FORTINET

Navigating Tomorrow's Cyber Seas: Unraveling the Mesh, ZTNA, and SASE for Innovating Secure Business Horizons

Marion Renaldo Rotensulu, Principal Consultant

Fortinet, inc

Q4 2023

Trends and Market Drivers

More External Forces Than Ever Are Driving Security Decisions

DIGITAL EVOLUTION

Digital innovation is creating tremendous opportunity, but more risk.

TECHNOLOGY DISRUPTION

More companies are rapidly implementing AI to transform business operations.

ECONOMIC HEADWINDS

Budget changes and skills shortage are resulting in more delays and more risk.

SKILLS SHORTAGE

With 3.4M unfilled jobs, the struggle to recruit and retain cybersecurity talent creates additional cyber risks.

ENVIRONMENTAL, SOCIAL, & GOVERNANCE

Consumers and boards are putting more pressure to deliver on ESG initiatives.

REGULATORY AND COMPLIANCE

Companies are reacting to more frequent reporting and regulatory changes.

THREAT LANDSCAPE
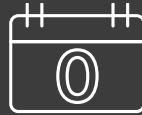
Attacks are growing in sophistication and frequency.

From a threat landscape that is more complex than ever

SPEAR PHISHING & DEEP FAKES

More targeted, more automated, and more channels

N DAY VULNERABILITIES

24% Growth in Published CVEs in 2022 over 2021

CYBER-PHYSICAL ATTACKS

Removal of Air Gaps is exposing OT

APT THREAT ACTORS

30% of APT groups were detected as active in just the 1H 2023

RANSOMWARE & WIPERS

Ransomware infections times falls from 5 days to 5 hours

CLOUD RISKS

69% of companies use two or more clouds

SUPPLY CHAIN ATTACKS

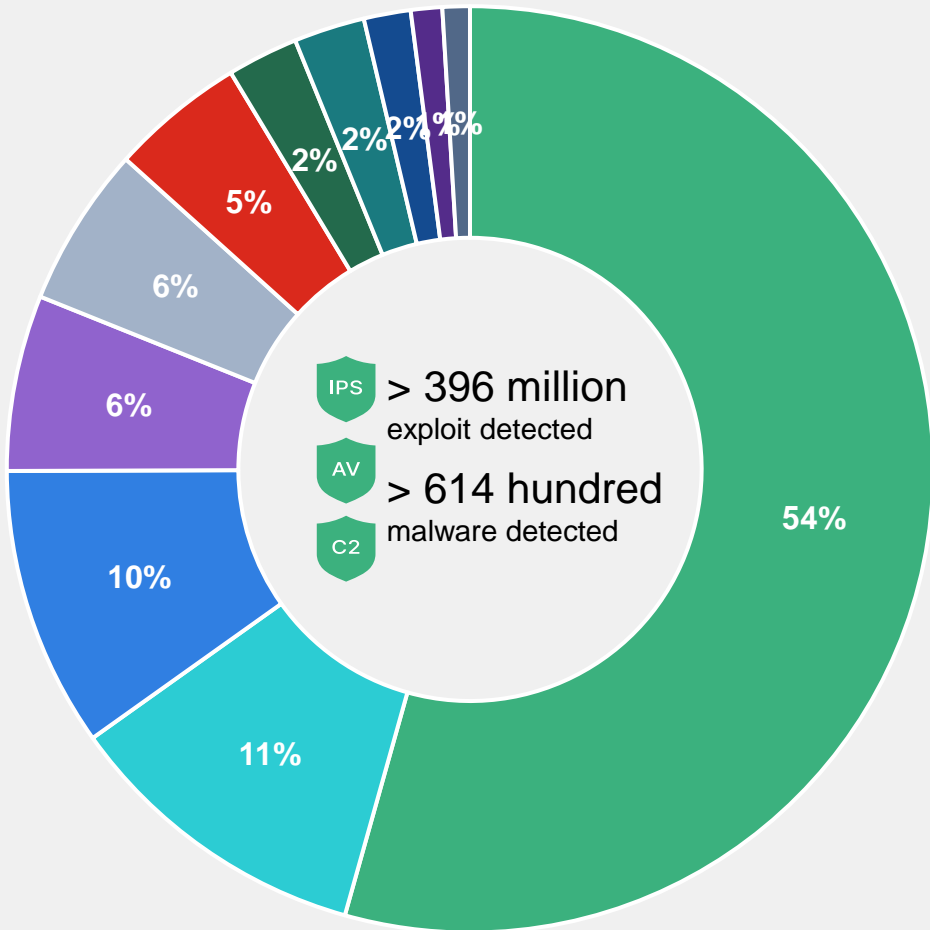12% of data breaches originated from a software supply chain attack

INSIDER RISK

+32% Year on Year Increase in Insider Risk Incidents

FortiGuard Lab Statistic

INDONESIA Security Outlook: 24 Sept 2023 – 30 Sept 2023

> 396 million exploit detected

> 614 hundred malware detected

IPS

No	Name	Total
1	DNS.PTR.Records.Scan	152.369.463
2	Backdoor.DoublePulsar	118.510.205
3	MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	82.990.524
4	MS.DNS.WINS.Server.Information.Spoofing	73.919.059
5	Memcached.UDP.Amplification.Detection	45.417.116

C2

No	Name	Total
1	Andromeda.Botnet	982.357
2	XorDDOS.Botnet	298.208
3	Mirai.Botnet	221.001
4	RotaJakiro.Botnet	217.000
5	BadRabbit.Botnet	202.065

AV

No	Name	Total
1	HTML/Phishing.CDM!tr	67.401
2	MSOffice/Agent.CF!tr.dldr	60.656
3	MSIL/Kryptik.AGIJ!tr	49.296
4	JS/ProxyChanger.GB!tr	26.492
5	NSIS/Injector.SCI4!tr	24946

No	Name	Total
1	Security Update 2023-02-07 from Google Chrome	11.757
2	VideoLAN Security Bulletin VLC 3.0.18	6.999
3	Microsoft .NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	2740
4	Microsoft Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2358
5	Microsoft .NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability	2327

Legend: ■ Government ■ Telco/Carrier ■ Construction ■ Retail/Hospitality ■ Technology ■ Healthcare ■ Energy & Utilities ■ Manufacturing ■ Education ■ Defense ■ Other

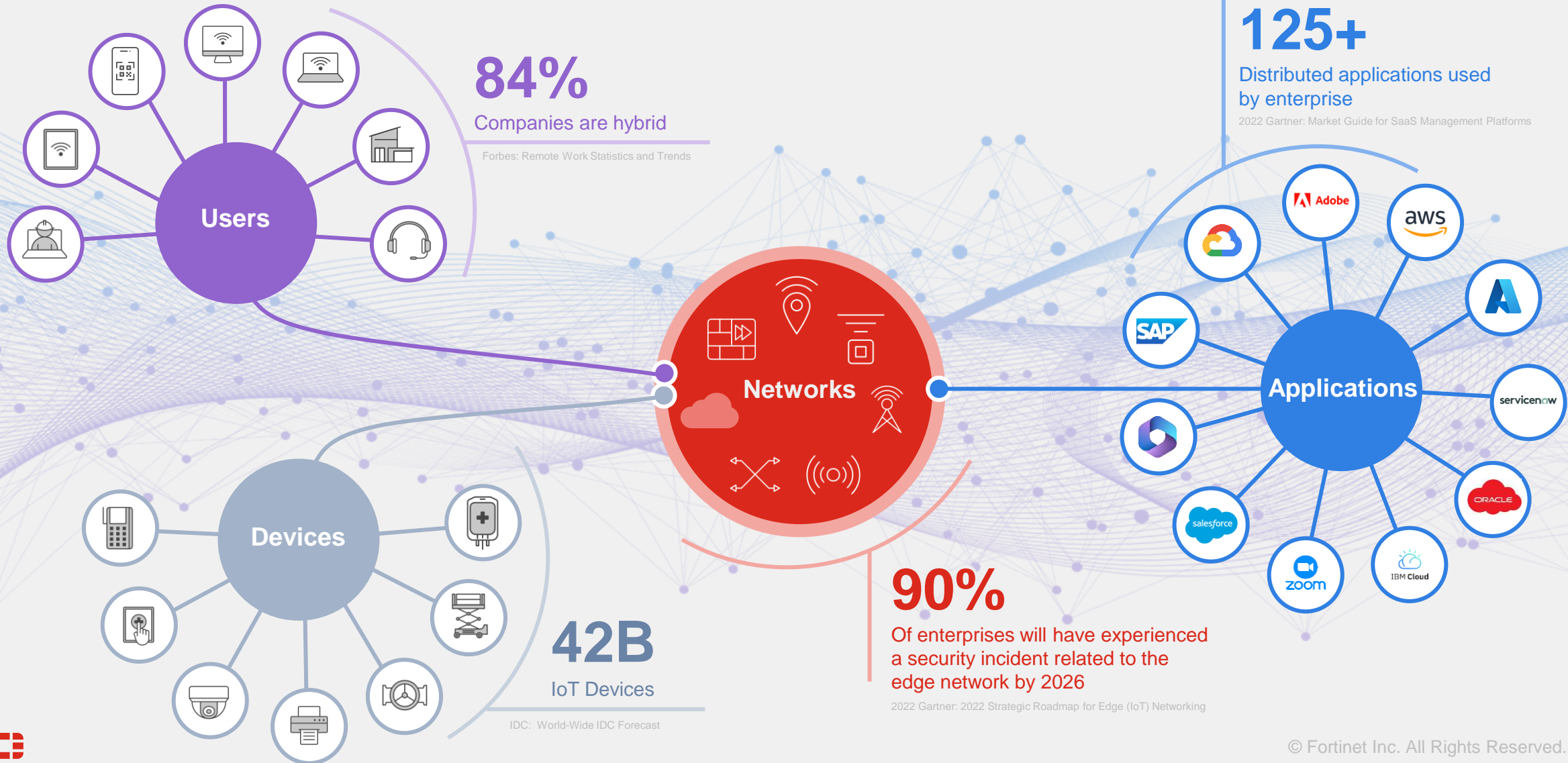# Threat Landscape Prediction by BSSN
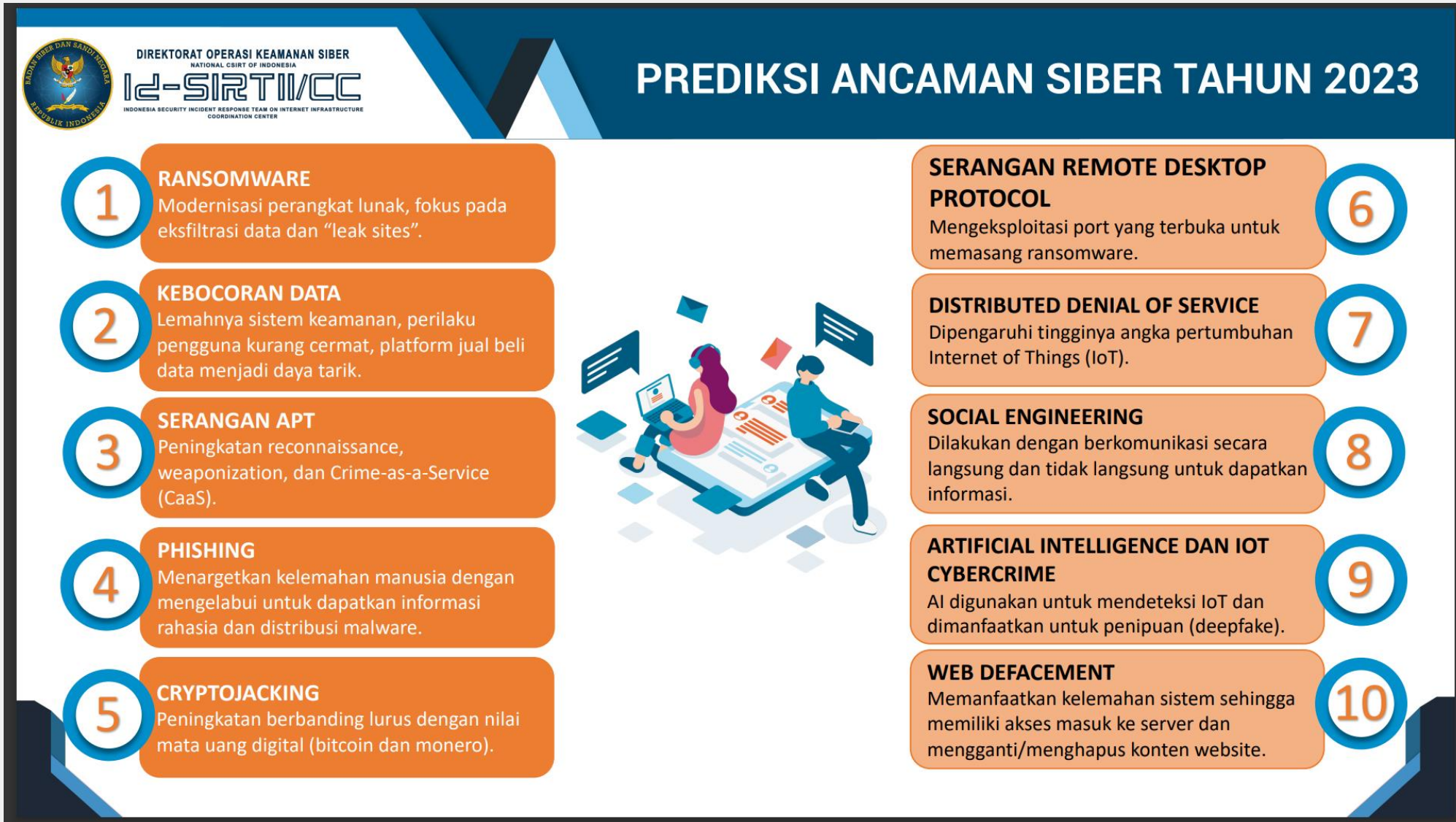
Sumber: LANSKAP KEAMANAN SIBER INDONESIA 2022, Direktorat Operasi Keamanan Siber, BSSN 2023

Infrastructure Has Become More Complex and More Vulnerable to Attack

84%
Companies are hybrid

Forbes: Remote Work Statistics and Trends

125+
Distributed applications used by enterprise

2022 Gartner: Market Guide for SaaS Management Platforms

Users

Networks

Applications

Devices

42B
IoT Devices

IDC: World-Wide IDC Forecast

90%
Of enterprises will have experienced a security incident related to the edge network by 2026

2022 Gartner: 2022 Strategic Roadmap for Edge (IoT) Networking

When attackers get in, they stay longer & cost you more

Average time from detection to remediation

21 Days (if at all)	12 hrs	6 hrs	12 hrs

■ Time to Detect   ■ Time to Contain   ■ Time to Investigate   ■ Time to Remediate
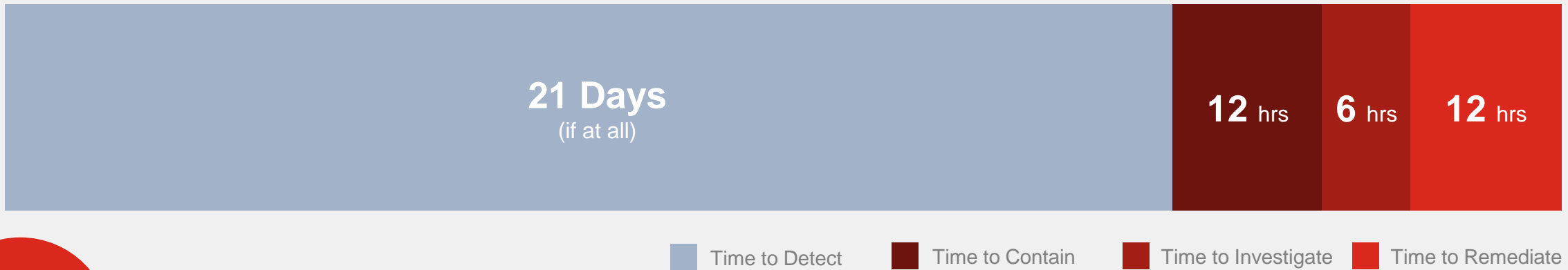
52%

of organizations report **SecOps** are harder than 2 years ago, cite threats, attack surface, volume/complexity[1]
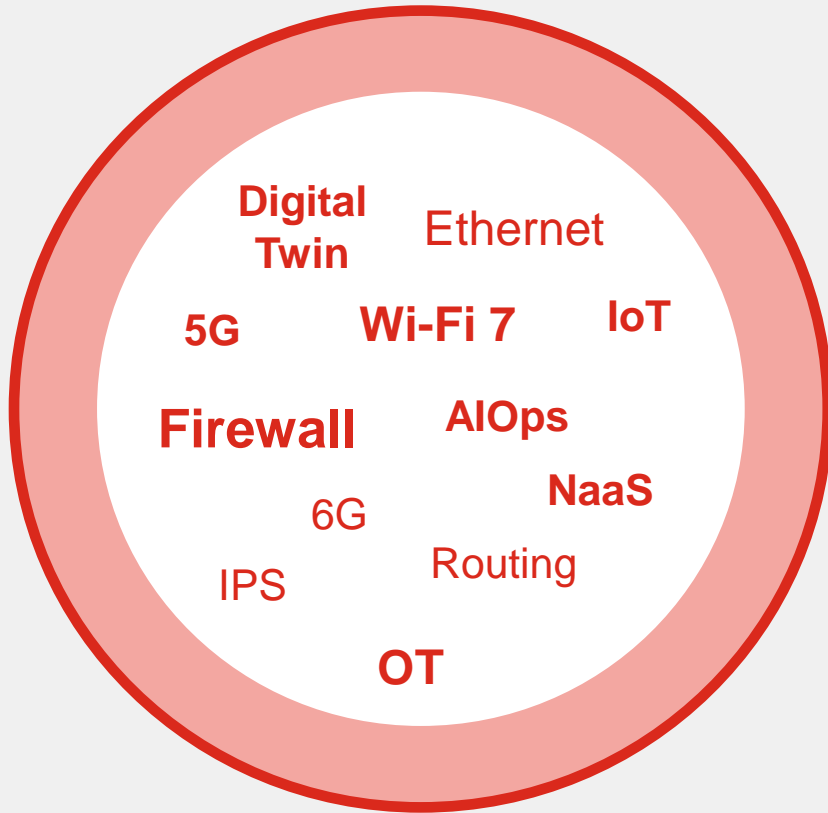
New SEC Rule

4 Days

to disclose material cybersecurity incident

$9.4M

Avg Breach Cost

The response has been a cybersecurity technology explosion

Secure Networking

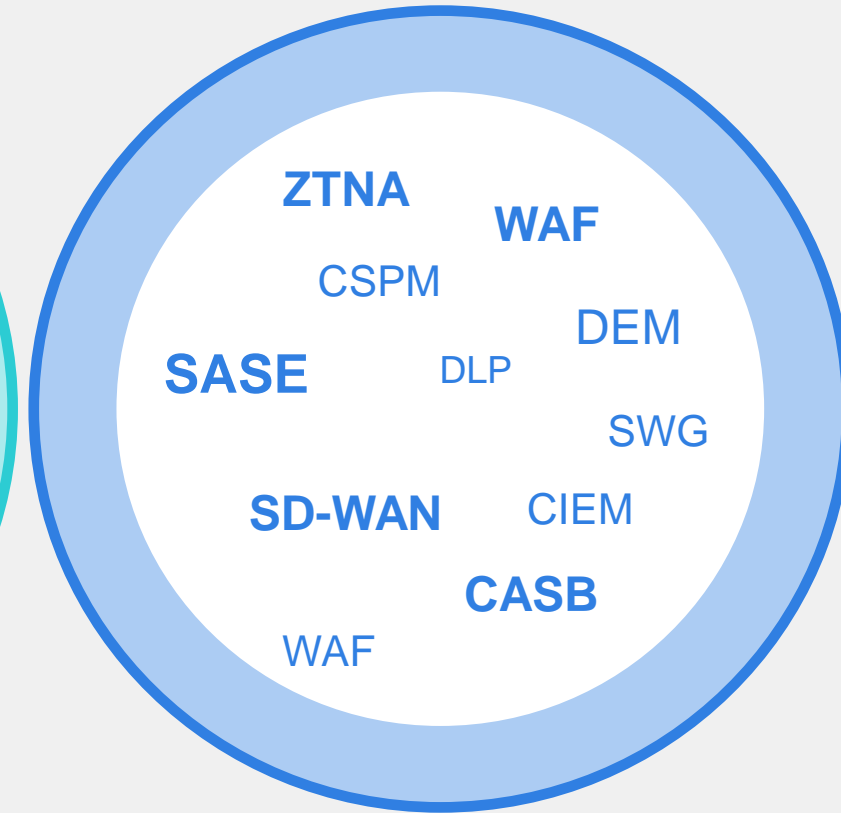Digital Twin
Ethernet
5G
Wi-Fi 7
IoT
Firewall
AIOps
6G
NaaS
IPS
Routing
OT

Security Operations

VMS
NDR
EASM
MDR
XDR
SOAR
MFA
EMAIL
EDR
SAT
SIEM
EPP
SANDBOX
DECEPTION
DRPS

SASE and Cloud

ZTNA
WAF
CSPM
SASE
DLP
DEM
SWG
SD-WAN
CIEM
CASB
WAF
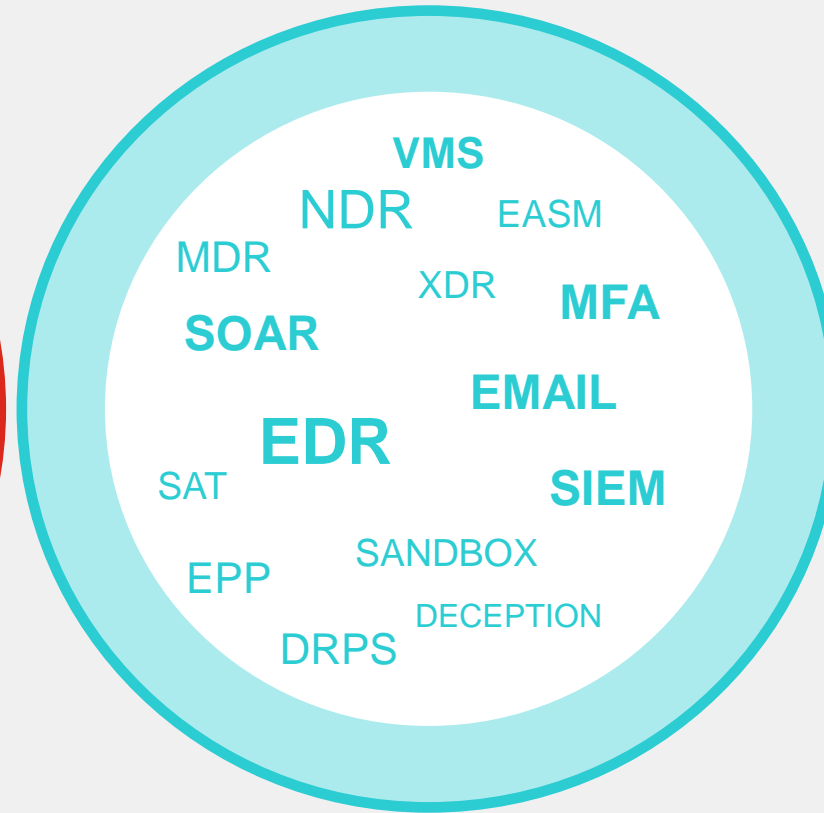
Consolidation is accelerating to reduce risk and minimize complexity

Organization pursuing a vendor consolidation strategy

2020

In 2-3 Years
51%

No
20%

Now
29%

80%

2022

This Year
18%

In 1-3 Years
4%

No
3%

Now
75%

97%
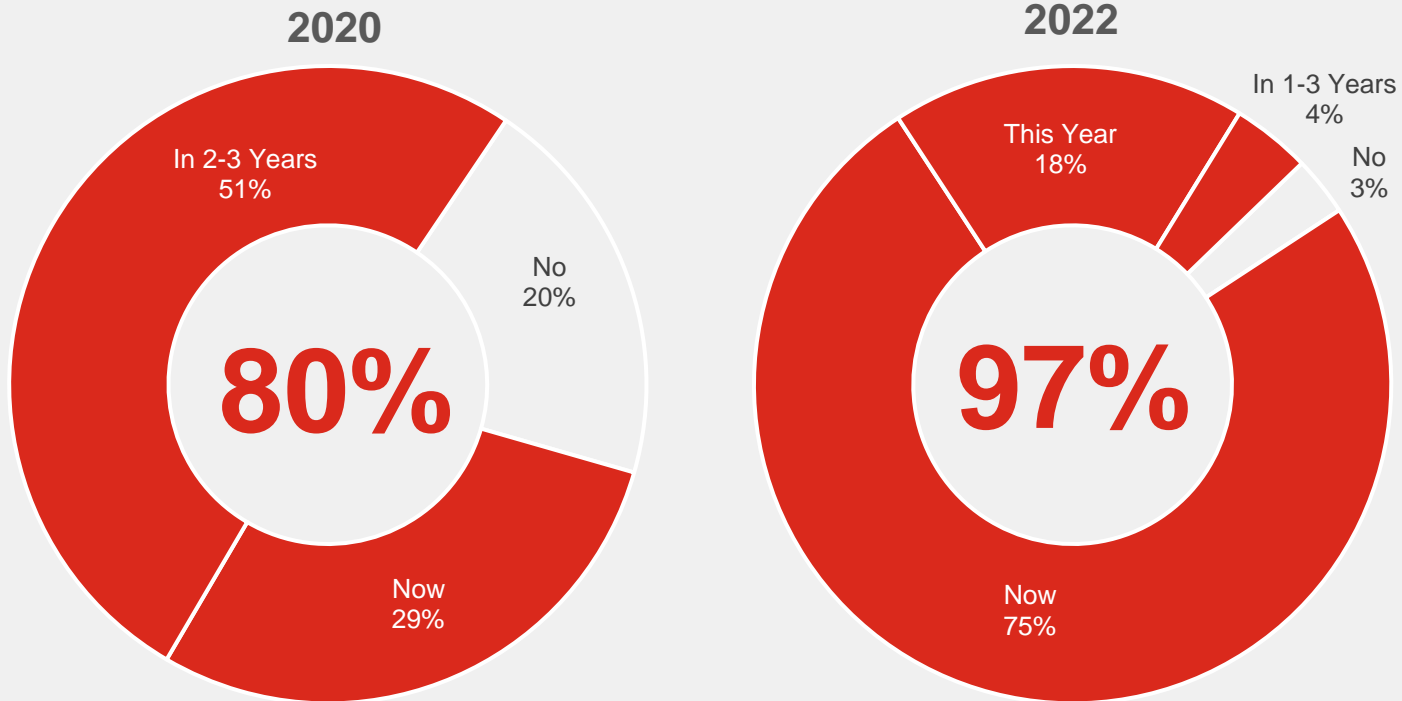
Primary reasons organizations are pursuing security vendor consolidation.

65%
Improve risk posture

59%
Improve security capabilities

42%
Fit vendor strategy within the organization

36%
Flat or reduced security team staffing

Gartner

How can we solve these problems?

One Platform – The Fabric Ecosystem

Secure Networking

CONVERGE

Security and networking convergence across all edges, users, and devices

Security Operations

CONSOLIDATE

Consolidated security operations platform to accelerate time to detect and respond

Universal SASE

CONSUME

Flexible consumption of security services to secure access & protect networks, applications & data on any cloud

AI-Driven Technologies   FortiCloud   FortiPoints   FortiGuard Labs   OT-Compliant   Ecosystem

Rev 1.0

Extend Protection Across the Entire Network with Unified Security

Secure Networking

Hybrid Mesh Firewall

Evolution of NGFW to Hybrid Mesh Firewall for unified management that simplifies operations, reduces risk and ensures compliance, at scale.

Accelerated ASIC | Branch | Campus | Data Center | Cloud Native | Virtual | FWaaS

Secure Connectivity

FortiLink converges networking and security for secure WLAN/LAN equipment to provide security and automation, improve visibility and control, and reduce TCO.

FortiLink | FortiAP | FortiSwitch | FortiExtender | FortiNAC
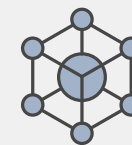
AI-Driven Technologies

FortiOS | FortiGuard Labs | AI for Networking (AIOPS) | Unified Management

Evolution to Universal SASE

Point Product Vendors

- SWG
- SD-WAN
- ZTNA
- Cloud
- NGFW
- CASB

50 Vendors

Dual-Vendor SASE

- SD-WAN
- NGFW
- SWG
- ZTNA
- CASB

20 Vendors

Universal SASE

- FWaaS
- Cloud
- SD-WAN
- SWG
- ZTNA
- CASB
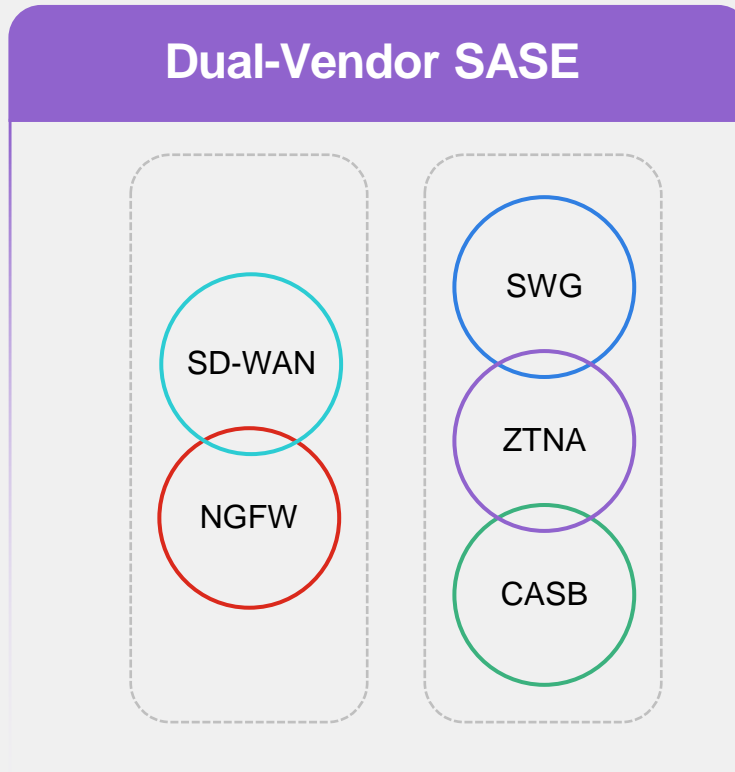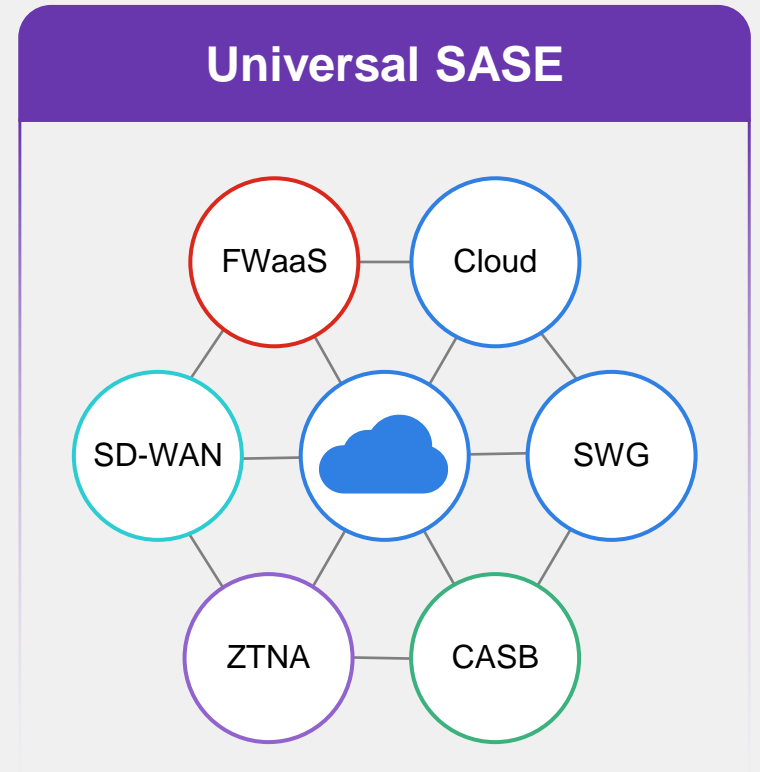
FORTINET

Universal SASE secures access and protects networks, applications, and data on any cloud

ZERO TRUST | DIGITAL EXPERIENCE

Remote Users

Branch, Campus

Users and devices are everywhere

FortiSASE SSE

FortiGate SD-WAN

Secure Internet Access
Secure SaaS Access
Secure Private Access

FortiWeb WAF

FortiGate Cloud Native Firewall

Appliance, Virtual, Cloud Native

Secure the Data
Secure the Applications & APIs
Secure the Network

Internet

salesforce Microsoft 365

SaaS

aws

Public Cloud

Data Center

Private Cloud

%

Customer Responsibility

Consistent security for applications that can live anywhere

Build → **Deploy** → **Run** →

Multi-cloud

	Application Security Testing	Cloud-Native FW Service	WAFaaS	Workload Protection	Global Server Load Balancing	Cloud-native Protection
	FortiDevSec	**FortiGate CNF**	**FortiWeb Cloud**	**FortiEDR**	**FortiGSLB**	**FortiCNP**
	DevSecOps	Network Security	Applications / APIs	Workload Protection	Load Balancing	Cloud-Native
	FortiDevSec	**FortiGate VM**	**FortiWeb VM**	**FortiEDR**	**FortiADC**	
	Application Security Testing	Virtual NGFW, SDWAN	WAF / WAAP	Workload Protection	Application Delivery Controller	Cloud Fabric Ecosystem

Data Center and Private Cloud

FortiManager / Security Fabric
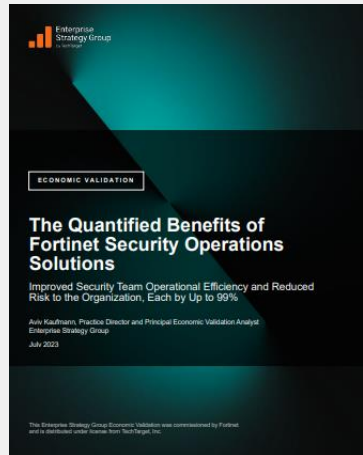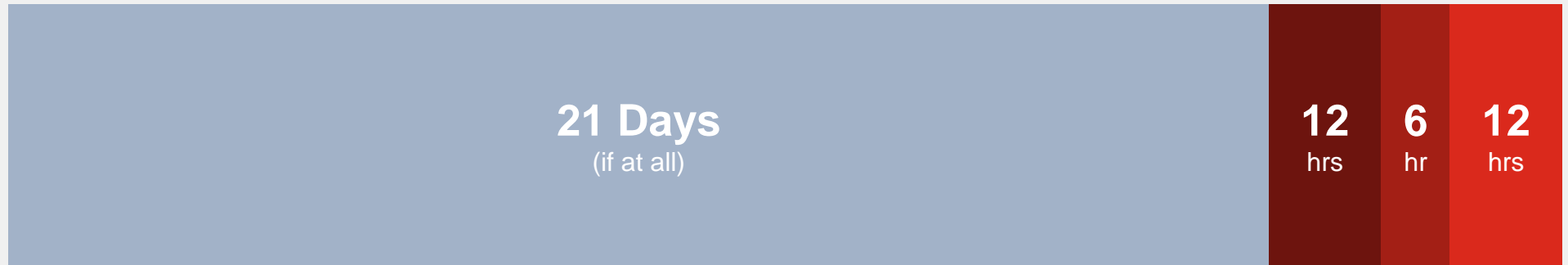
FortiGuard AI-Powered Security Services

Speed the time to fully investigate and remediate incidents from 18.5 hours to an average of 10 minutes.

Before
Fortinet SecOps Platform

| 21 Days (if at all) | 12 hrs | 6 hr | 12 hrs |

After
Fortinet SecOps Platform

■ Time to Detect   ■ Time to Contain   ■ Time to Investigate   ■ Time to Remediate

<1 hr

ECONOMIC VALIDATION

The Quantified Benefits of Fortinet Security Operations Solutions

Improved Security Team Operational Efficiency and Reduced Risk to the Organization, Each by Up to 99%

Aviv Kaufmann, Practice Director and Principal Economic Validation Analyst
Enterprise Strategy Group

July 2023

This Enterprise Strategy Group Economic Validation was commissioned by Fortinet and is distributed under license from TechTarget, Inc.

Fortinet Fabric Portfolio

Secure Networking

Hybrid Mesh Firewall

FortiGate Firewall

FortiGate VM Virtual Firewall

FortiCNF Cloud-native Firewall

FortiSASE Firewall-aaS

FortiGate Rugged NGFW

Secure Connectivity

FortiSwitch Switching

FortiAIOps AI For Networking

FortiAP Access Point

FortiNAC NAC

FortiSwitch Rugged Switch

FortiExtender LTE/5G

FortiAP Rugged AP

FortiExtender Rugged Extender

Universal SASE

FortiSASE SSE

FortiClient ZTNA

FortiGate VM Virtual Firewall

FortiCNP Cloud-native Protection

FortiGate SD-WAN

FortiMonitor DEM

FortiWeb (WAAP)

FortiADC Application Delivery

FortiToken MFA

FortiPAM PAM

FortiGate CNF Cloud-native Firewall

FortiDevSec Application Security Testing

FortiAuthenticator IAM

FortiTrust Identity

Security Operations

FortiEDR/XDR EDR/XDR

FortiAnalyzer Analytics

SOCaaS

FortiNDR NDR

FortiSIEM SIEM

MDR Service

FortiDeceptor Deception

FortiSOAR SOAR

IR Service

FortiRecon DRPS

FortiSandbox Sandbox

FortiMail SEG

One Platform – The Fortinet Security Fabric

Secure Networking

CONVERGE
Security and networking convergence across all edges, users, and devices

Security Operations

CONSOLIDATE
Consolidated security operations platform to accelerate time to detect and respond

Universal SASE

CONSUME
Flexible consumption of security services to secure access & protect networks, applications & data on any cloud

AI-Driven Technologies

FortiCloud

FortiPoints

FortiGuard Labs

OT-Compliant

Ecosystem