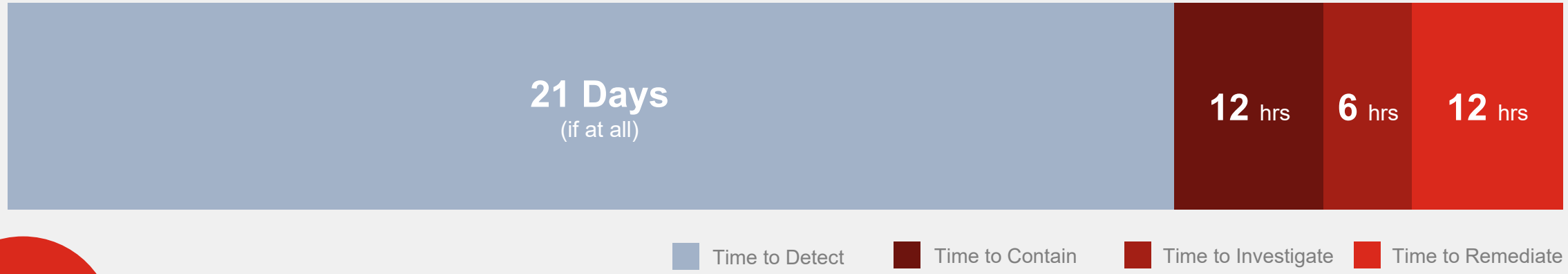
FORTINET

The Cyber Threat Landscape

Mike Lauer- National Director of Public Sector Programs

When Attackers Get In, They Stay Longer and Cost More

Average time from detection to remediation



52%

of organizations report SecOps is harder than 2 years ago, citing threats, attack surface, volume/complexity[1]

New SEC Rule

4 Days

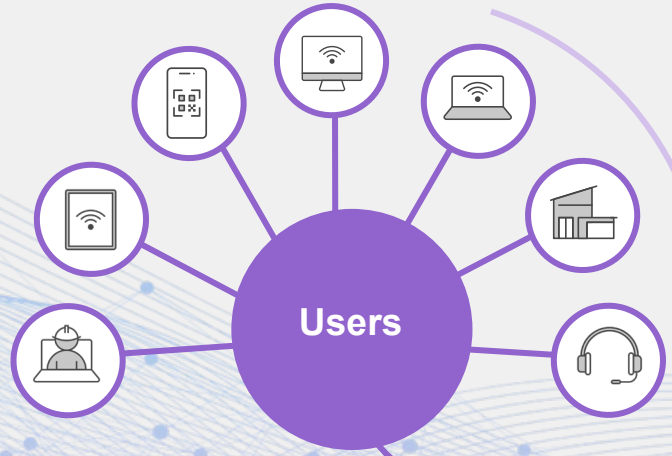
to disclose material cybersecurity incident

$9.4M

Avg Breach Cost

Source: Enterprise Strategy Group, 1. ESG Research, SOC Modernization Survey, October 2022.

Infrastructure Has Become More Complex and More Vulnerable to Attack



84%

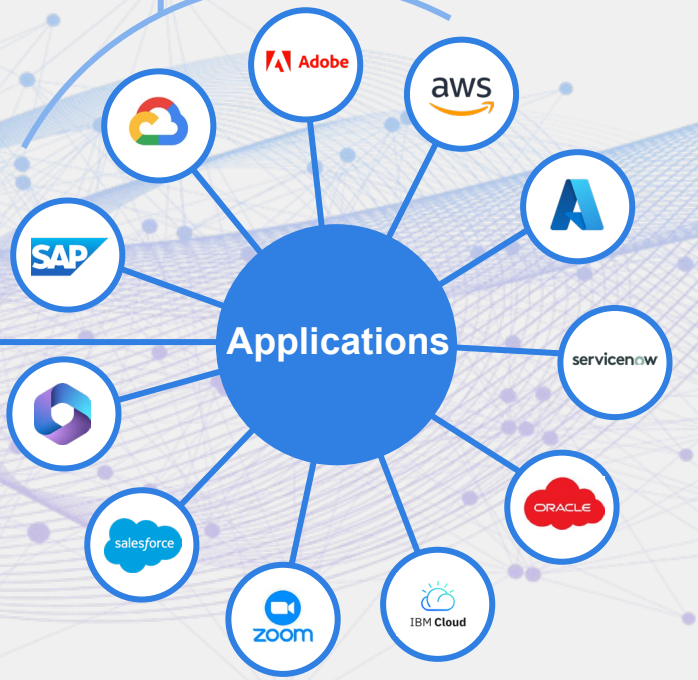
Companies are hybrid

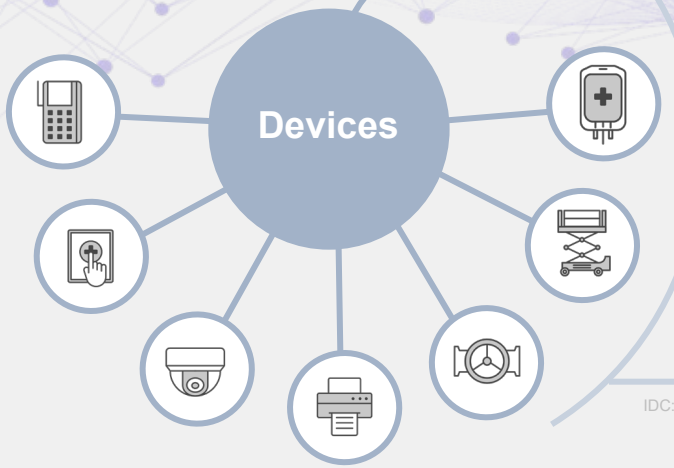
Forbes: Remote Work Statistics and Trends

125+

Distributed applications used by enterprise

2022 Gartner: Market Guide for SaaS Management Platforms





42B

IoT devices

IDC: World-Wide IDC Forecast

90%

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

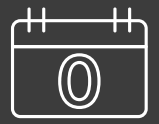
2022 Gartner: 2022 Strategic Roadmap for Edge (IoT) Networking

To 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 2023

RANSOMWARE & WIPERS

Ransomware infection times falls from 5 days to 5 hours

CLOUD RISKS

69% of companies use two or more clouds

SUPPLY CHAIN ATTACKS

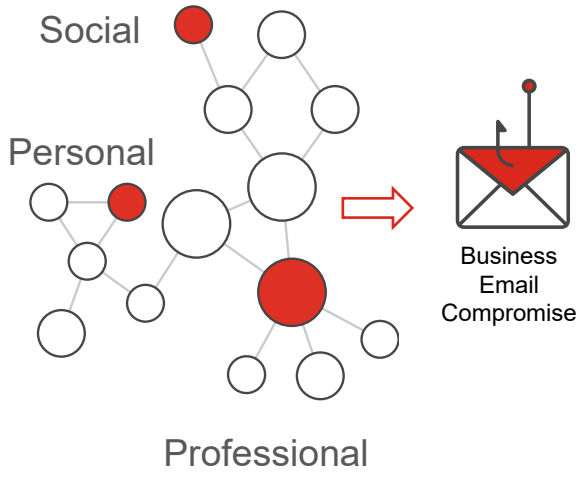
12% of data breaches originated with a software supply chain attack

INSIDER RISK

+32% year-on-year increase in insider risk incidents

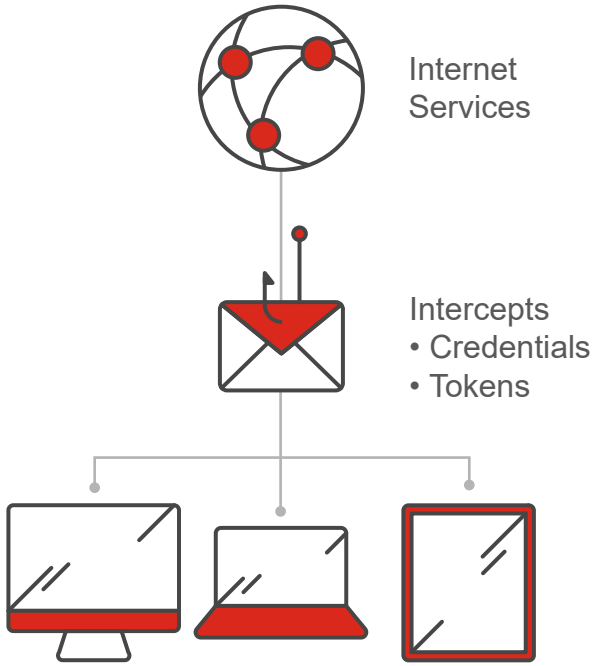
Spear Phishing and Deep Fakes

More Targeted



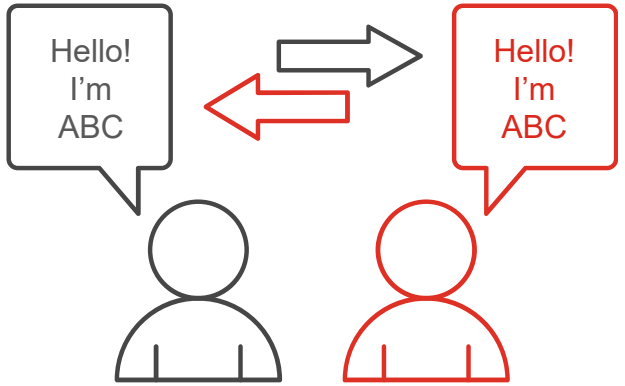
Cross-Platform Profiling

More Automated



Phishing-as-a-Service

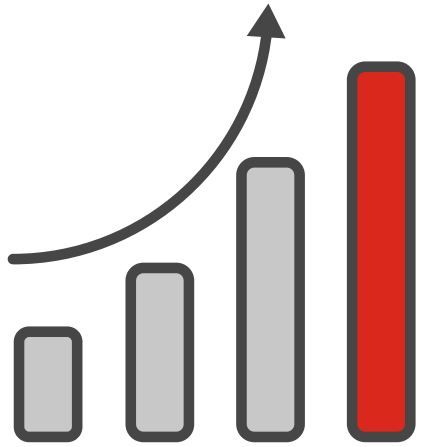
More Channels



Voice impersonation

Zero-Day Vulnerabilities

Vulnerabilities are Increasing

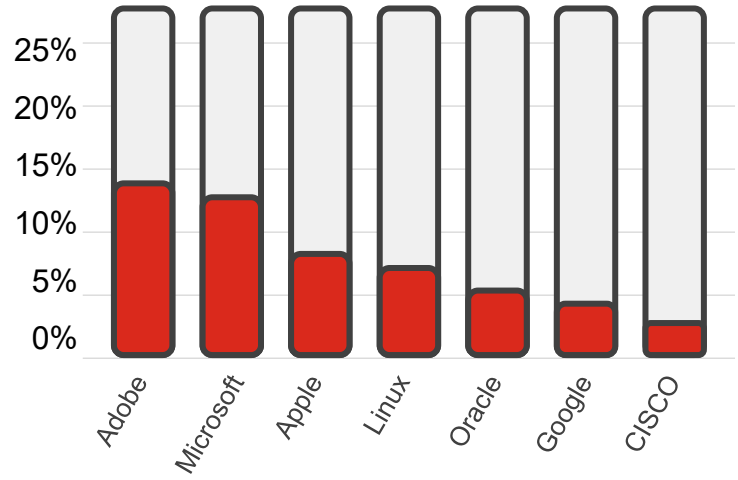


24% Growth in Published CVEs

Exploit Speed is Increasing

MOVEit vulnerability disclosed just **5 days** before exploit attempts seen

Platform Exploitation

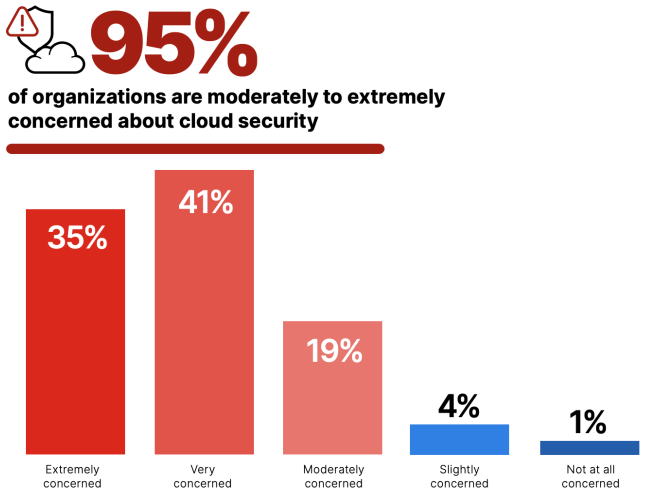


The larger the platform the more vulnerabilities and attacks

Cloud Risks

Hybrid and Multi-Cloud

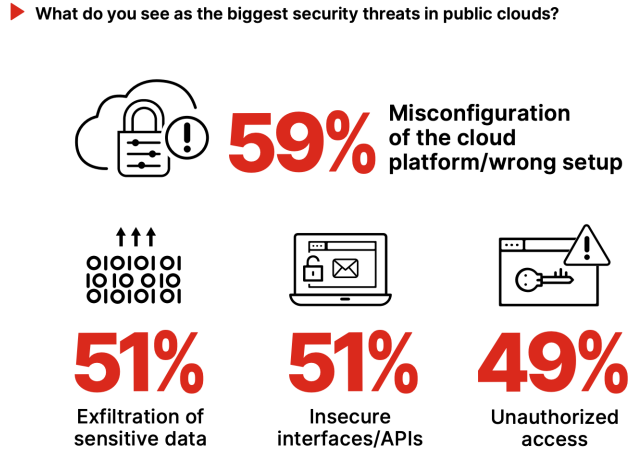
Increased Complexity is outpacing the team's Skills



Fortinet | 2023 Cloud Security Report

Misconfiguration

Moving too fast



Fortinet | 2023 Cloud Security Report

Breaches of Dark Data

Rapid cloud transition has resulted in a data dumping ground

82%

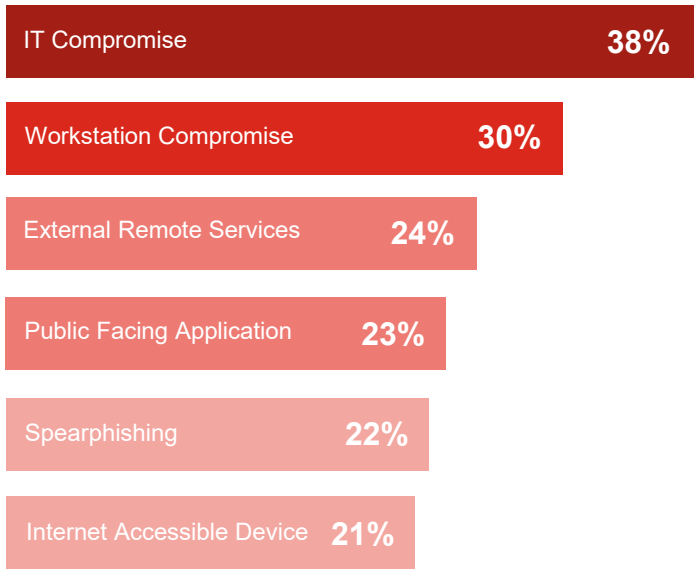
Share of breaches that involved data stored in cloud environments—public cloud, private cloud or across multiple environments

https://www.ibm.com/reports/data-breach

Cyber-Physical System Attacks

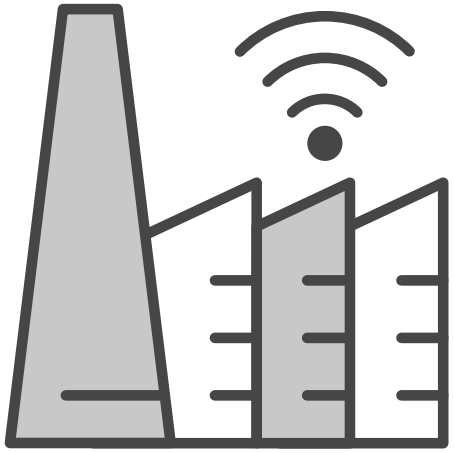
Convergence of IT/OT

Ranking of initial attack vectors in OT/control systems incidents



Removal of Air Gaps is exposing OT

Manufacturing & Energy Held Hostage



Cyber Crime shifting industries to monetize production disruption

Weaponization of OT

Pipedream Impact Summary

5

ICS protocols abused:
FINS, MODBUS, CODESYS, OPC UA, Schneider Electric NetManage

3

ICS-specific malware components inside Pipedream

1000s

of suppliers impacted

1000s

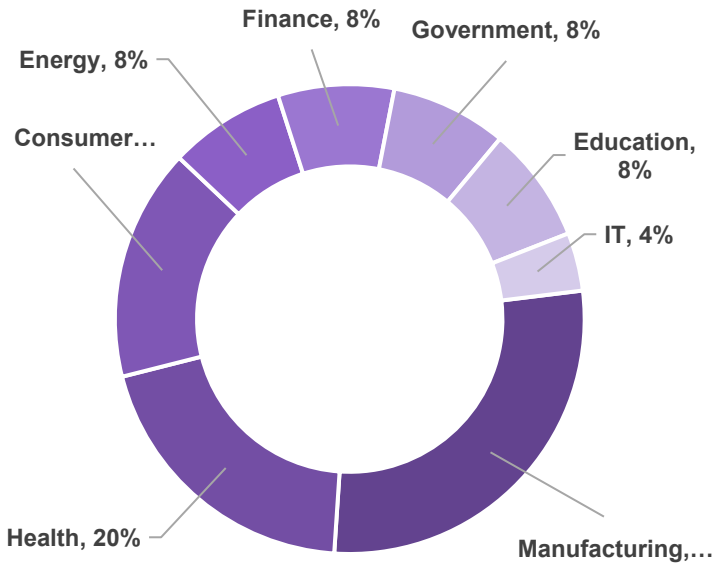
of devices impacted

OT attack kits like Pipedream are lowering the bar, no expertise needed

1. SANS ICS/OT Cybersecurity Survey: 2023's Challenges and Tomorrow's Defenses, 2. *Internal report, FGD Labs Spotlight on Manufacturing and Energy & Utilities* (https://fortinet.highspot.com/items/65034442d240f6c3ba787c58), 3. https://www.dragos.com/year-in-review/

Ransomware & Wipers

More Targeted to Industry



Ransomware incident and recovery engagements by industry

Faster Infections

2021

5.5 days

2022

4.5 days

2023

< 24 Hours

Ransomware infections times falls from 5 days to 5 hours

More Levels

Extortion

$ Encrypt data and hold for ransom

Double Extortion

$ $ + threat to release publicly if ransom not paid

Triple Extortion

$ $ $ + threaten to release customer's data if ransom not paid

Quadruple Extortion

$ $ $ $ + threaten to destroy the data to make it unrecoverable

Increasing pressure to keep paying

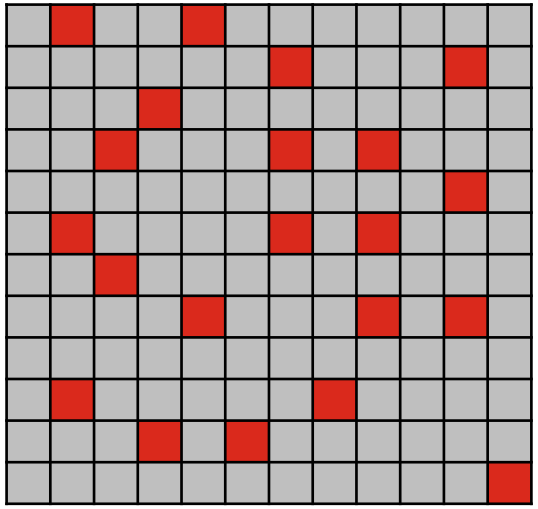
APT Threat Actors

More Nation State Attacks

- Intellectual Property
- Financial Gain
- Terrorism
- Political Espionage
- Hacktivism

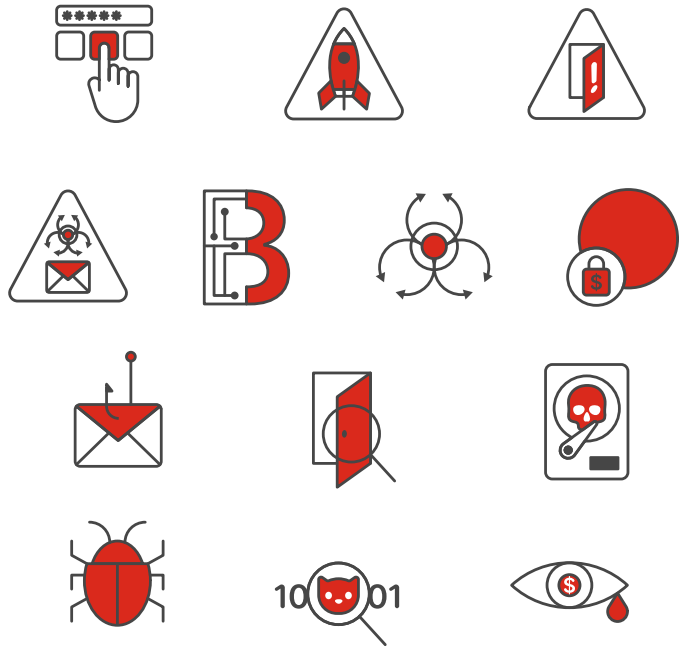
Nation states have different motives

More APT Groups Active



30% of APT groups were detected as active in 2023

More Sophistication



Threat actors are expanding their playbooks

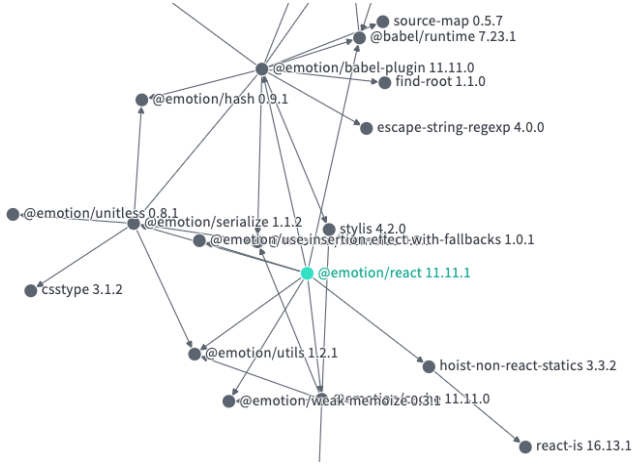
Supply Chain Attacks

Open Source Software is Leveraged Everywhere

The building blocks of modern enterprise applications

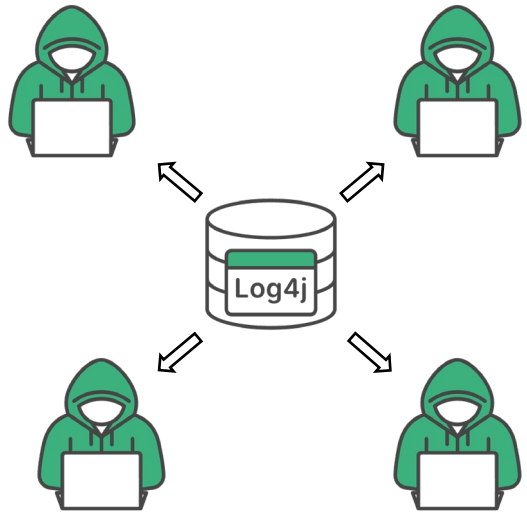
Most Apps Have Many Direct and Indirect Dependencies

They all come with the potential for vulnerabilities



Vulnerabilities in Widely Used Components Hit Hard and Fast

Multiple threat actors jump in with their own attacks



[Addressing Cybersecurity Challenges in Open Source Software - Report.pdf (hubspotusercontent-na1.net)]

Insider Risks

Not All Insider Threats are Malicious Intent

Process negligence and careless accidents difficult to detect

Privileged IT Users Pose the Highest Risk

Especially if disgruntled

2023_Insider_Threat_Report-16d8d8f7.pdf (cybersecurity-insiders.com)

Misuse of Privilege to Commit Fraud

Privileged access-based fraud on the rise

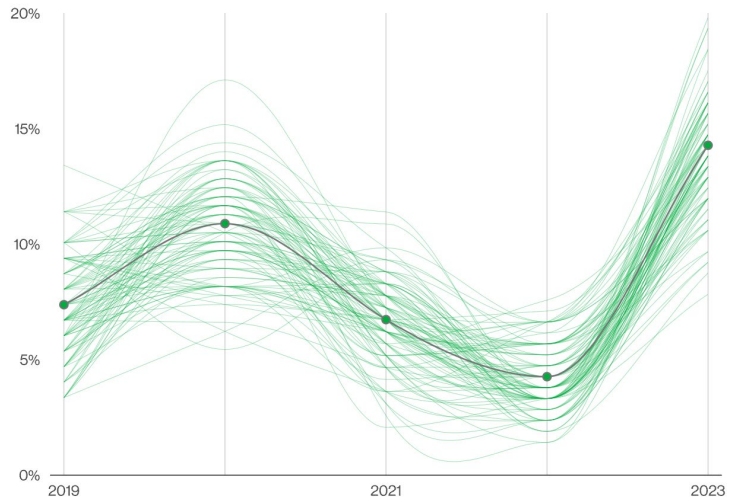


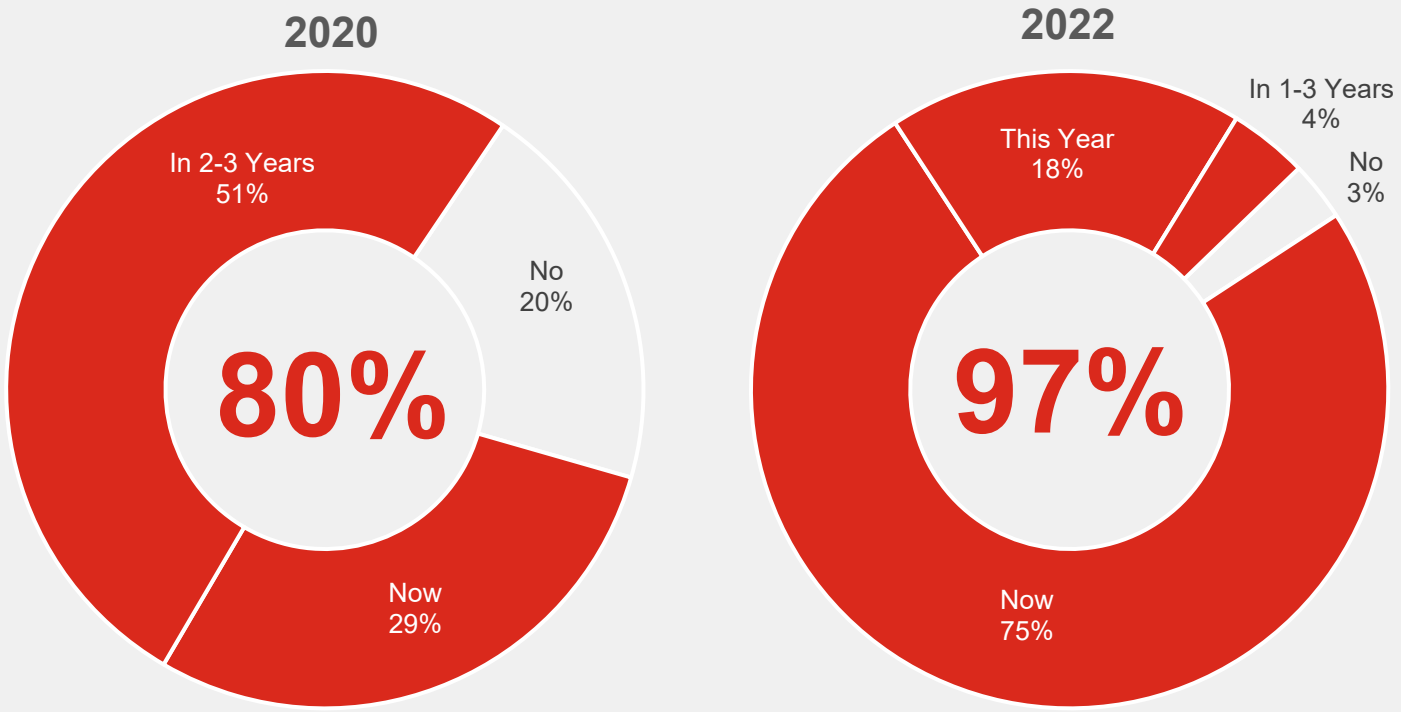
Figure 49. Fraudulent transactions in Privilege Misuse breaches

2023 Data Breach Investigations Report | Verizon

Addressing the Threats

Consolidate: Accelerating to Reduce Risk and Minimize Complexity

Organizations pursuing a vendor consolidation strategy



Primary reasons organizations are pursuing security vendor consolidation

65%
Improve risk posture

59%
Improve security capabilities

42%
Fit vendor strategy within the organization

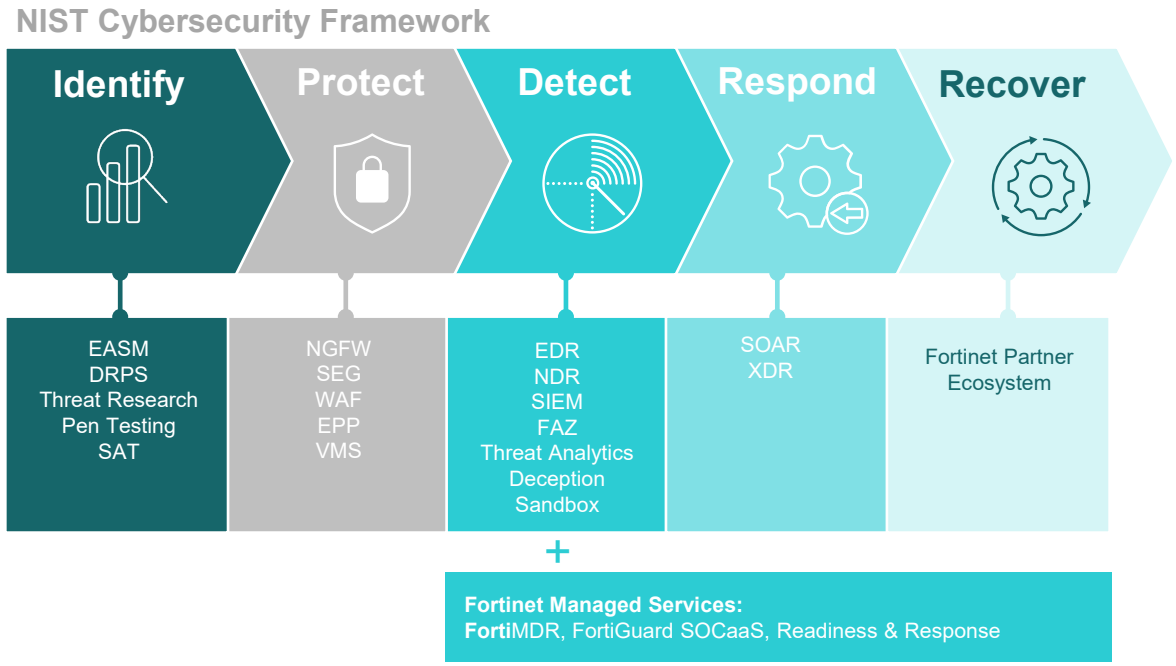
36%
Flat or reduced security team staffing

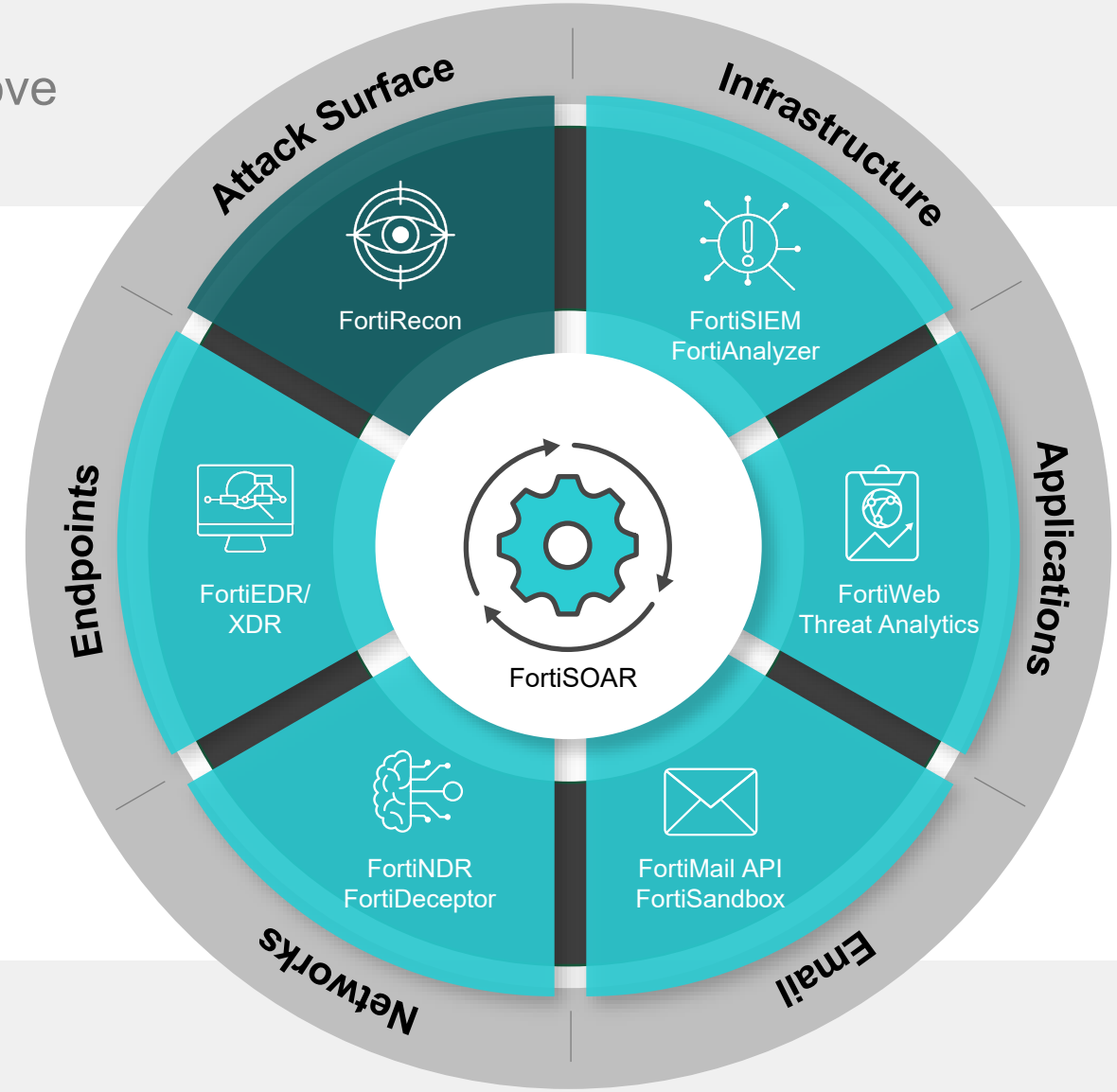
Gartner

Source: 2022 Gartner CISO Security Vendor Consolidation XDR and SASE Trends Survey

Automate: Using AI Solutions to Detect and Respond to Threats Faster

Alignment to NIST cybersecurity framework to improve risk management





Federate: Whole-of-State approach with a Mesh Platform

Source: MS-ISAC Whole-of-State Webinar Series April 28, 2022

- Shared Cyber Risk
- Economies of Scale
- Reduced Duplication of Effort
- Reduced Cost
- Consistency of Service
- Knowledge Sharing and Collaboration
- Standardized Processes, Methods, Technologies
- Increased Training Efficiencies
- Streamlined Visibility
- Improved Measurement