CYBER SECURITY MESH ARCHITECTURE (CSMA) – A NEW KID IN TOWN

ABBAS KUDRATI
APAC CHIEF CYBERSECURITY ADVISOR
@askudrati
https://aka.ms/abbas

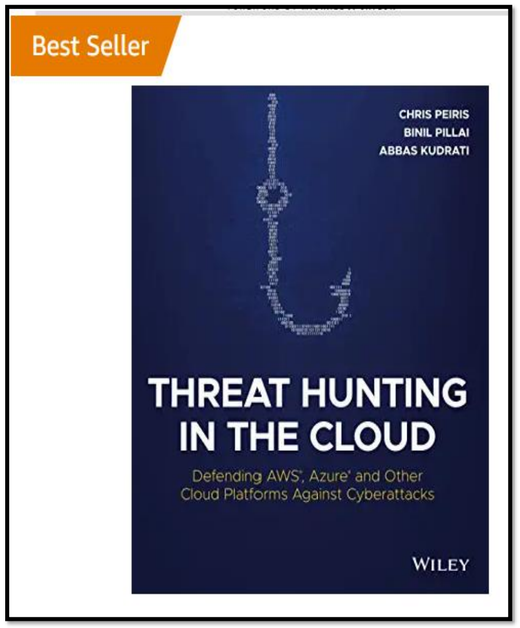
AUSTRALIAN CYBER CONFERENCE 2022

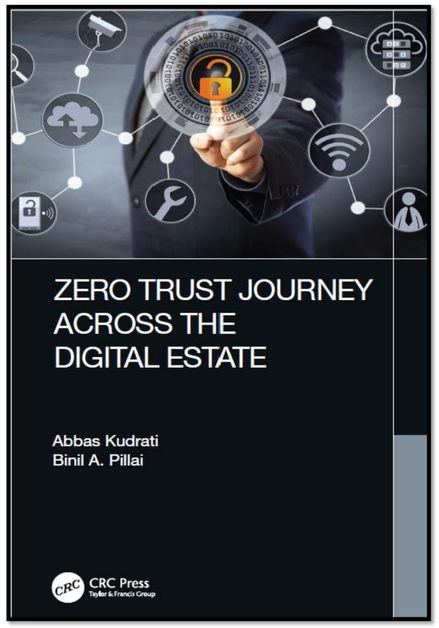
About me

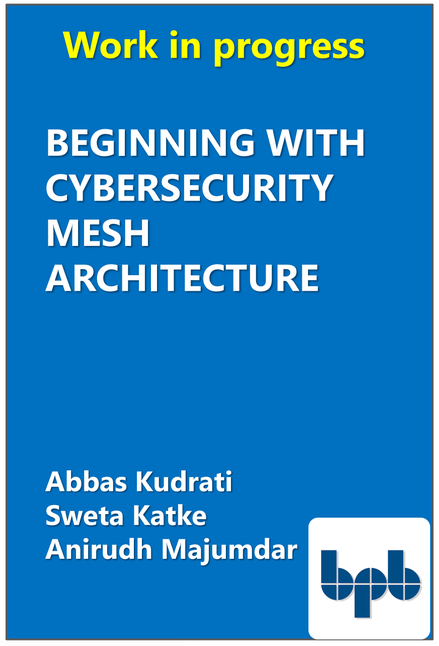
"You join Microsoft, not to be cool
but to make others cool"
Satya Nadella

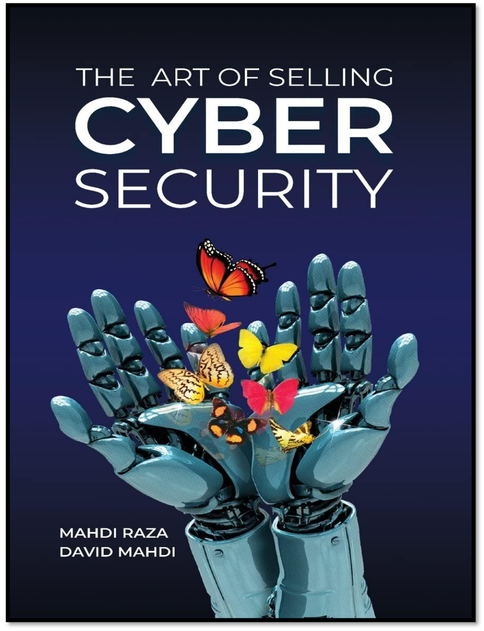
- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

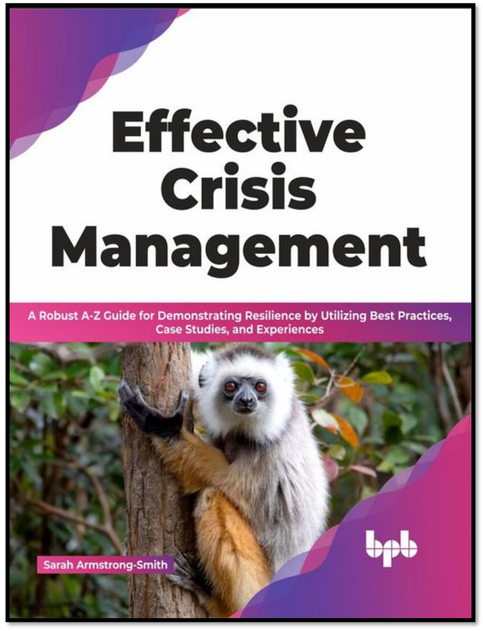
My Publications (Author, Contributor & Tech Editor)

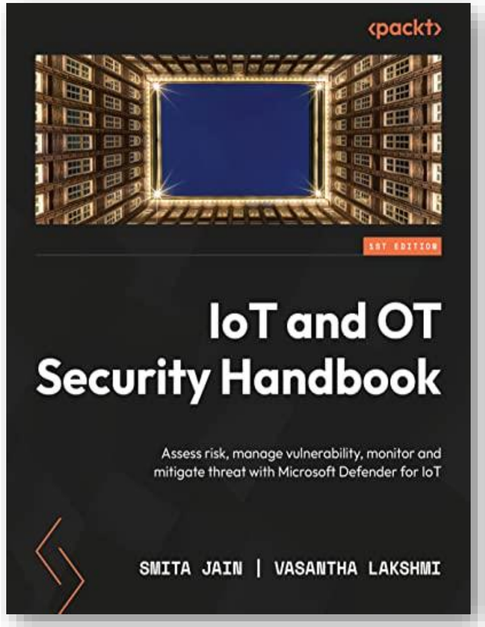




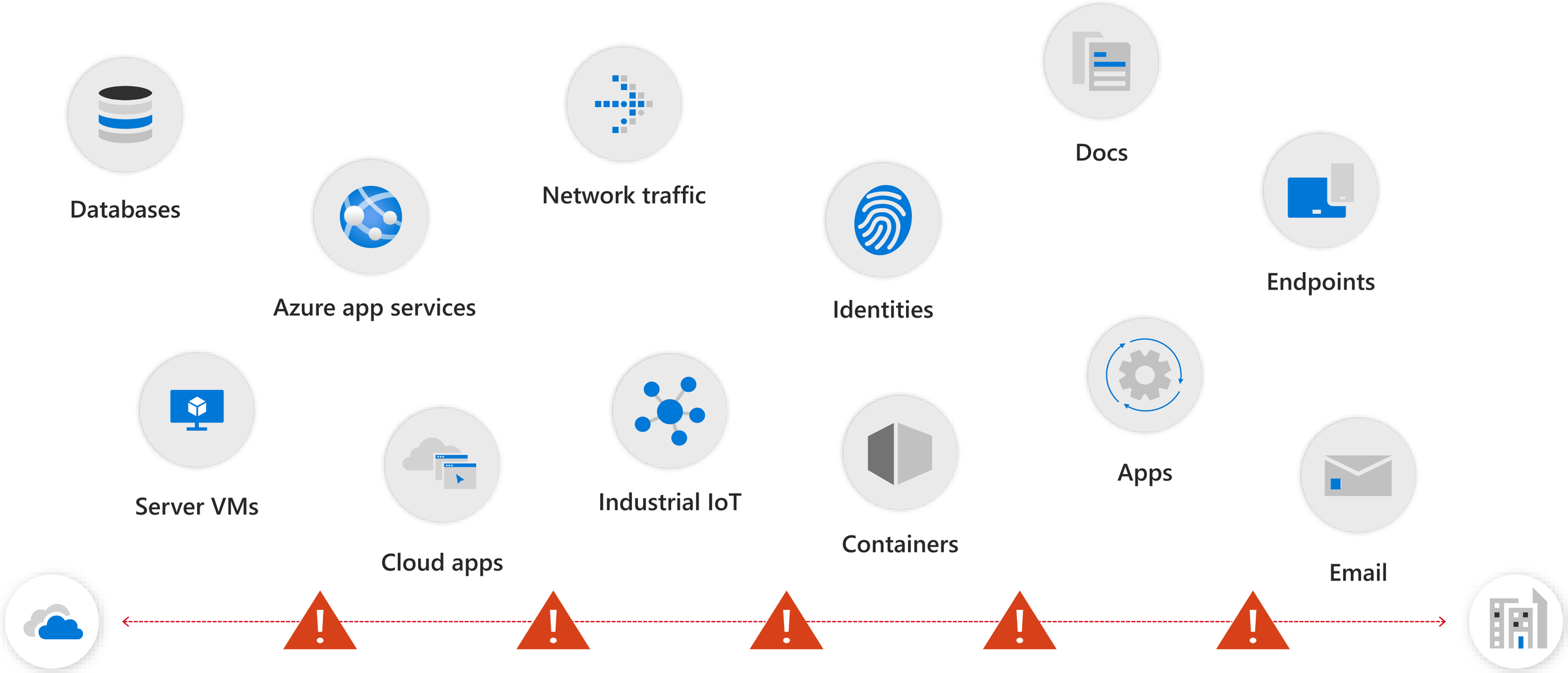


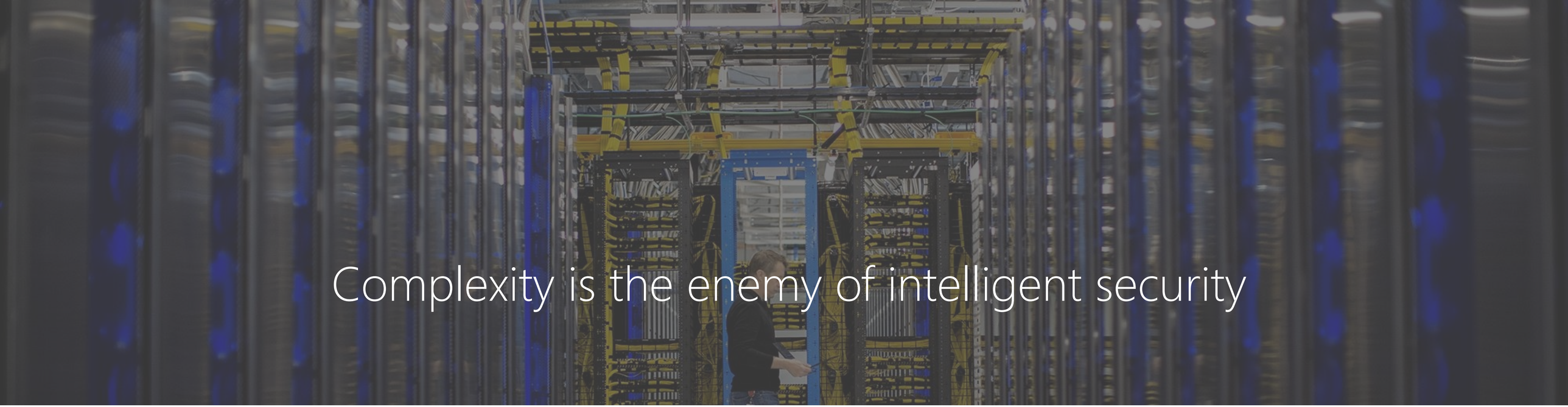






Managing complexity





Complexity is the enemy of intelligent security

$1.37M

On average that an organization spends annually in time wasted responding to erroneous malware alerts

"The Cost of Insecure Endpoints" Ponemon Institute© Research Report, June 2017

1.87M

Global cybersecurity workforce shortage by 2022

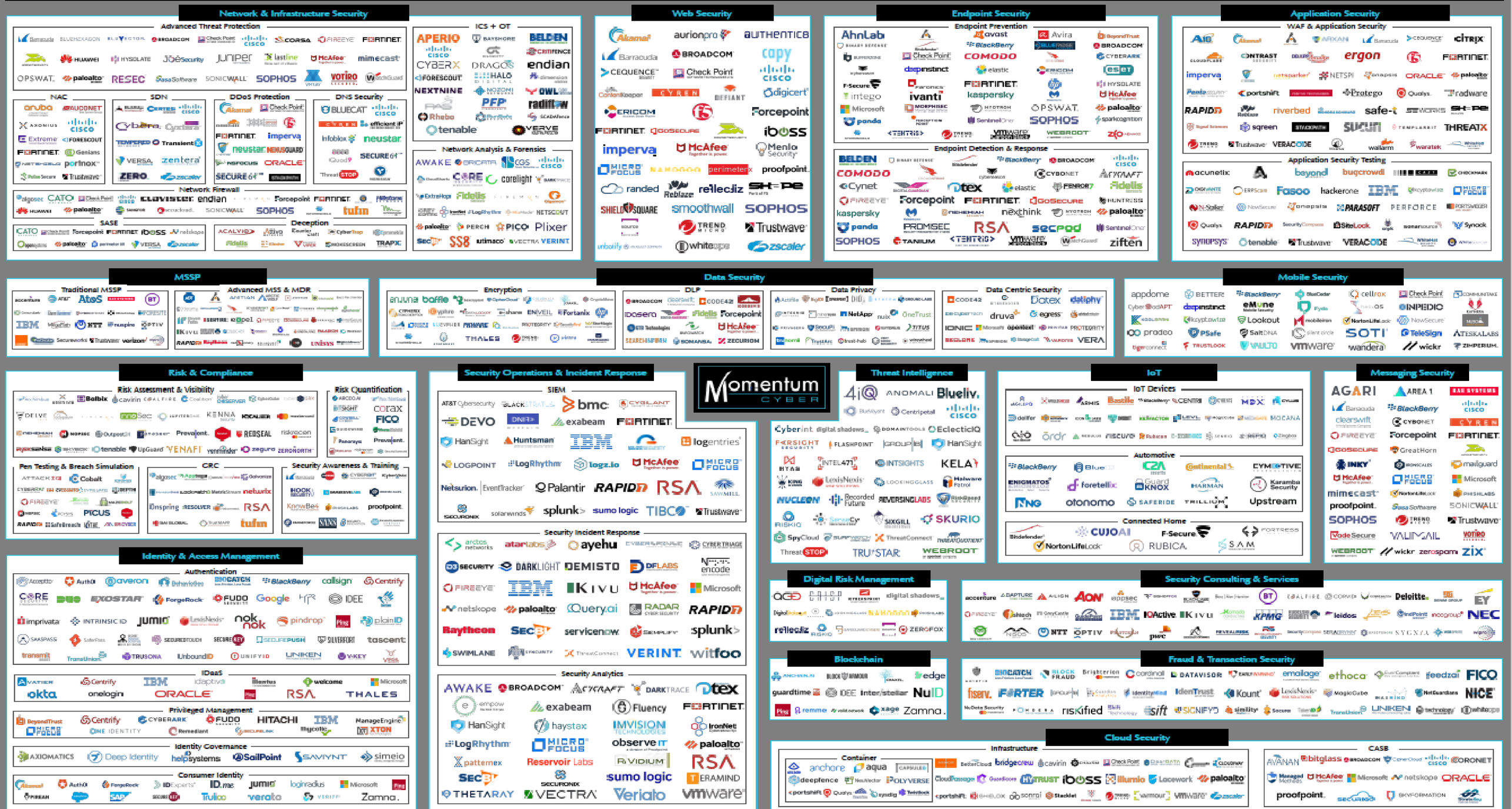
Global Information Security Workforce Study 2017

70 **Security products** from **35** **Security vendors**

Is the average for companies with over 1,000 employees

Nick McQuire, VP Enterprise Research CCS Insight.

CYBER SCAPE 2021



"In design principles, means that software / architecture / infrastructure is designed from the foundation to be secure"

Built-in Security

Built into platform design

Security management and operation simplified

No add-on resources

Bolt-on Security

Not integrated

Complex

Operational burden

Limited Utilization

Vendor Contract Lock in

Best of Breed — Pros and Cons

Pros	Cons
• No vendor lock-in • Components can be best in class • No CISO has been fired by best-of-breed purchases • Vendors focus on their area of expertise	• No centralized policy management • No centralized threat database • Slower incident response • Multiple vendors for support and licensing • No centralized playbooks and automation • Integrations are spotty or nonexistent • Different vendors have different types of management, usage and scripting

Summary: Top Security and Risk Trends

The Top Security & Risk Management Trends for 2021 (Gartner Webinar)

1. Remote Work Is the New Normal
2. The "Cybersecurity Mesh" Architecture
3. Security Product Consolidation
4. Identity First Security
5. Machine Identity Management
6. Breach and Attack Simulation Tools
7. Privacy Enhancing Computation
8. Boards Are Adding Cybersecurity

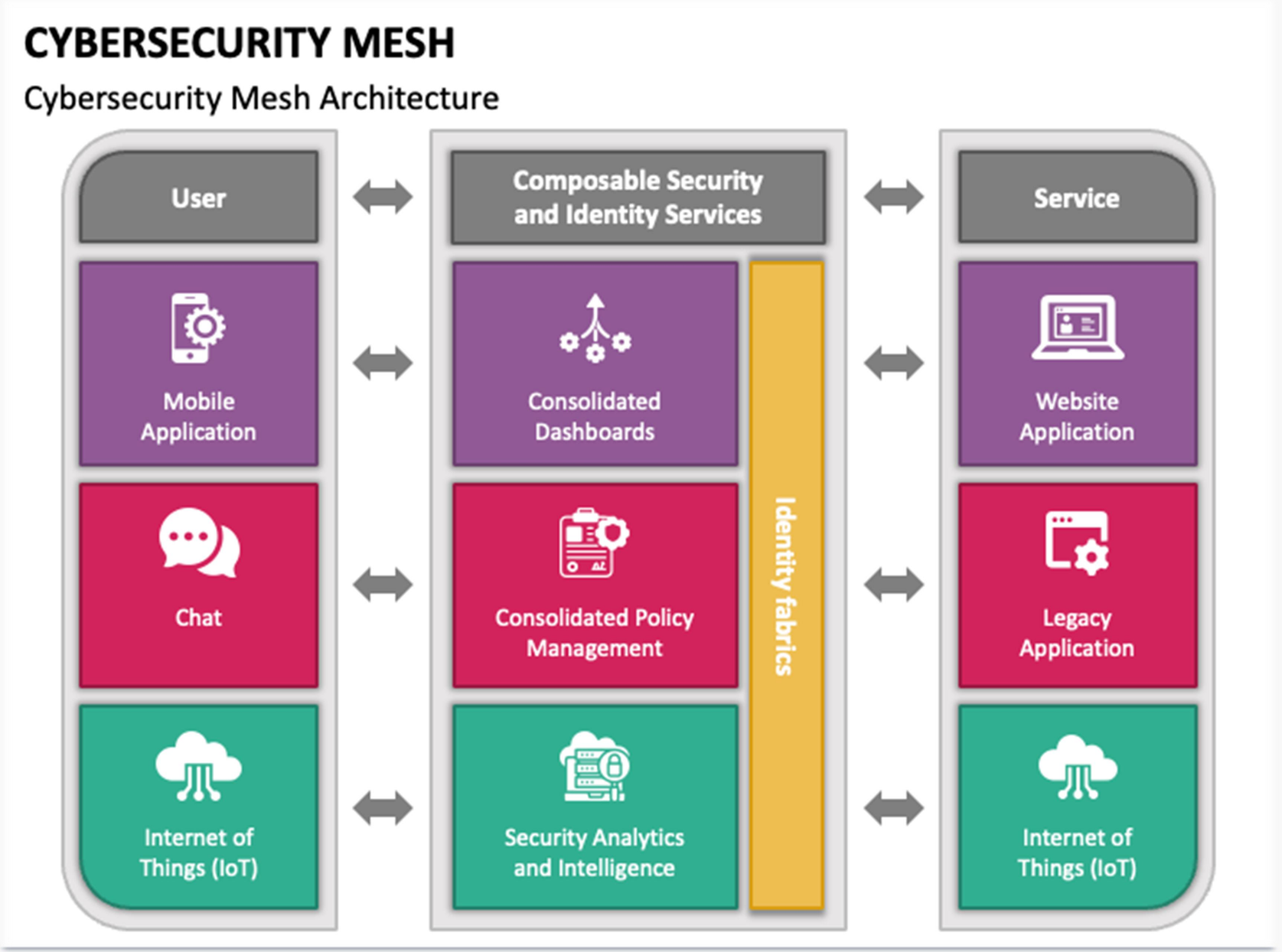
Gartner

What is CSMA ? (Gartner's definition)

Cybersecurity mesh, or cybersecurity mesh architecture (CSMA), is a collaborative ecosystem of tools and controls to secure a modern, distributed enterprise.

It builds on a strategy of integrating composable, distributed security tools by centralizing the data and control plane to achieve more effective collaboration between tools.

Outcomes include enhanced capabilities for detection, more efficient responses, consistent policy, posture and playbook management, and more adaptive and granular access control — all of which lead to better security.



What is CSMA ? (Gartner's definition)

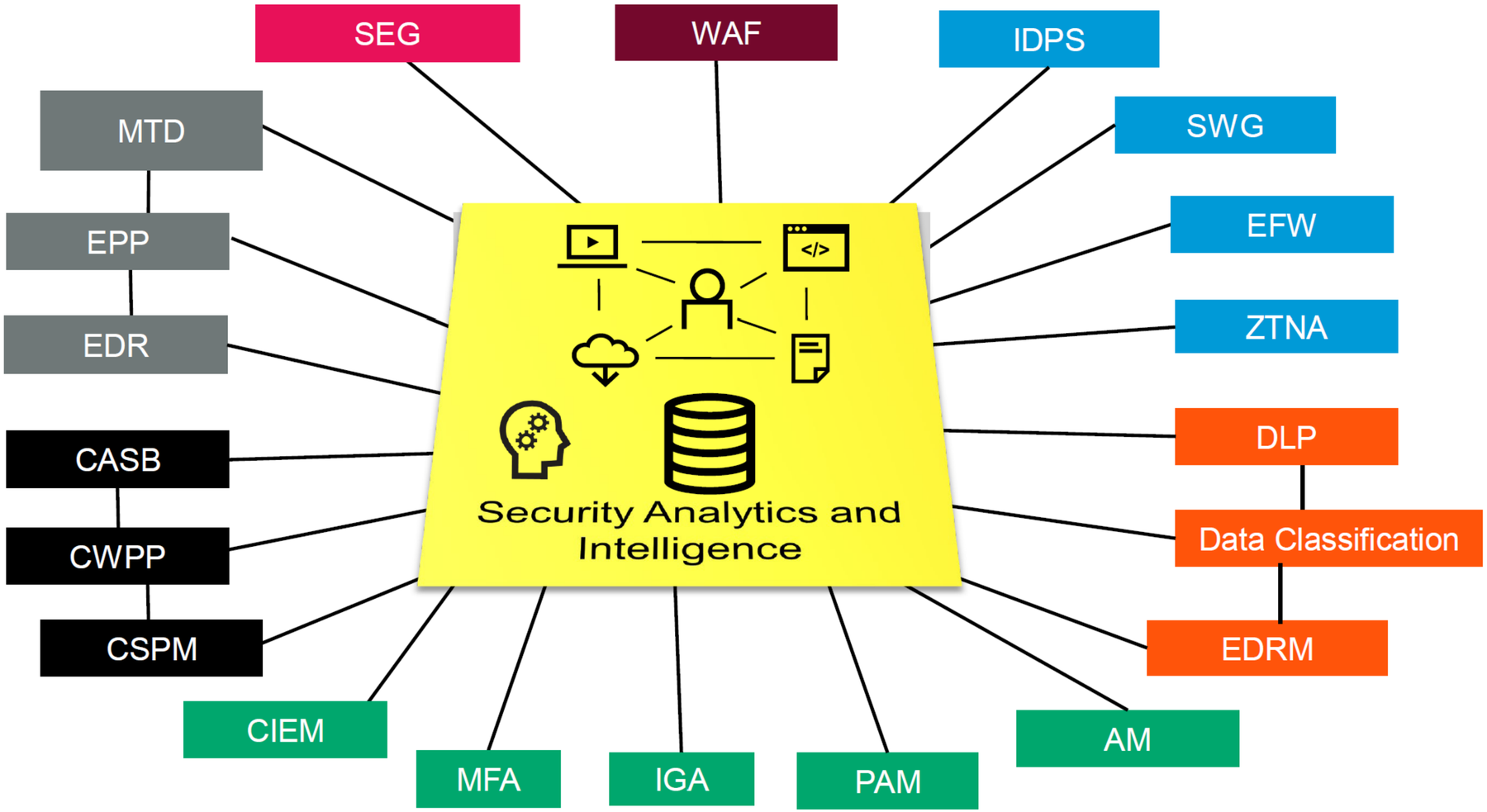
In essence, each tool in the IT infrastructure within the CSMA operates as a cog in a greater machine. The framework proposed by Gartner is based on four layers:

- Security analysis and intelligence: which analyses past cybersecurity attacks, as well as data and lessons from other tools, to inform future trigger responses and actions
- Distributed identity fabric: a decentralization of identity management, identity proofing and entitlement management, creating an environment of adaptive access
- Consolidated policy and posture management: the ability to translate central policy into native configuration of each individual security tool
- Consolidated dashboards: offering a holistic view of the entire security ecosystem
- The CSMA framework appears to offer significant benefits over the traditional IT security model.

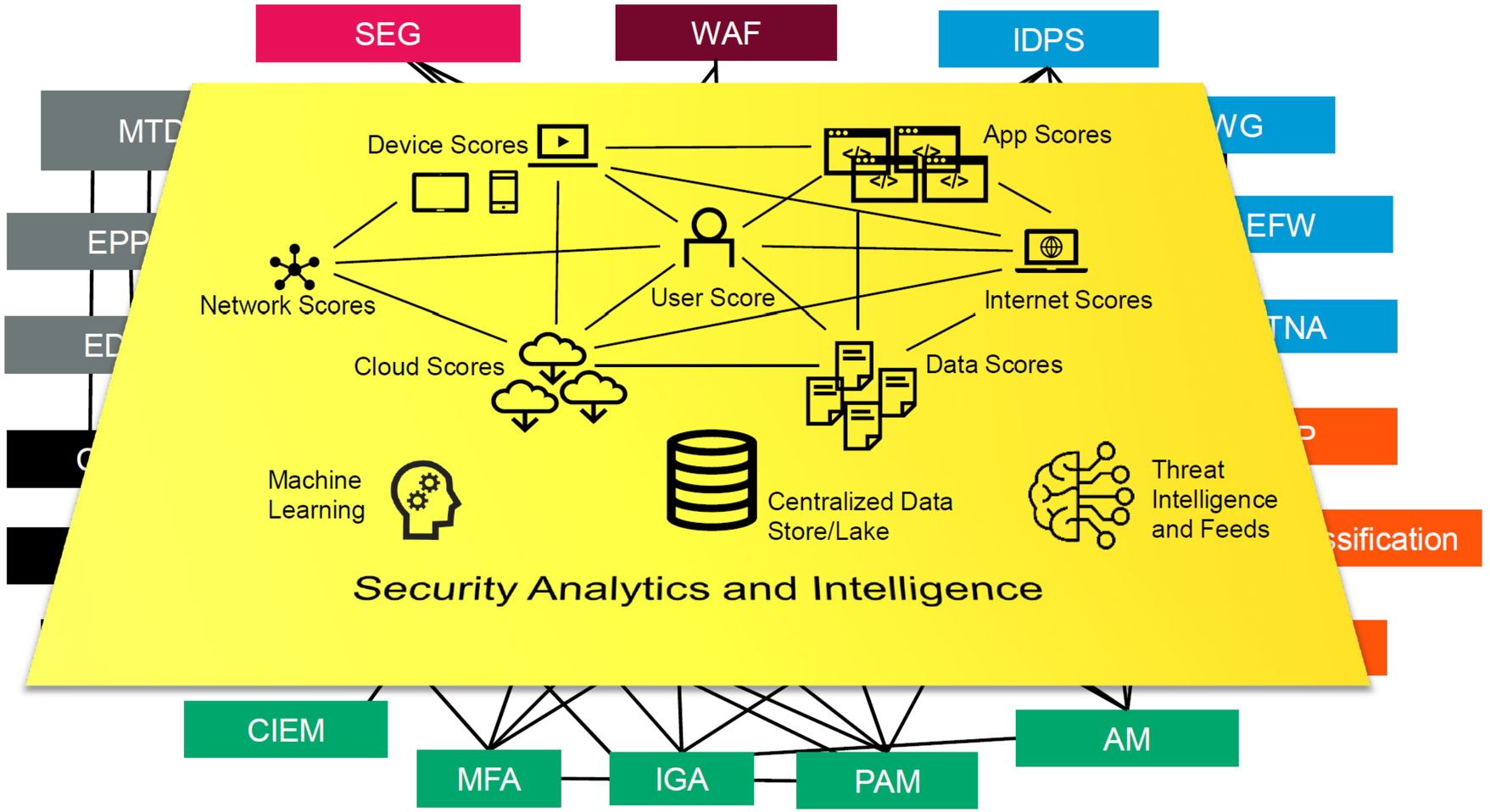
CYBERSECURITY MESH

By 2024, organisations adopting cybersecurity mesh architecture will reduce the financial impact of individual security incidents by an average of 90%.

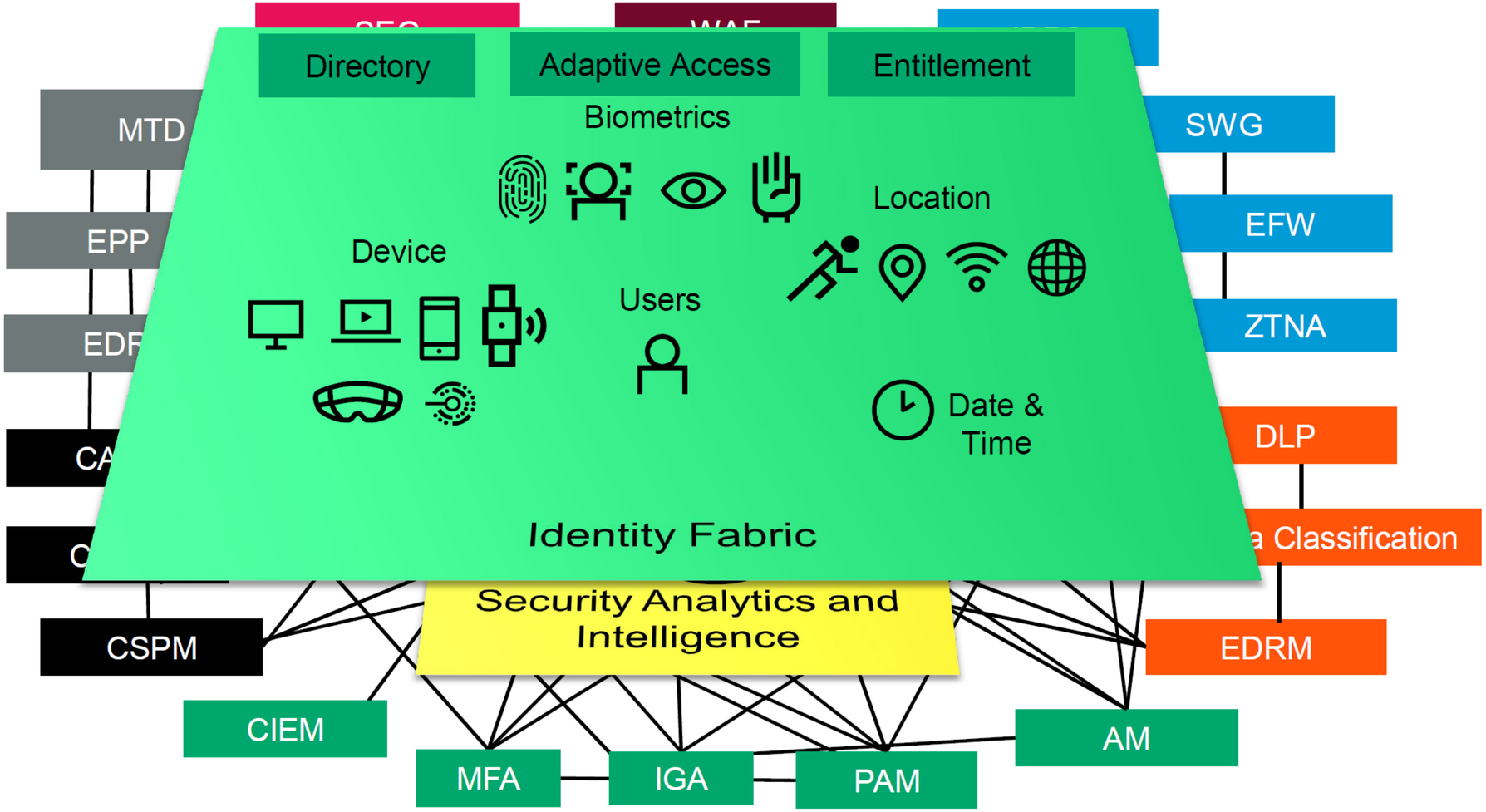
How to Build a Cybersecurity Mesh Architecture



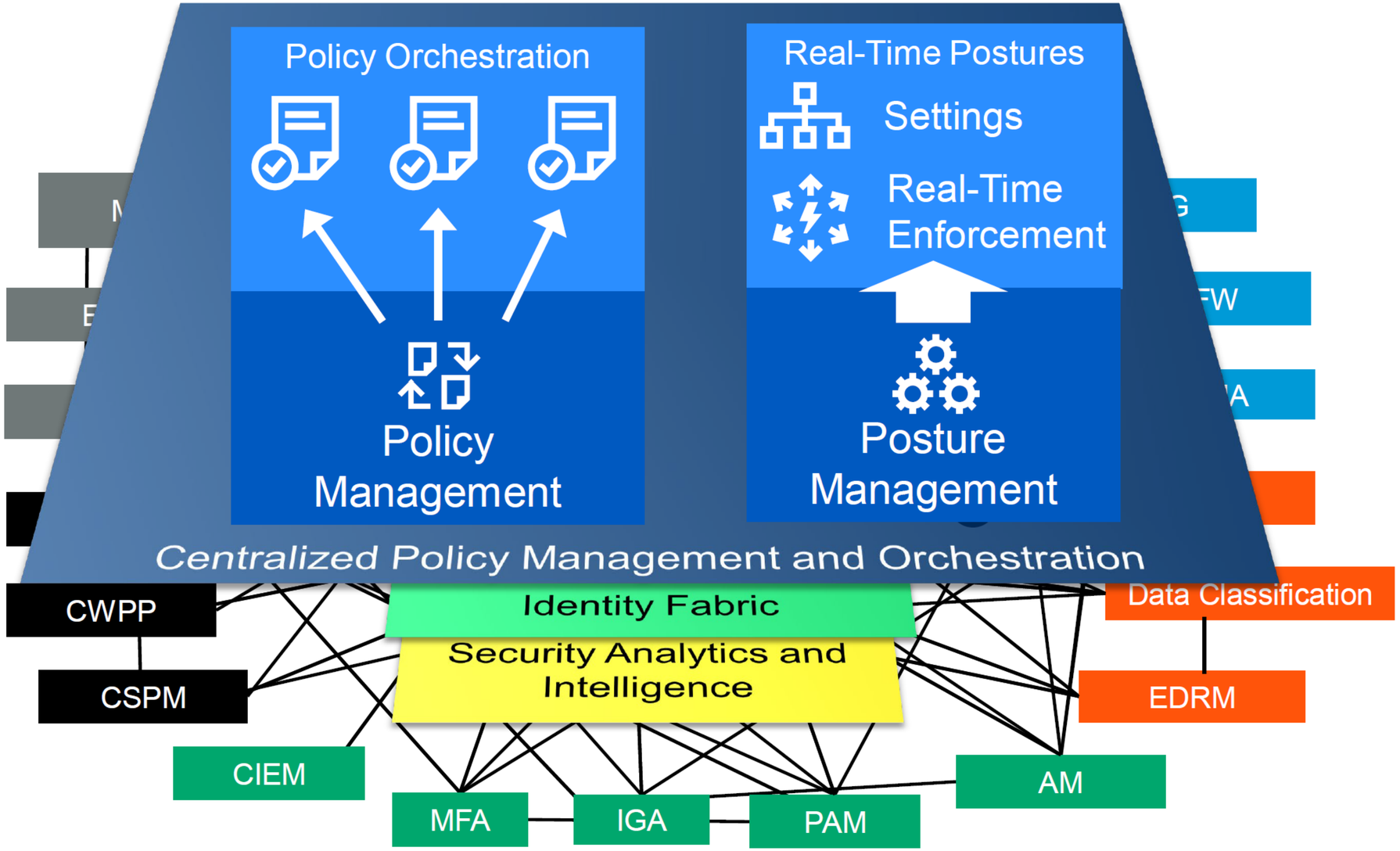
Security Analytics and Intelligence Layer



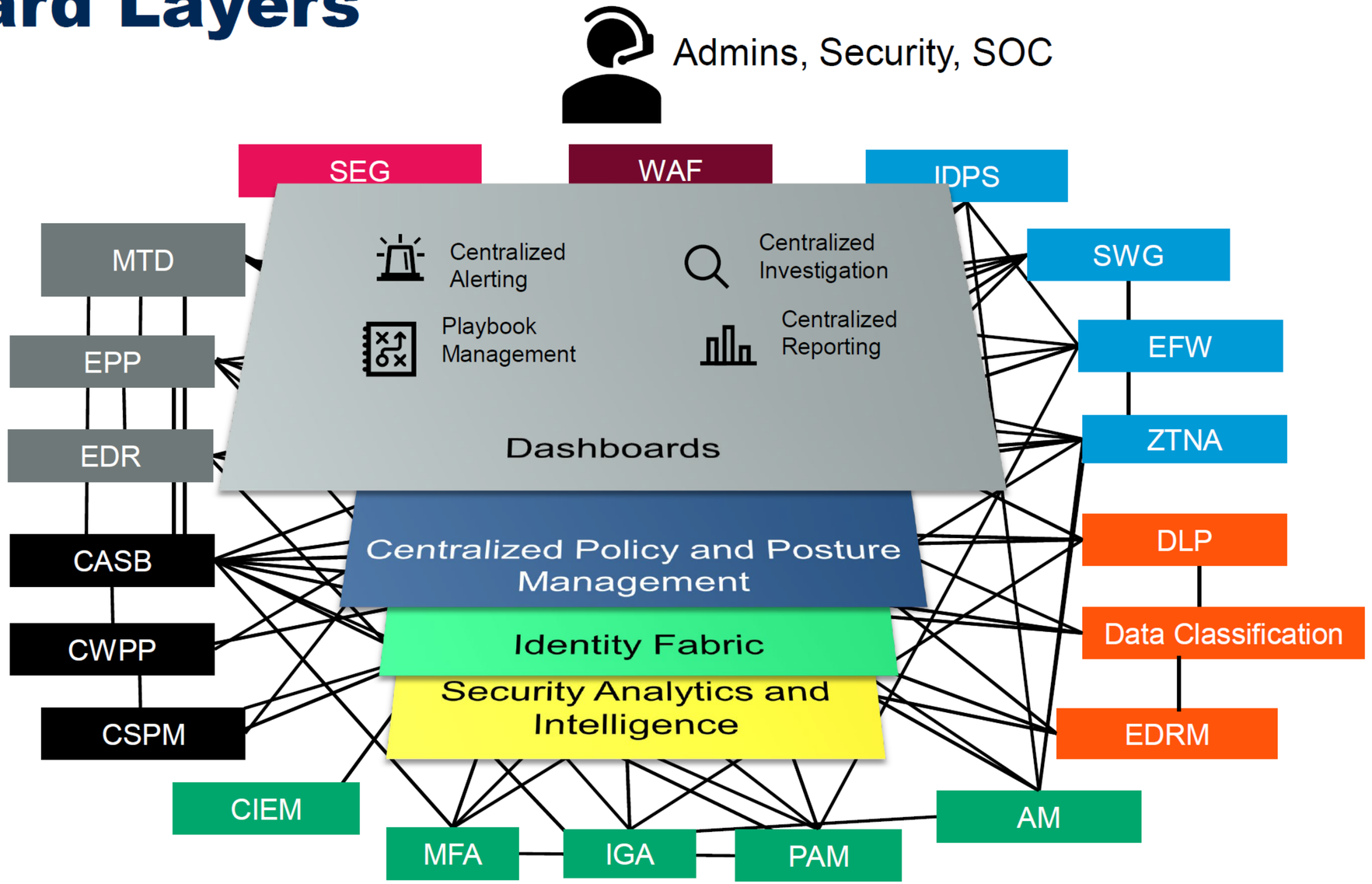
Identity Layer



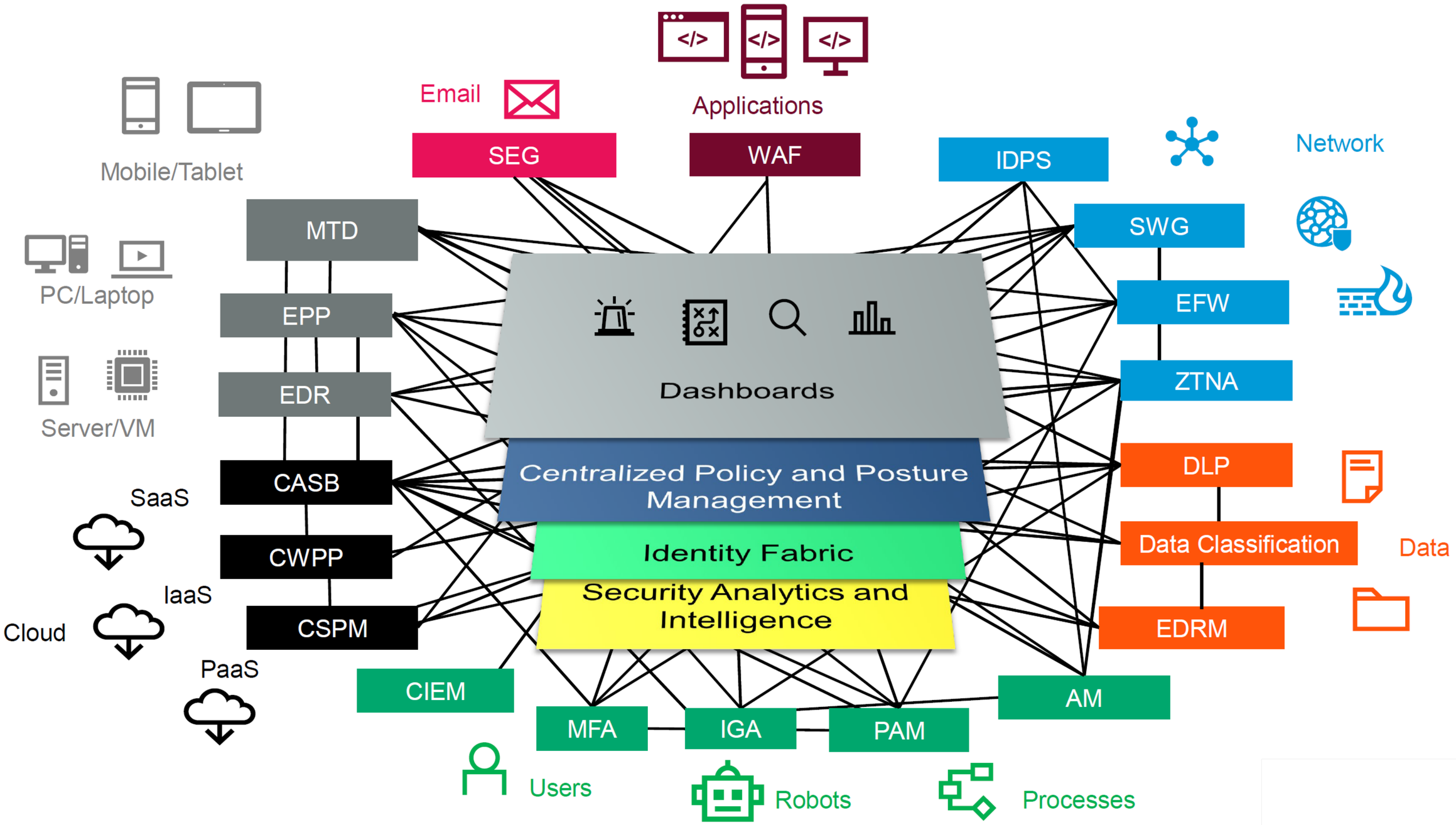
Policy and Posture Management Layer



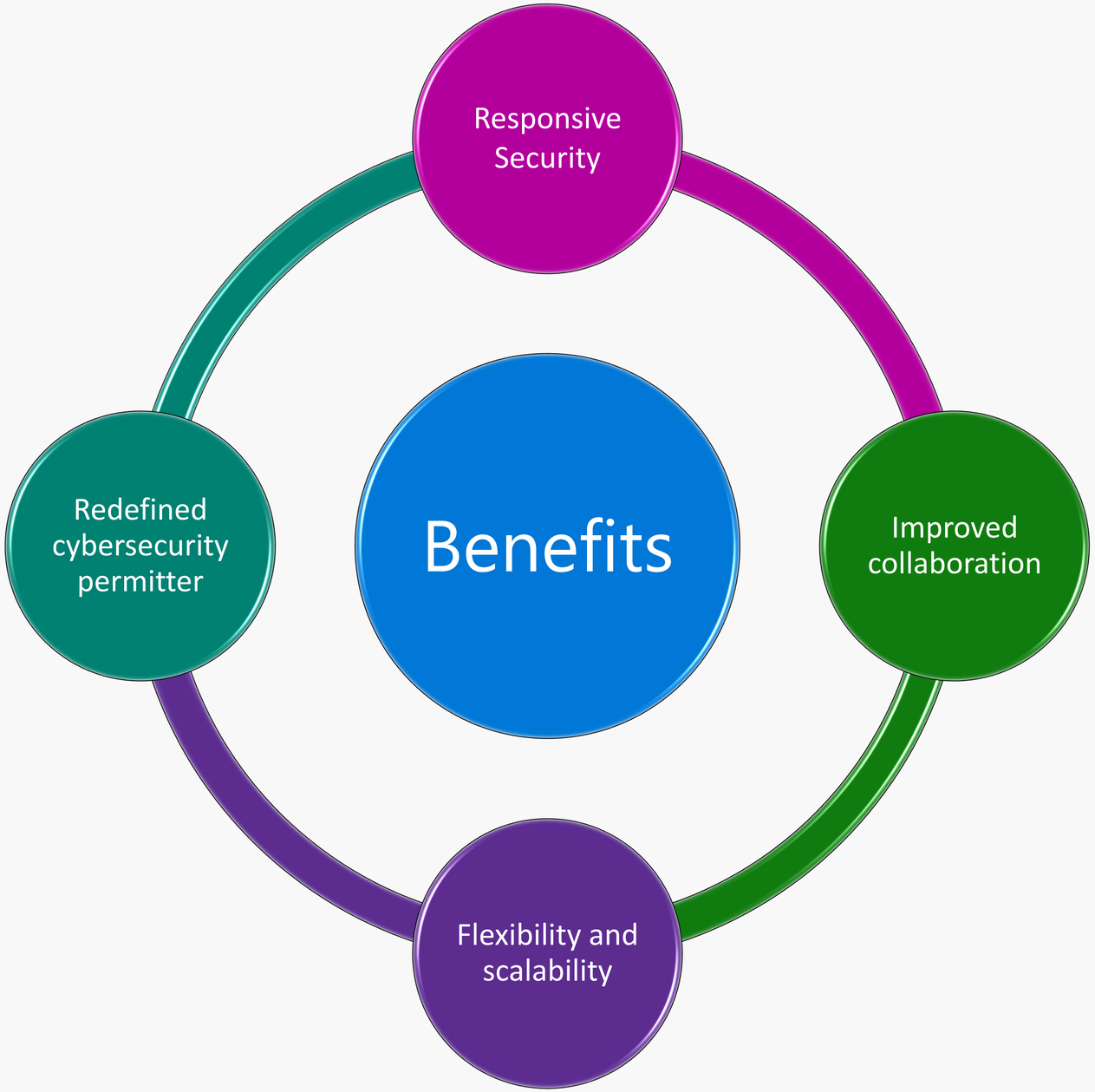
Dashboard Layers



Cybersecurity Mesh Architecture Complete



Benefits of CSMA



- Cybersecurity mesh architecture (CSMA) provides a foundational support layer that enables distinct security services to work together to create a dynamic security environment.

- CSMA provides a more consistent security posture to support increased agility for the composable enterprise. As organizations invest in new technology to enable digitalization, CSMA provides a flexible and scalable security foundation that provides bolt-on security for assets in hybrid and multi-cloud environments.

- CSMA creates a better defensive posture through a collaborative approach between integrated security tools and detective and predictive analytics. The outcome is enhanced responsiveness to breaches and attacks.

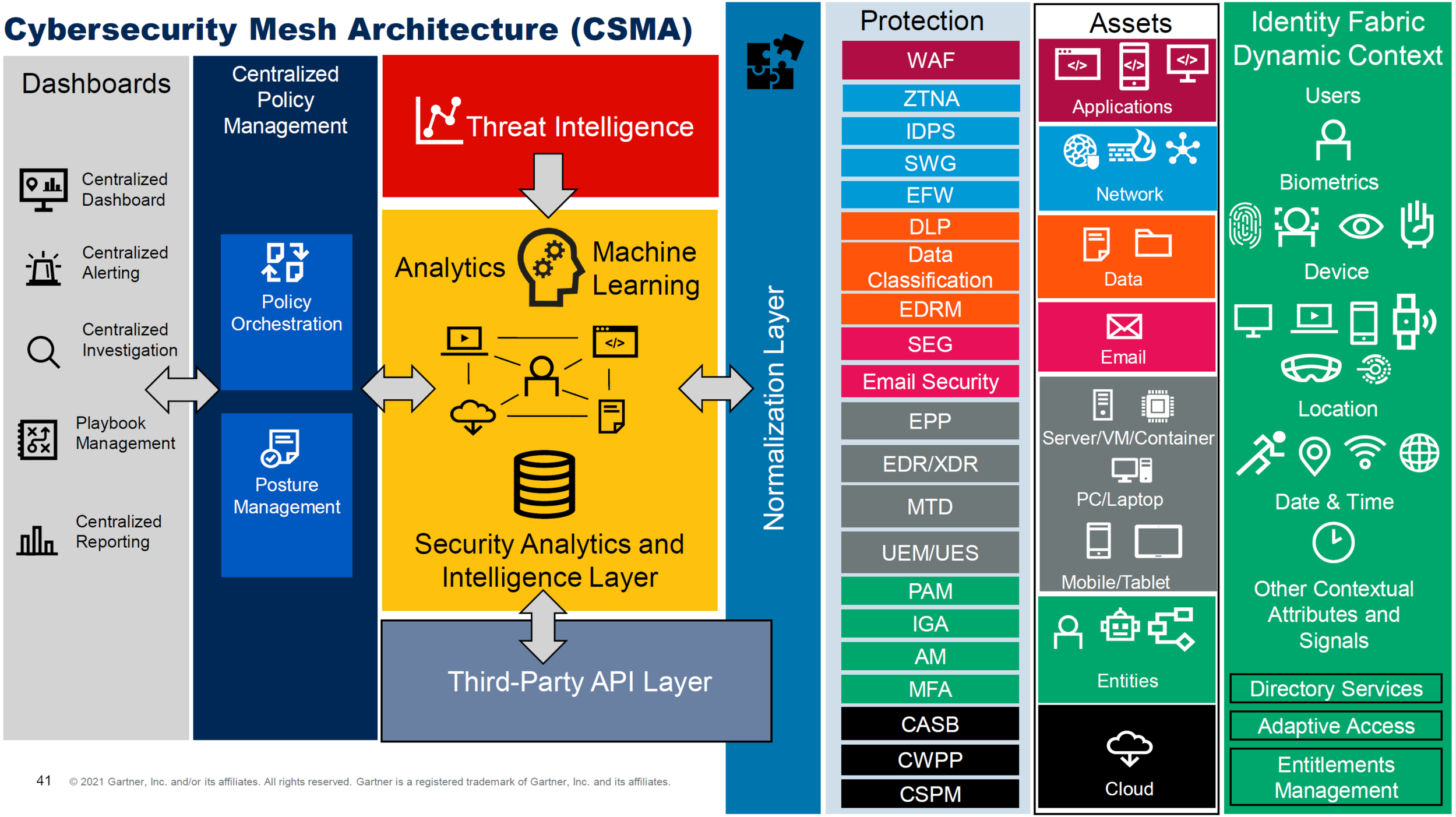
- Cybersecurity technology delivered through this model takes less time to deploy and maintain, while minimizing the potential for security dead ends that cannot support future needs. This frees cybersecurity teams for more value-added activities.

Challenges of CSMA

Recommendations

- Build supportive layers for a long-term CSMA strategy — security analytics, identity fabric, policy management, dashboards.
- Evaluate security controls with interoperability in mind: inversion of control APIs, standards support, extensible analytics.
- Familiarize yourself with current and emerging standards, and open-source code projects as a potential alternative to supplement vendor interoperability gaps.

Cybersecurity Mesh Architecture (CSMA)



Microsoft Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

May 2021 – https://aka.ms/MCRA

Security Operations / SOC

Threat Experts | *Detection and Response Team (DART)* | MSSP/MDR

Azure Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

Azure	Endpoint	Office 365	Identity	SaaS	Other Tools, Logs, and Data Sources
& 3rd party clouds	*& Server/VM*	*Email and Apps*	*Cloud & On-Premises*	*Microsoft Cloud App Security*	

Extended Detection and Response (XDR)

Azure Defender — **Microsoft 365 Defender**

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF

Software as a Service (SaaS)

Microsoft Cloud App Security

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Microsoft Endpoint Manager
Unified Endpoint Management (UEM)
Intune | Configuration Manager

Microsoft Defender for Endpoint
Unified Endpoint Security
- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Azure Security Center – Cross-Platform Cloud Security Posture Management (CSPM)

On Premises Datacenter(s) | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet: NGFW, Edge DLP, IPS/IDS, Azure AD App Proxy *Beyond User VPN*

Intranet: Express Route, Private Link, Azure Arc, Azure Stack

Azure Marketplace

Secure Score
Compliance Dashboard

- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- *Security & Other Services*

Information Protection

Classification Labels

- Azure Purview
- Microsoft Information Protection (MIP): Discover, Classify, Protect, Monitor
- File Scanner *(on-premises and cloud)*
- Data Governance
- Advanced eDiscovery

Compliance Manager

Azure Active Directory

Passwordless & MFA
- Hello for Business
- Authenticator App
- FIDO2 Keys

Identity Protection
- Leaked cred protection
- Behavioral Analytics

- Azure AD PIM
- Identity Governance
- Azure AD B2B & B2C

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 Security

Network protection	*App control*
Credential protection	*Exploit protection*
Full Disk Encryption	*Behavior monitoring*
Attack surface reduction	*Next-generation protection*

IoT and Operational Technology (OT)

Azure Sphere

Azure Defender for IoT
- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

Azure Defender – Cross-Platform, Cross-Cloud XDR
Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

Attack Simulator | Insider Risk Management | Communication Compliance

GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Conclusion

- Cybersecurity mesh architecture is a distributed security architecture that decentralizes security controls across the network, application, and data layers.

- Cybersecurity mesh architecture provides enhanced security, scalability, and resilience, making it ideal for managing modern distributed systems such as microservices, cloud-native applications, and IoT.

- Implementation of cybersecurity mesh architecture requires careful planning, integration, training, and maintenance to ensure its effectiveness and address new security threats.

Thank You !

Abbas Kudrati
APAC Chief Cybersecurity Advisor
Abbas.Kudrati@Microsoft.com
@askudrati
https://aka.ms/abbas