RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: PART2-W01

Importance of Cybersecurity Mesh Platform in Securing Digital Acceleration

John Maddison

Fortinet
CMO and EVP Products and Solution

RSAConference2022

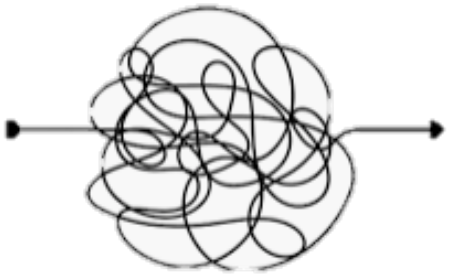
How Did We Get Here

Cybersecurity Historical Prospective

	2000 - 2010	2011-2020	2020+
Cybersecurity Technology	Signature Based Protection	Detection and Response	AI & Automation
	Antivirus, Antispam, URL Filtering	EDR, Sandbox, NDR	ML/AI, Operations
Infrastructure	New Threat Vectors	Expanded Attack Surface	Distributed Attack Surface
	Files, Email, Web	WFA, Mobile, Cloud	OT/IoT, 5G, Edge
Industry	Endpoint Security	Network Security	Platform Security
	Endpoint	Network	Endpoint, identity, Network, Native

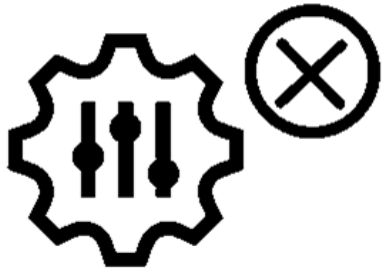
Current State – No Synergy

In other words: lack of foundation to capitalize on today's advanced technologies delivering centralized and automated Detection to Response at machine speed



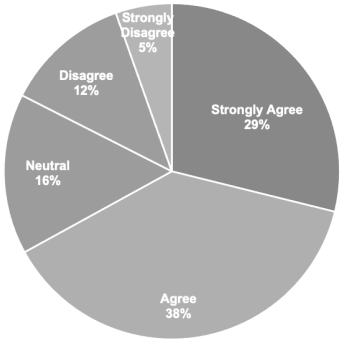
Complexity

Security and networking
Point product complexity



Many Silver Bullet(s)

Hard to balance best of breed with integrated and synergetic security



Silo Operations

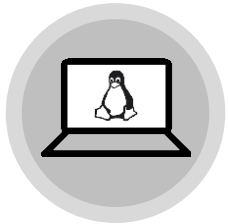
Security tools and teams that work in silos, and require manual work

Overwhelmed Humans

Skill shortage + high volume threat = overwhelmed security teams

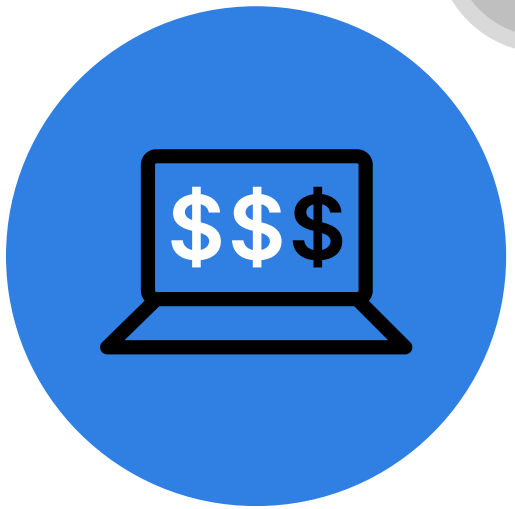
Why Should We Shift to Prioritize Synergy Over Silver Bullets?

2022 threat landscape summary



Sharp Increase in
Linux Malware & Exploits

E-Sport Platforms
Targeted



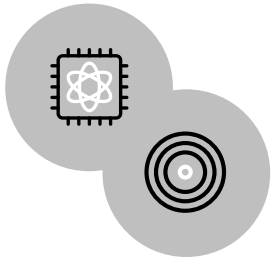
Advanced Persistent Cybercrime

MITRE ATT&CK Techniques

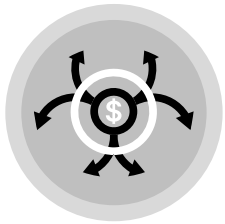
Sophistication and Speed

Weaponization of AI

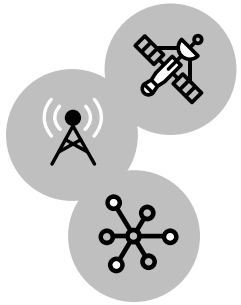
Edge Environment
Attacked



OT Targeted with
Ransomware & Killware



Aggressive, Destructive
Ransomware

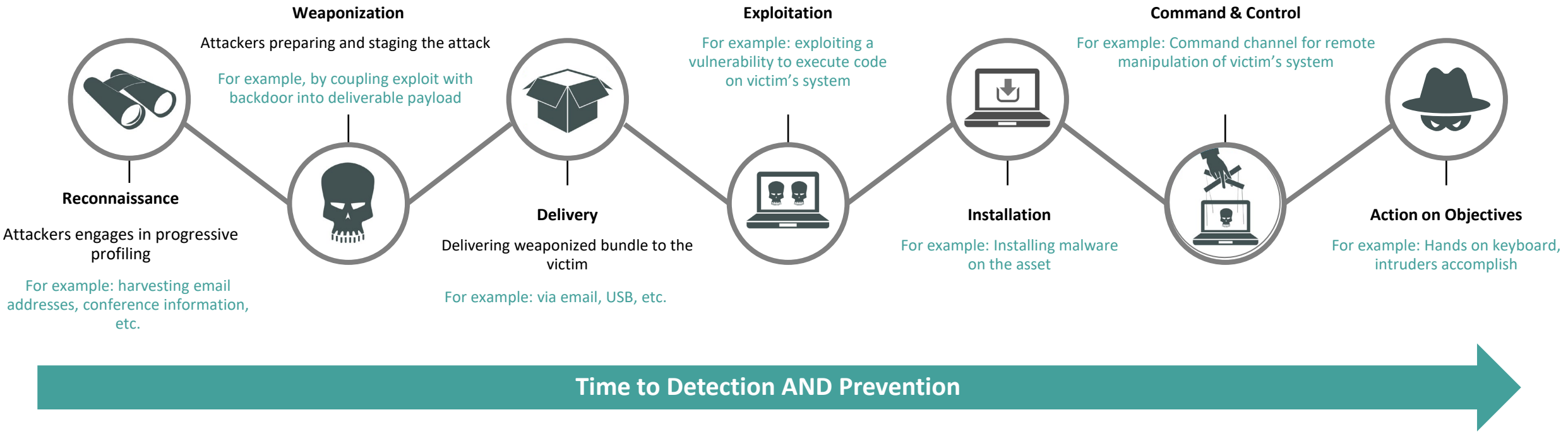


Threats Traverse Satellite
Communication

Cryptominers,
Crypto Wallets Targeted

Why Should We Shift to Prioritize Synergy Over Silver Bullets?

- Attacks are a progressive sequence of well coordinated, automated morphing events.
- WE are fighting against time, that can be shorten only by AI-powered automation.
- The foundation to effective automation is cybersecurity ecosystem level Synergy.



Current Problem to Be Solved

Gain the ability to operate at machine capacity and speed against machines

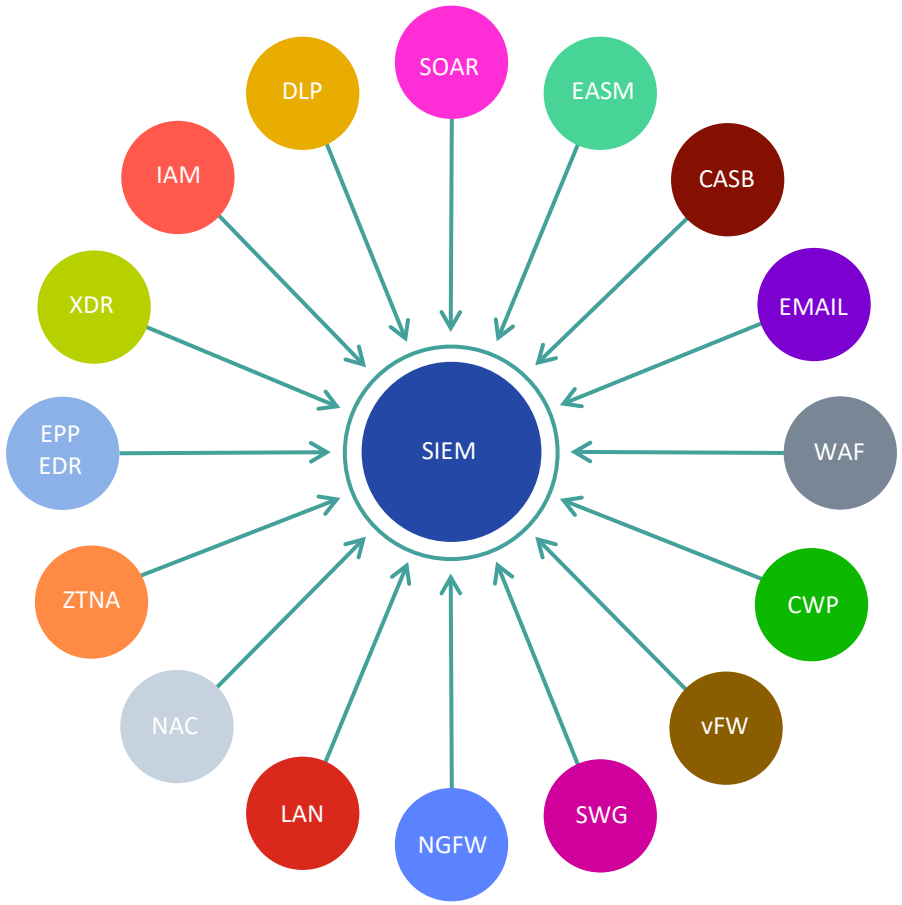
Click to add text

The Mesh architecture levels up the battlefield and highlight a path to
Autonomous Security Posture

Consolidation of Security Point Product Vendors

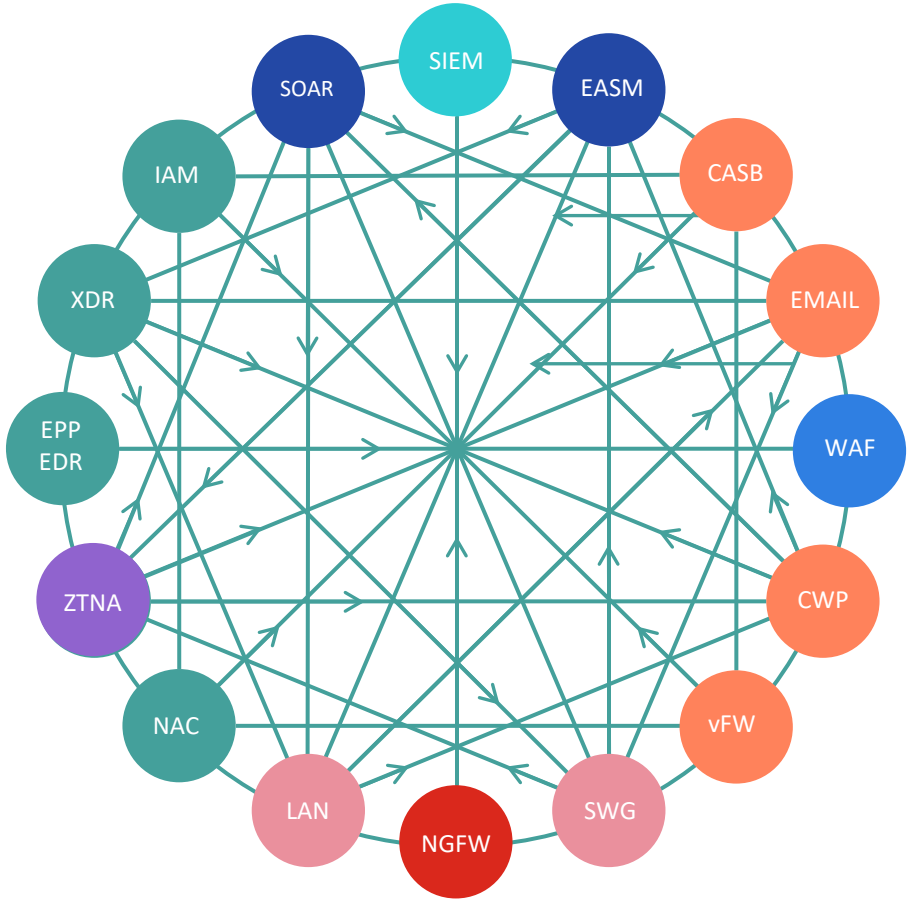
Gartner Cybersecurity Mesh Architecture (CSMA)

Cybersecurity Point Products



20 Vendors

Cybersecurity Platform Approach



4-6 Platforms

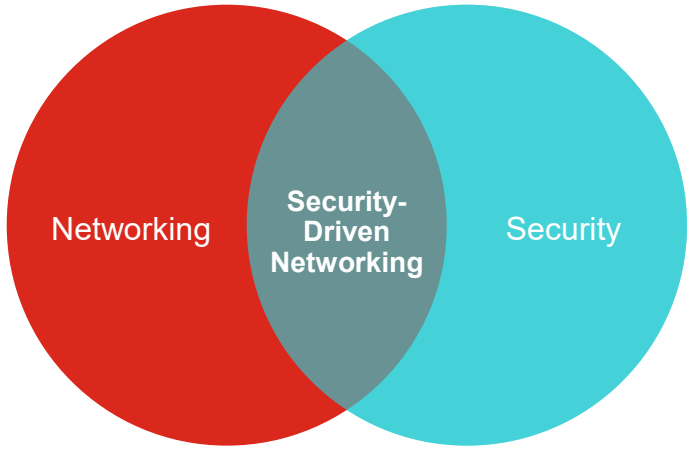
RSAConference2022

A Path to Autonomous Security Posture

Autonomous Security Posture

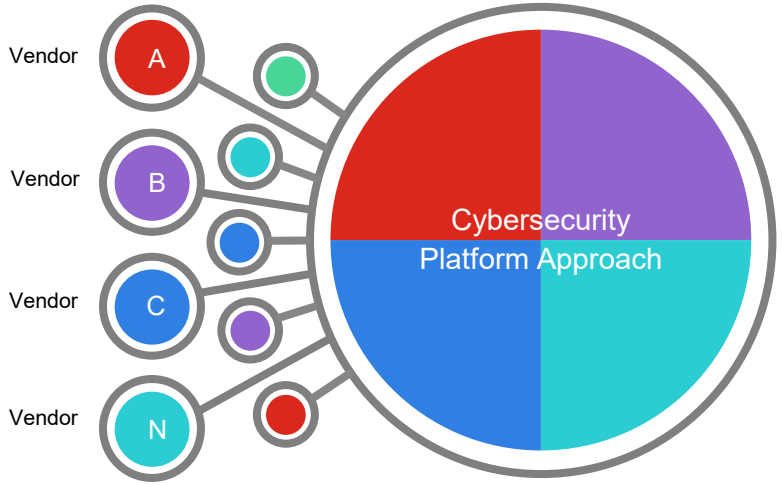
What needs to be done

Reduce Complexity



Convergence of Networking and Security

Create Synergy



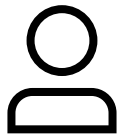
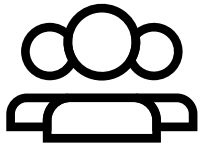
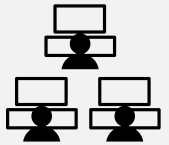
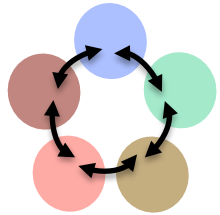
Consolidation of Security Point Product Vendors

Centralize & Automate

AI Powered Network and Security Operations

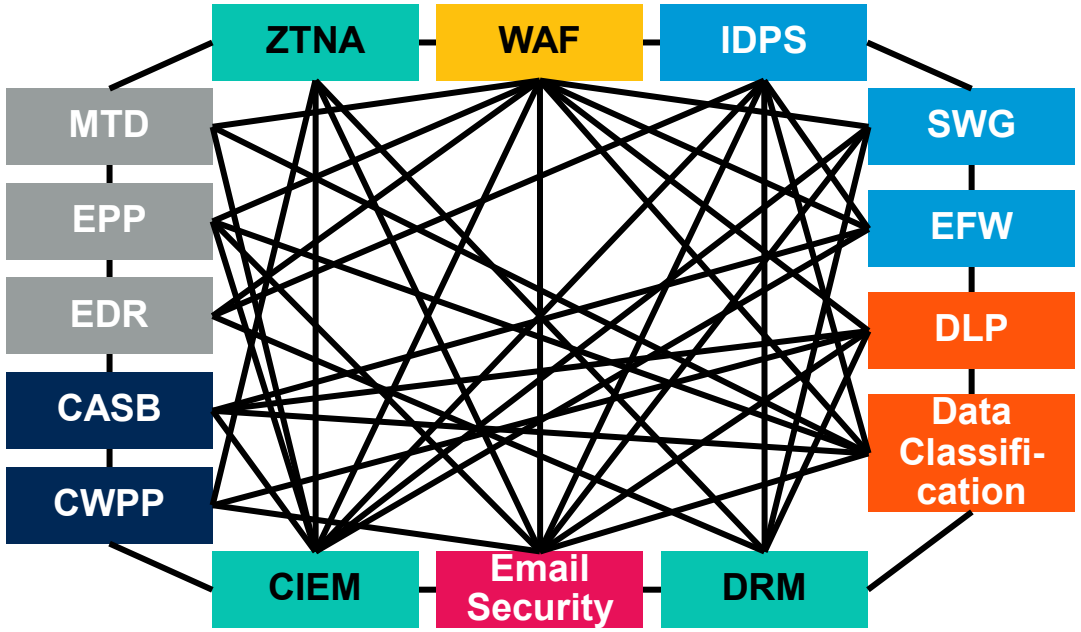
Convergence vs. Consolidation

What are the differences?

	Convergence	Consolidation
Vendors	1	1-3
Teams	 One	 Multiple
Consoles	 One	 Multiple
Products	 One	 Multiple

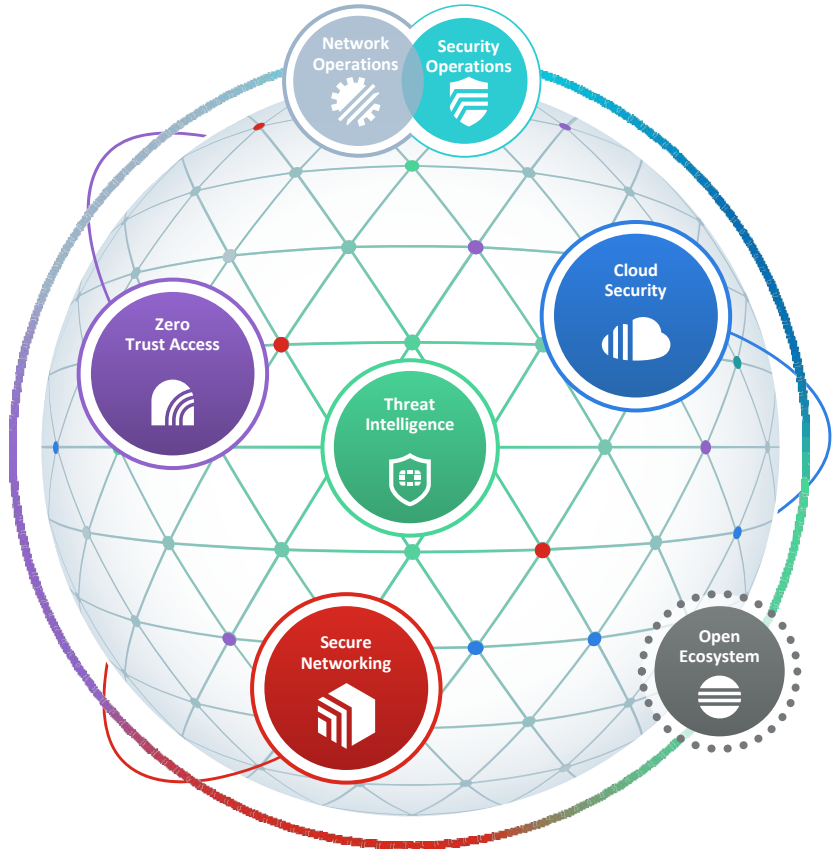
Gartner Cybersecurity Mesh Architecture

Gartner®



Executive Guide to Cybersecurity Mesh, 2022 Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021.

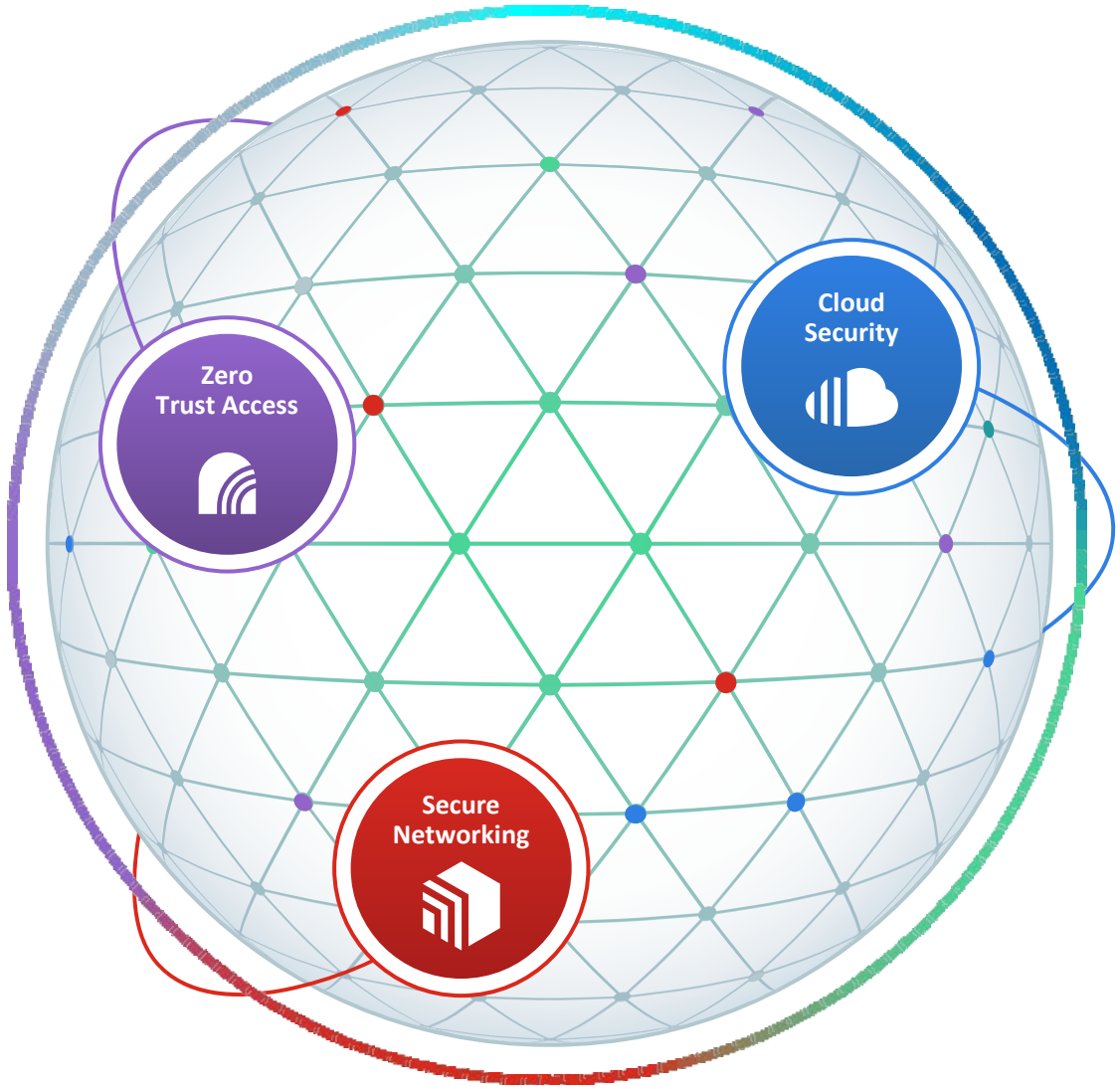
FORTINET®



Fortinet Security Fabric

Broad

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



Appliance

Virtual

Hosted

Cloud

Agent

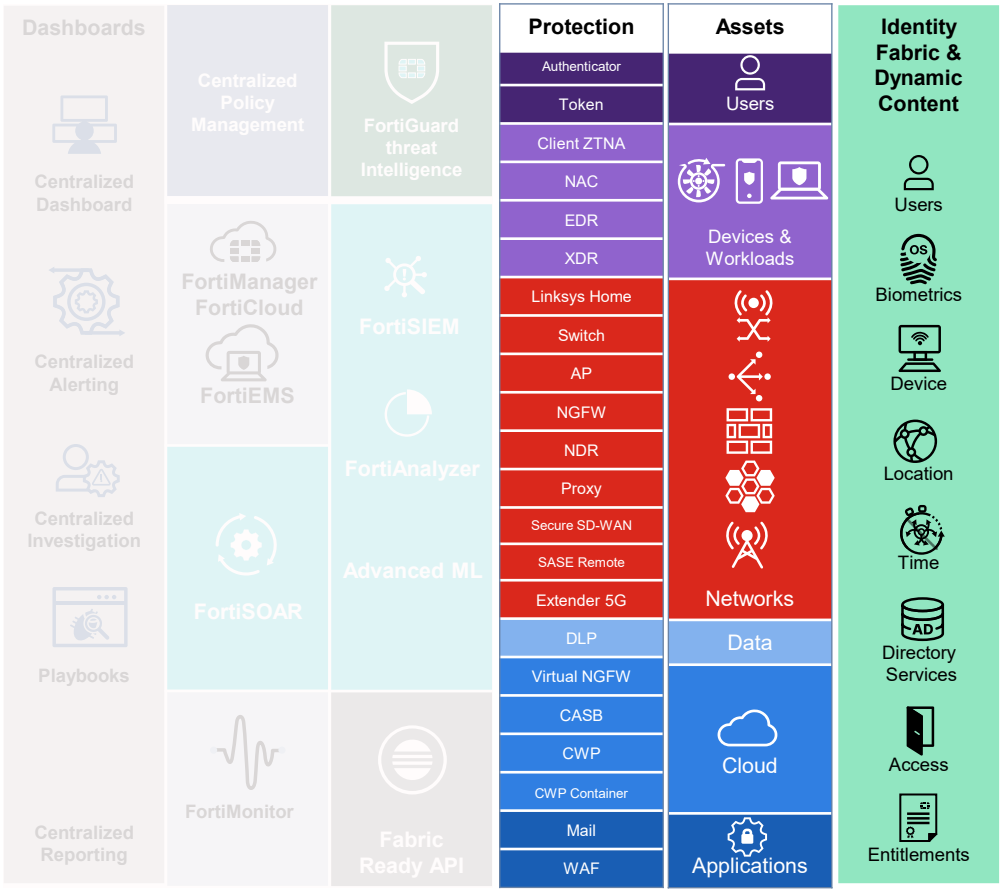
Container

Under the Hood

Implementing a Cybersecurity Mesh Fabric Architecture

Broad

- Have **broad reach across the attack surface** for detection, signals, IoC, incident and enforcement close to the protected assets
- **Gain coverage** across the attack cycle **with domain expertise**
- **Share context** and **intelligence** to provide granular risk and Identity score



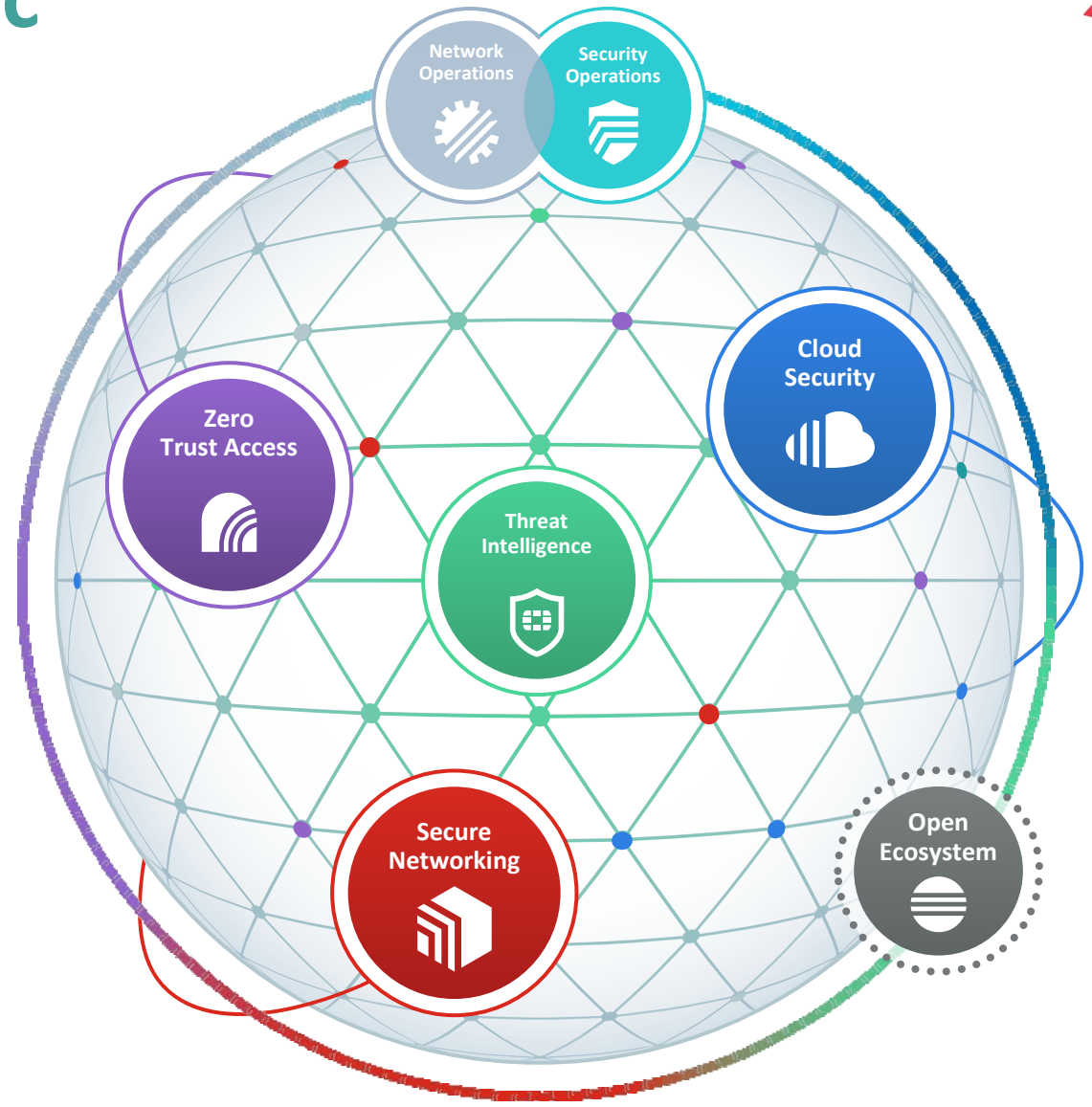
Fortinet Security Fabric

Broad

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

Integrated

solution that reduces management complexity and shares threat intelligence.

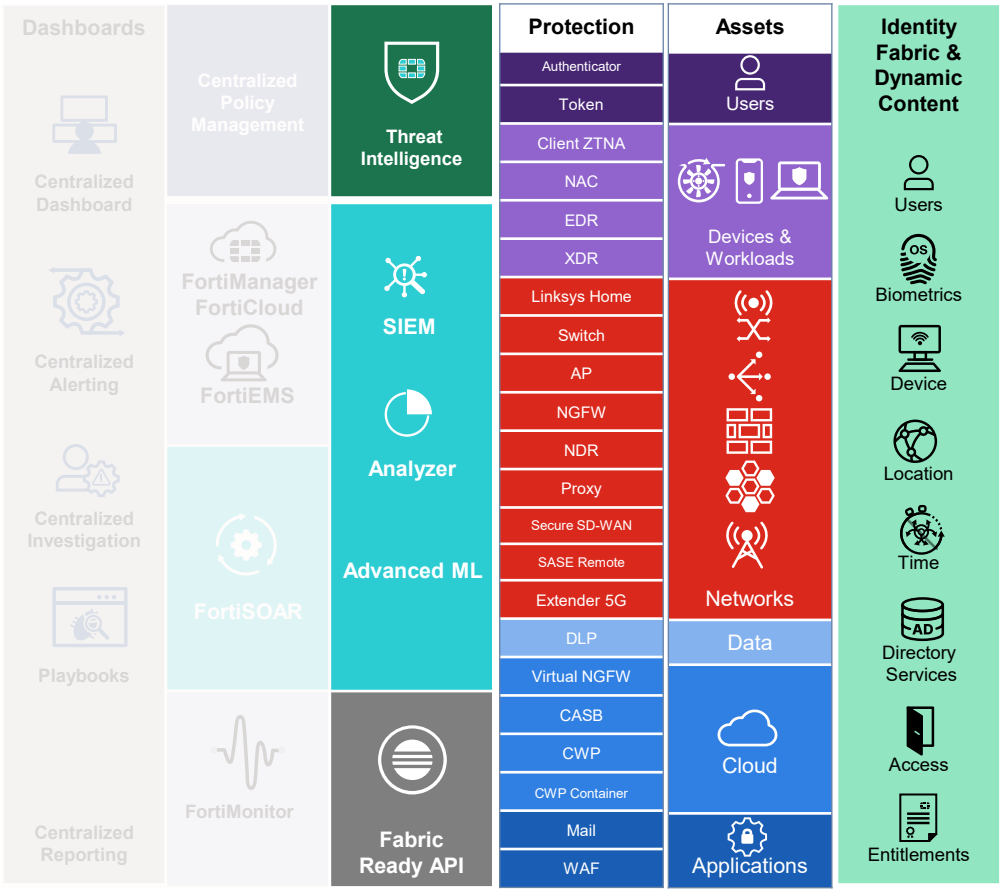


Under the Hood

Implementing a Cybersecurity Mesh Fabric Architecture

Integrated

- **Normalize security and networking data** to create a complete view across your organization's attack surface and attack cycle
- **Enrich** your data
- Create a **central point of correlation,** and leverage multiple forms of ML (centralized, distributed, and federated) to build proactive and centralized intelligence.



Ecosystem Is A Must

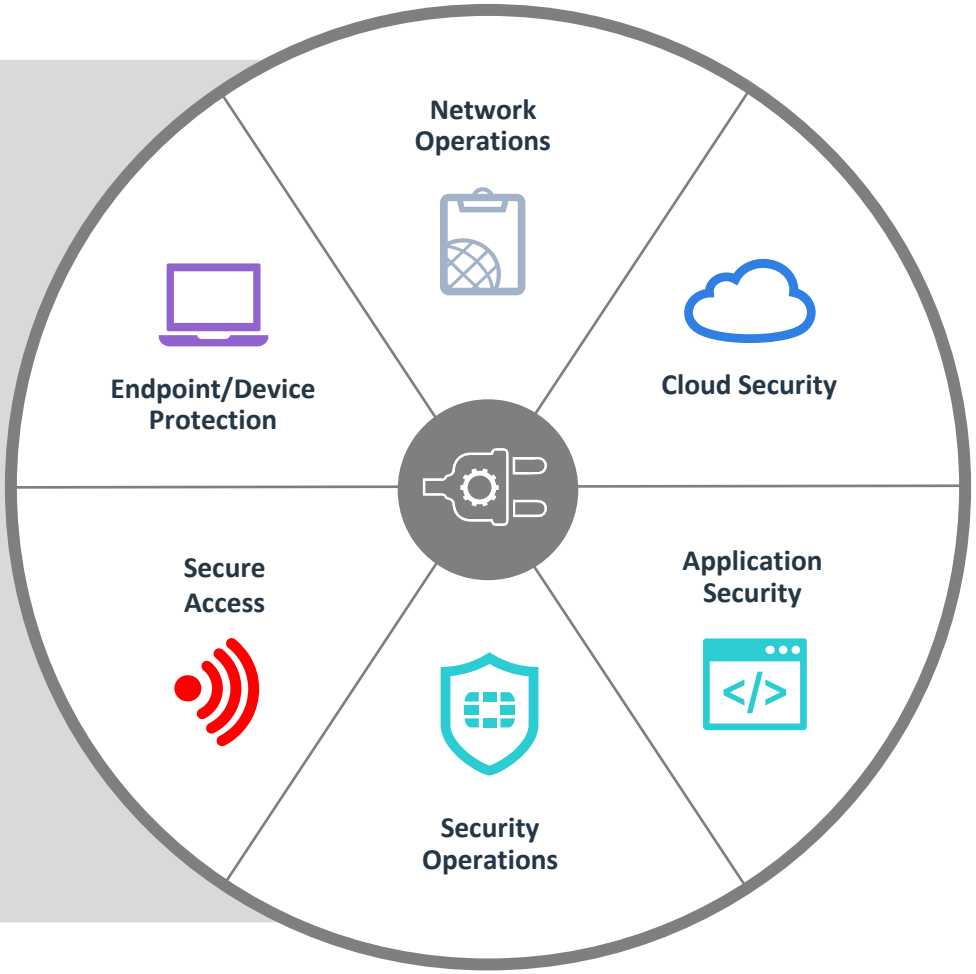
A cybersecurity mesh should work with an extensive ecosystem of integrated solutions

Fortinet-developed
Fabric Connectors

Partner-led
Fabric API Integrations

Fortinet & Community-driven
DevOps Tools and Scripts

Threat sharing/other tech vendors
Extended Ecosystem



Increased Customer Confidence
Pre-validated, documented joint solutions

Faster Time To Value
Speed deployment of Fortinet solutions into a multivendor environment

Improved Fabric Visibility and Protection
Provide greater end-to-end visibility and more effective/coordinated protection

Facilitate Security Fabric Adoption
Facilitate future consolidation and adoption of Security Fabric solutions

*Over **500** integrated and automated vendor solutions for better end-to-end protection across your digital environment*

Fortinet Security Fabric

Broad

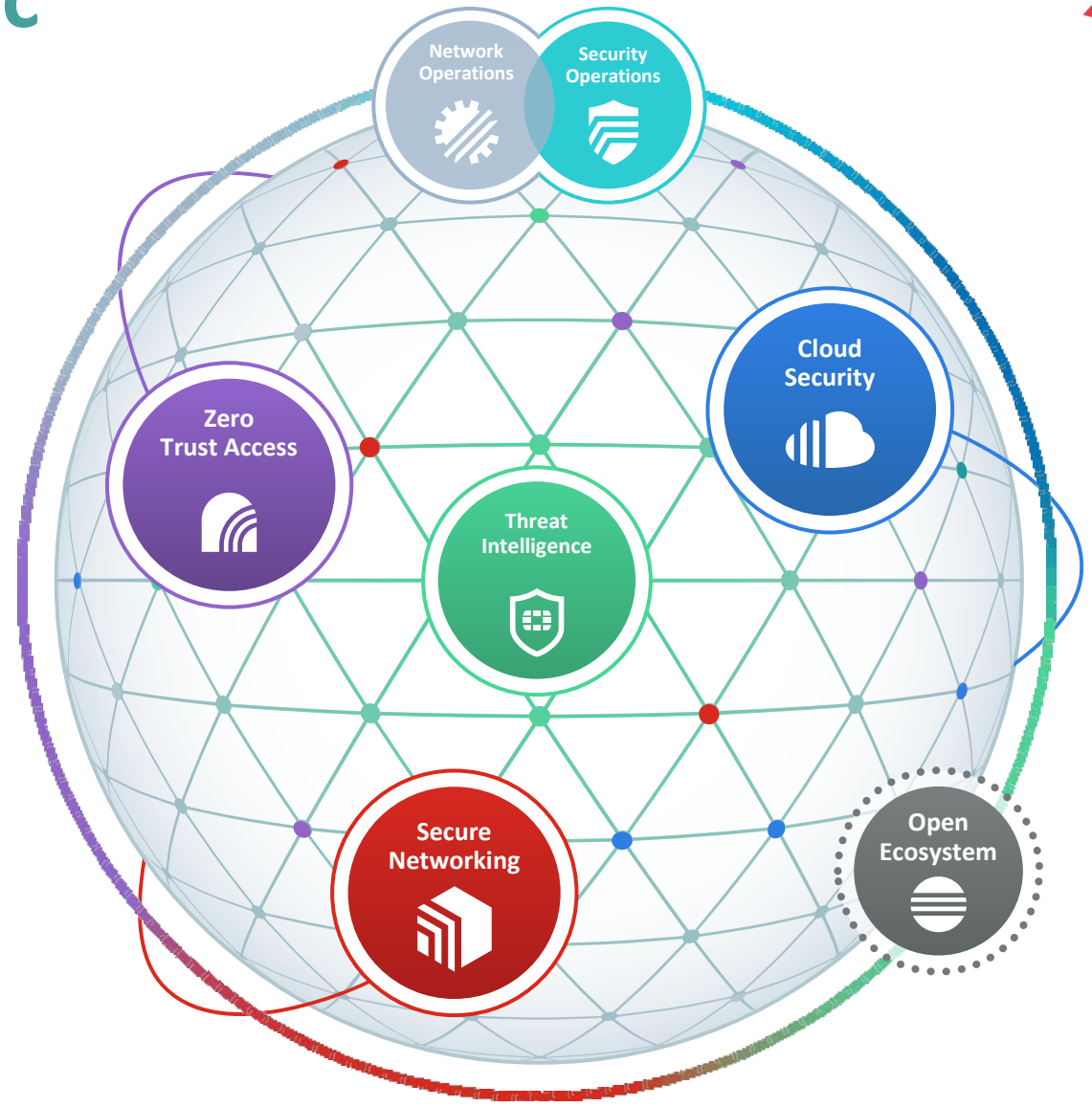
visibility and protection of the entire digital attack surface to better manage risk.

Integrated

solution that reduces management complexity and shares threat intelligence.

Automated

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

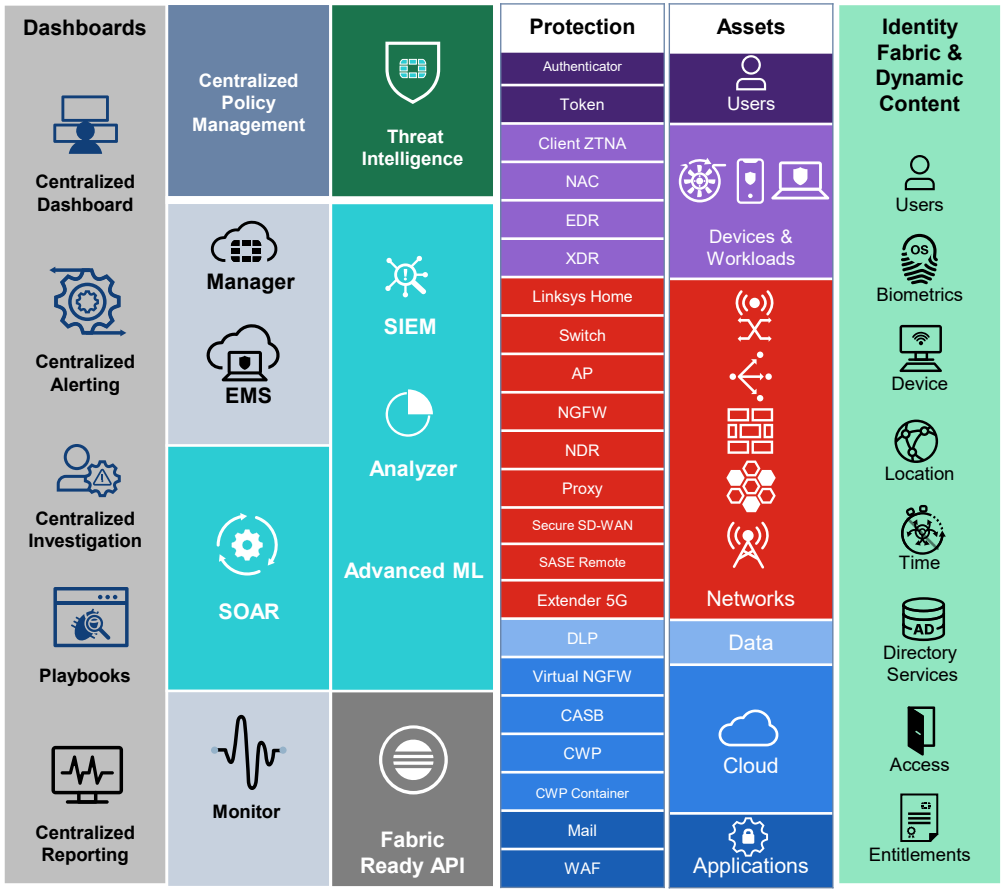


Under the Hood

Implementing a Cybersecurity Mesh Fabric Architecture

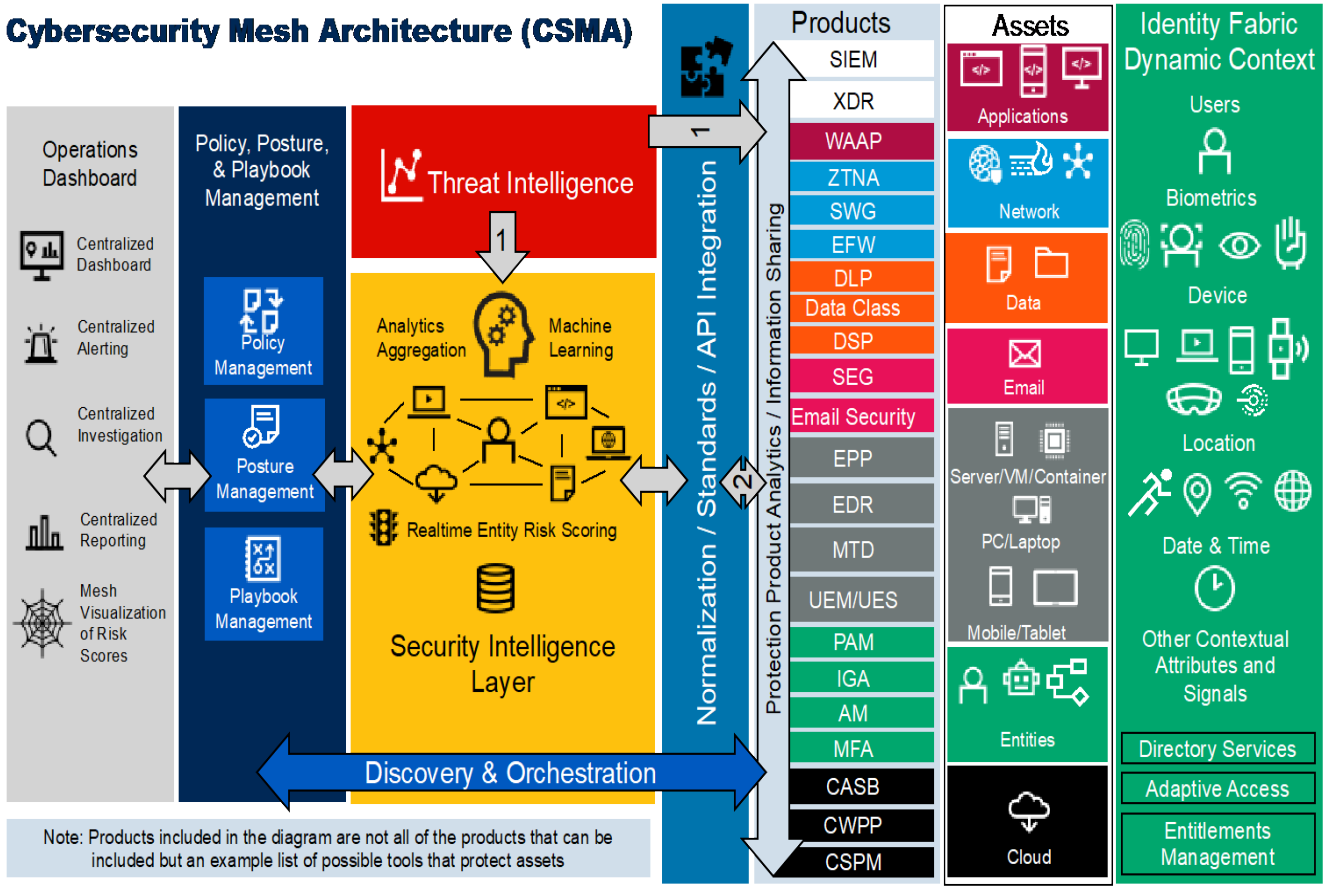
Automated

- **Automate** your ability to trigger coordinated and synergetic responses (predictive and reactive) across endpoints, applications, networks, and clouds
- Provide a **single pane of glass** for incidents, IoC, Scores, attack campaigns, etc.
- Deliver **centralized and unified policy** (think hybrid)
- **Orchestrate** and push new intelligence across the fabric



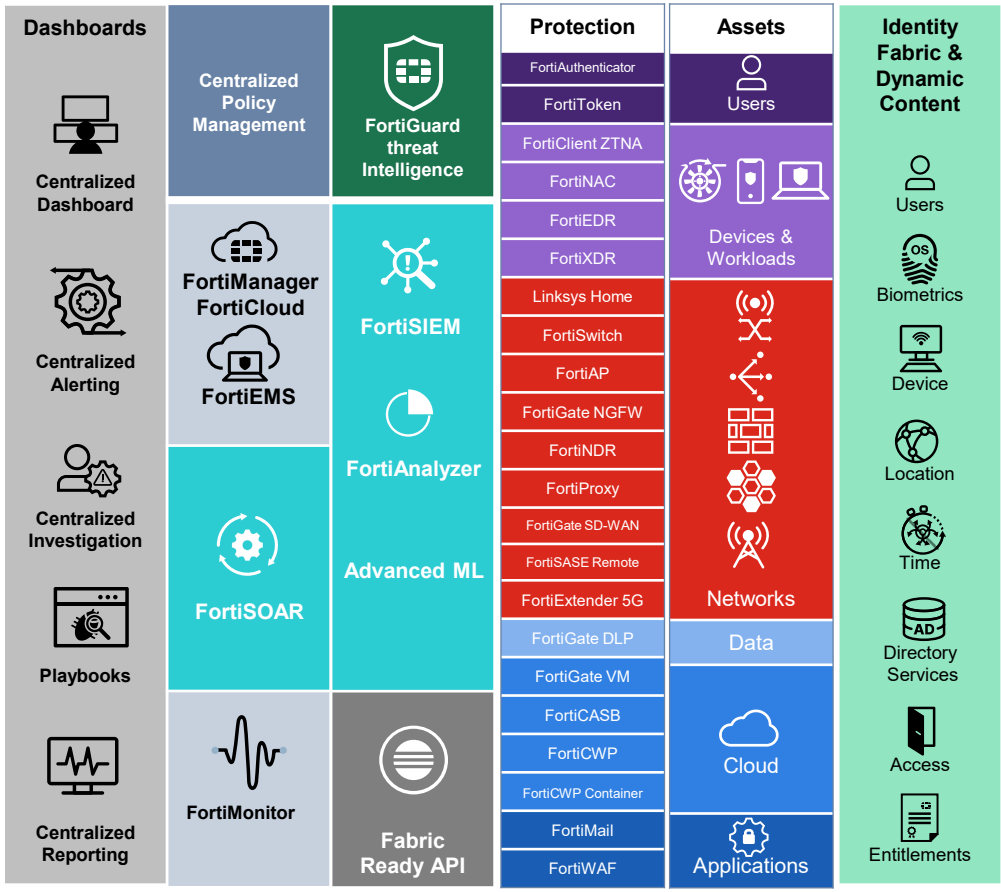
Implementing a Cybersecurity Mesh Architecture

Gartner



Source: *Gartner "Cybersecurity Mesh Architecture"*, Felix Gaehtgens. April, 2022

FORTINET



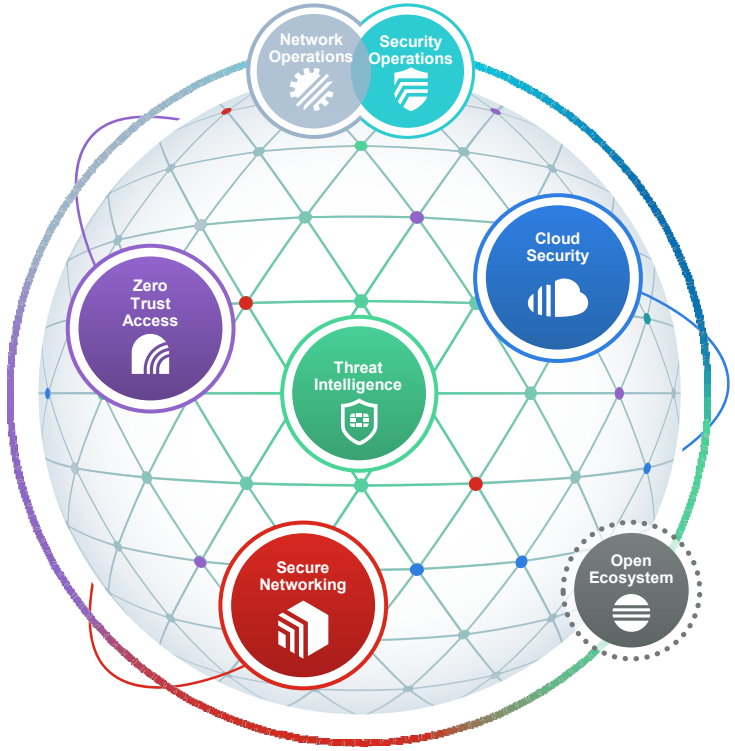
RSAConference2022

How It All Comes Together

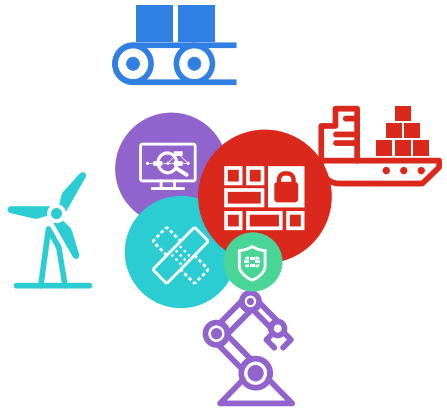
Cybersecurity Mesh Examples

Work From Anywhere

Hybrid Multi-cloud



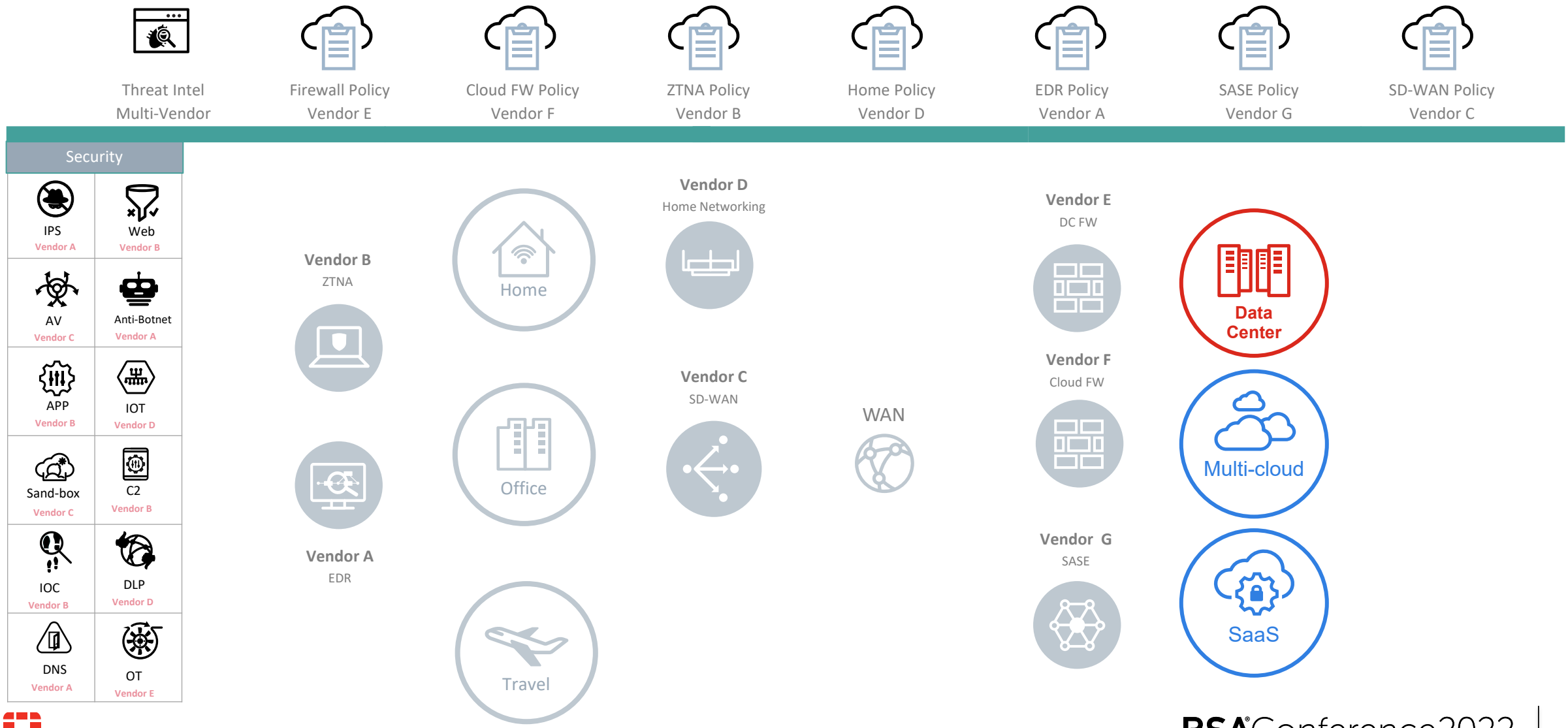
Zero Trust Edge



Operational Technology Security

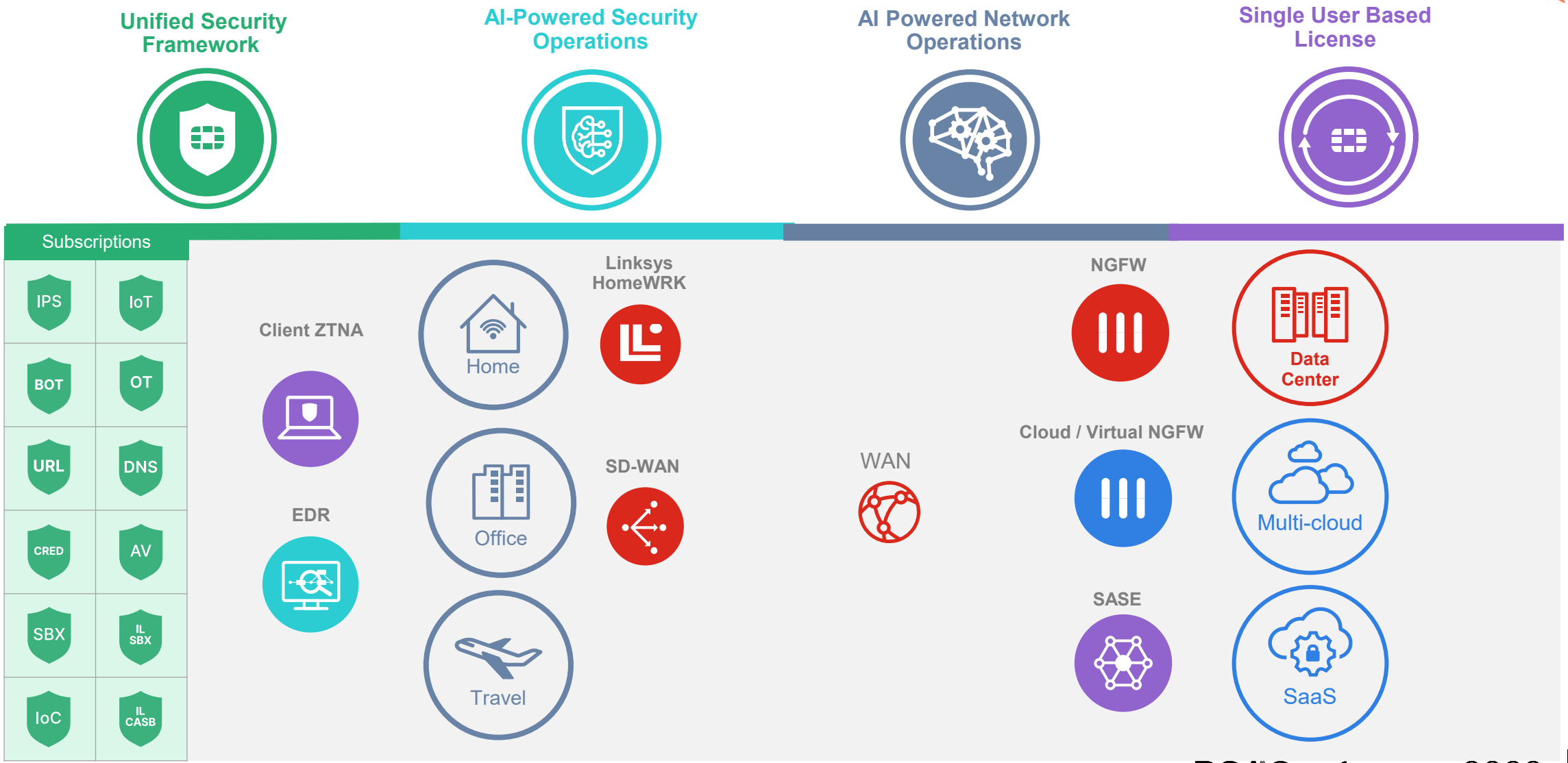
Work from Anywhere – Multi-Vendor Solution

Inconsistent Security and Complex to Manage

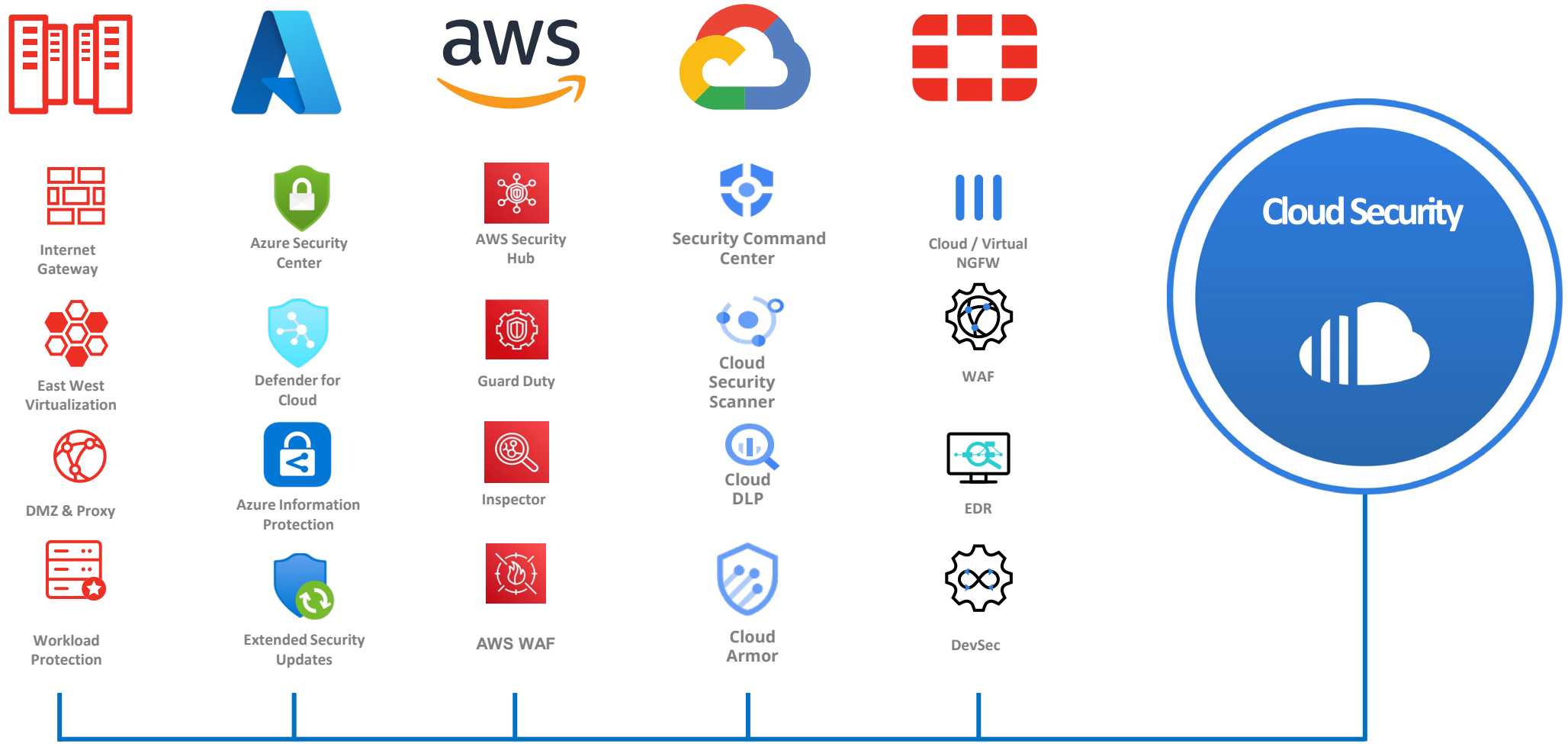


Fabric Solution – Work from Anywhere

Consistent, enterprise-class security in all locations

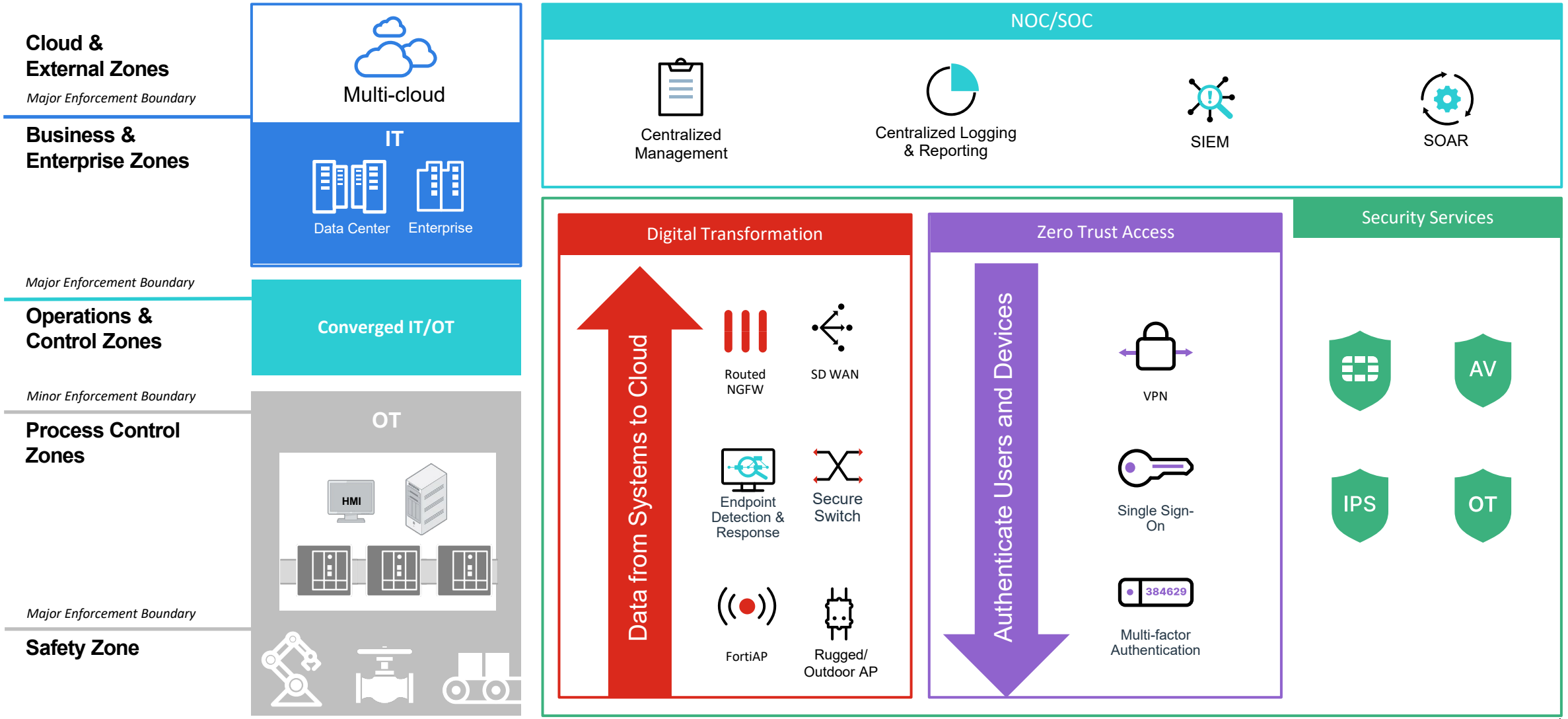


Fabric Solution – Harmonizing Enterprise Security with Cloud Native



Fabric Solution – Operational Technology

Most commonly deployed Fabric Solution



RSAConference2022

2022+ Focus Areas

Act Early(er)
Play Smart(er)
Win Fast(er)

Act Early(er)

Don’t show any weakness

Starting as early as the reconnaissance phase

Early Risk Reduction

- External attack surface management
- Brand protection
- EDR

Always be looking

For potential gaps – and fix them

Cybersecurity Assessments

- Vulnerability
- Targeted incident readiness assessments
  - (ransomware, phishing, email)

People are your vulnerability

– asses and “patch” them well

CyberSafe Training

- Cybersecurity hygiene
- Social engineering
- Anti-phishing

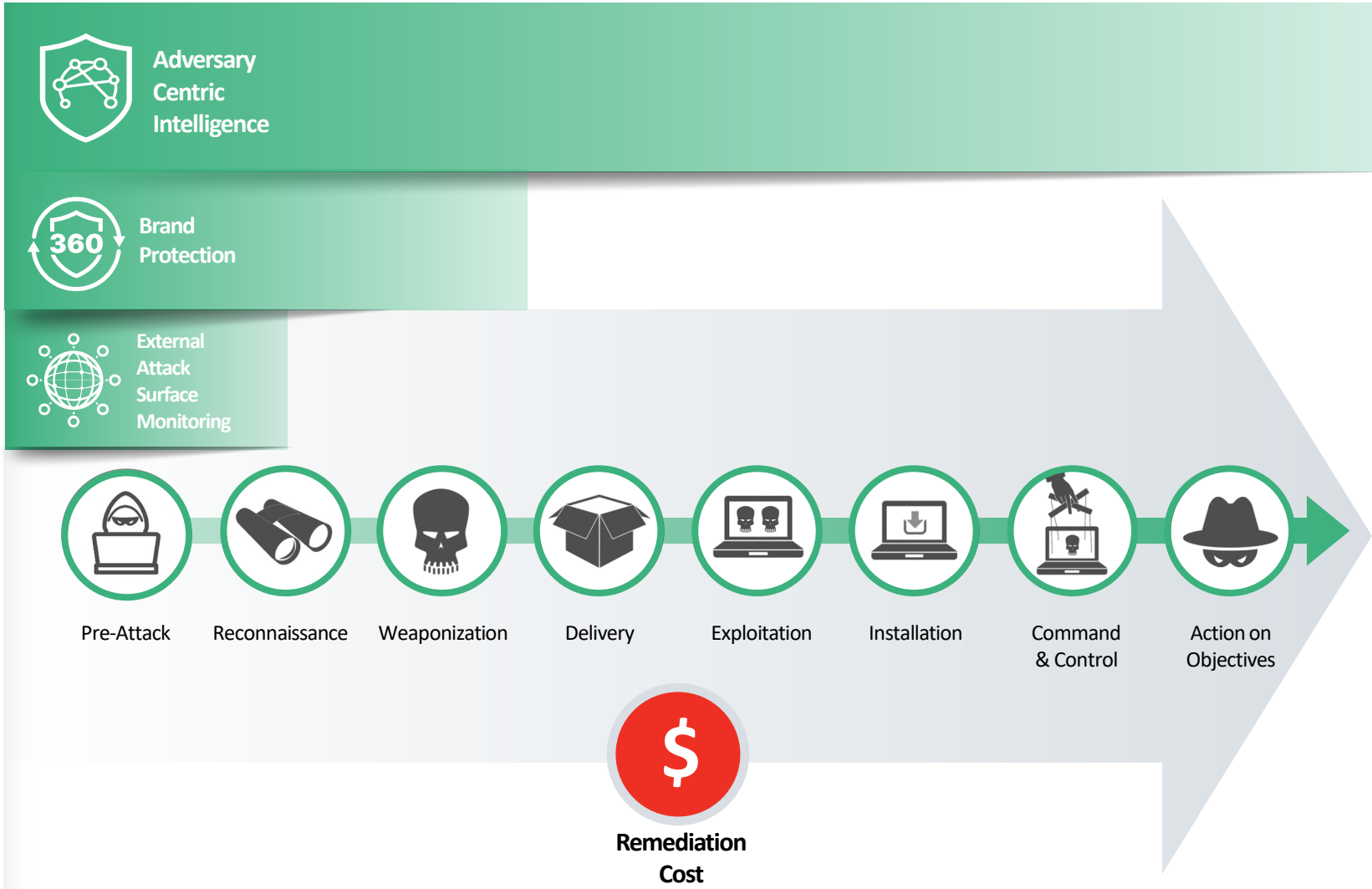
Strive to Know More – Adversary Centric Intelligence (ACI)

DRPS

Digital Risk Protection Services

- Provides a view on what adversaries are seeing (EASM)
- Provides a view on what adversaries are doing (Brand Protection)*
- Provides a view on what adversaries are planning (ACI)*

Supports mitigating / remediating actions earlier reducing the impact and cost of cyber attack



External Attack Surface Management (EASM)

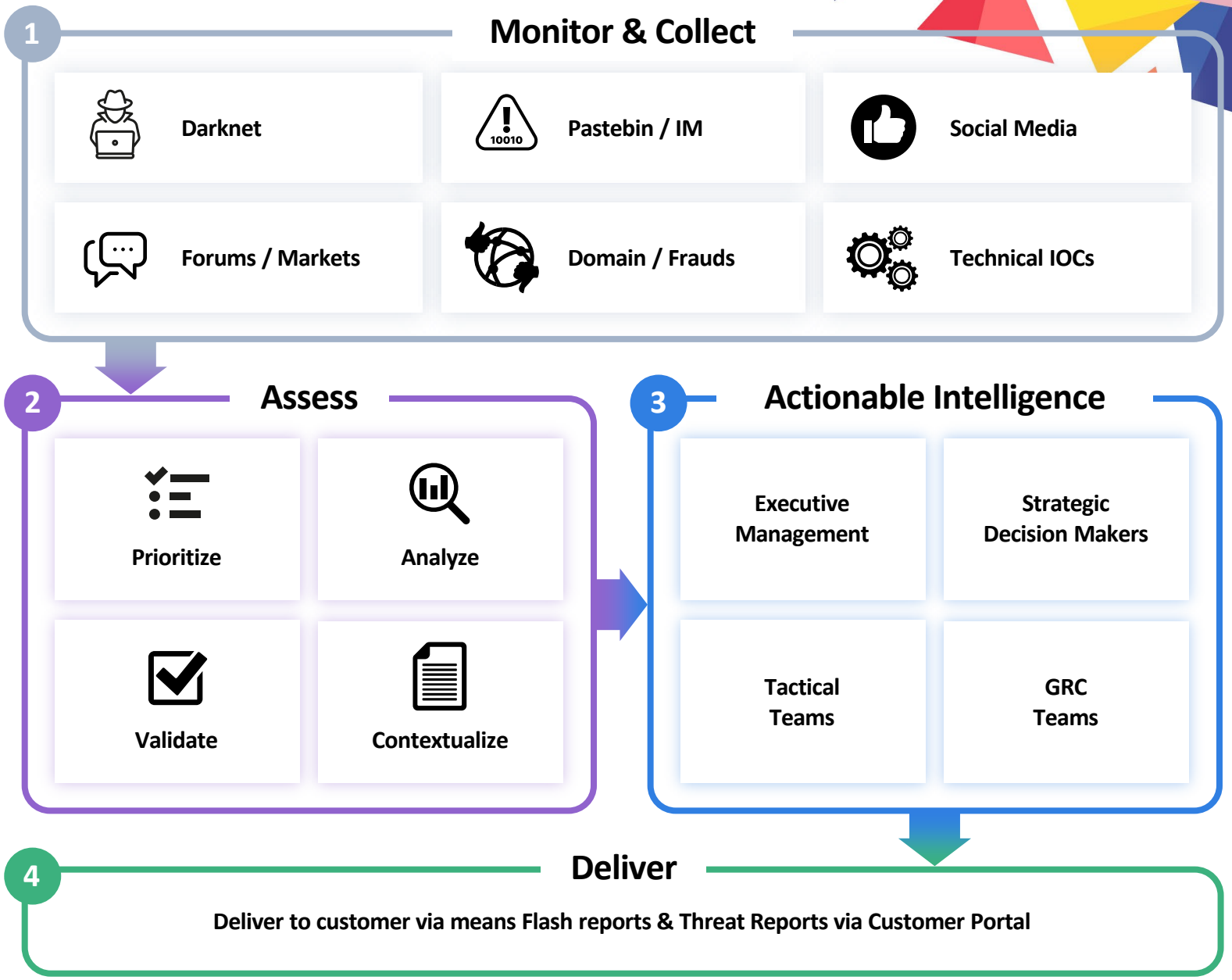
EASM will helps identify servers, credentials, public cloud service misconfigurations and third-party partner software code vulnerabilities that could be exploited by malicious actors.

Brand Protection (BP)

Brand Protection(BP) detect activity early and taking action such as web-site or application takedown, Brand Protection helps organizations to protect their brand value, trust, integrity, and reputation.

Adversary Centric Intelligence (ACI)

Adversary Centric Intelligence (ACI) includes threat actor insights to help organizations proactively assess risks, look for vulnerabilities in the existing setup and increase the security awareness of their staff.



Play Smart(er)

Invest in Threat Intelligence

- Strive to create the bigger picture
- Normalized and centralized security data
- Global threat intelligence feeds
- Activate security features
- Make sure your logs have meaningful data in them

Slow Adversary Down

- Decrypt
- Zero Trust and segmentation
- Honeypot technology
- Network detection and response

Transform Data to Intelligence

Correlate and leverage multiple forms of ML (centralized, distributed and federated) to build proactive, predictive and centralized intelligence

Win Fast(er)

Automate

- Smart ML (Local & Cloud delivered)
- Proactive & Unified policy
- Think hybrid
- Invest in Playbooks
- Outbreak Detection

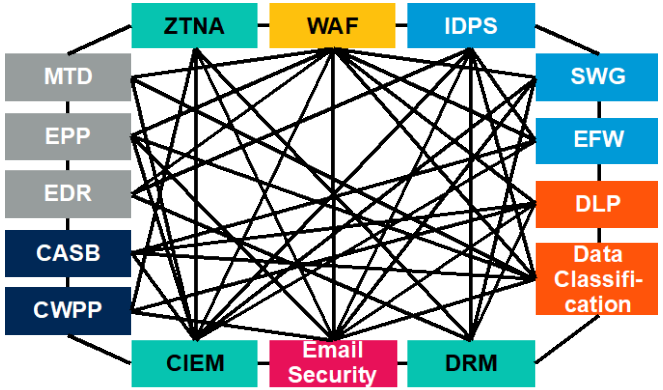
SOC Augmentation

- Soc as a Service
- Client Level Forensics
- MDR
- IR
- Outbreak Alerts

Practice makes you Better (& faster)

- Educate
- Tabletop Training
- Playbook Development
- Attacks Simulation

Gartner

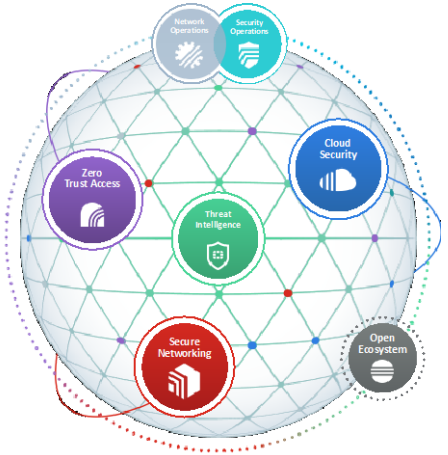


"By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%"

"Top Strategic Technology Trends for 2022: Cybersecurity Mesh, Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021"

Executive Guide to Cybersecurity Mesh, 2022
***Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi**. As of October 2021*

FORTINET



To implement a cybersecurity mesh architecture today, look for:

- Deep visibility across all edges
- Centrally managing distributed solutions
- Consistent enforcement of policies
- Real-time global threat intelligence across Security Fabric deployments
- Automating actionable responses
- Broadest, most integrated open ecosystem

RSAConference2022

Q&A

RSAConference2022

End