Securing the Evolution of Cyber-Physical Systems

Chris Blauvelt | Director, OT Consulting Systems Engineering

Q2 2023

Here’s what we will cover

Learn more at fortinet.com/ot

01 Trends impacting industrial operations

02 Operational Benefits by Securing ICX

03 Fortinet’s solutions | specialized offerings, threat intelligence, teams and partners for OT

04 Fireside Chat | 8th Avenue Food & Provisions

Trends and Market Drivers

Cybersecurity Market & Industry Drivers

Driving Infrastructure Evolution

How we interact with customers, suppliers, infrastructure, and employees is changing

Work from Anywhere

Digital Acceleration

Application Journey

Operational Technology Connectivity

Evolving Threat Landscape

Cybercriminals are adopting APT-like tactics to develop and scale attacks faster than ever

Cloud

Kaseya VSA

Nation Sponsored

Hermetic Wiper

Ransom as a Service

REvil

Growing Attack Surface

SolarWinds | Log4j

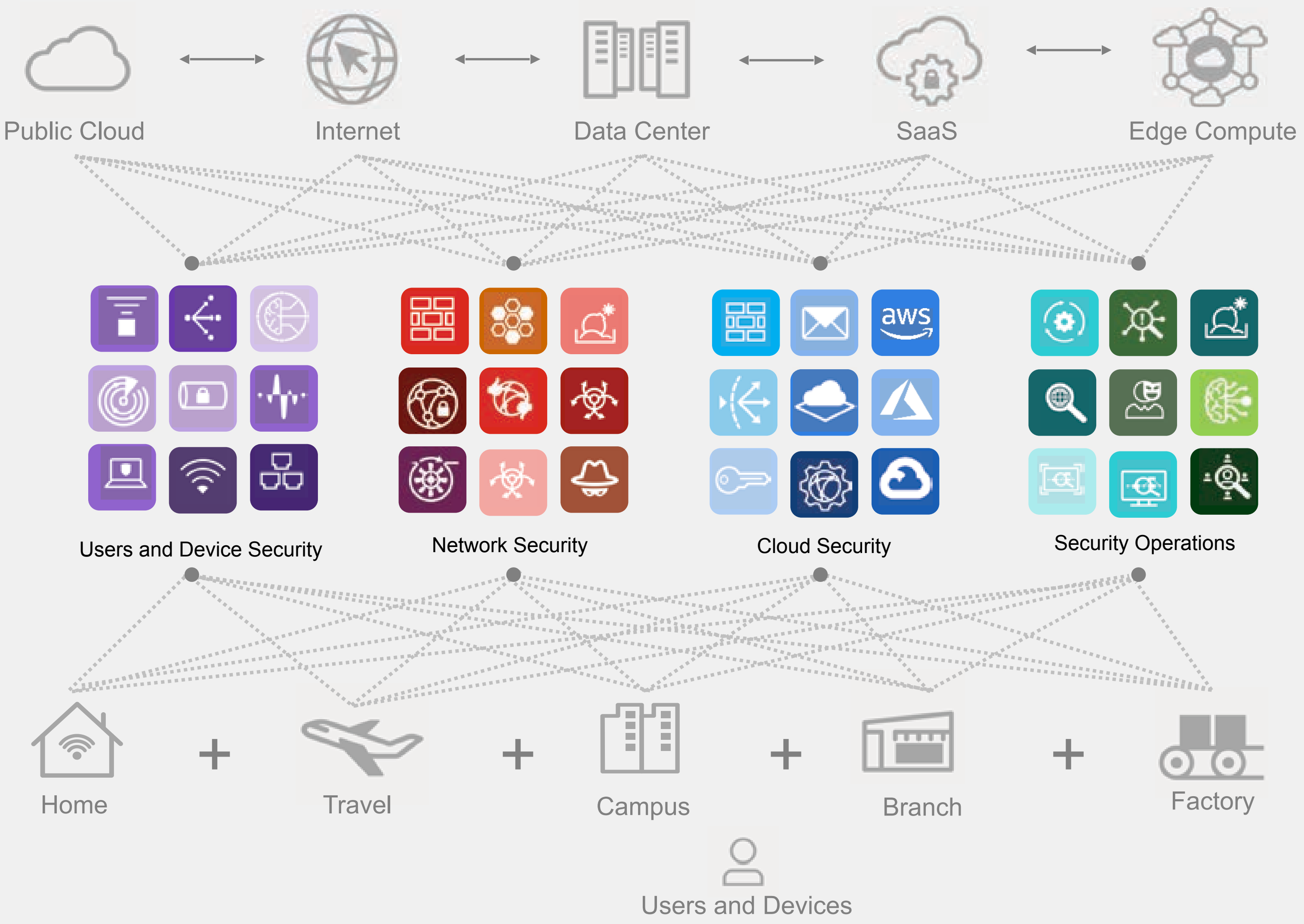
AI-enabled

Swarmbot

OT

Wipers | Colonial Pipeline

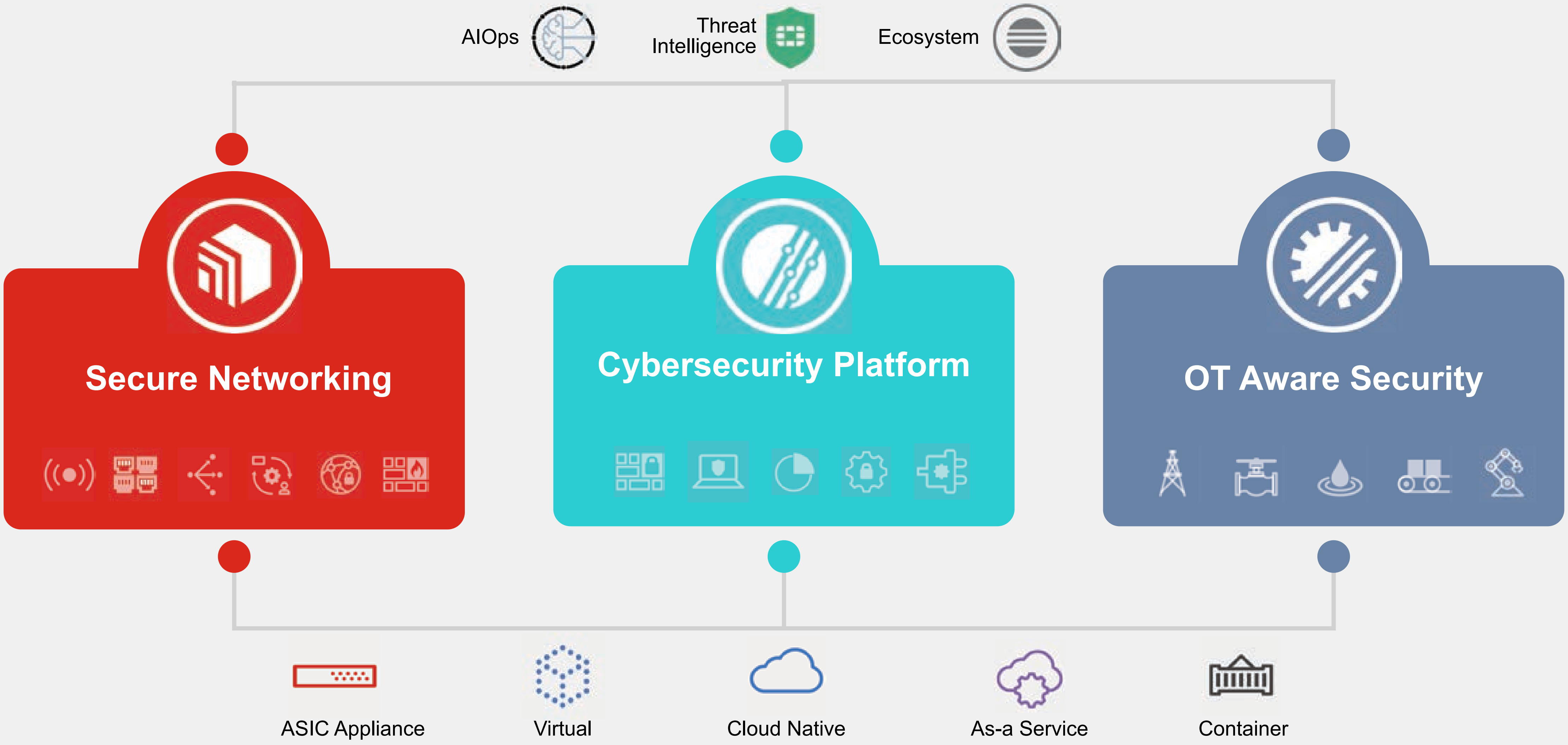
Complexity is Slowing Digital Initiatives



Today's Challenges

- Applications are distributed
- Users are working from anywhere
- More devices are attaching to applications
- Too many IT and security stacks
- Too many vendors
- Cybersecurity skills shortage

Consolidation Reduces Complexity & Accelerates Outcomes



AIOps

Threat Intelligence

Ecosystem

Secure Networking

Cybersecurity Platform

OT Aware Security

ASIC Appliance

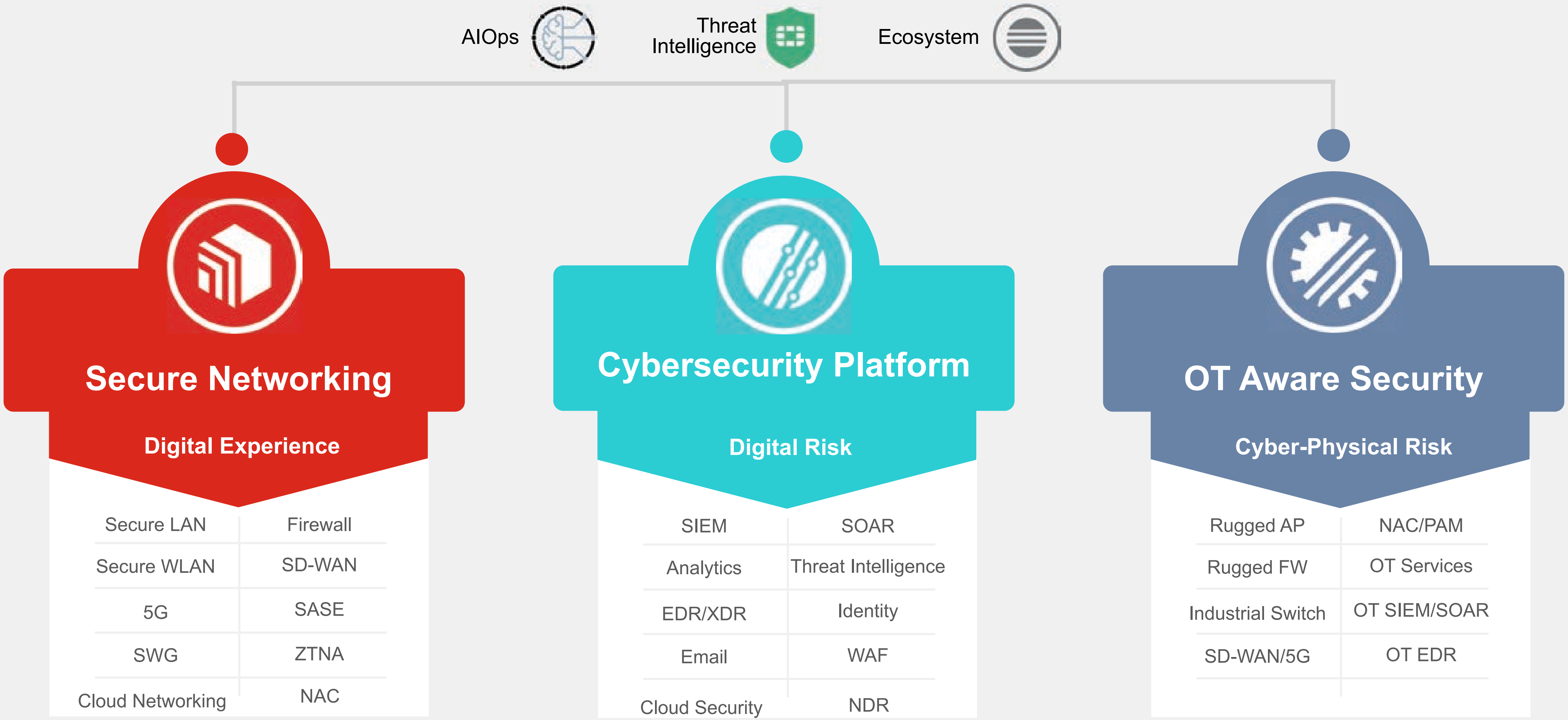
Virtual

Cloud Native

As-a Service

Container

Consolidation Reduces Complexity & Accelerates Outcomes



AIOps

Threat Intelligence

Ecosystem

Secure Networking

Digital Experience

- Secure LAN
- Secure WLAN
- 5G
- SWG
- Cloud Networking
- Firewall
- SD-WAN
- SASE
- ZTNA
- NAC

Cybersecurity Platform

Digital Risk

- SIEM
- Analytics
- EDR/XDR
- Email
- Cloud Security
- SOAR
- Threat Intelligence
- Identity
- WAF
- NDR

OT Aware Security

Cyber-Physical Risk

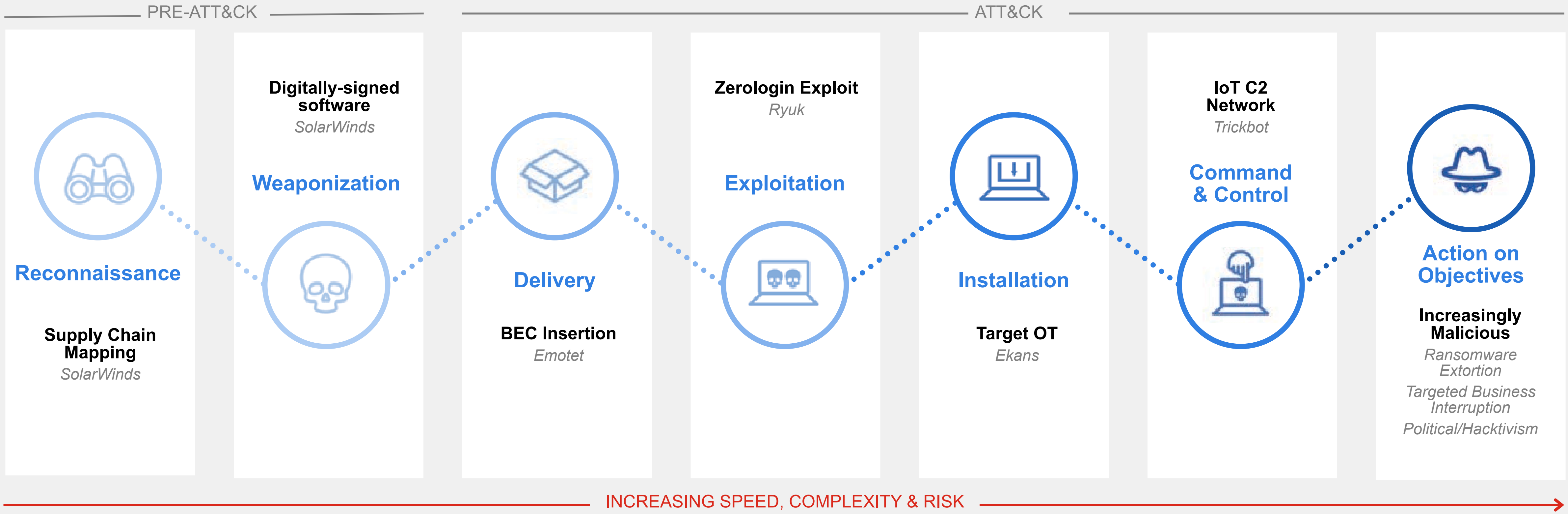
- Rugged AP
- Rugged FW
- Industrial Switch
- SD-WAN/5G
- NAC/PAM
- OT Services
- OT SIEM/SOAR
- OT EDR

Maximizing Operational Benefits

Securing Industrial Control Systems

Speed: The key to breaking the kill chain

To break the attack sequence and protect the organization, we need to detect and rapidly adjust the security posture to effectively protect against newly discovered attack's tactics across ever expanding attack surface.



PRE-ATT&CK

ATT&CK

Reconnaissance

Supply Chain Mapping
SolarWinds

Digitally-signed software
SolarWinds

Weaponization

Delivery

BEC Insertion
Emotet

Zerologin Exploit
Ryuk

Exploitation

Installation

Target OT
Ekans

IoT C2 Network
Trickbot

Command & Control

Action on Objectives

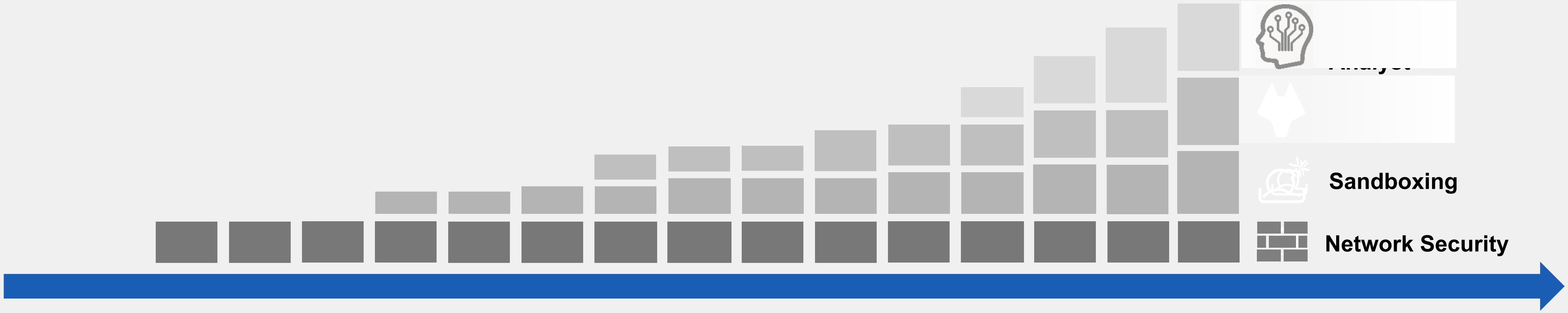
Increasingly Malicious
Ransomware Extortion
Targeted Business Interruption
Political/Hacktivism

INCREASING SPEED, COMPLEXITY & RISK

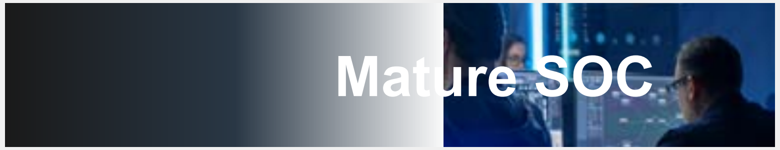
Security Framework for Digital Security

Security Maturity Model

NIST Identify Protect Detect Response Recovery



Foundation



Mature SOC

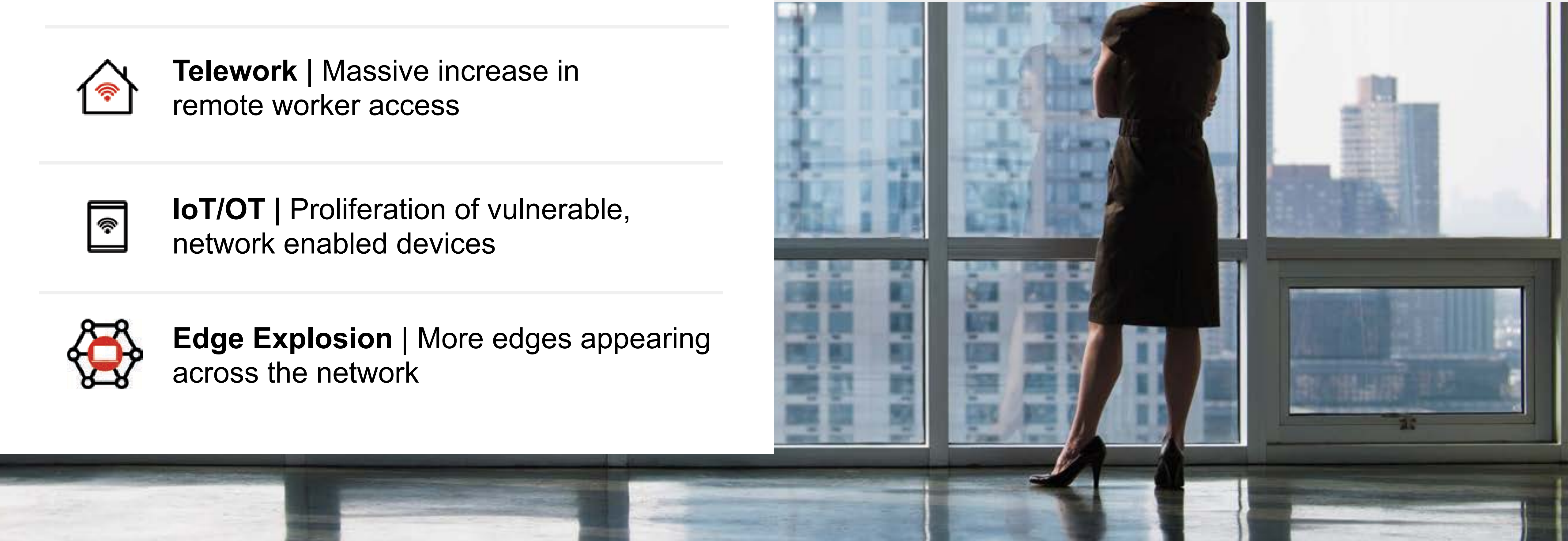
Operational Benefits from Secure ICS

#1 Visibility into your network

Telework | Massive increase in remote worker access

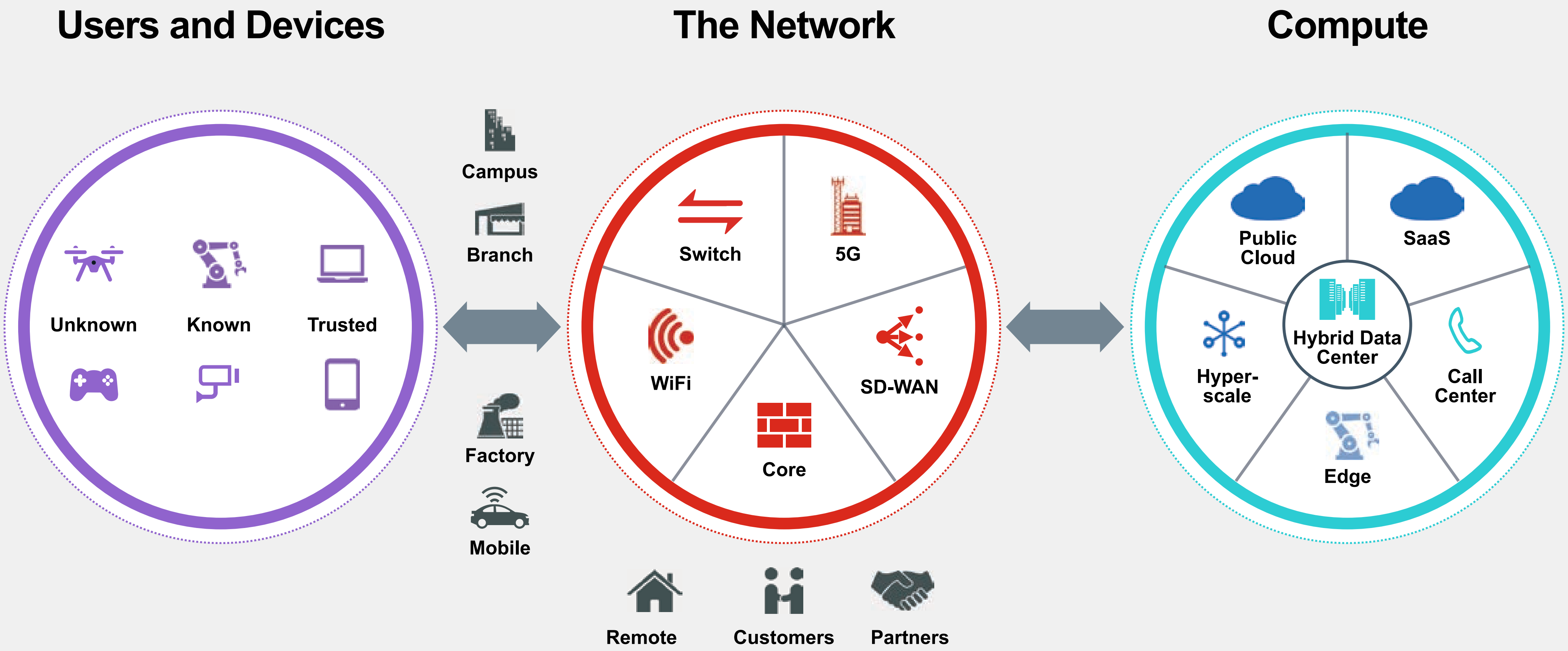
IoT/OT | Proliferation of vulnerable, network enabled devices

Edge Explosion | More edges appearing across the network



Billions of "Edges" Expanding the Attack Surface

The digital perimeter is everywhere



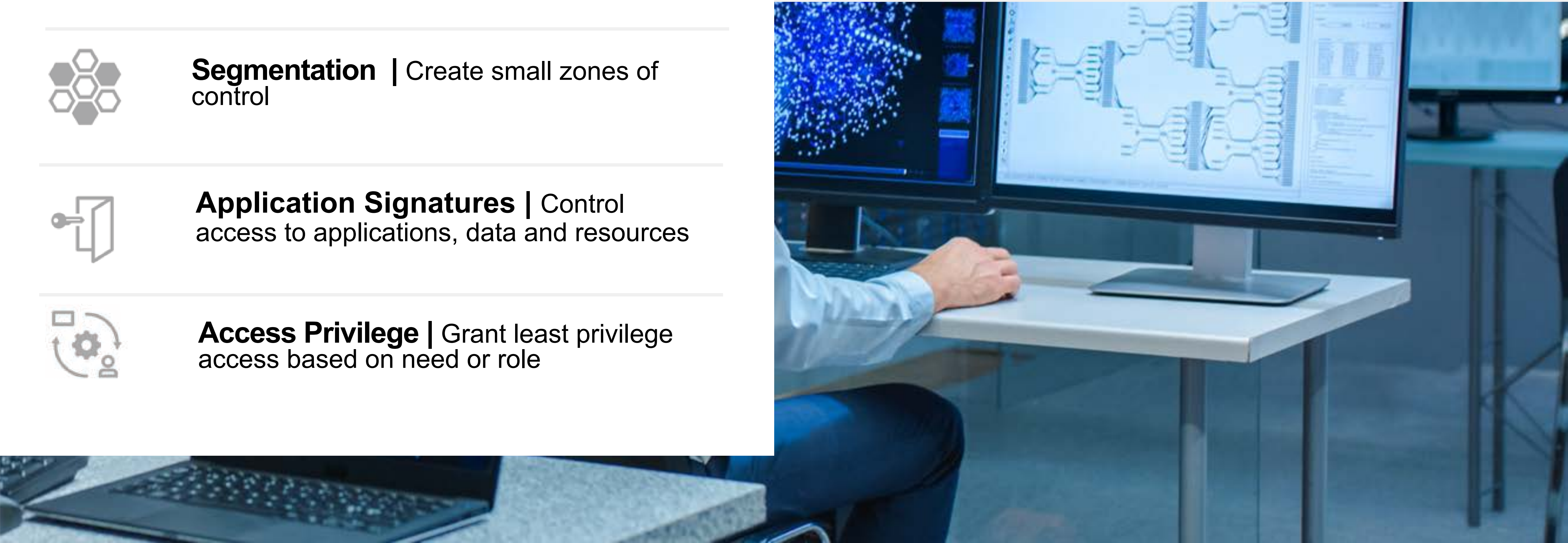
Operational Benefits from Secure ICS

#2 Enforcement across the network

Segmentation | Create small zones of control

Application Signatures | Control access to applications, data and resources

Access Privilege | Grant least privilege access based on need or role



Enhanced Identity Governance

Classification of Assets, Types and Dataflow to determine appropriate control measures

Identify Devices

- Type
- Host Name
- Vendor OUI
- Operating System
- Firmware Version
- Communication Protocols
- Physical Asset
- OT Asset
- IT Asset
- Authentication Capabilities

Classify

- End Point Class
- Modern
- Legacy
- Headless
- Industrial Internet of Things
- Internet of Medical Devices
- Telemetry & Logging
- Governance Requirements
- Risk Tolerance

Zones & Conduits

- Policies
- Operational Context
- Segmentation Type
  - Physical Segmentation
  - Virtual LAN & VDOM
  - Micro Segmentation
  - Host Segmentation

IT Assets

Operational Assets

Process Automation Assets

Building Automation Assets

Physical Assets

Internet of Things Assets

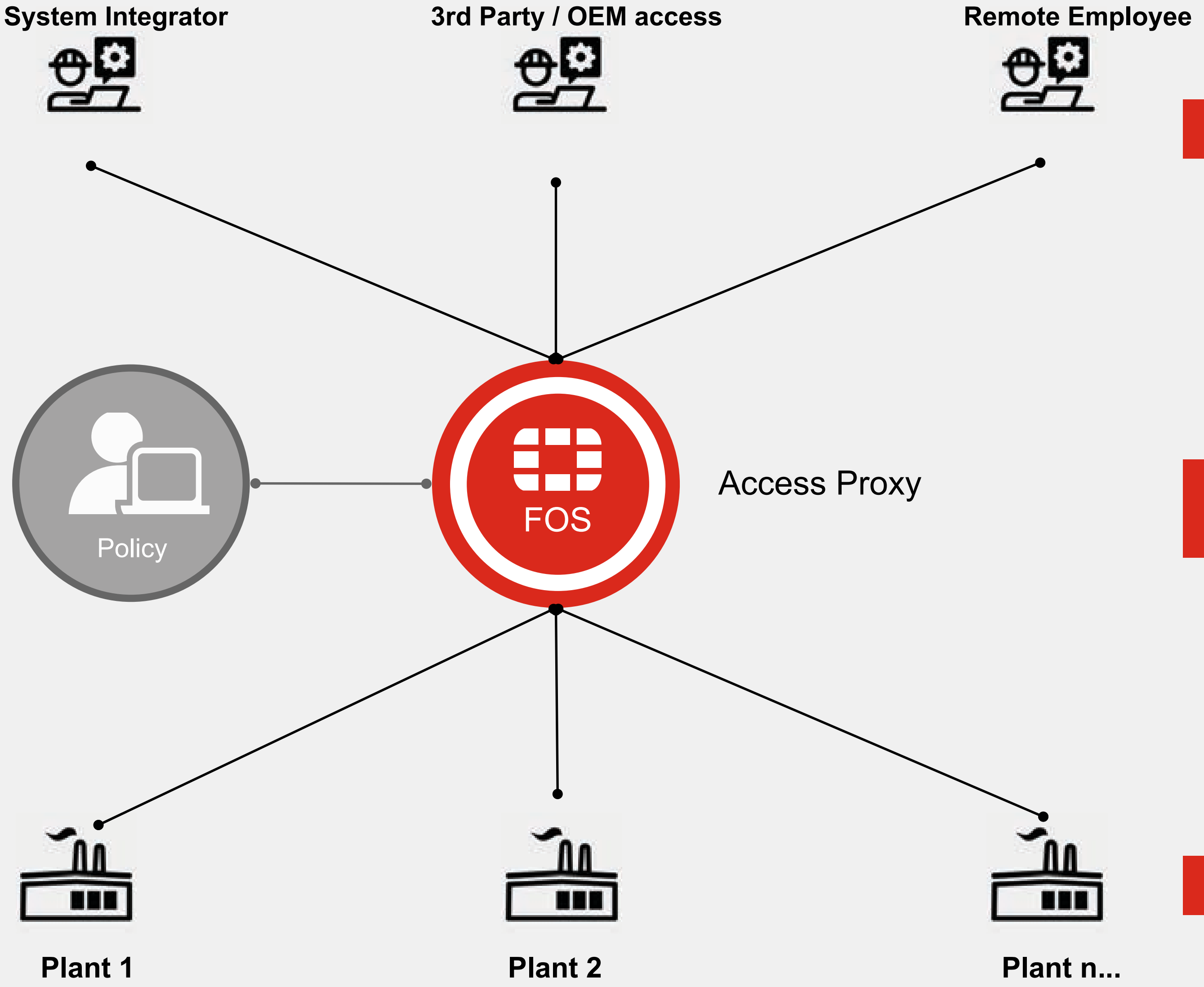
Modern Assets

Legacy Assets

Headless Assets

Specialized Assets

Enabling Secure Access



Wherever the user is located

Verified user identity and device posture prior to access

Industrial asset location

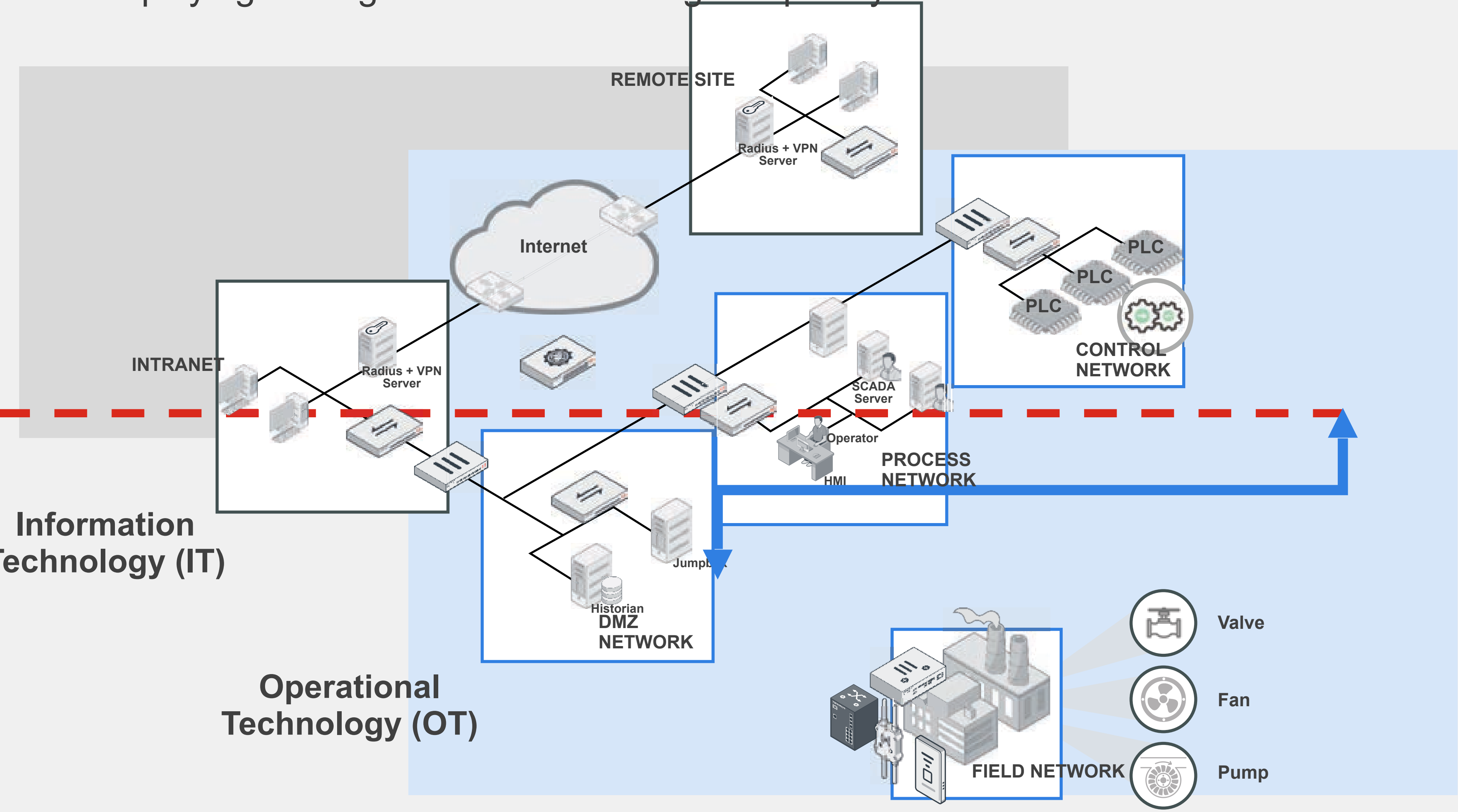
Operational Benefits from Secure ICS

#3 Continuous analysis of behaviors

- Central security tool for logging, reporting and analytics
- Continuous trust, threat assessments inside out, outside in
- Orchestrated, automated response to known and unknown advanced threats

Continuous Analysis across OT & IT

Simplifying management and reducing complexity



Operational Benefits from Secure ICS

#4 Response planning

Already been breached	Plan as if attackers are inside and outside of the network
No trusted zones	Forget the concept of a ‘trusted zone’, e.g. ‘in the office’; ‘on the plant floor’
Test the plan	Testing your plan by running a drill or through table top exercises

Security Fabric Strategies for OT

Preserve business continuity and compliance in the face of changing technology and digitalization

Threat Detection & Protection

- Network segmentation and micro-segmentation
- Broad coverage for OT protocols and applications
- Virtual patching for legacy ICS and OT systems
- ICS and OT specific dashboards
- Simplified user interfaces

Threat & Vulnerability Management

- Comprehensive OT threat and vulnerability management
- FortiGuard Threat-Intel and Industrial Security Service for OT
- IPS signatures and DPI for industrial protocols
- Integration with major 3rd party industrial IDS platforms
- Endpoint management and security

Compliance

- Industry certified and accredited solutions
- Industry compliant solution architecture
- Compliance monitoring and reporting on major OT cybersecurity frameworks
- Centralized auditing and management
- Unified compliance assurance across Cloud/ IT and OT

Accelerated Digitalization

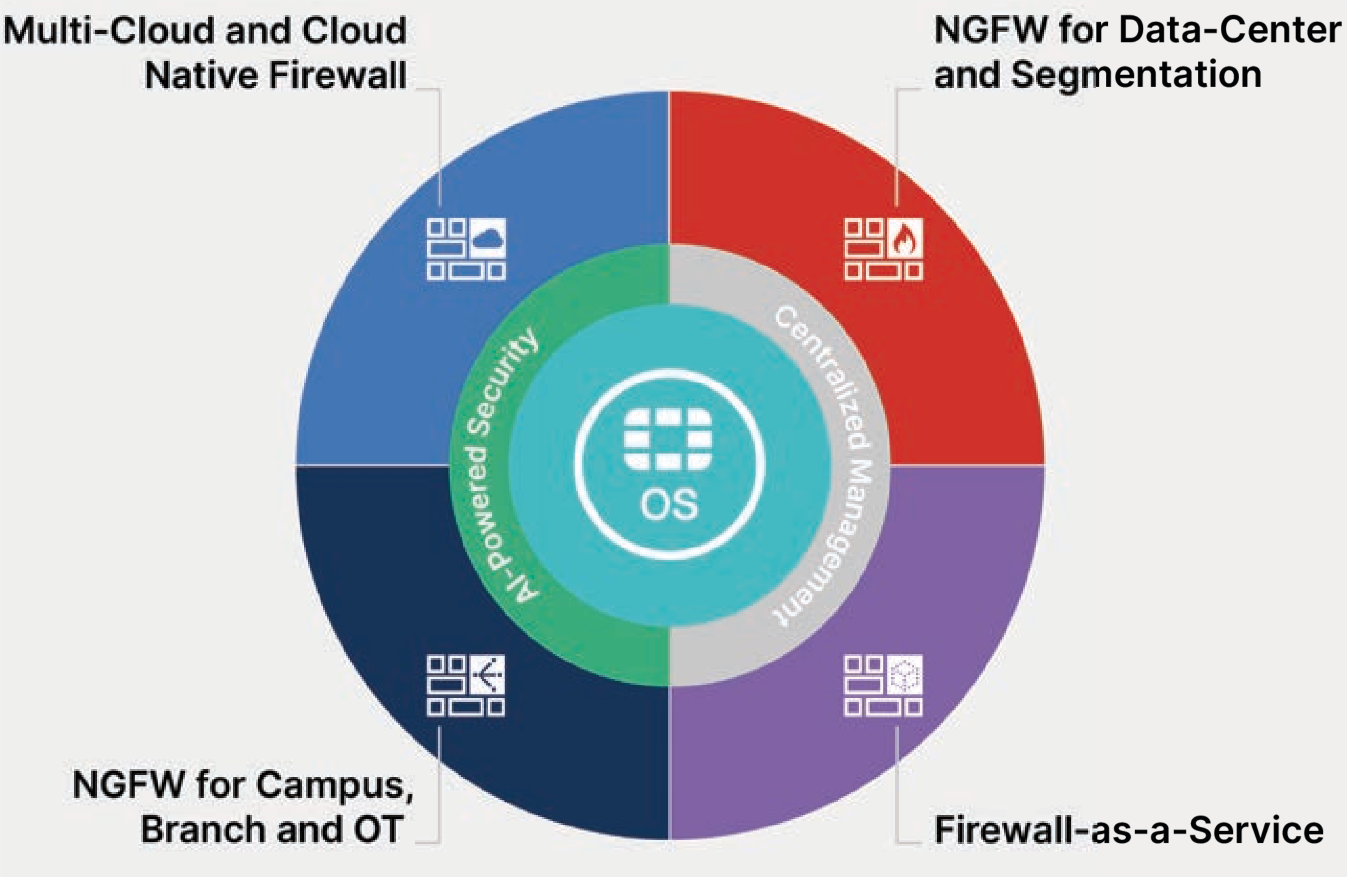
- Specialized solutions for OT
- Secure by design solution architecture
- Security automation and orchestration
- Partnerships and alliances with industrial automation and control system vendors
- Open Fabric integration platform for 3rd parties

Simplifying Security Operations

A Fabric Approach to Securing Industrial Controls

Hybrid Mesh Firewall

Centralized and unified management simplifying cybersecurity operations

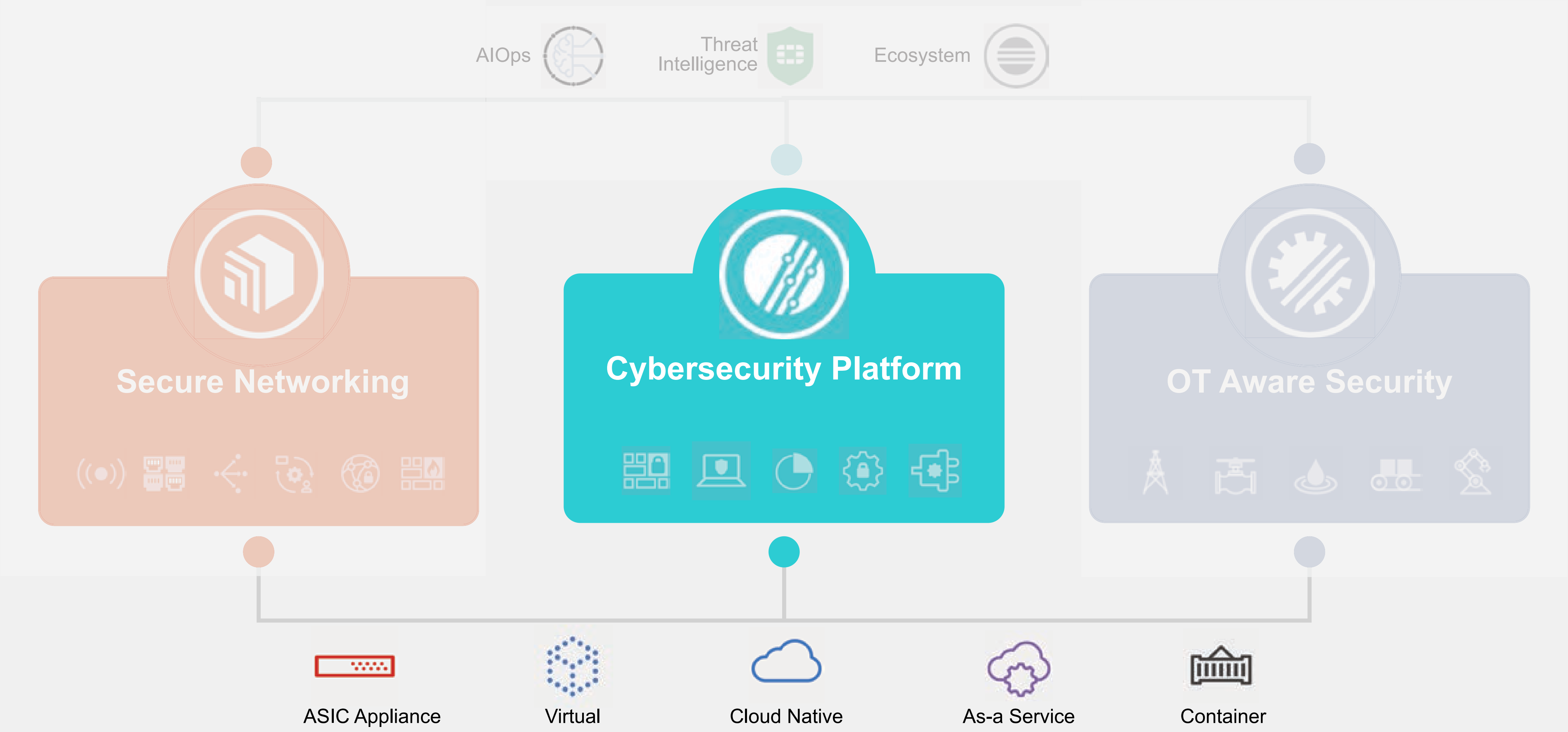


Multi-Cloud and Cloud Native Firewall
NGFW for Data-Center and Segmentation
Centralized Management
AI-powered Security
OS
NGFW for Campus, Branch and OT
Firewall-as-a-Service

"By 2026, more than 60% of organizations will have more than one type of firewall deployment, which will prompt adoption of hybrid mesh firewalls."

Source: Gartner Network Firewall MQ 2022

Consolidation Reduces Complexity & Accelerates Outcomes



AIOps

Threat Intelligence

Ecosystem

Secure Networking

Cybersecurity Platform

OT Aware Security

ASIC Appliance

Virtual

Cloud Native

As-a Service

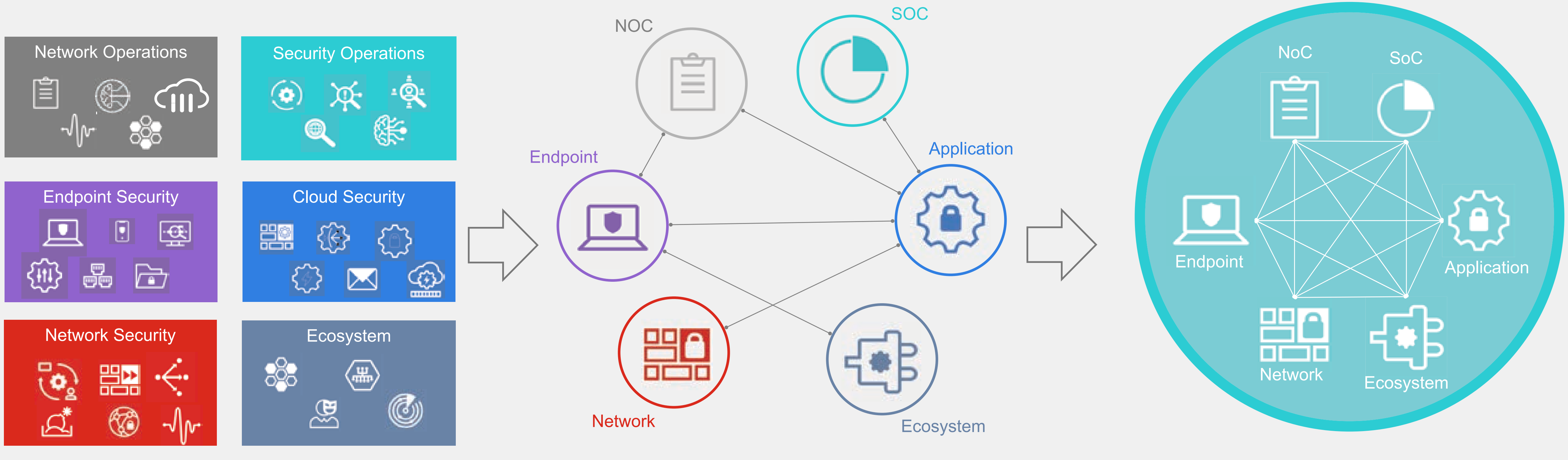
Container

Cybersecurity Platform Journey

30+ Vendors

10 Vendors

2-3 Platforms



Network Operations

Security Operations

Endpoint Security

Cloud Security

Network Security

Ecosystem

NOC

SOC

Endpoint

Application

Network

Ecosystem

NoC

SoC

Endpoint

Application

Network

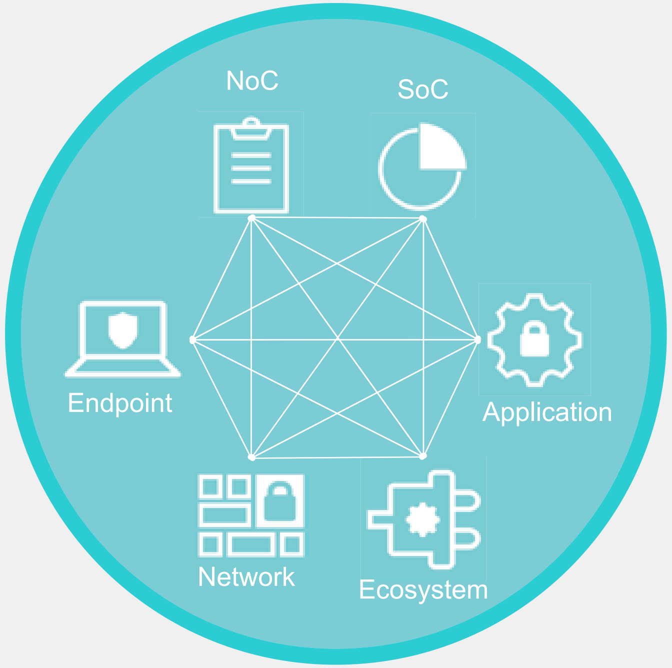
Ecosystem

Your Journey to SOC Automation Maturity

Cybersecurity Platform

97% of organizations plan to have an active vendor consolidation strategy within the next three years.

Consolidate point products and vendors into a cybersecurity platform



Primary Reasons Organizations are Pursuing Security Vendor Consolidation:

55%
Increase efficacy by integrating multiple components

55%
Increase effectiveness by allowing broader reach and visibility

43%
Easier management by reducing the number of separate tools

35%
Cost/budgeting/to save money

Gartner

Gartner, Accelerate SASE Adoption by Leveraging the Security Vendor Consolidation Wave, Published 5 May 2023 - ID G00785334 - By Analyst(s): Evan Zeng, Naresh Singh

Cybersecurity Platform

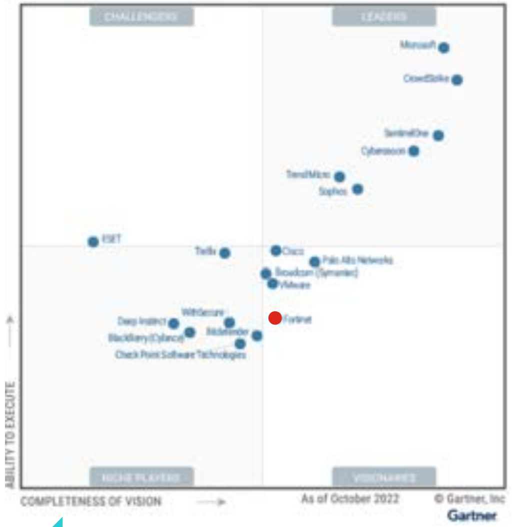
One Platform

Enterprise “best of breed” and “platform” are not mutually exclusive

Endpoint Protection

Gartner Magic Quadrant for Endpoint Protection Platforms, 2023

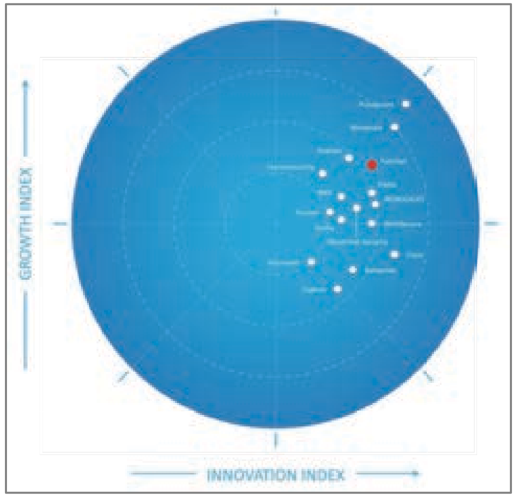
Fortinet Recognized as a Visionary Vendor



Email Security

Frost & Sullivan...Frost RadarTM: Email Security, 2022

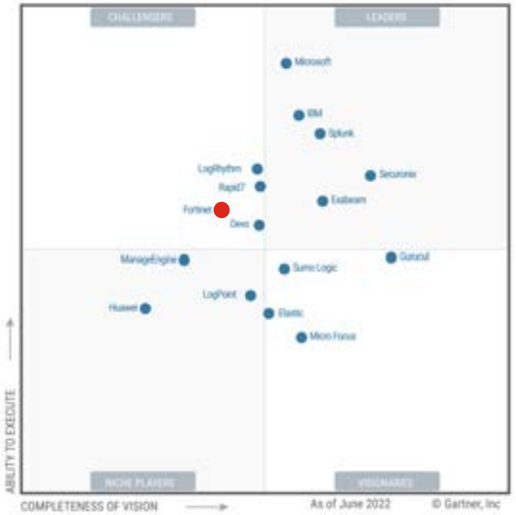
Fortinet Recognized as a Top Vendor



SIEM

Gartner Magic Quadrant for SIEM 2023

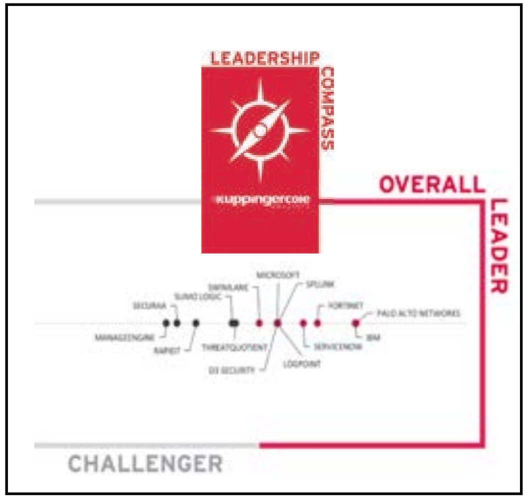
Fortinet Recognized as a Challenger



SOAR

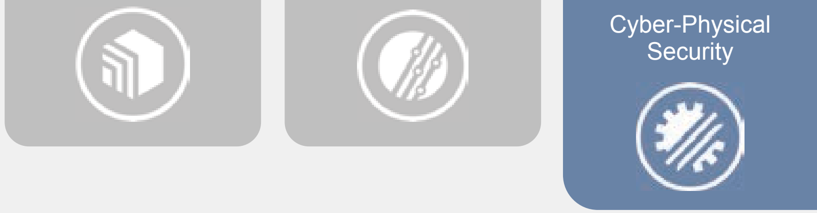
KuppingerCole Leadership Compass for SOAR, 2023

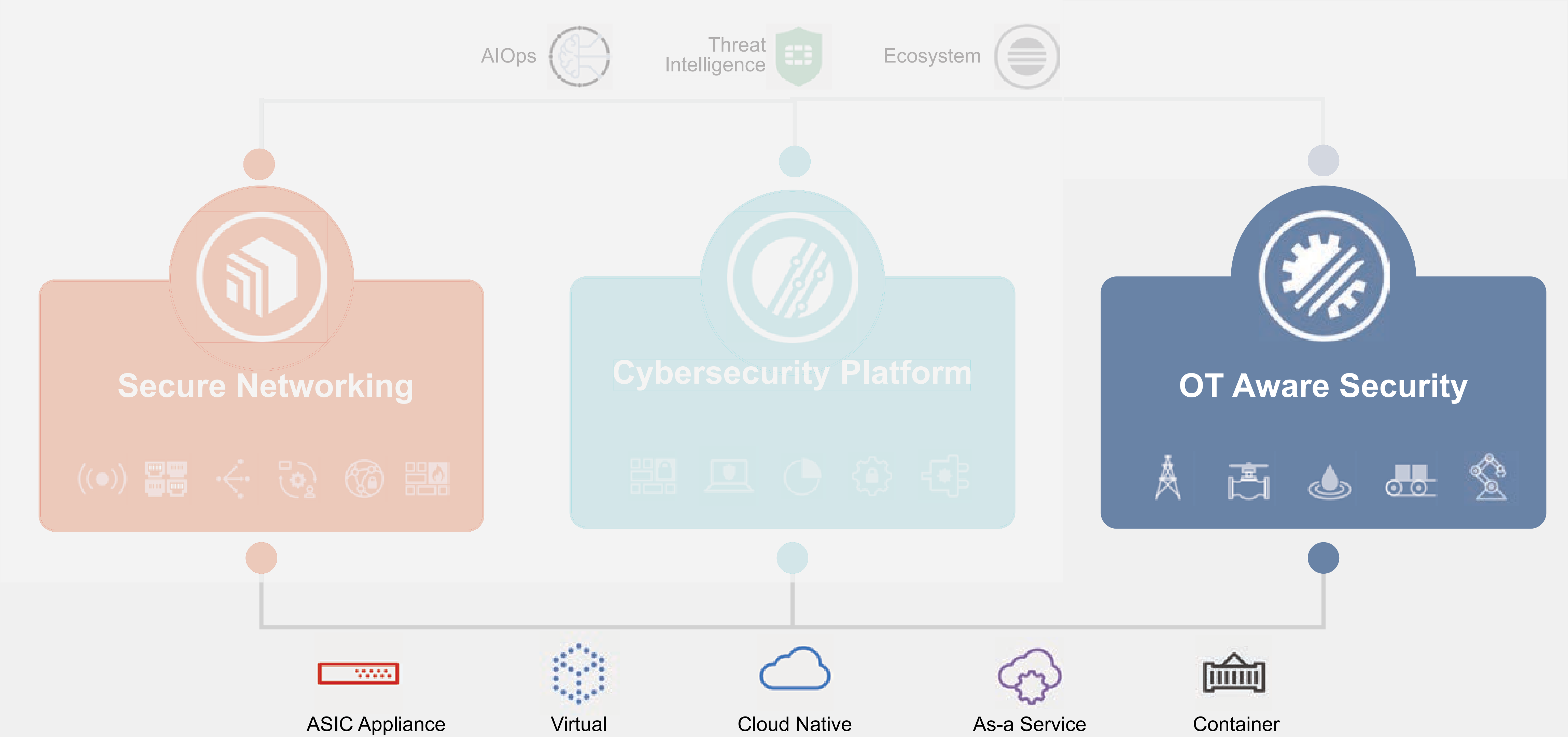
Fortinet Recognized as a Leader



The Fortinet Security Fabric

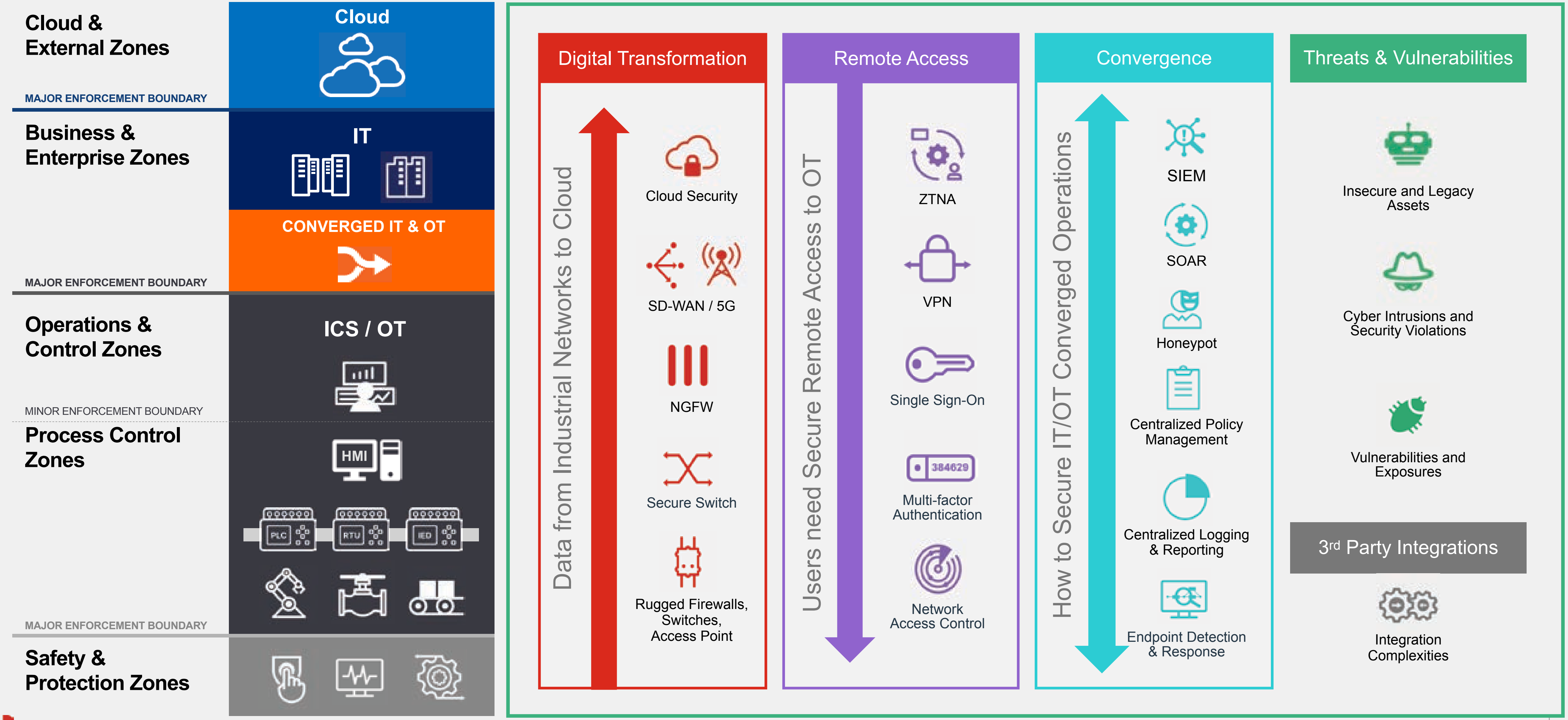
Consolidation Reduces Complexity & Accelerates Outcomes





Cyber-Physical Aware Security Fabric

Extend cyber-physical security capabilities to OT networks in factories, plants, remote locations, and ships.



Cloud & External Zones — Cloud

MAJOR ENFORCEMENT BOUNDARY

Business & Enterprise Zones — IT

CONVERGED IT & OT

MAJOR ENFORCEMENT BOUNDARY

Operations & Control Zones — ICS / OT

MINOR ENFORCEMENT BOUNDARY

Process Control Zones

MAJOR ENFORCEMENT BOUNDARY

Safety & Protection Zones

Digital Transformation

Data from Industrial Networks to Cloud

- Cloud Security
- SD-WAN / 5G
- NGFW
- Secure Switch
- Rugged Firewalls, Switches, Access Point

Remote Access

Users need Secure Remote Access to OT

- ZTNA
- VPN
- Single Sign-On
- Multi-factor Authentication
- Network Access Control

Convergence

How to Secure IT/OT Converged Operations

- SIEM
- SOAR
- Honeypot
- Centralized Policy Management
- Centralized Logging & Reporting
- Endpoint Detection & Response

Threats & Vulnerabilities

- Insecure and Legacy Assets
- Cyber Intrusions and Security Violations
- Vulnerabilities and Exposures

3rd Party Integrations

- Integration Complexities

FortiGuard Labs: Threat Intelligence & Security Services

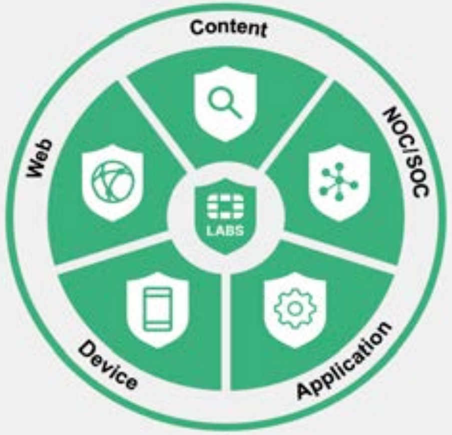
Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. We develop and utilize leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence.

Global Leadership & Collaboration:

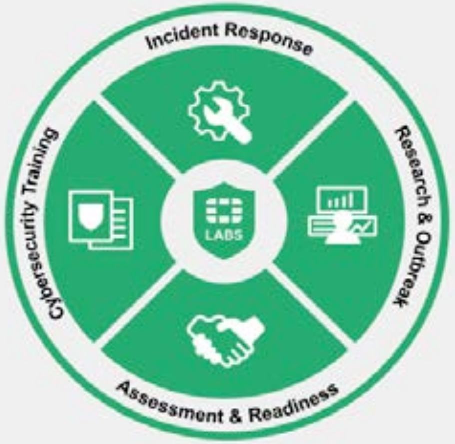
CYBER THREAT ALLIANCE · WORLD ECONOMIC FORUM · INTERPOL · NCI AGENCY

FortiGuard Labs Real-Time Threat Intelligence

FortiGuard AI-Powered Security Services



FortiGuard Expert Services



500+ FortiGuard Labs Global Threat Hunters and Researchers

600K+ Hours of Threat Research a Year

100+B global security events analyzed per day

Fortinet Security Fabric

Broad

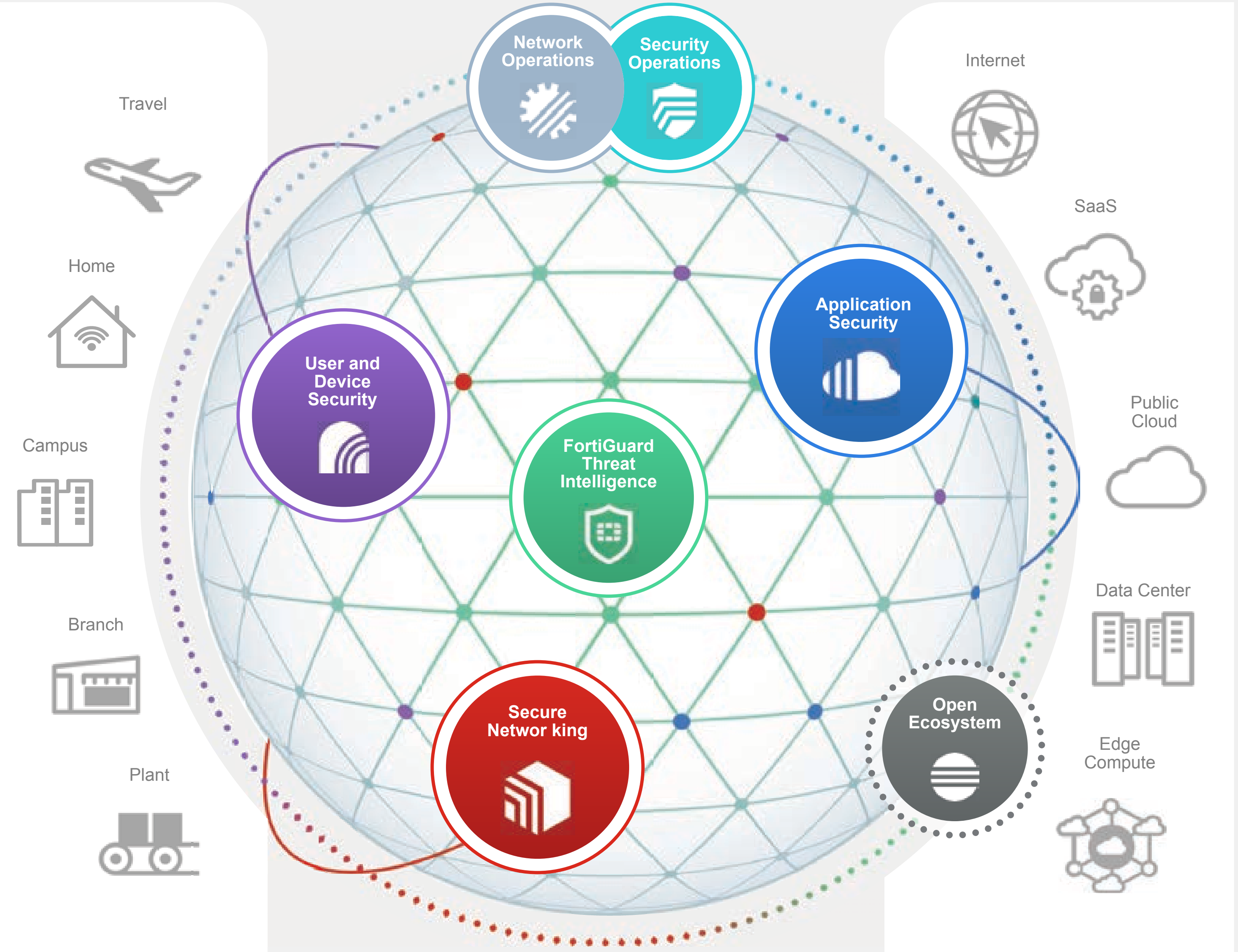
visibility and protection of the entire digital attack surface to better manage risk

Integrated

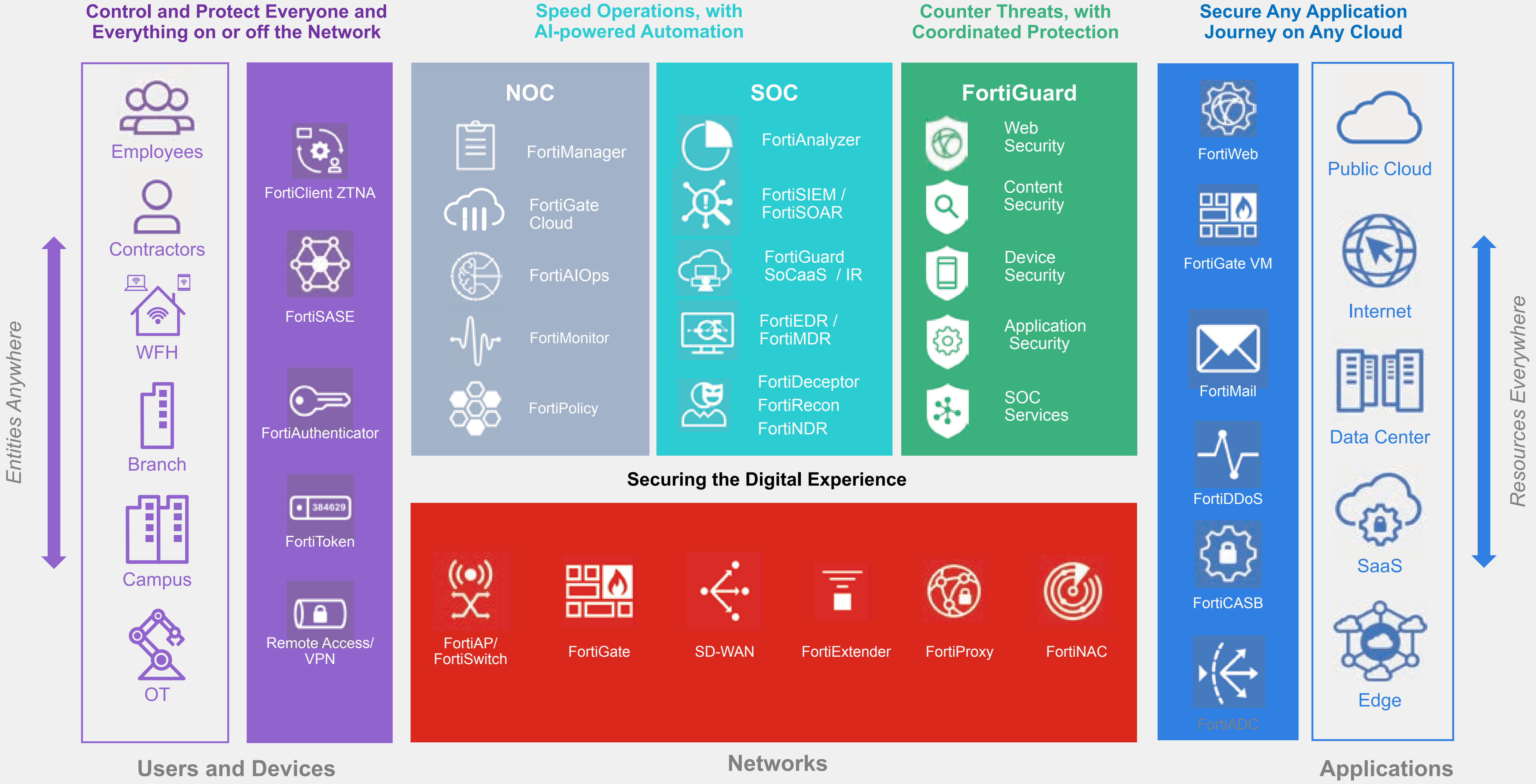
solution that reduces management complexity and shares threat intelligence

Automated

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



Fortinet Security Fabric Expansion



Control and Protect Everyone and Everything on or off the Network

Speed Operations, with AI-powered Automation

Counter Threats, with Coordinated Protection

Secure Any Application Journey on Any Cloud

Entities Anywhere

Employees

Contractors

WFH

Branch

Campus

OT

FortiClient ZTNA

FortiSASE

FortiAuthenticator

FortiToken

Remote Access/ VPN

NOC

FortiManager

FortiGate Cloud

FortiAIOps

FortiMonitor

FortiPolicy

SOC

FortiAnalyzer

FortiSIEM / FortiSOAR

FortiGuard SoCaaS / IR

FortiEDR / FortiMDR

FortiDeceptor

FortiRecon

FortiNDR

FortiGuard

Web Security

Content Security

Device Security

Application Security

SOC Services

Securing the Digital Experience

FortiAP/ FortiSwitch

FortiGate

SD-WAN

FortiExtender

FortiProxy

FortiNAC

FortiWeb

FortiGate VM

FortiMail

FortiDDoS

FortiCASB

FortiADC

Public Cloud

Internet

Data Center

SaaS

Edge

Resources Everywhere

Users and Devices

Networks

Applications

Maximize your existing investments

Fortinet integrates with 500+ security and networking solutions

Fabric Connectors

Fortinet-developed deep integration automating security operations and policies

Microsoft Azure · Symantec. · ORACLE · aws · nuagenetworks · openstack. · vmware · servicenow · Google Cloud · cisco · IBM Cloud

Fabric APIs

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

OT/ IoT	FinServ	Healthcare/ Life Sciences & Pharma	Retail	SLED
NOZOMI NETWORKS DRAGOS CLAROTY	splunk> intel. EQUINIX tufin NVIDIA. servicenow	ordr asimily ARMIS.	ARISTA AMD Gigamon	vmware NUTANIX rubrik

+300 other Fabric-Ready Partners

Fabric DevOps

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

aws · ORACLE · HashiCorp · Microsoft Azure · Alibaba Cloud · Google Cloud · Red Hat · refactr · openstack. · vmware

Extended Ecosystem

Integrations with other vendor technologies & open systems

cisco · paloalto NETWORKS · Hewlett Packard Enterprise · CROWDSTRIKE · vmware

Figures as of Dec 1, 2022
Note: Logos are a representative subset of the Security Fabric Ecosystem

Fireside Chat

Adam Dauphiniais

Sr. Mgr Core Infrastructure

8th Avenue Food & Provisions

Q&A

More information at Fortinet.com/OT

Thank You!

FORTINET®