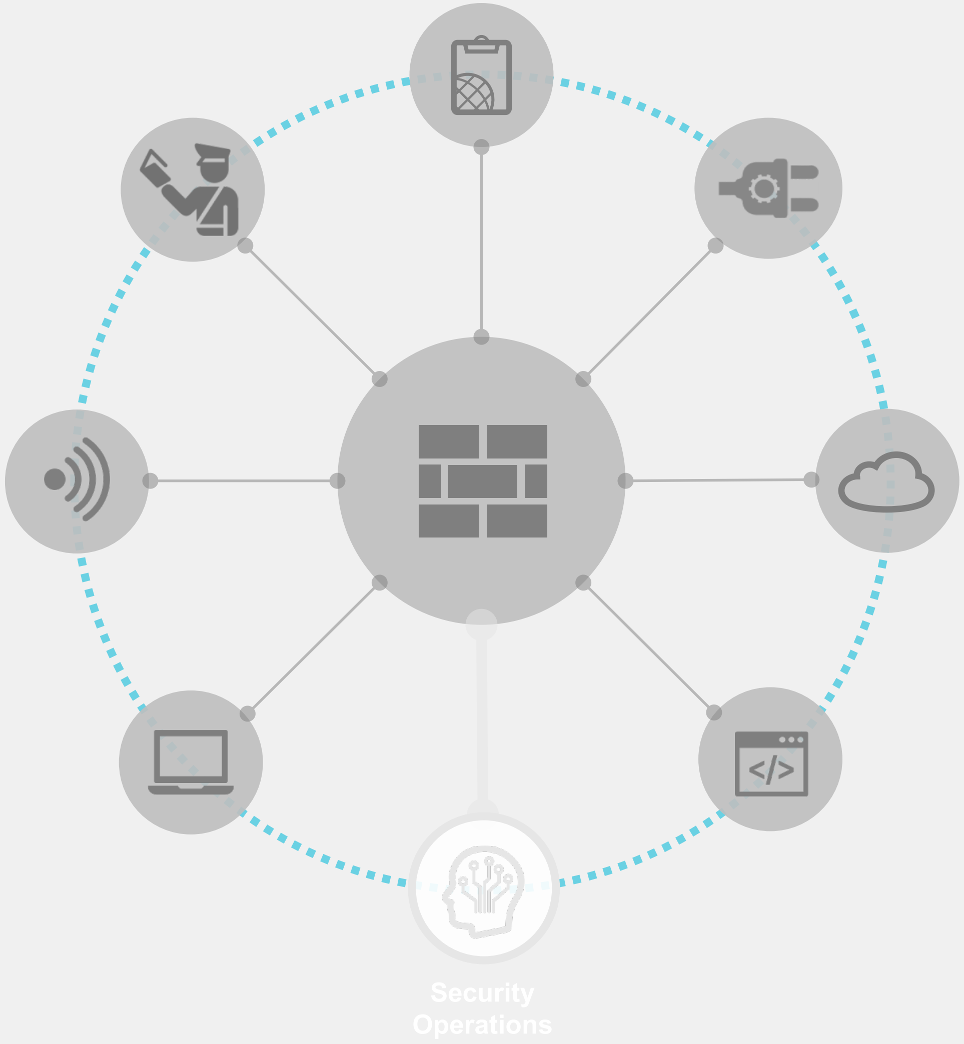


AI-powered Security Operations

Predict and Prevent Attacks
Global machine learning for proactive defense

Detect Unknown and Insider Threats
Custom machine learning for early warning

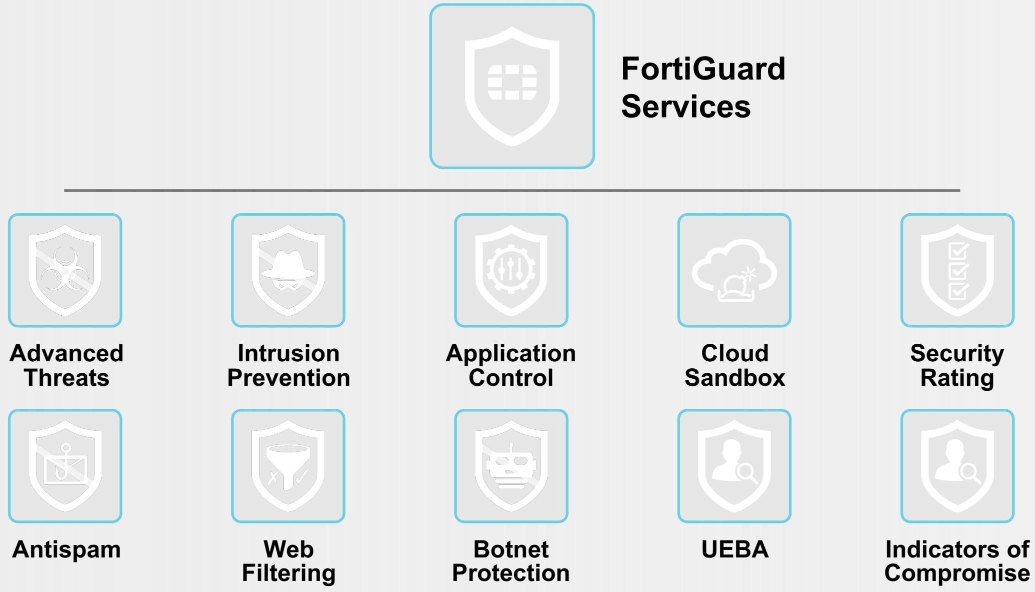
Orchestrate and Automate Response
Expert systems for faster containment



Predict and Prevent Attacks

Global machine learning for proactive defense

Legacy security products have fallen behind an evolving threat landscape. Next generation technologies, global intelligence and analytics, and AI-powered protection are required.



Zero Trust Network Access	Two-Factor Authentication	Dynamic Cloud Security

Detect Unknown and Insider Threats

Custom machine learning for early warning

There is growing recognition that 100% prevention is not possible given today's sophisticated threats. Organizations are investing in advanced detection capabilities to avoid breaches.

FortiDeceptor	**FortiSandbox**	**FortiInsight**
Identify Unknown Adversaries	Detect Unknown Malware	Uncover Insider Risk

Orchestrate and Automate Response

Expert systems for faster containment

Given the shortage of cyber security skills, organizations look to orchestrate and increasingly automate investigation/ response efforts.

FortiAnalyzer	**FortiSIEM**	**FortiSOAR**	**FortiAI**
Security Fabric Analytics	Multivendor Visibility	Guided Response	Virtual Analyst

AI-powered Security Operations - Endpoint

Predict and Prevent Attacks

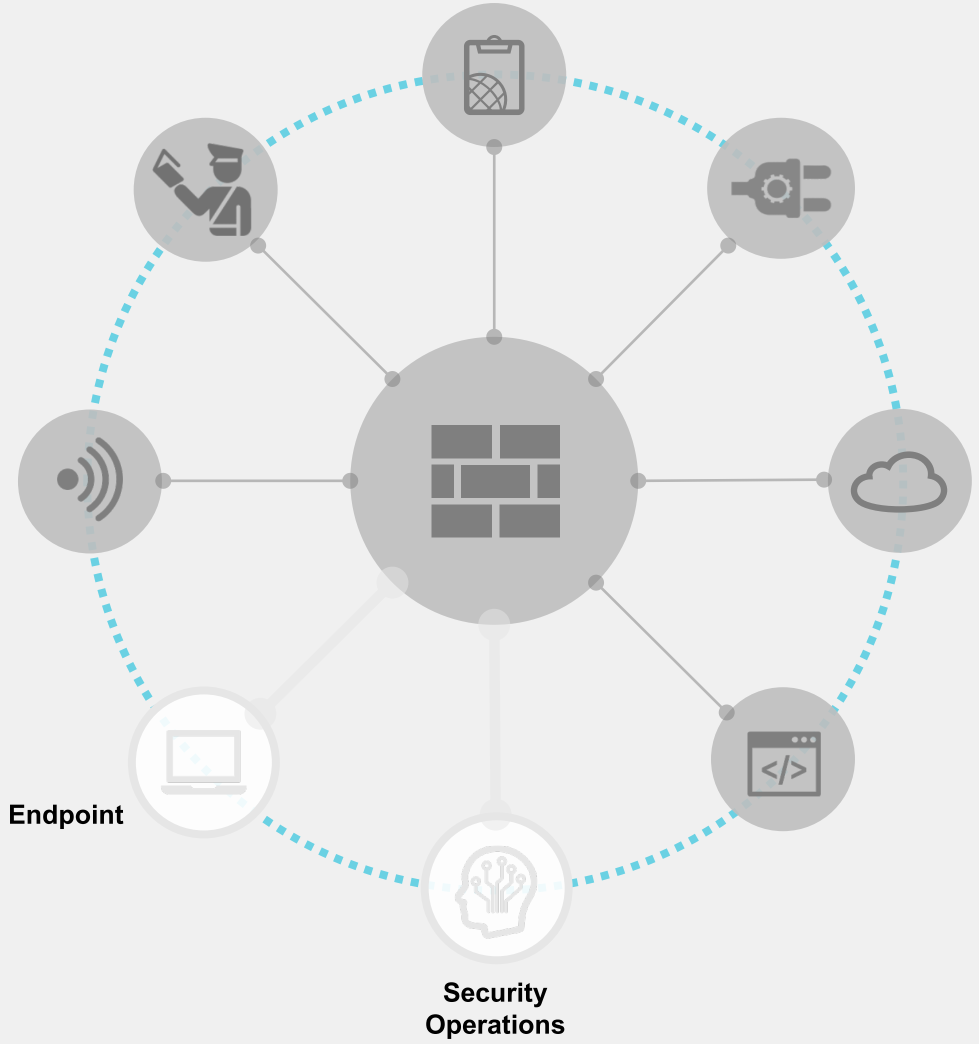
Attack surface reduction and malware prevention

Detect and Defuse Threats

Stop breaches with real-time detection & disarmament

Respond, Investigate & Hunt

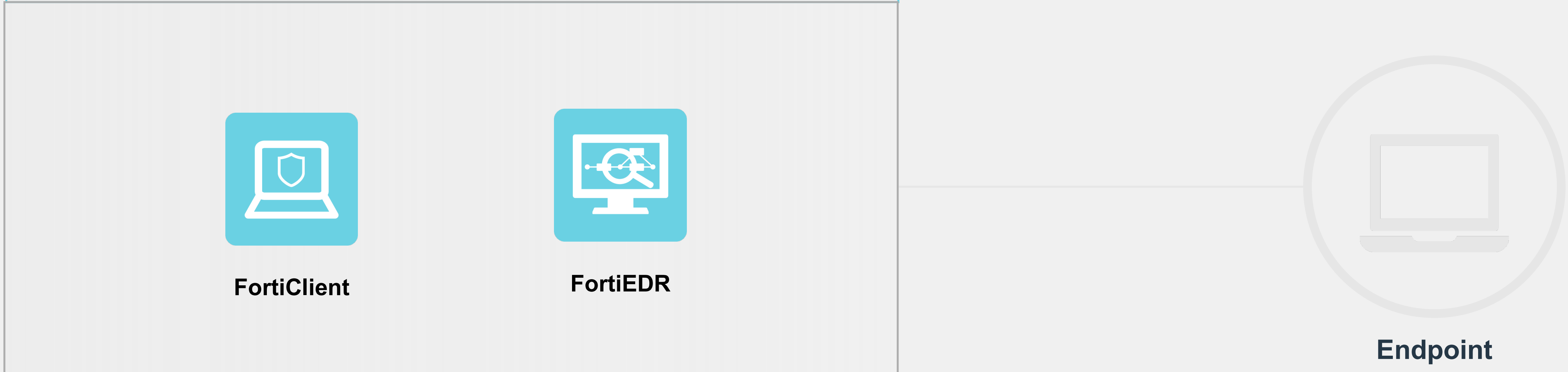
Orchestrated remediation and forensic investigation



Predict and Prevent

Attack Surface Reduction, Malware Prevention

For many reasons, IT and OT devices are not always up to corporate security standards for OS upgrades, patches and other configurations. Such systems become low hanging fruits for attackers.

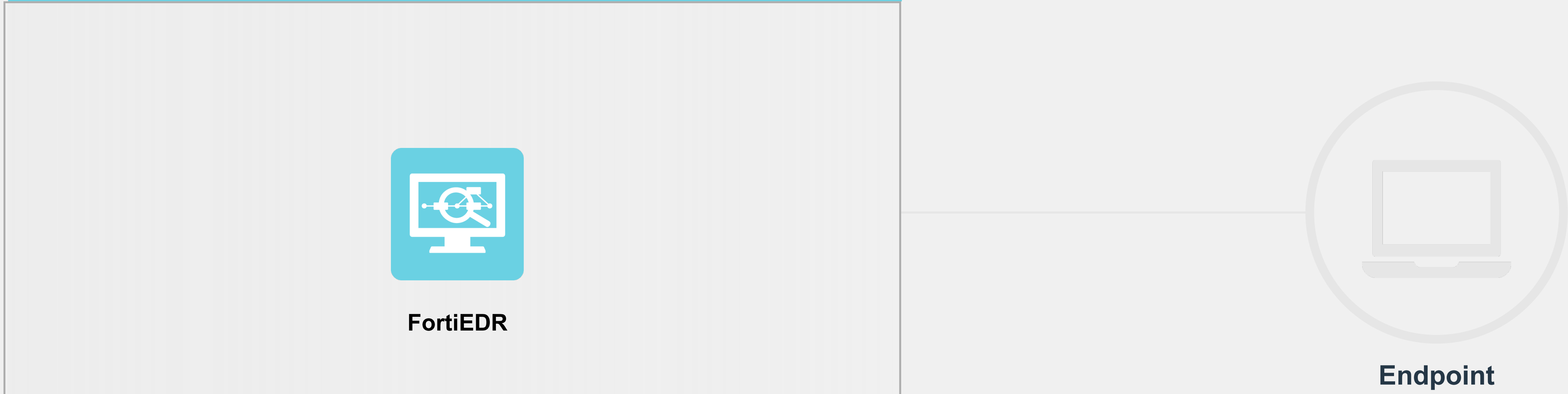


- Vulnerability scanning, patching, and virtual patching
- Exploit prevention
- Machine learning AV
- Support for air gapped environment

Detect and Defuse

Avoid breaches with real-time detection & disarmament

Prevention is not 100% due to increasingly sophisticated threats and attack methods, fileless malware, ransomware masquerades, and “living off the land attacks”.

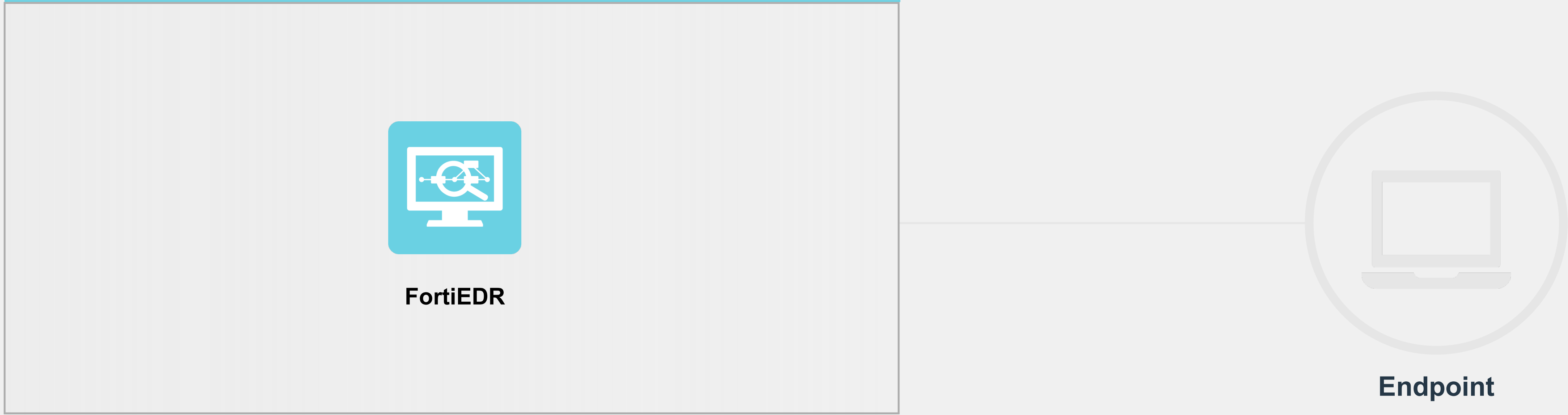


- Real-time detection and post-compromise protection
- Prevent file tampering and ransomware encryption
- Stop data exfiltration, C&C communication, and lateral movement

Respond, Investigate and Hunt

Orchestrated remediation and forensic investigation

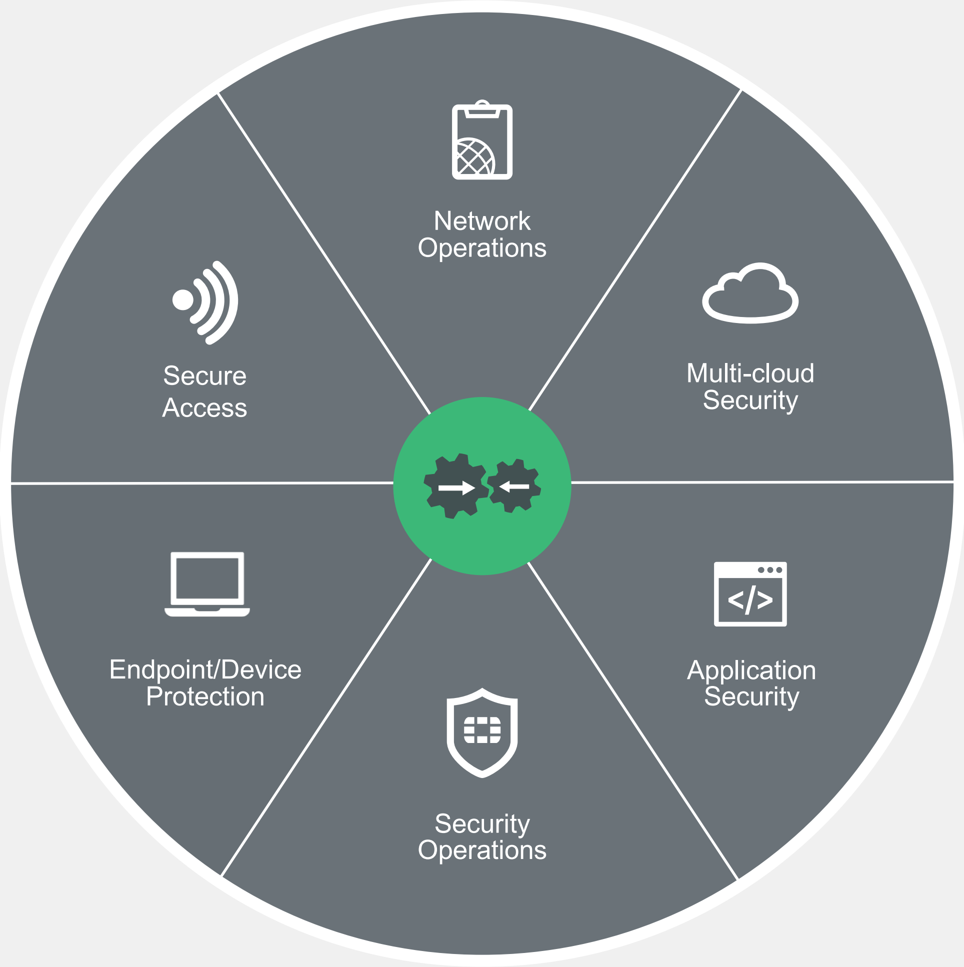
Cybersecurity skill shortage. Incident response is often manual, requires costly processes, and can interfere with business operation or employees productivity.



- Remediation without taking machine offline
- Risk-based threat response
- Remediation recipe for IT operations – no need to re-image
- Optional MDR for threat monitoring, alert triage, and response

Endpoint Ecosystem

Fabric API Partnerships with FortiClient



Fabric Connector

Symantec

Fabric API

AREA 1, Carbon Black., CIGENT, Infoblox, Lightspeed Systems, McAfee, MEDIGATE, OPSWAT, SentinelOne, VOTIRO SECURED., wandera, ziften

Fabric Management Center

Centralized Network Management

Single console management

Unified Application Management

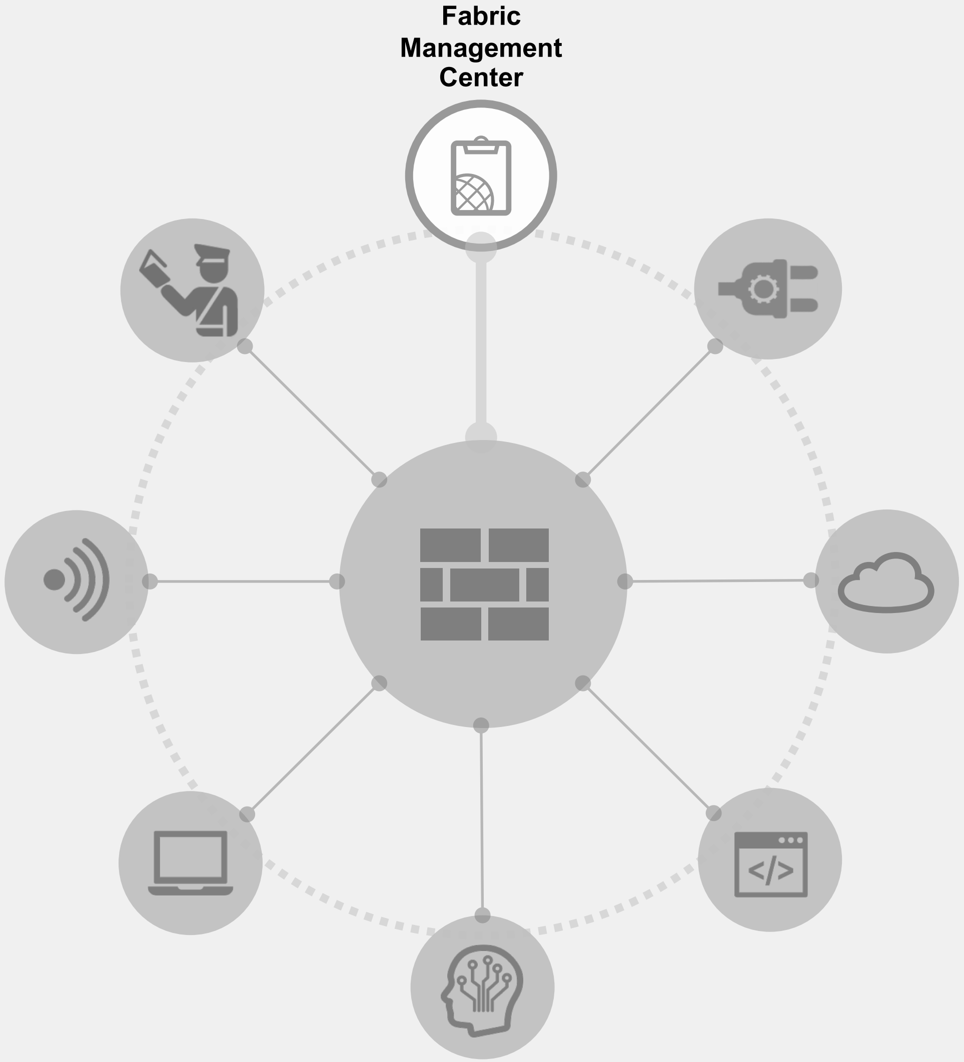
SSO across Security Fabric applications

Automation & Orchestration

Integrated workflows within Security Fabric

Network Analytics & Reporting

Real-time network insights and reporting



Fabric Management Center

Single console network management

Human errors and system glitches are a key root cause for network anomalies and cyber risks. Automation-driven network management is critical.

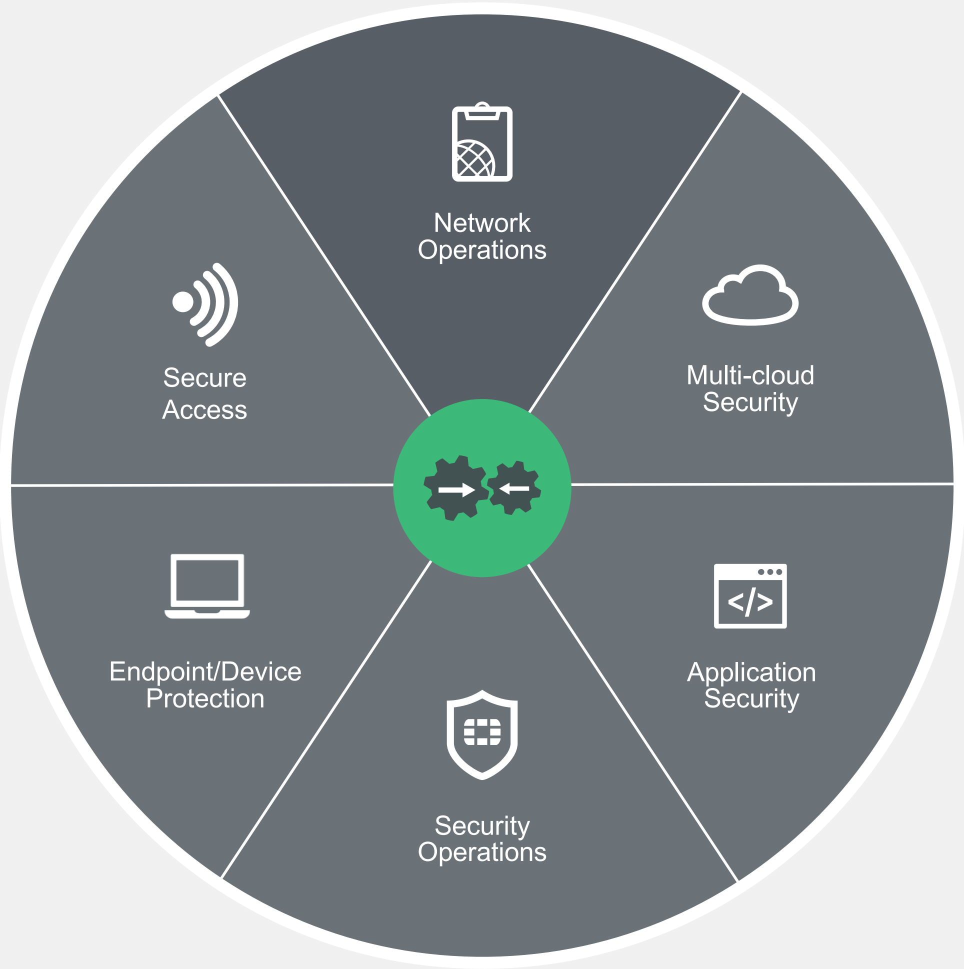
FortiManager

FortiGate Cloud

- Single console management, reporting, and analytics
- Automated workflows
- Central network monitoring

Network Operations Ecosystem

Fabric API Partnerships with FortiGate and FortiManager



Fabric API

algosec · appviewX · AREA 1 · ARISTA · auvik · BACKBOX · CASQUE SNR

Centrify · CSPi · chronicle · cyber OBSERVER · cyr3con · DELL · Eleven Paths

Edge Velocity Corporation · ERICOM · ERICSSON · Extreme · FIREMON · FIRESEC · Flowmon

FRIXTEL · Gigamon · HUGHES · indeni · Infoblox · infovista · intel · ixia

JASK · lightspeed · LiveAction · METTCARE · mistnet · MODE

NIAGARA NETWORKS · PICUS · REDSEAL · ribbon · SAASPASS · saasyan · SECLORE

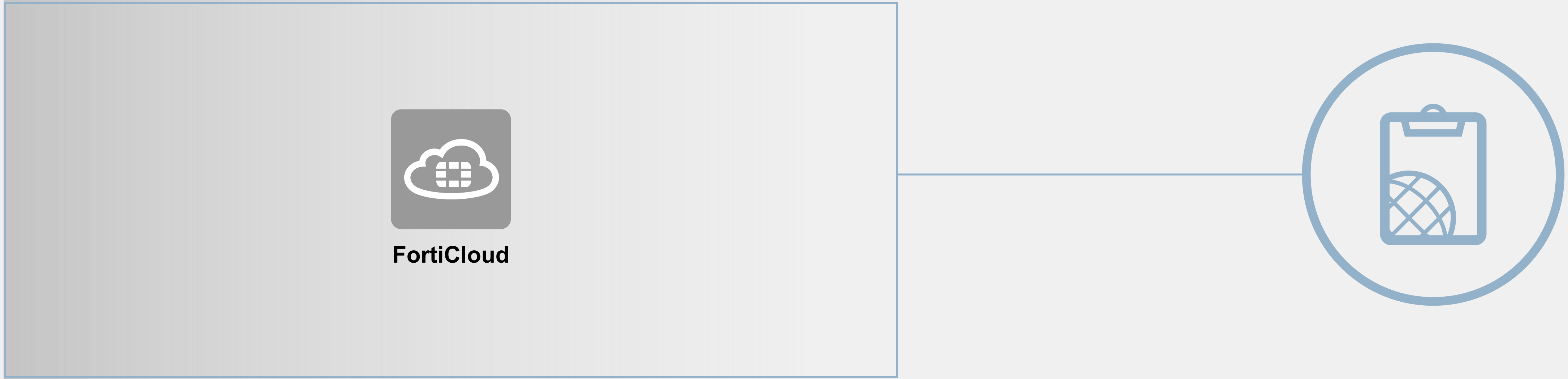
SKYBOX · smart hive · SMOKESCREEN · SYNCURITY · SYSCOM · TelcoBridges · Telco Systems

THREATQUOTIENT · TRAPX · TRUEFORT · tufin · VOIP.MS · WIND RIVER · ZERO NINES

Fabric Management Center

Simple access for all Fortinet cloud services

Customers leveraging multiple cloud services require a single point of access and single sign-on (SSO) to simplify user experience and reduce complexity.



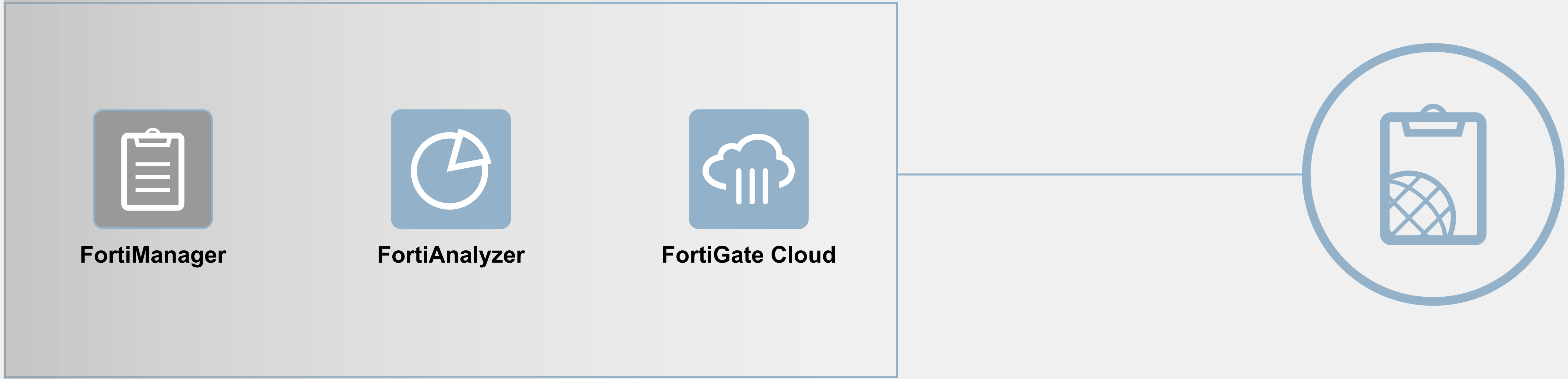
FortiCloud

- Single sign-on (SSO)
- Portal to 15 Fortinet SaaS and MaaS services
- FortiCare Services Portal

Fabric Management Center

Automation & orchestration

Consolidation of point products is happening across verticals. Leveraging a single console to manage, orchestrate, and automate the point products is critical.



- Add-on controllers
- Fabric topology
- Connectors and integrations

Fabric Management Center

Network analytics & reporting

Real-time network analytics is hard to achieve when it’s not an integral part of the Security Fabric. Integrated analytics is required for real-time network analytics.

FortiAnalzyer

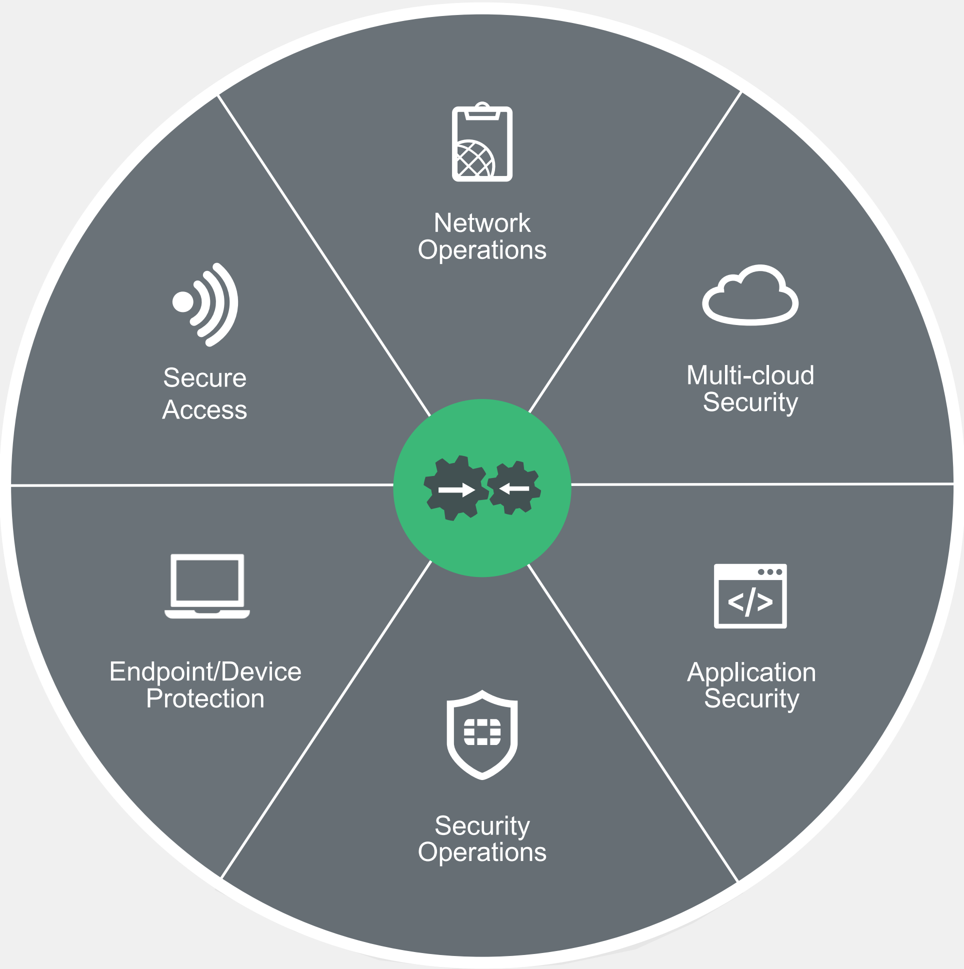
FortiGate Cloud

FortiManager

- Real-time network insights and health
- Network log management
- Compliance reporting

Security Operations Ecosystem

Fabric API Partnerships with FortiSandbox, FortiAnalyzer, and FortiSIEM



Fabric Connector

servicenow

Fabric API

Attivo Networks · BROCADE · CITRIX · CYBERARK

D3 SECURITY · graylog · INTSIGHTS · METTCARE Techn o | o gies

rubrik · SAFE-T Smart Security Made Simple. · safetica · SECLYTICS Accurate · Verifiable · Attack Predictions

Siemplify · splunk> · spirent Promise. Assured. · STRATOZEN

SWIMLANE · ThreatConnect · TRAPX SECURITY · vijilan IT Security. Enabled.

Open Fabric Ecosystem

Fabric Connectors

Fortinet-developed deep integration automating security operations and policies

Fabric API

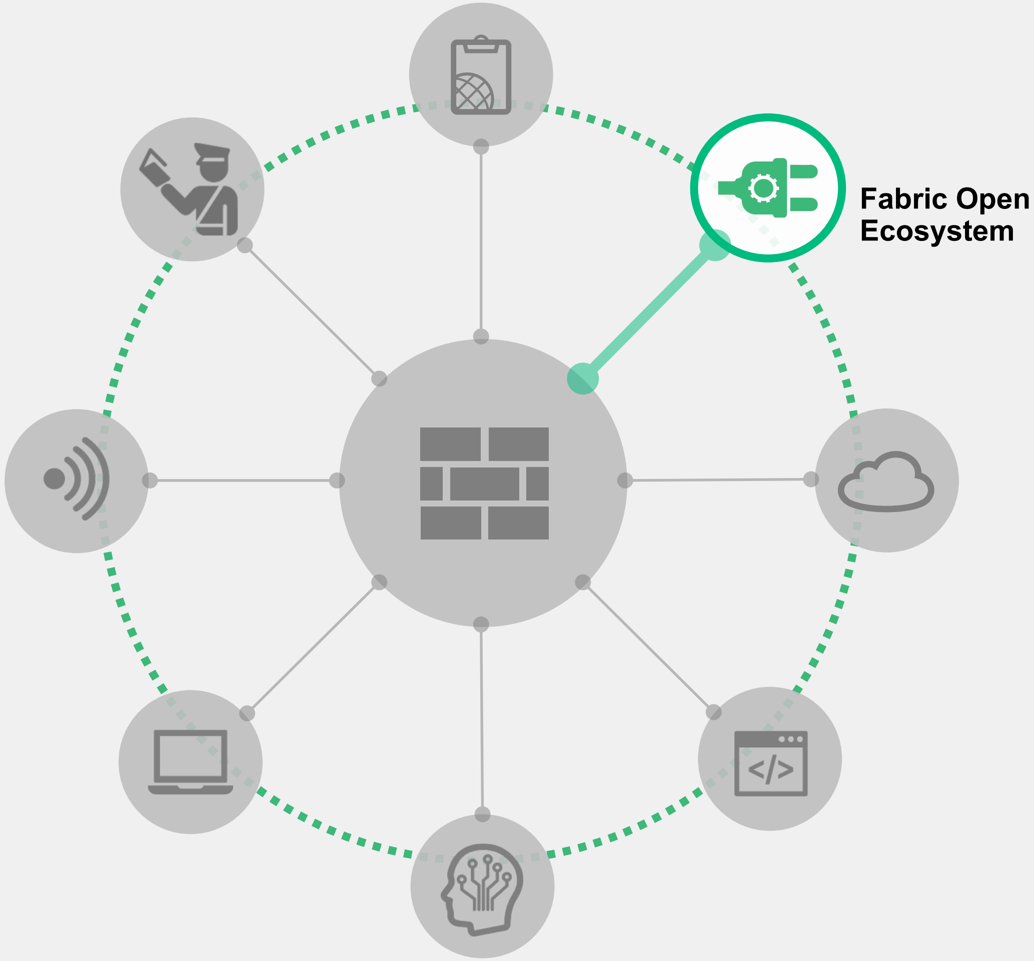
Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

Fabric DevOps

Community-driven DevOps scripts automating network and security provisioning, configuration, and orchestration

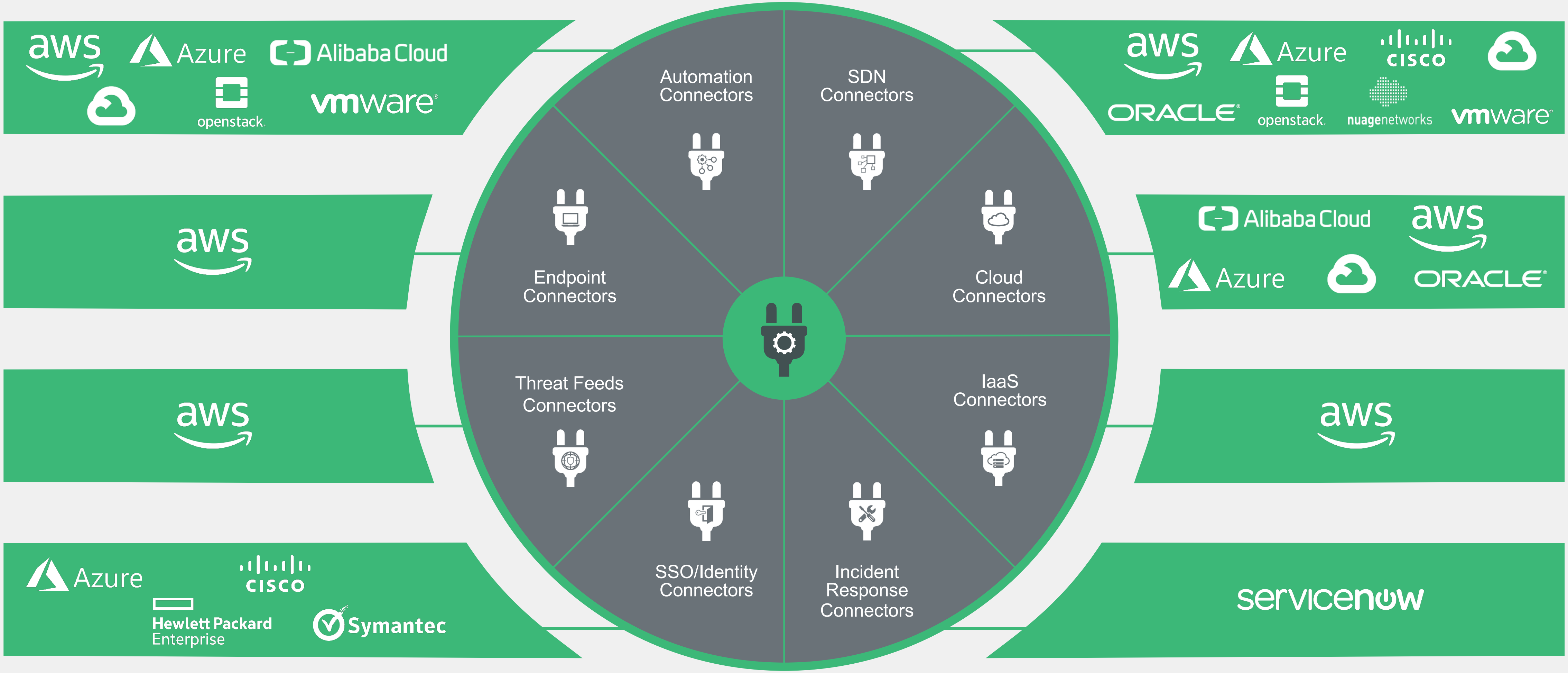
Extended Fabric Ecosystem

Collaboration with threat-sharing initiatives and other vendor technology integrations



Fabric Connectors

Fortinet-developed deep integration into customer ecosystem platforms



Extensive Industry Cybersecurity Ecosystem

250+ Security Fabric Ecosystem integrations

Fabric Connectors (12)

Fortinet-developed deep integrations that automate security operations and policies

Alibaba Cloud aws aruba a Hewlett Packard Enterprise company CISCO Google Cloud Azure ORACLE Symantec. vmware

Fabric APIs (135+)

Partner-developed integrations using Fabric APIs that provide broad visibility with end-to-end solutions

ABB ARISTA DELL IBM intel Lenovo Lightspeed Systems NOZOMI NETWORKS splunk> TANIUM TIGERA

Fabric DevOps (9)

Community-driven DevOps scripts that automate network and security provisioning, configuration, and orchestration

Alibaba Cloud aws Google Cloud HashiCorp Terraform Azure openstack RED HAT ANSIBLE TOWER vmware

Extended Security Fabric Ecosystem (130+)

Collaboration with threat-sharing organizations (30+) and integrations with other vendor products (100+)

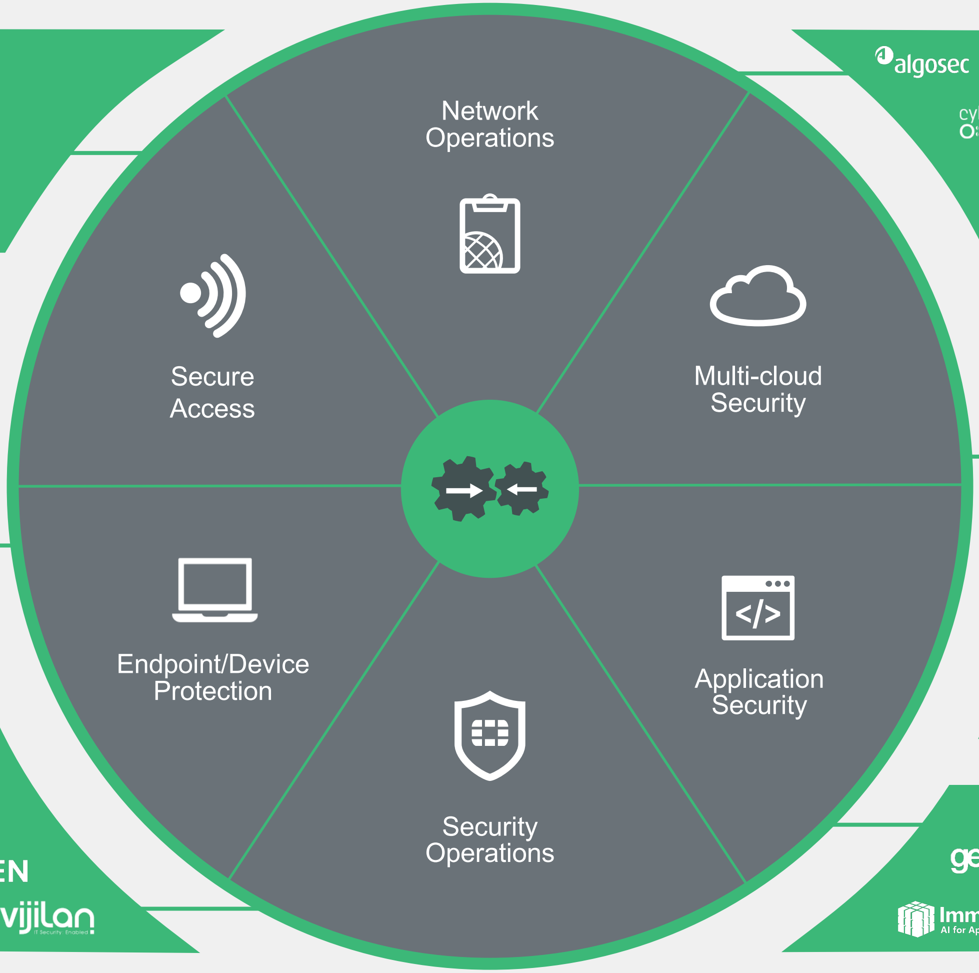
CYBER THREAT ALLIANCE MITRE STIX INTERPOL OT CSA

Firewalls Switching Wireless Endpoint Security

Note: Logos are a representative subset of the Security Fabric Ecosystem

Fabric APIs

End-to-End security solutions with complementary integrations



Network Operations

Multi-cloud Security

Application Security

Security Operations

Endpoint/Device Protection

Secure Access

cyglass Extreme networks FORESCOUT ixia Pulse Secure Gigamon Restorepoint

AREA 1 Carbon Black. CASQUE SNR CLAROTY CyberX DRAGOS Edge Velocity Corporation ENSILO eset Indegy Infocyte McAfee MEDIGATE NOZOMI NETWORKS OPSWAT SCADAfence SentinelOne SIEMENS RAD data communications VOTIRO SECURED wandera ziften

Attivo NETWORKS BROCADE CITRIX CYBERARK D3 SECURITY INTSIGHTS METTCARE Technologies rubrik SAFE-T safetica SECLYTICS Siemplify splunk> spirent STRATOZEN SWIMLANE ThreatConnect TRAPX SECURITY vijilan

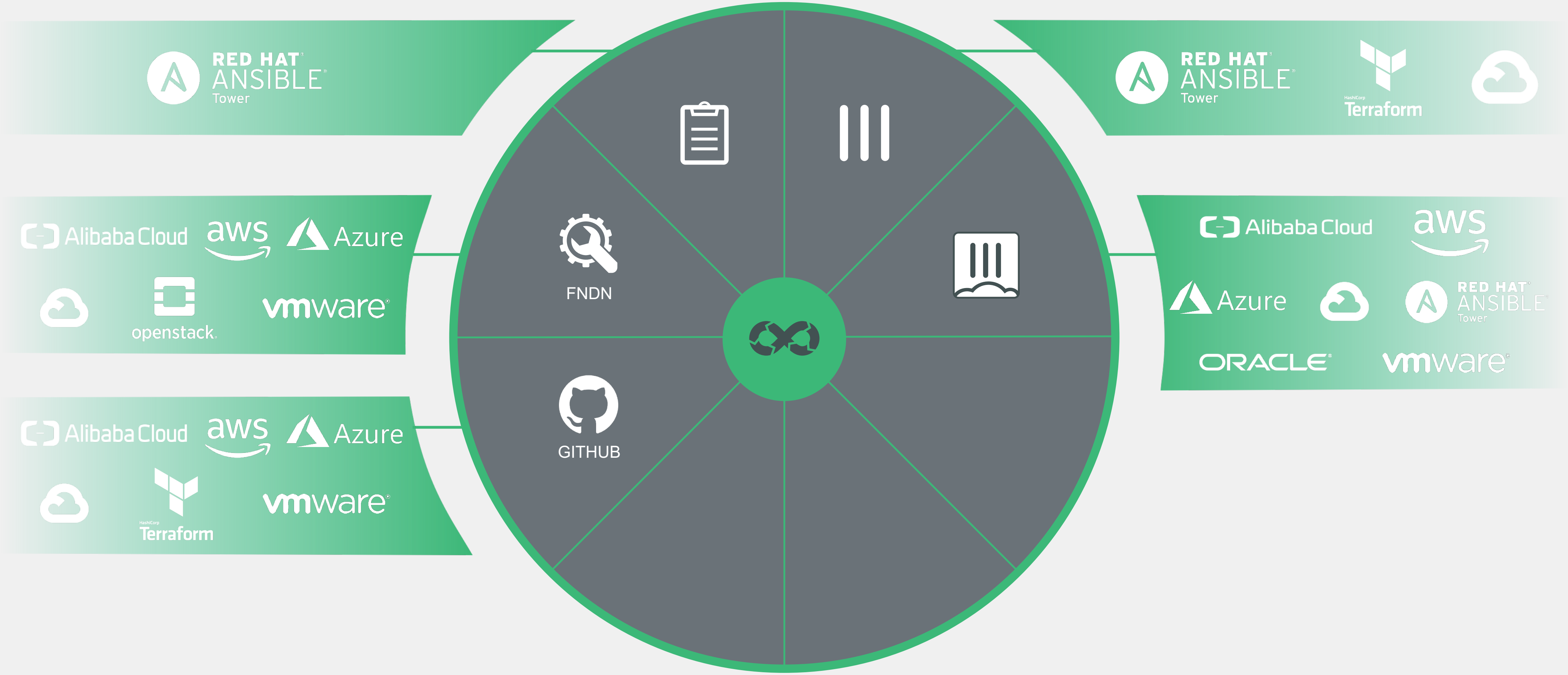
algosec appviewX ARISTA auvik BACKBOX Centrify CSPi chronicle cyber OBSERVER cyrecon DefendEdge Eleven Paths ERICOM ERICSSON FIREMON FIRESEC Flowmon FRIXTEL Service Provider Solutions HUGHES Infoblox infovista intel JASK lightspeed METTCARE Technologies mistnet PICUS REDSEAL ribbon SAASPASS saasyan SECLORE SKYBOX SECURITY SMOKESCREEN SYNCURITY SYSCOM THREATQUOTIENT TRUEFORT tufin WIND RIVER ZERO NINES

ADVA alcide amdocs big switch networks CLOUDIFY corsa ENEA HYTRUST IBM Lenovo NOKIA NEC Alcatel·Lucent MODE NoviFlow NUTANIX Pluribus NETWORKS Telco Systems A BATM Company TelcoBridges UBiqube

atarlabs CYBERSPONSE DFLABS gemalto security to be free illapa IMAGE ANALYZER ImmuniWeb AI for Application Security MICRO FOCUS Qualys WhiteHat SECURITY

Fabric DevOps

Off-the-shelf scripting automation



Extended Security Fabric Ecosystem

Threat-sharing partnerships and other vendor technology integrations

CYBER THREAT ALLIANCE

Co-founded by Fortinet

CYBER THREAT ALLIANCE

For enabling near real-time, high-quality cyber-threat information sharing among cybersecurity companies and organizations

COMMUNITY-SUPPORTED STANDARD

CSSC

JC3 Japan Cybercrime Control Center

OASIS

STIX

TAXII

MITRE

Defining industry standards and protocols for automating information sharing, complex analysis, and real-time defense

ENTERPRISE TECHNOLOGY LEADERS

Adobe

IBM

Microsoft

verizon

For timely response to application vulnerabilities, threats, and trends

COMPUTER EMERGENCY RESPONSE TEAMS

US-CERT United States Computer Emergency Readiness Team

FIRST Improving Security Together

HKCERT

MyCERT Malaysia Computer Emergency Response Team

CERT-EU computer emergency response team for the EU institutions, bodies and agencies

certego

UNAM CERT

KISA

NCCST

FINANCIAL SERVICES Information Sharing and Analysis Center

Financials ISAC Japan

For timely disruptions of cyber campaigns and threat actors

LAW ENFORCEMENT AND GOVERNMENT

InfraGard

U.S. Department of Homeland Security

INTERPOL

NCCIC

CISCP & NCCIC

NCI Agency

NATO

certnz

San Francisco Electronic Crimes Task Force

Canadian Cyber Threat Exchange

Sharing cyber data for disrupting nation-state and advanced cyber criminals in action to improve and advance the security efficacy of the digital ecosystem

Integrations With 100+ Other Vendor Technologies

- Firewall
- Endpoint Security
- Switching
- Wireless
- Mobile Device

… and more

Integrations that ensure Fortinet solutions work well with other vendor products in your infrastructure

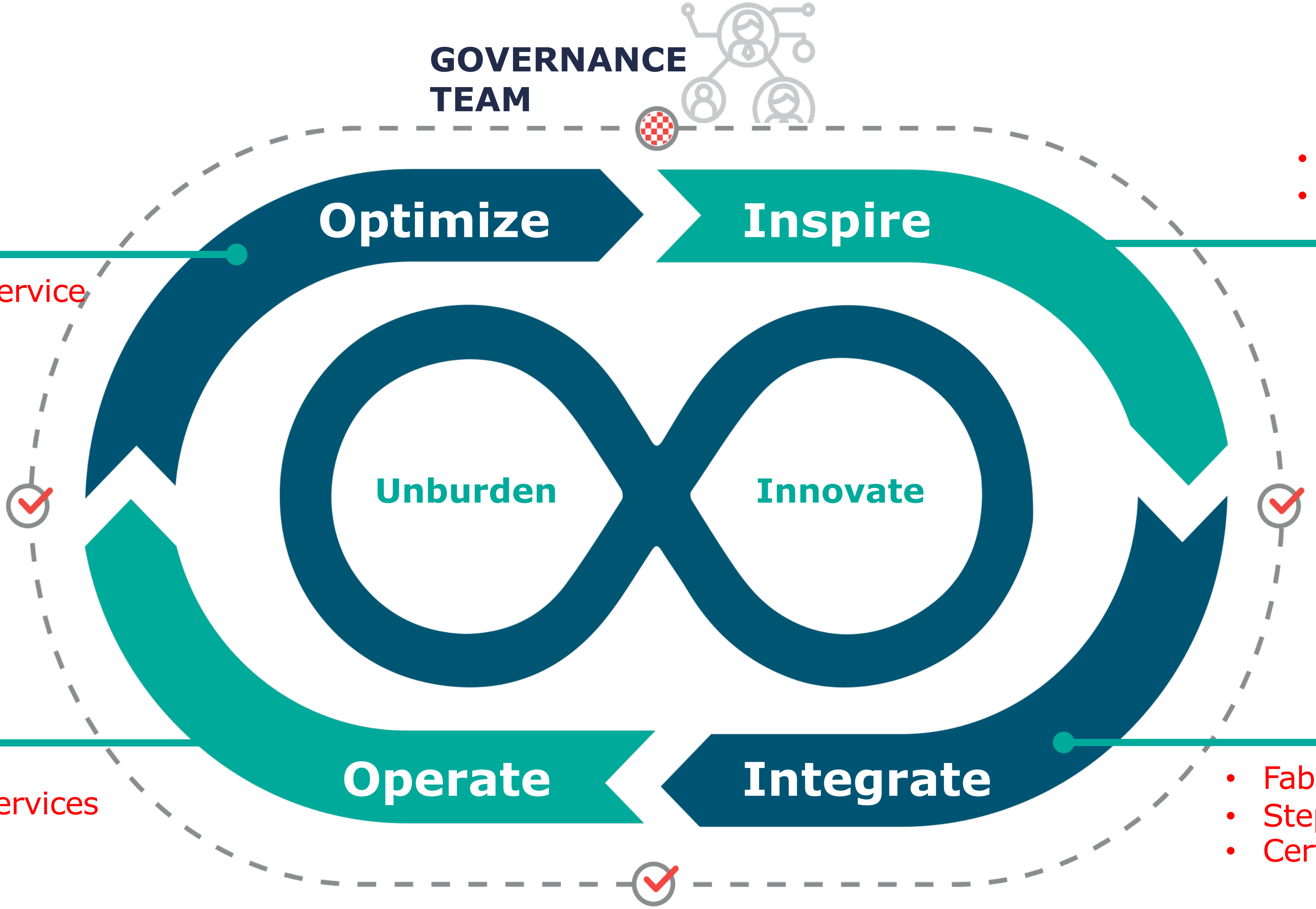
Extended Fabric Ecosystem

Integrations with other technology vendors

TECHNOLOGY VENDORS

- 3Com
- Access Credentials
- Adtran
- Aerohive
- AirWatch
- Alert Logic
- Allied Telesis
- Alteon
- Apache Tomcat
- APC NetBotz
- Apple
- Authentium
- Avast
- Avaya
- AVG
- Avira
- Barracuda Networks
- Bit9
- Blink
- Box.com
- BullGuard
- CA
- Check Point
- ClamAV
- CloudPassage
- Colubris
- CrowdStrike
- Cylance
- Cyphort
- Cyxtera AppGuard
- Damballa
- Dell SonicWall
- Digital Guardian
- Dropbox
- D-Link
- Dr. Web
- EMC
- Enigma
- Enterasys
- F5
- FireEye
- Foundry Networks
- F-PROT
- F-Secure
- G DATA
- GitHub
- Green League
- H3C
- Imperva
- Intego
- Javacool
- Juniper Networks
- Lantronix
- Lastline
- Lavasoft
- Open LDAP
- Liebert
- Lightspeed
- Linux Server
- LiveAction
- MaaS360
- Malwarebytes
- Medigate
- MicroWorld
- MikroTik
- MobileIron
- Motorola
- MySQL
- Nessus
- NetApp
- Nginx
- Nimble
- Norman
- Nortel
- Norton
- Okta
- One Identity
- PacketFence
- Palo Alto Networks
- PC Tools
- QNAP Turbo NAS
- Radiflow
- Radius
- Radware
- Rapid7
- Rising
- Riverbed Accelerator
- Ruckus
- Smart Hive
- Snort
- Softwin
- Sophos
- Spyware Bot
- SSH Comm Security
- StackRox
- Sun Solaris
- Sunbelt
- Tenable
- Trend Micro
- VASCO DIGIPASS
- Vexira
- Webroot
- WatchGuard
- Websense
- ZoneAlarm
- XenMobile
- Xirrus
- XYLink

…and other technology vendors and standards groups



- Fabric Fast Track
- Security Roadmap

- Security Fabric as a Service

- Fortinet Managed Services

- Fabric implementation
- Step by step
- Certified engineers

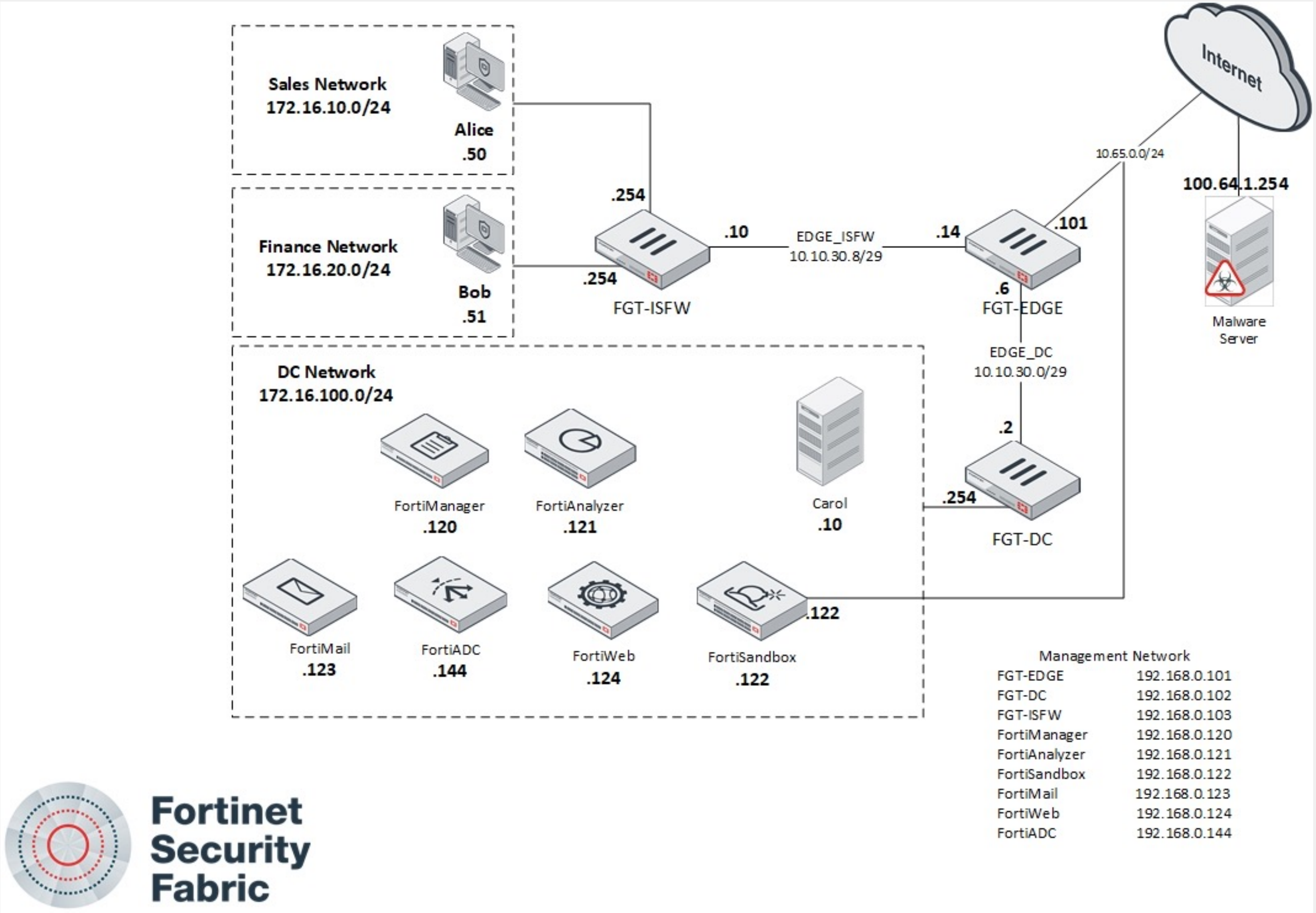
Contacteer ons via:

- info@realdolmen.com
- Uw vertrouwde contactpersoon bij Inetum-Realdolmen
- Evaluatieformulier

Google “realdolmen fortinet **podcast**”

Lab Exercise

Network Diagram



Management Network

FGT-EDGE	192.168.0.101
FGT-DC	192.168.0.102
FGT-ISFW	192.168.0.103
FortiManager	192.168.0.120
FortiAnalyzer	192.168.0.121
FortiSandbox	192.168.0.122
FortiMail	192.168.0.123
FortiWeb	192.168.0.124
FortiADC	192.168.0.144

Fortinet Fast Track Lab credentials

- **Course link**:

https://training.fortinet.com/course/view.php?id=14560

- **Enrolment key**: fef5fb8844

FORTINET®