IT ti

integragroup

Security Fabric

Marko Ugrin, Integra Group

Ivan Galinac, Integra Group

Rujan 2020.

Security Fabric

- Što je Security Fabric i koje probleme rješava?
- Komponente Fortinet Security Fabrica
- Scenariji primjene
- Demo
- Q&A

Ciljevi sigurnosne infrastrukture?

Zero-trust Network Access

Identify and secure users and devices, on and off network

Security-driven Networking

Secure and accelerate the network and user experience

Dynamic Cloud Security

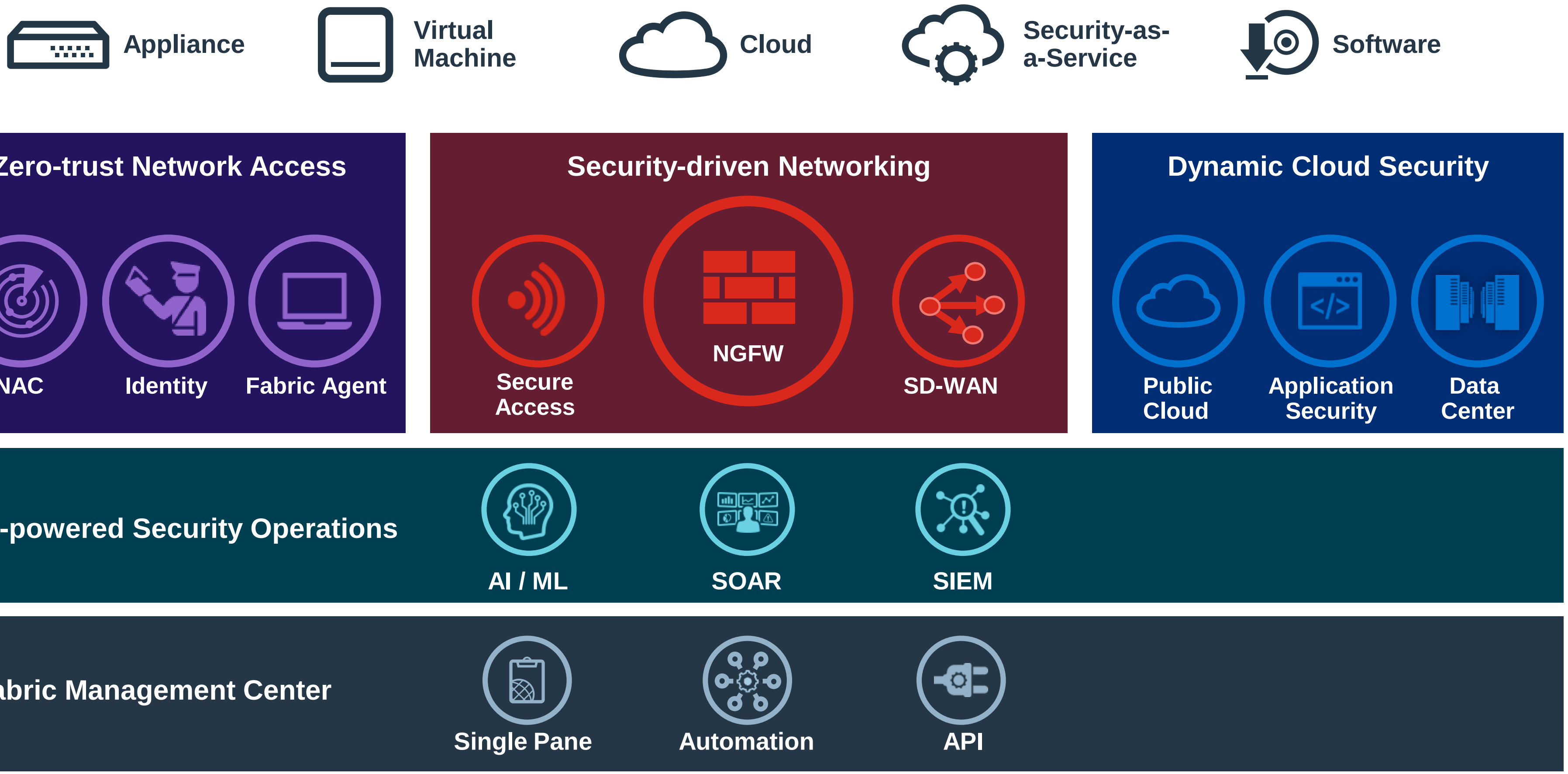
Secure and control cloud infrastructure and applications

AI-powered Security Operations

Automatically prevent, detect, and respond to cyber threats

Fortinet Security Fabric

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

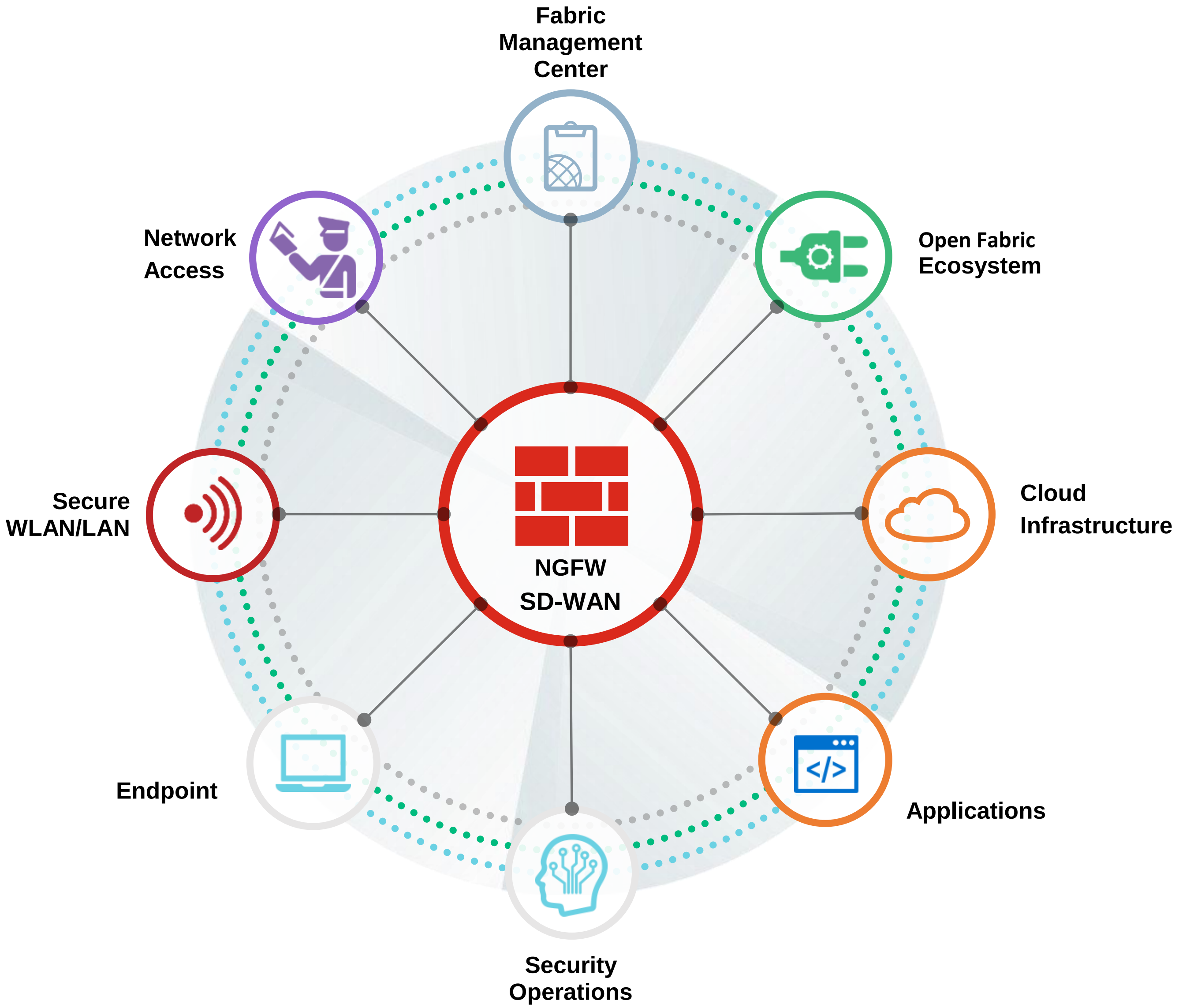
visibility of the entire digital attack surface to better manage risk

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

FortiClient Fabric Agent

FortiAuthenticator

FortiAP

FortiSwitch

FortiExtender

FortiGate

FortiGate VM

FortiCWP

FortiWeb

FortiMail

FortiCASB

FortiADC

FortiClient

FortiEDR

FortiAnalyzer

FortiSIEM

FortiSandbox

FortiSOAR

FortiManager

FortiGate Cloud

FortiCloud

FortiGuard Services

Network Security

Next-generation Firewall

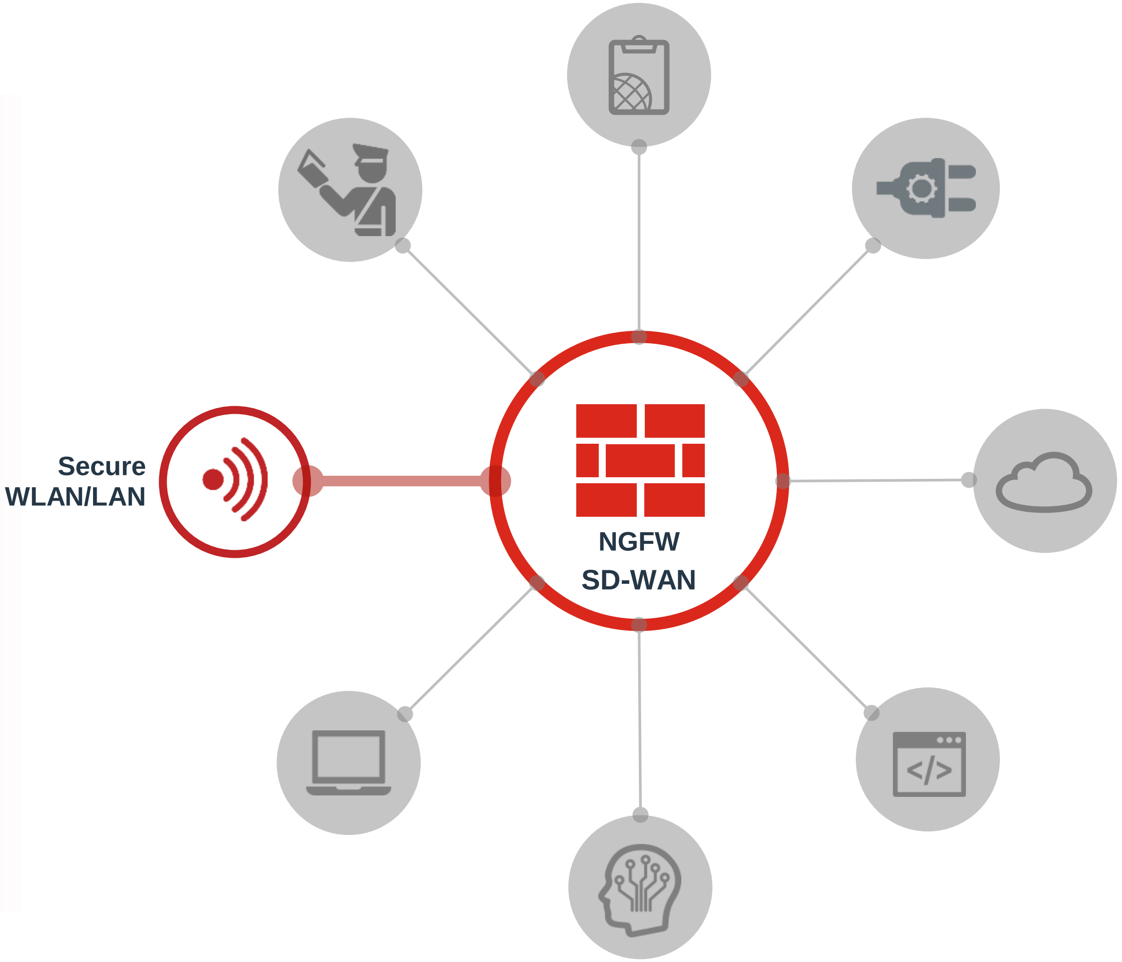
Manage all security risks & protect hyperscale

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.

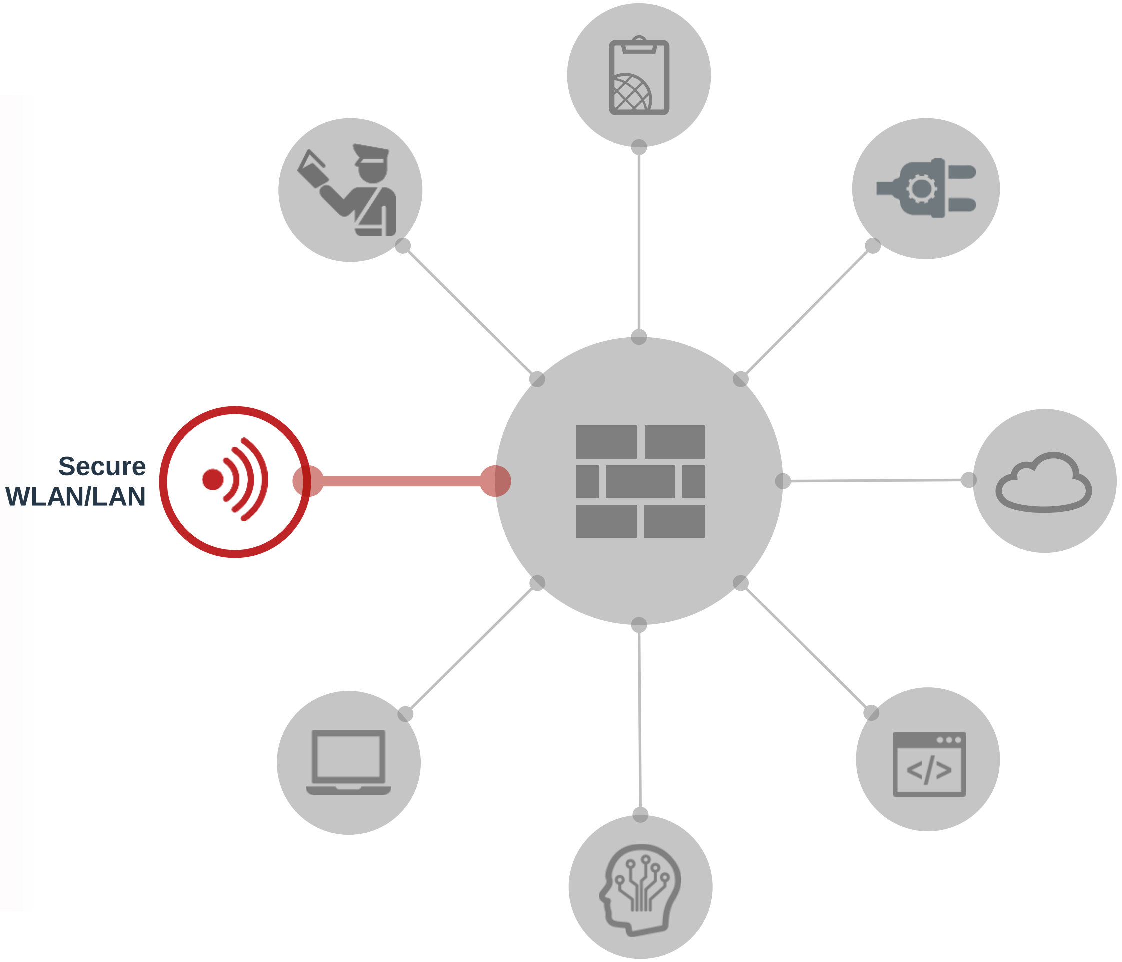
FortiGate
SWG
NGFW

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

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

Fabric Management Center

FortiManager

Simplified Provisioning

Centralized Management

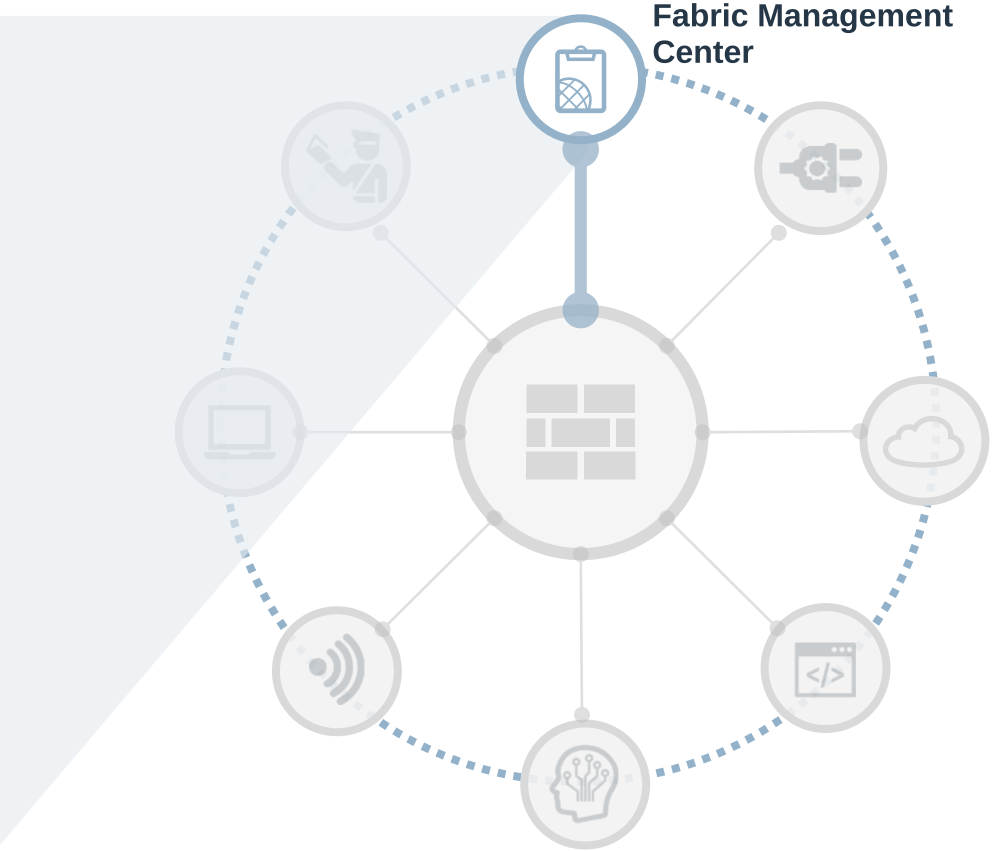
FortiAnalyzer

Security Fabric Analytics

Compliance Reporting

Network Automation

FortiManager & FortiAnalyzer



Fabric Management Center

Demo

- Security Fabric Visibility
- Security Rating
- Security Fabric konektori

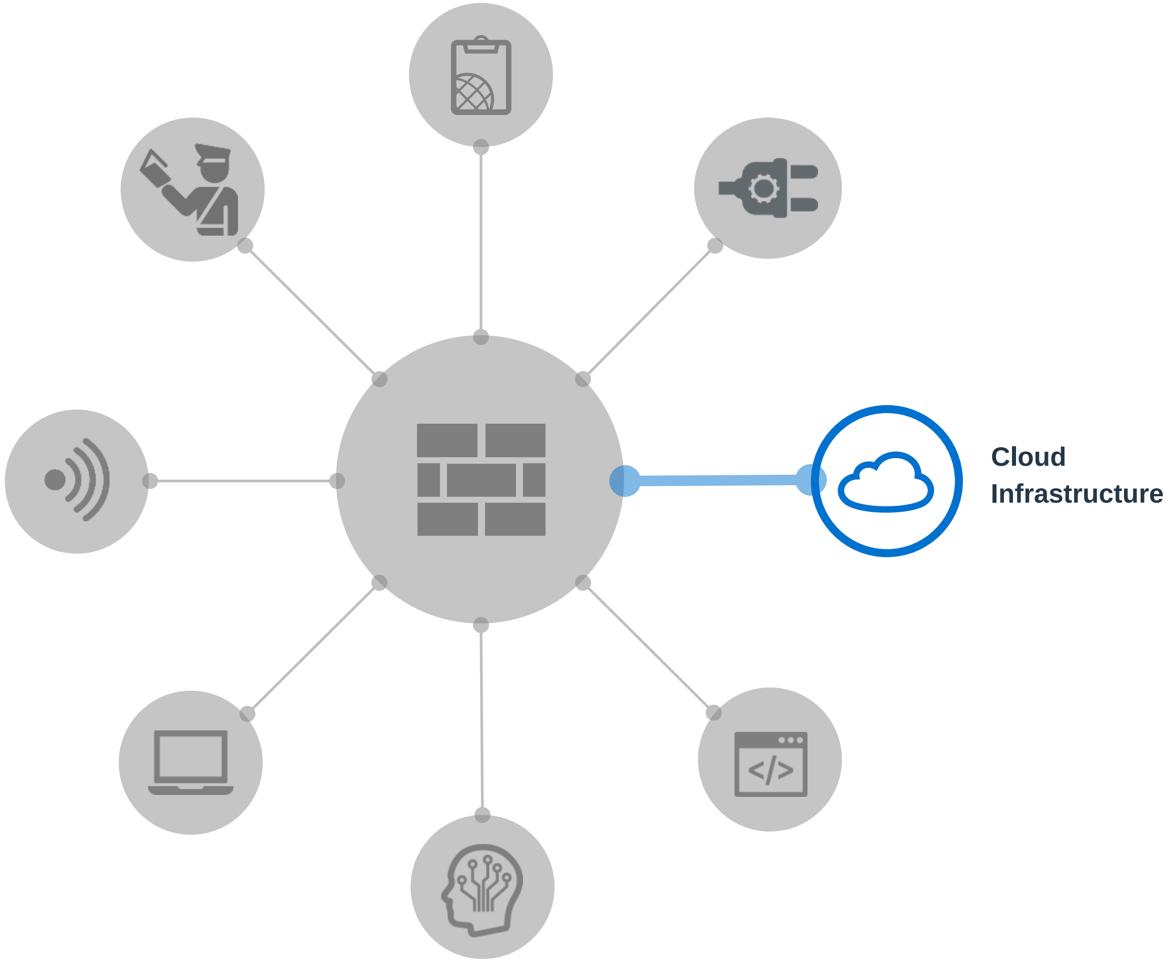
Dynamic Cloud Security

Public Cloud Infrastructure

Security for Compute & Applications Built in the Cloud

Private Cloud & SDN

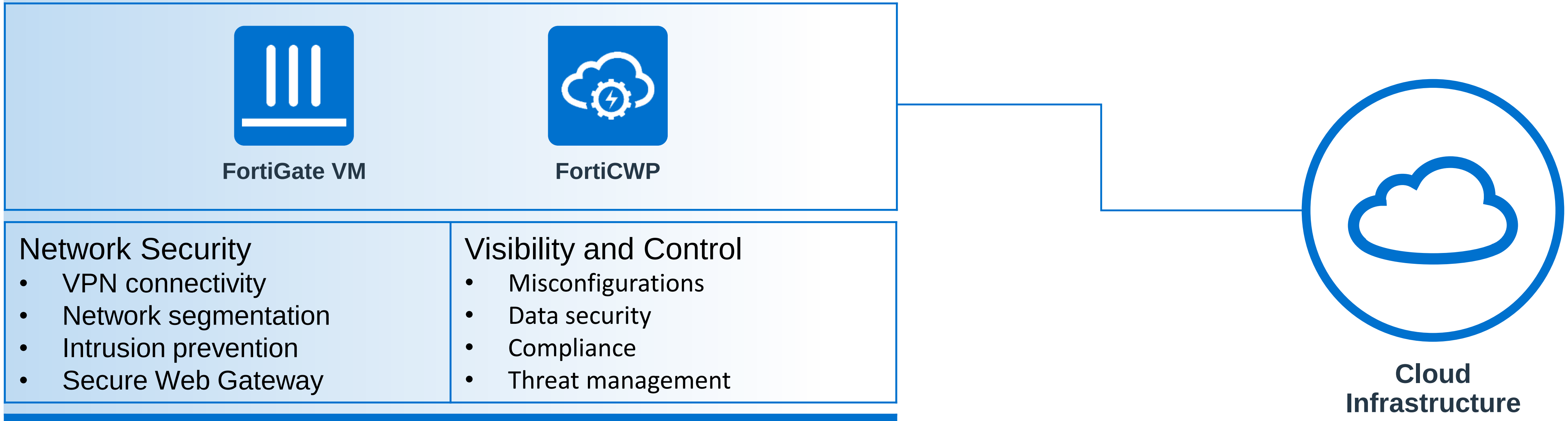
Security Automation & Integration for Private Clouds



Dynamic Cloud Security

Public cloud infrastructure, Private Cloud, SDN

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



FortiGate VM

FortiCWP

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

Visibility and Control
- Misconfigurations
- Data security
- Compliance
- Threat management

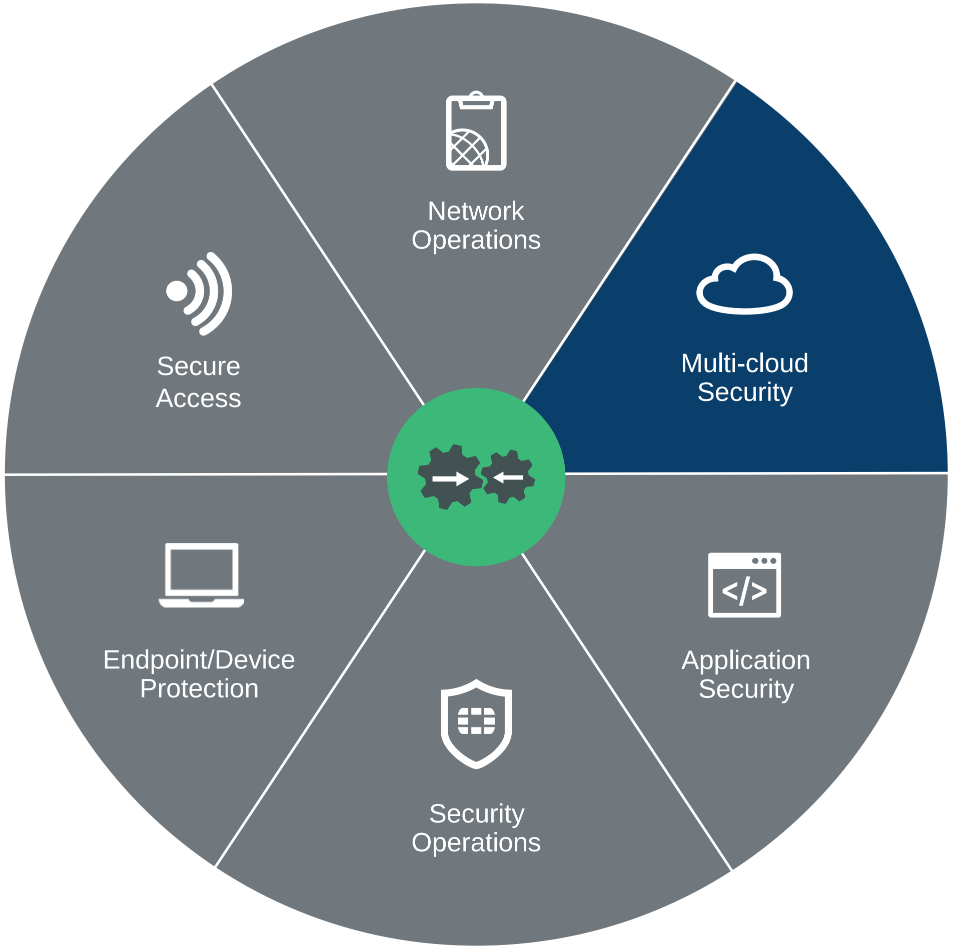
Cloud Infrastructure

aws Google Cloud Platform Microsoft Azure

Alibaba Cloud ORACLE IBM

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

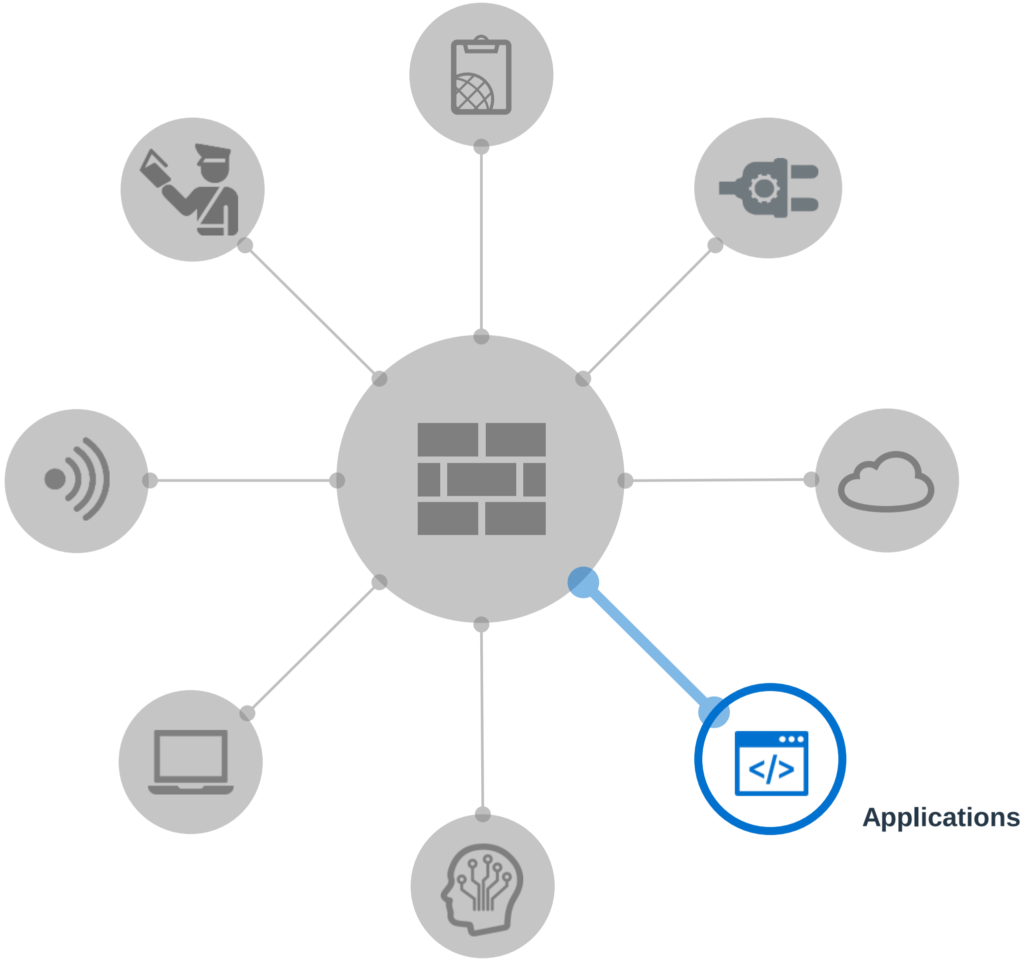
Securing web applications and APIs from application layer attacks

Email Security

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

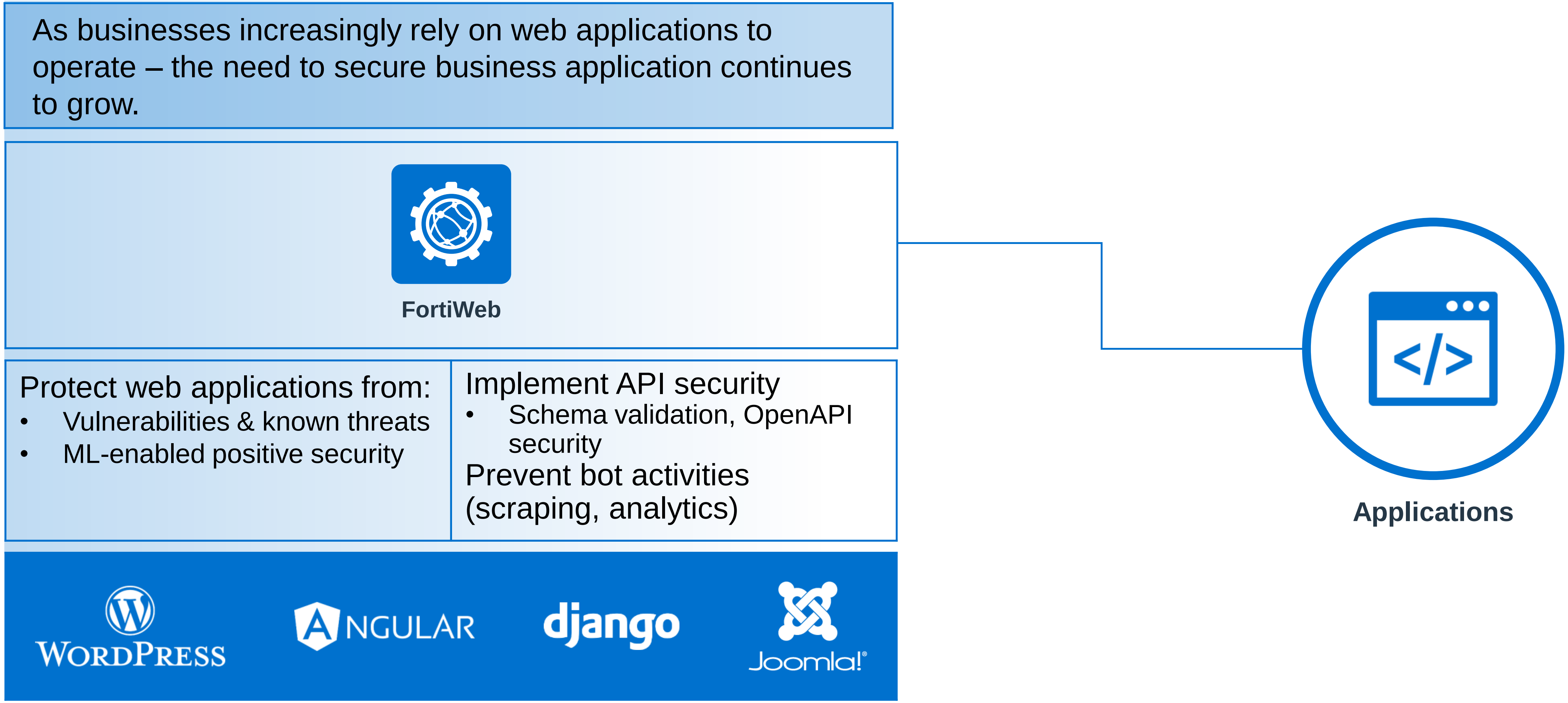
SaaS Security

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.

Protect web applications from:

- Vulnerabilities & known threats
- ML-enabled positive security

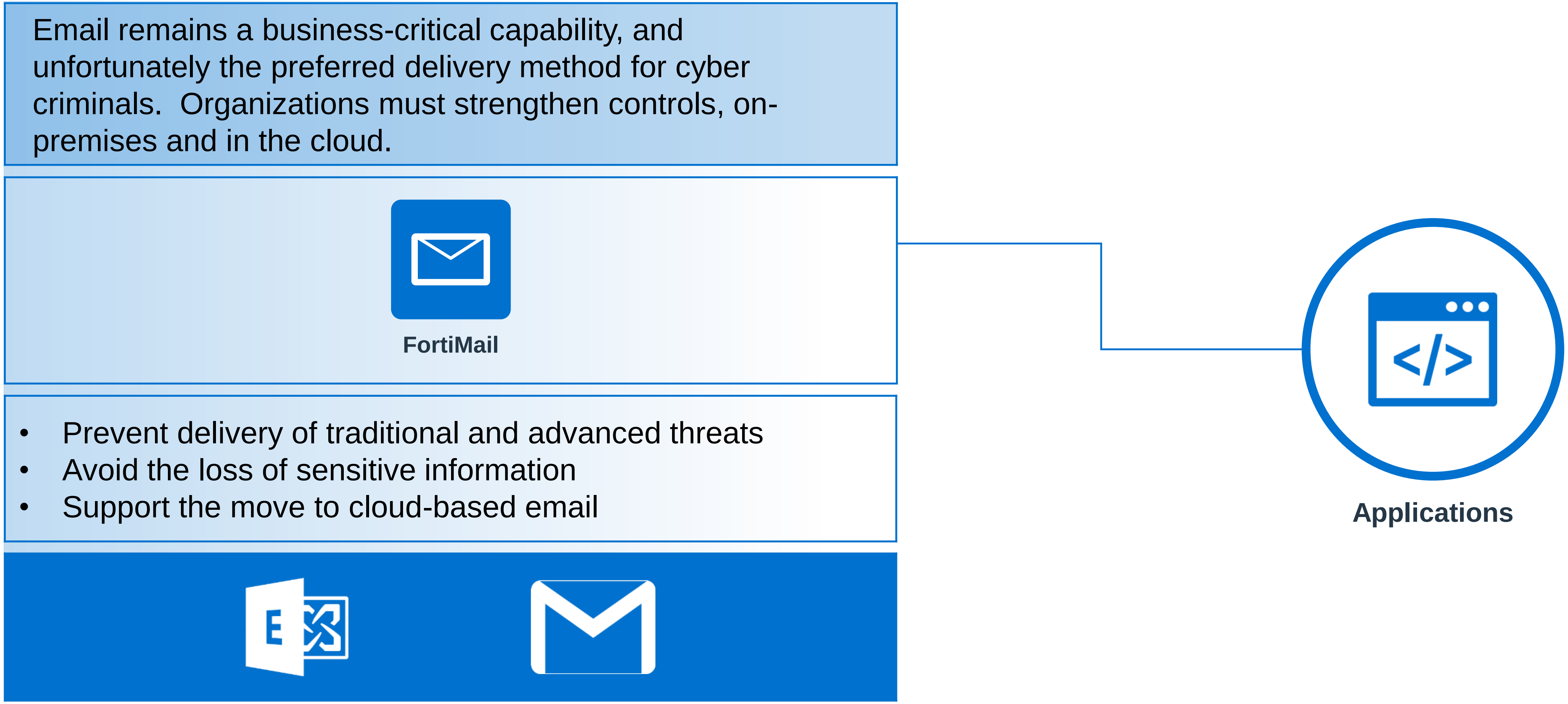
Implement API security

- 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

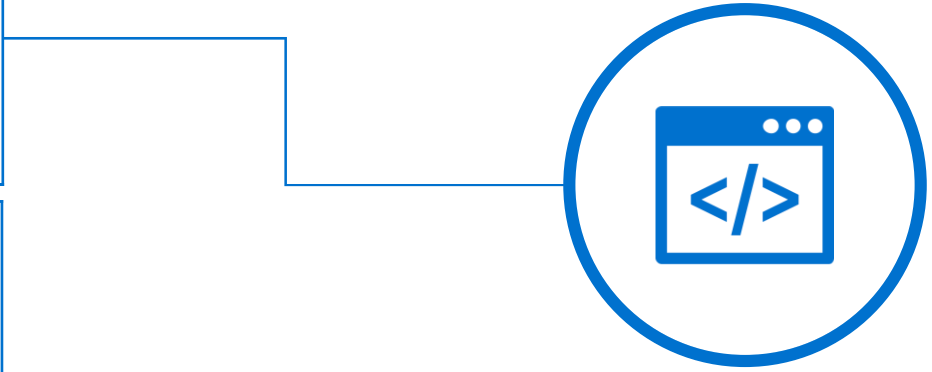
SaaS security

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

FortiCASB

- 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

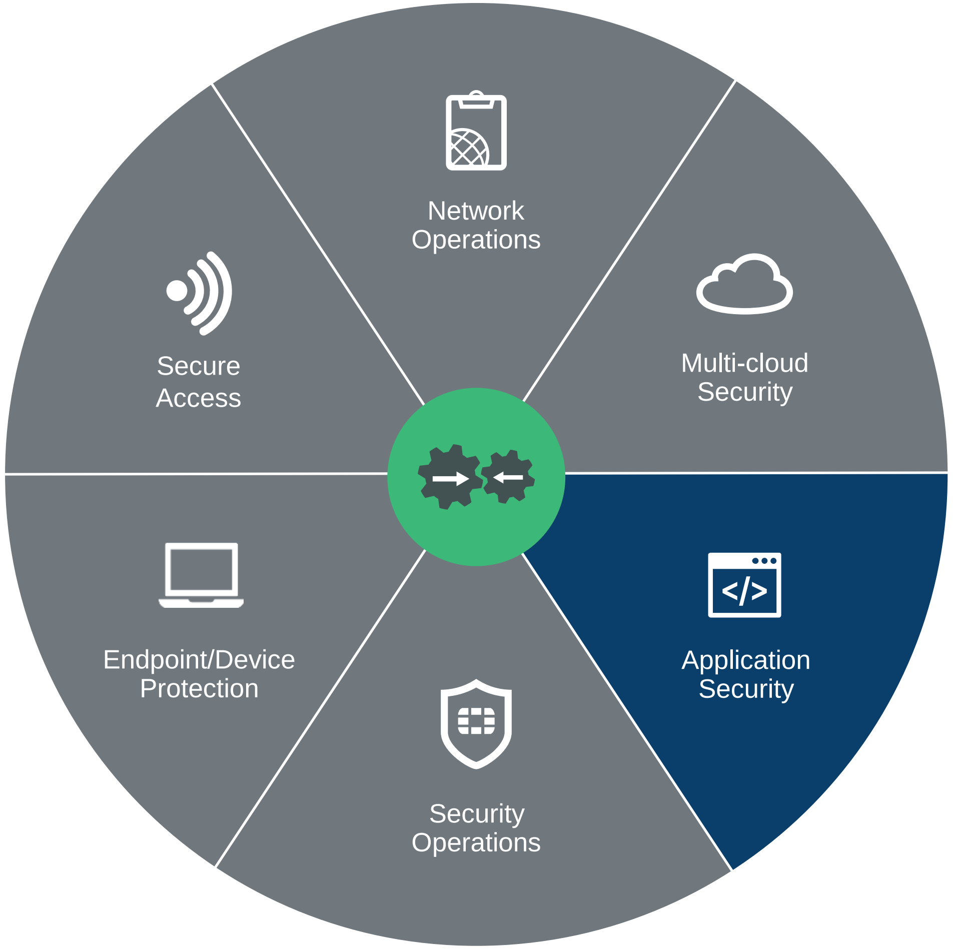
box Office 365 Dropbox salesforce



Applications

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

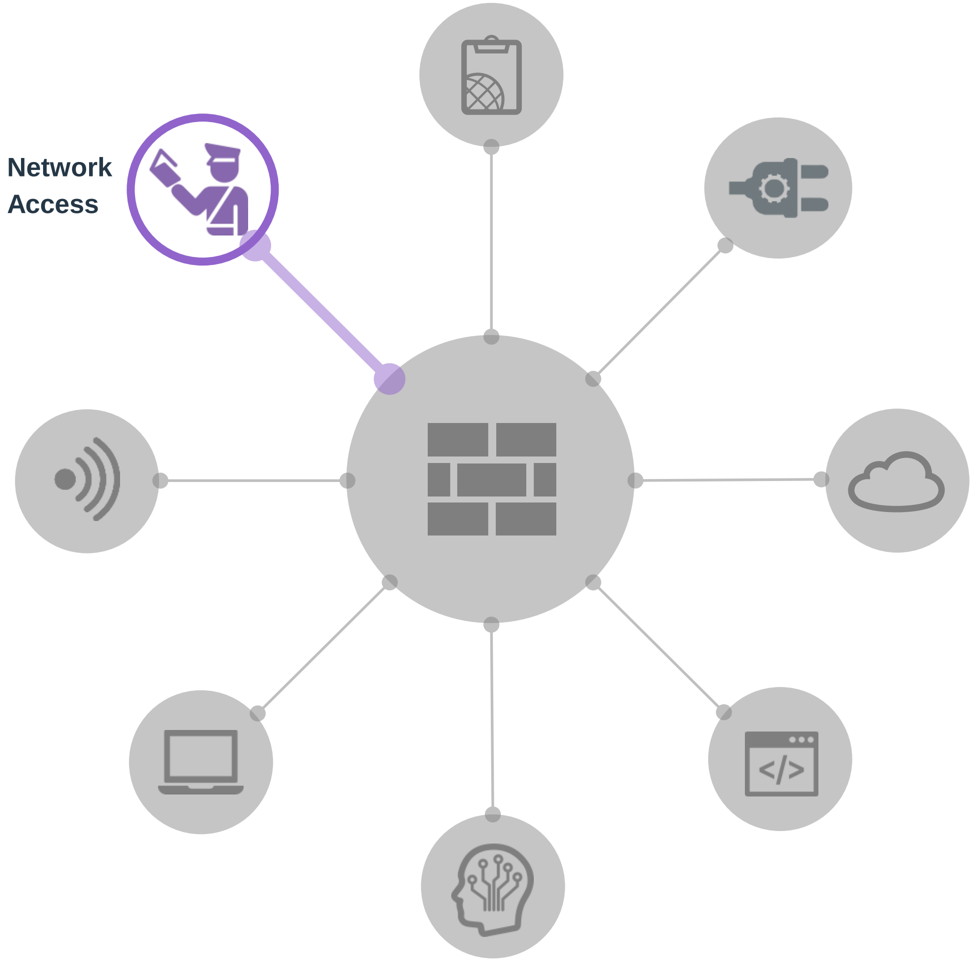
Know and control what is on your network

Identity

Know and control who is on your network

Endpoint

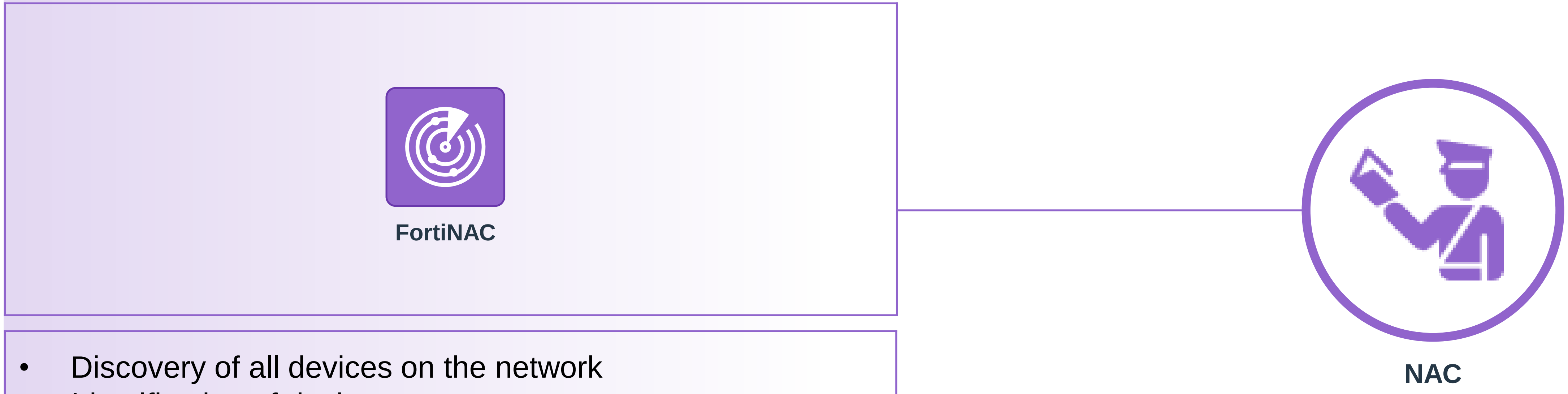
Track users and devices on-net, off-net



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.



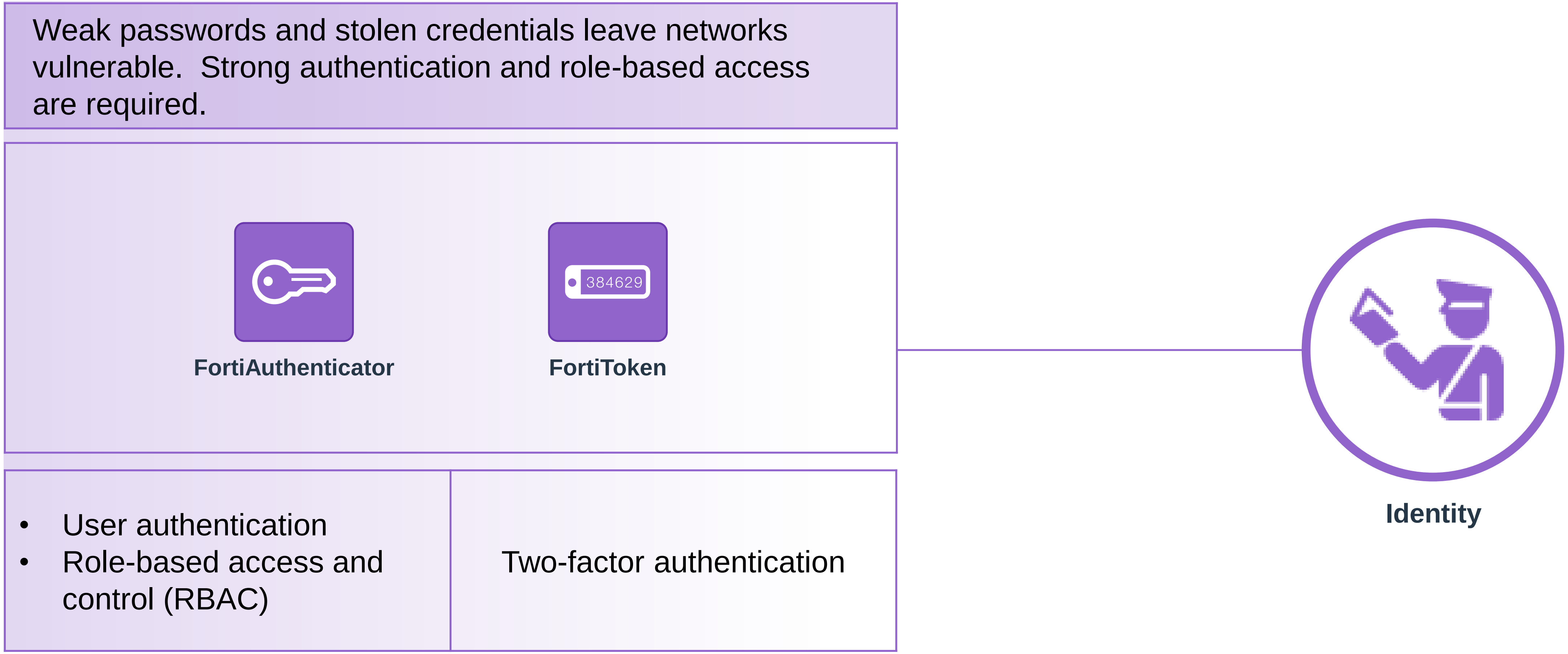
FortiNAC

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.

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

Two-factor authentication

Zero-trust Network Access

Track users & devices on-net, off-net

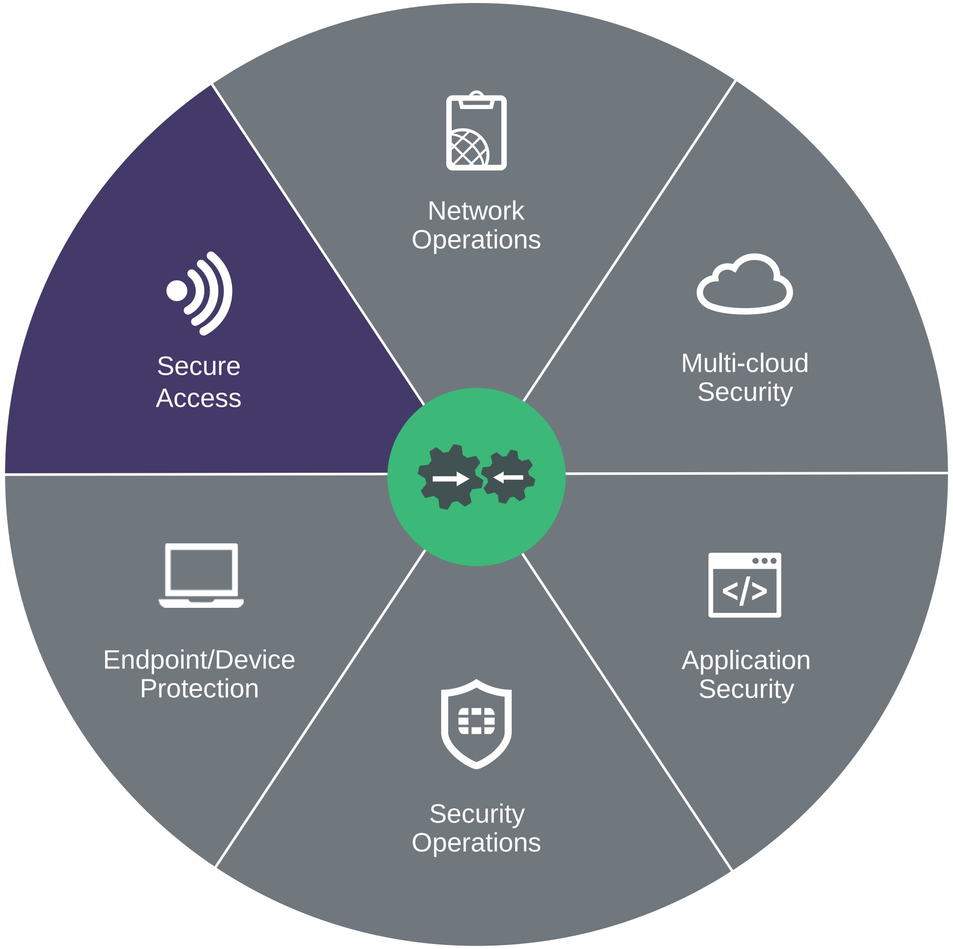
Today's digital business requires that employees work anytime, anywhere, on most any device. Endpoint agent must provide visibility and control.

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

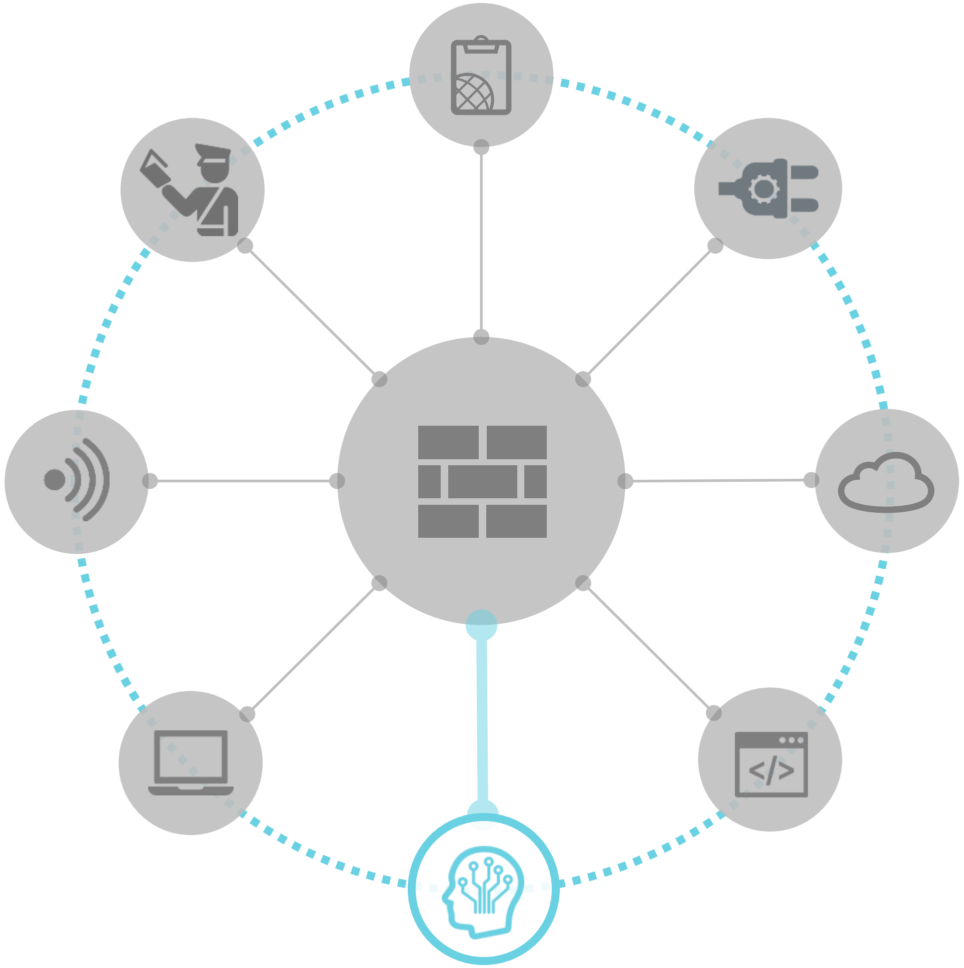
MEDIGATE | ordr | Pulse Secure® | zentera Connect · Protect · Shield

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



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

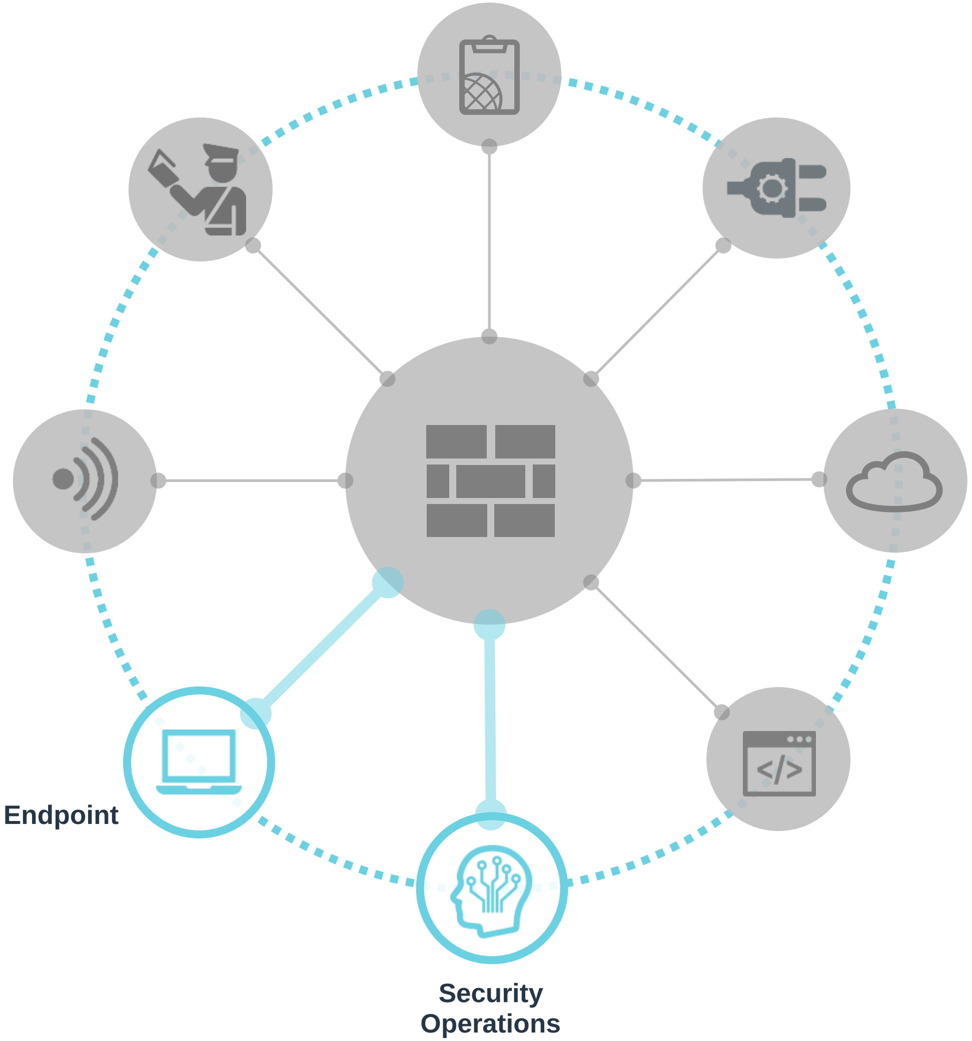
Attack surface reduction and malware prevention

Detect and Defuse Threats

Stop breaches with real-time detection & disarmament

Respond, Investigate & Hunt

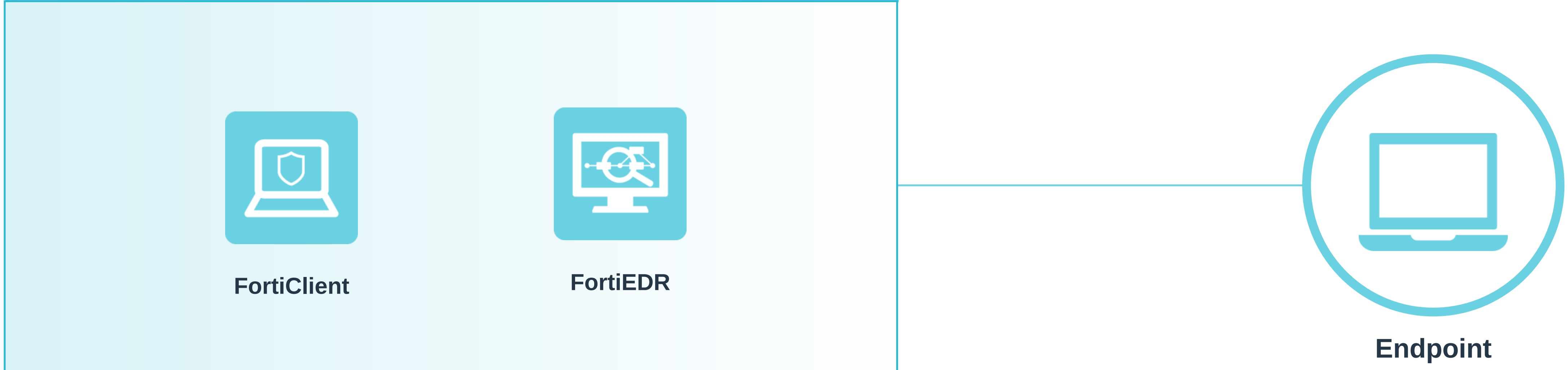
Orchestrated remediation and forensic investigation



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.



FortiClient

FortiEDR

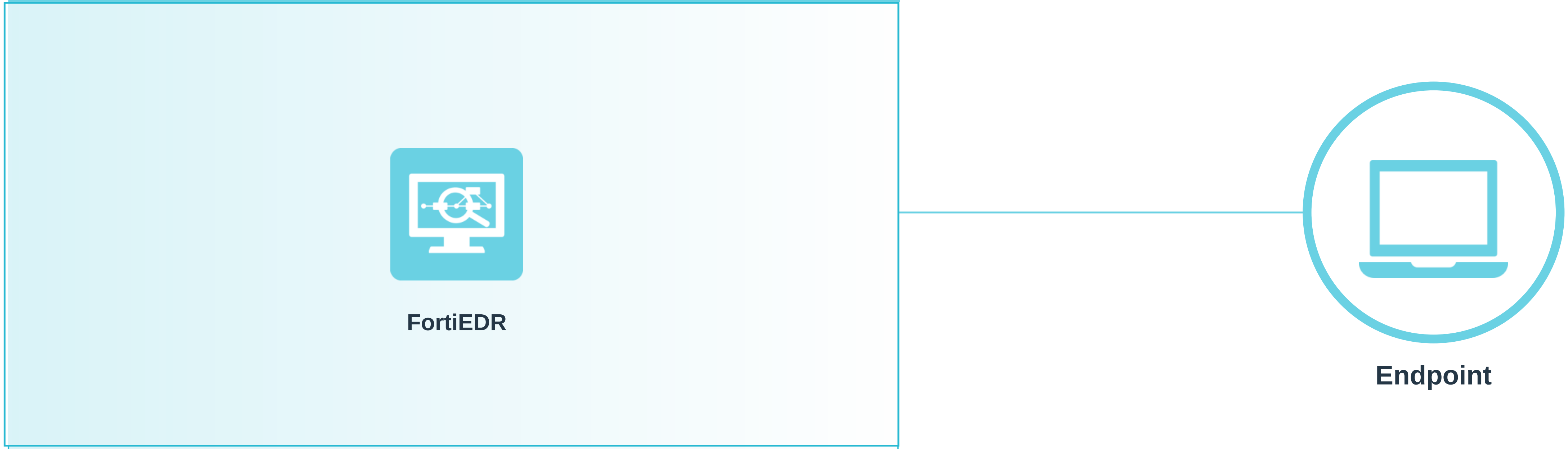
Endpoint

- 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”.

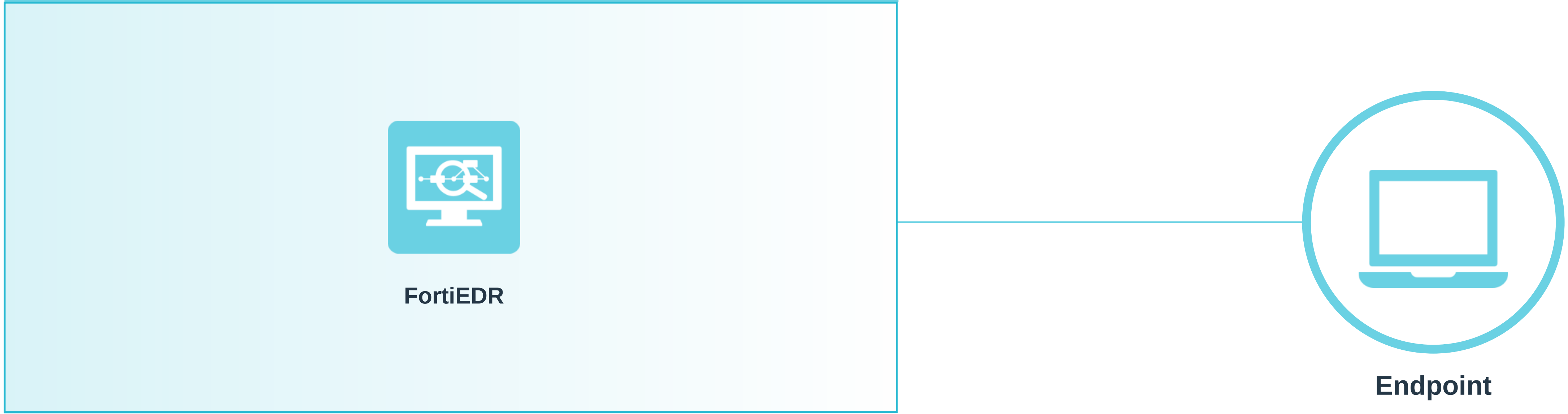


- Real-time detection and post-compromise protection
- Prevent file tampering and ransomware encryption
- Stop data exfiltration, C&C communication, and lateral movement

Respond, Investigate and Hunt

Orchestrated remediation and forensic investigation

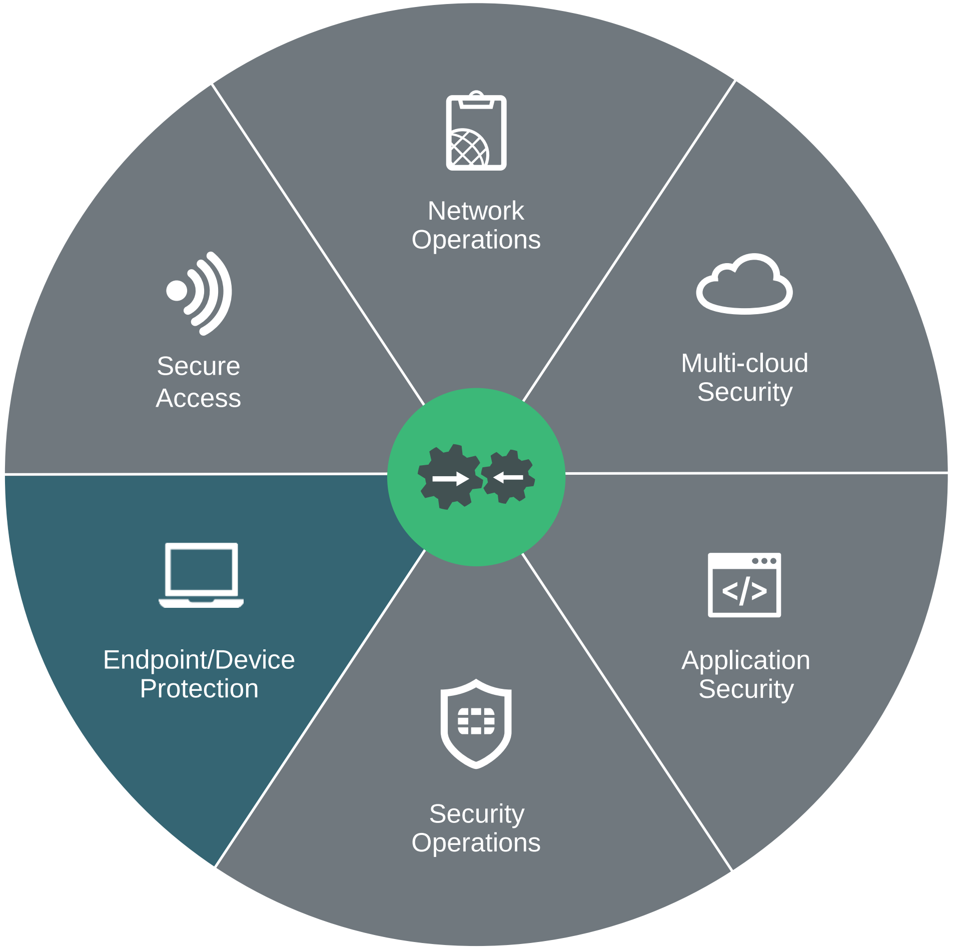
Cybersecurity skill shortage. Incident response is often manual, requires costly processes, and can interfere with business operation or employees productivity.



- 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

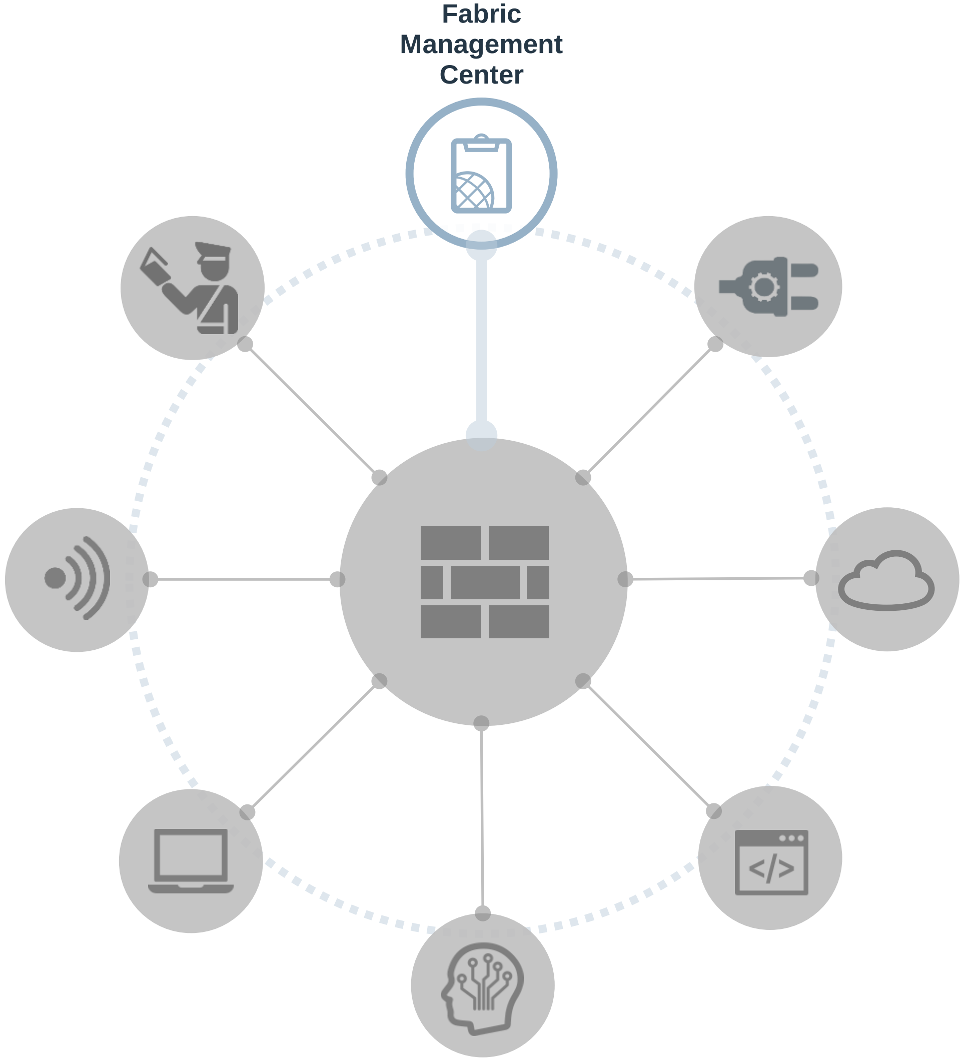
SSO across Security Fabric applications

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

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.

FortiManager

FortiAnalyzer

FortiGate Cloud

- 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

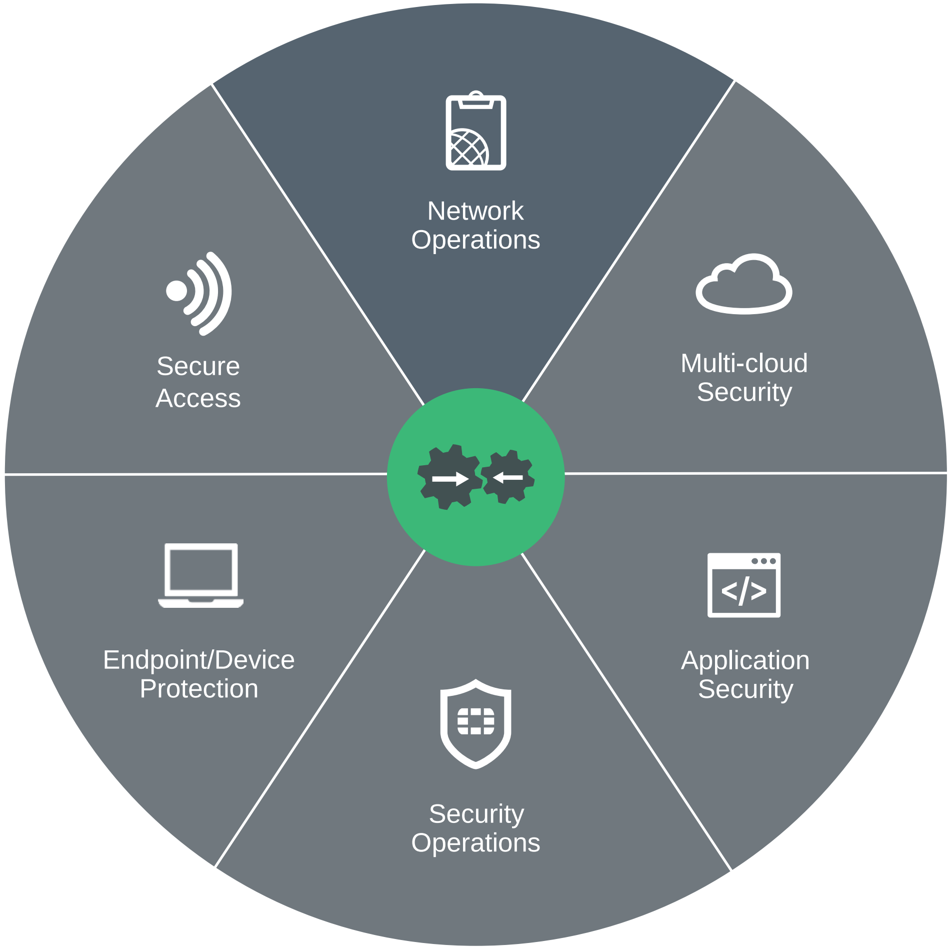
FortiGate Cloud

FortiManager

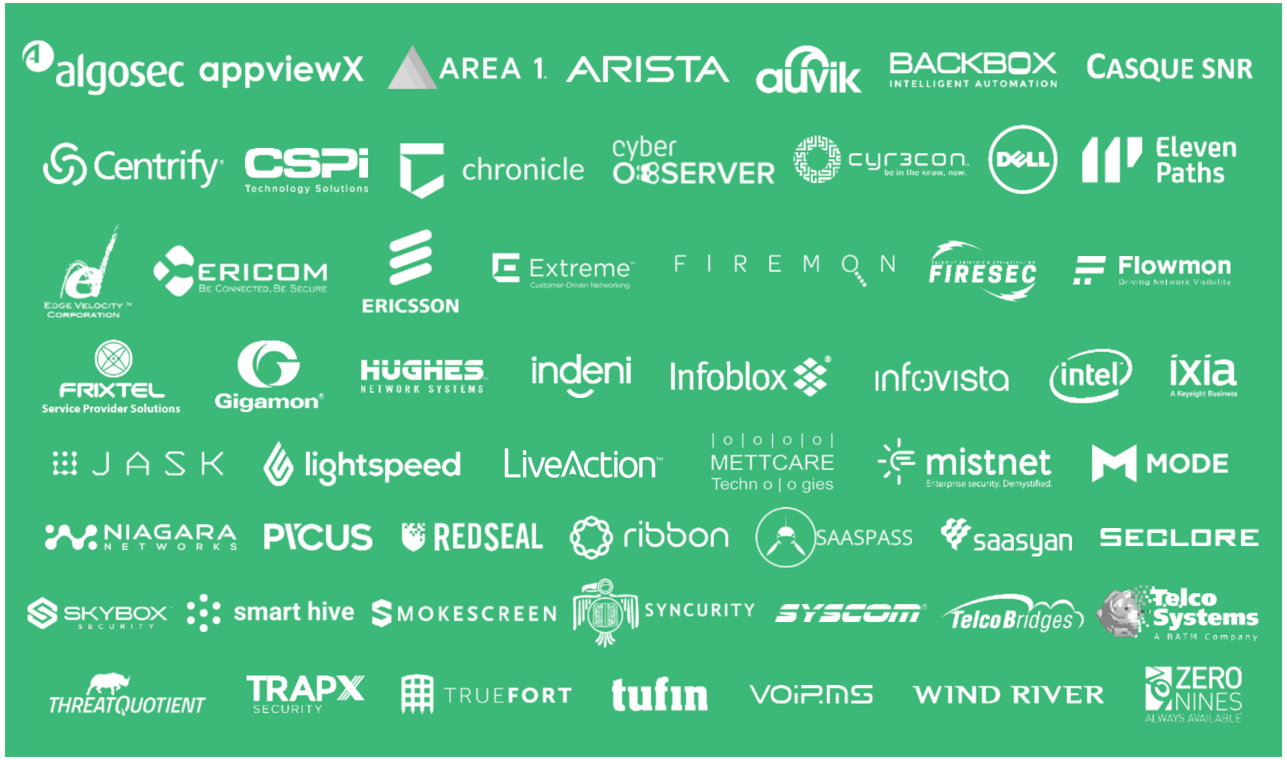
- Real-time network insights and health
- Network log management
- Compliance reporting

Network Operations Ecosystem

Fabric API Partnerships with FortiGate and FortiManager



Fabric API



Open Fabric Ecosystem

Fabric Connectors

Fortinet-developed deep integration automating security operations and policies

Fabric API

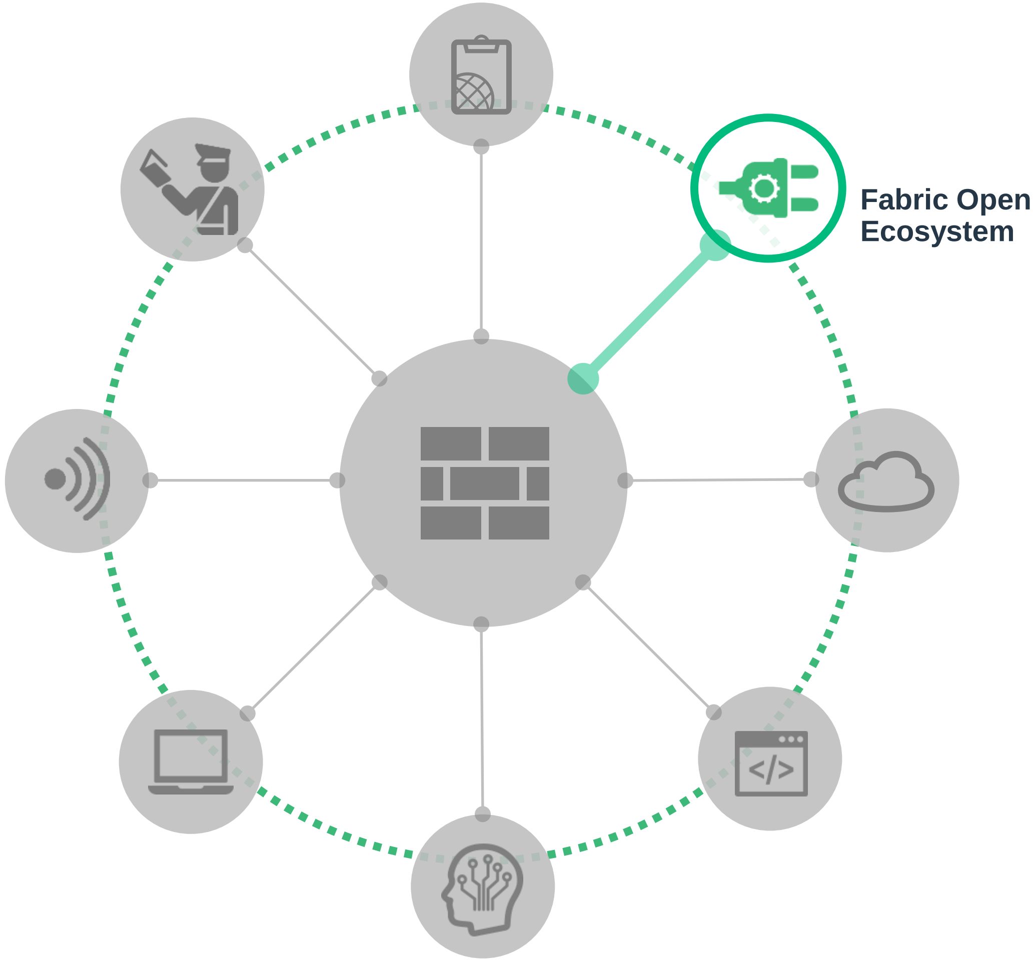
Partner-developed integration using Fabric APIs providing broad visibility with end-to-end solutions

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



Demo

- FortiOS 6.4 novosti – novi konektori i out-of-the-box automatizacija
- IoC
- Host isolation automation
- EMS, dynamic tagging
- FortiSoC

Cybersecurity Platform for the Digital Attack Surface

Appliance

Virtual Machine

Cloud

Security-as-a-Service

Software

Zero Trust Network Access

- FortiClient Fabric Agent
- FortiToken
- FortiNAC
- FortiAuthenticator
- Offnet Cloud

Security-driven Networking

- High Performance
- NGFW
- SD-WAN + SD-Branch
- FortiSwitch
- FortiAP
- FortiExtender

Dynamic Cloud Security

- FortiGate-VM
- VM Private Cloud
- FortiWeb SaaS
- FortiCASB
- 6k / 7k series
- FortiWeb

AI-powered Security Operations

- FortiAnalyzer
- FortiSIEM
- FortiSOAR
- FortiSandbox
- FortiDeceptor
- FortiAI
- FortiInsight
- FortiClient
- FortiEDR

Fabric Management Center

- Fabric Connectors
- FortiManager
- FortinetOne
- FortiGate Cloud
- FortiCare
- FNDN

Fortinet i Integra Group

- Integra Group – Expert Fortinet partner!

ENGAGE

FORTINET EXPERT PARTNER

Integrator

Data Center SPECIALIZATION

Secure SD-WAN SPECIALIZATION

Q & A

Zagreb / Osijek / Rijeka / Split

www.integragroup.hr

marko.ugrin@integragroup.hrr
ivan.galinac@integragroup.hr
nikolina.mihic@integragroup.hr