



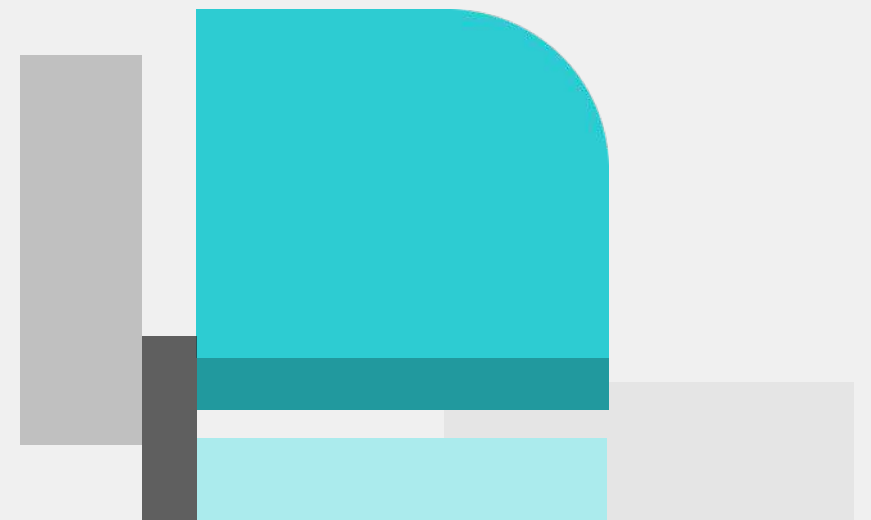
# Cybersecurity Mesh Architecture (CSMA)

A New Paradigm in Cybersecurity

Rupsan Shrestha

November 2024

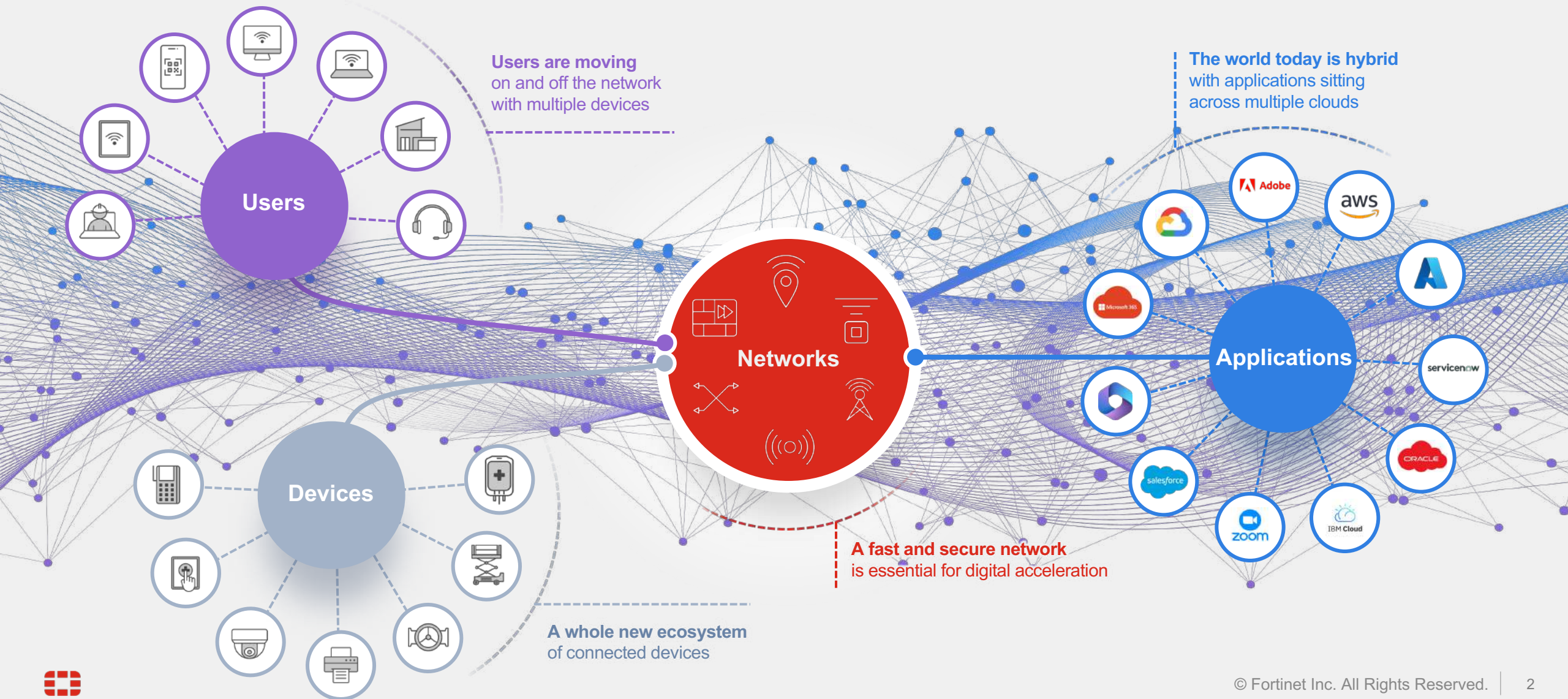
Fortinet Technologies Pvt. Ltd.



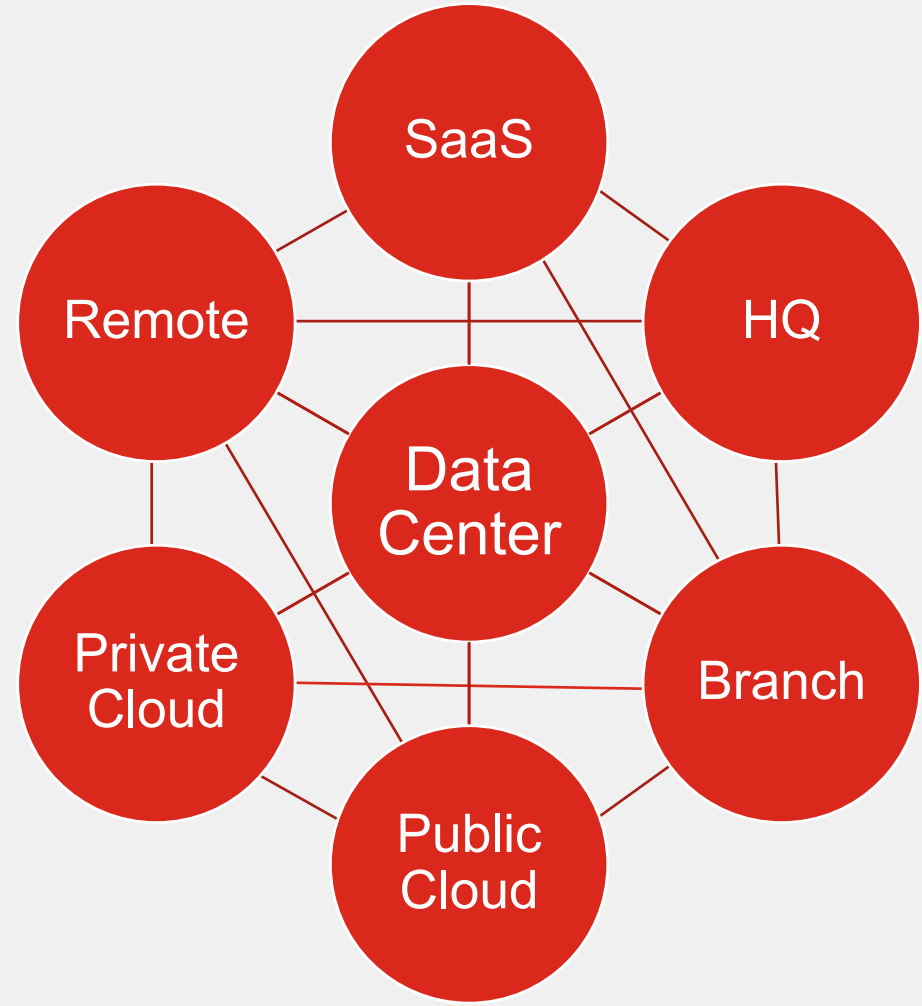
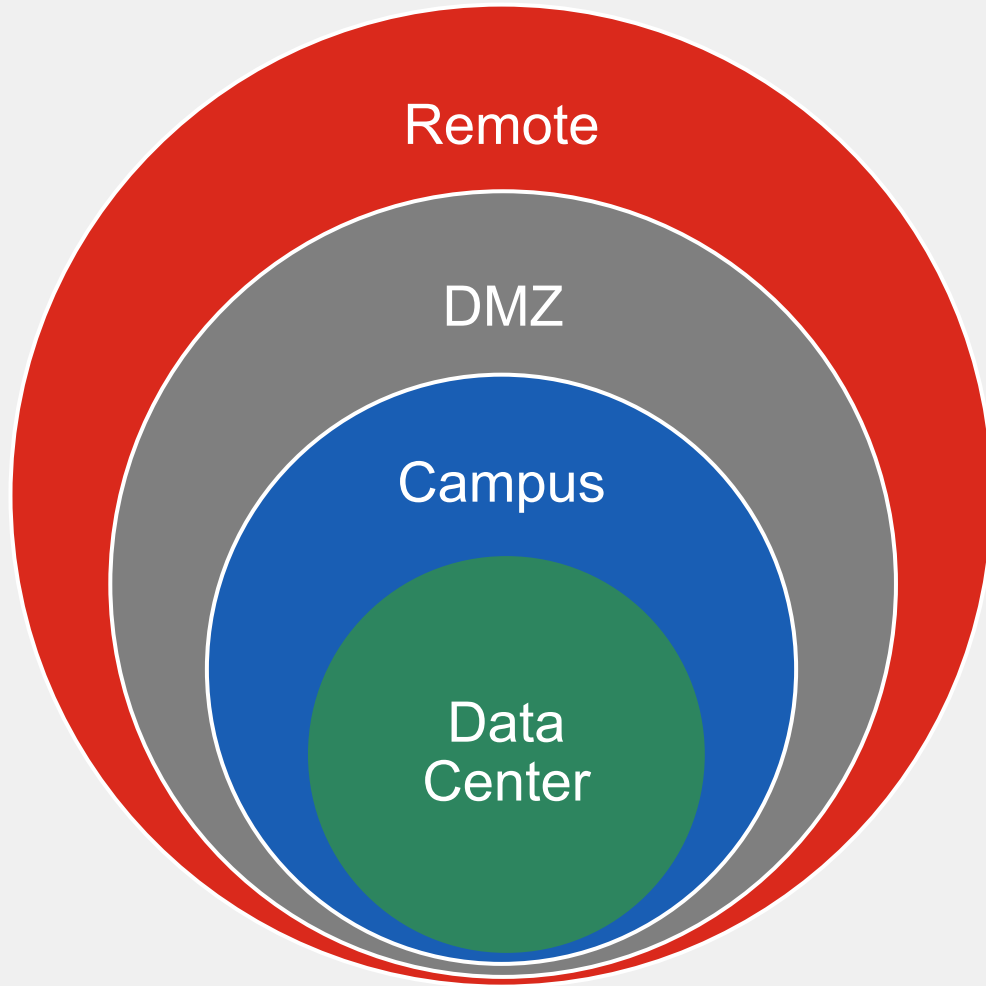


# Infrastructure has become more Complex...

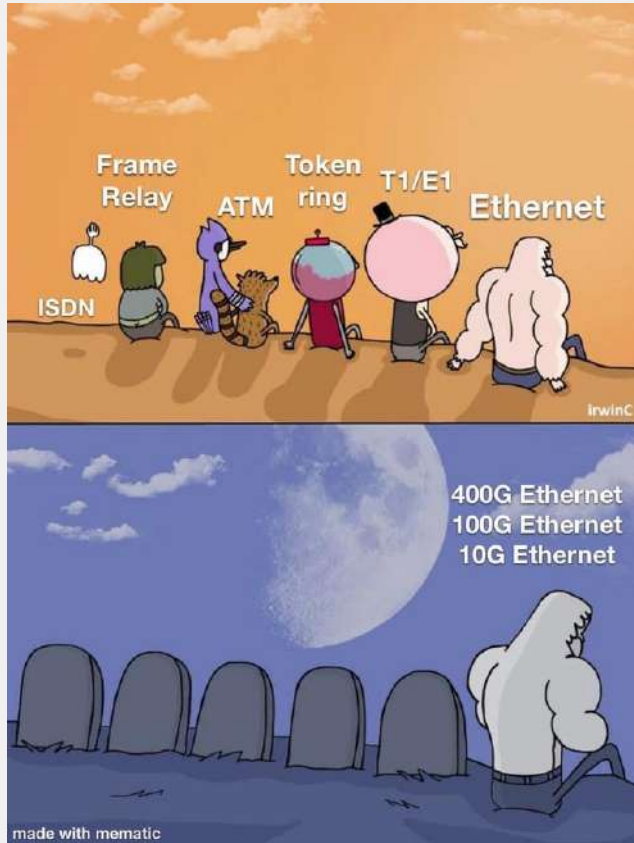
...leaving It Vulnerable to Attack



# Architectures Change





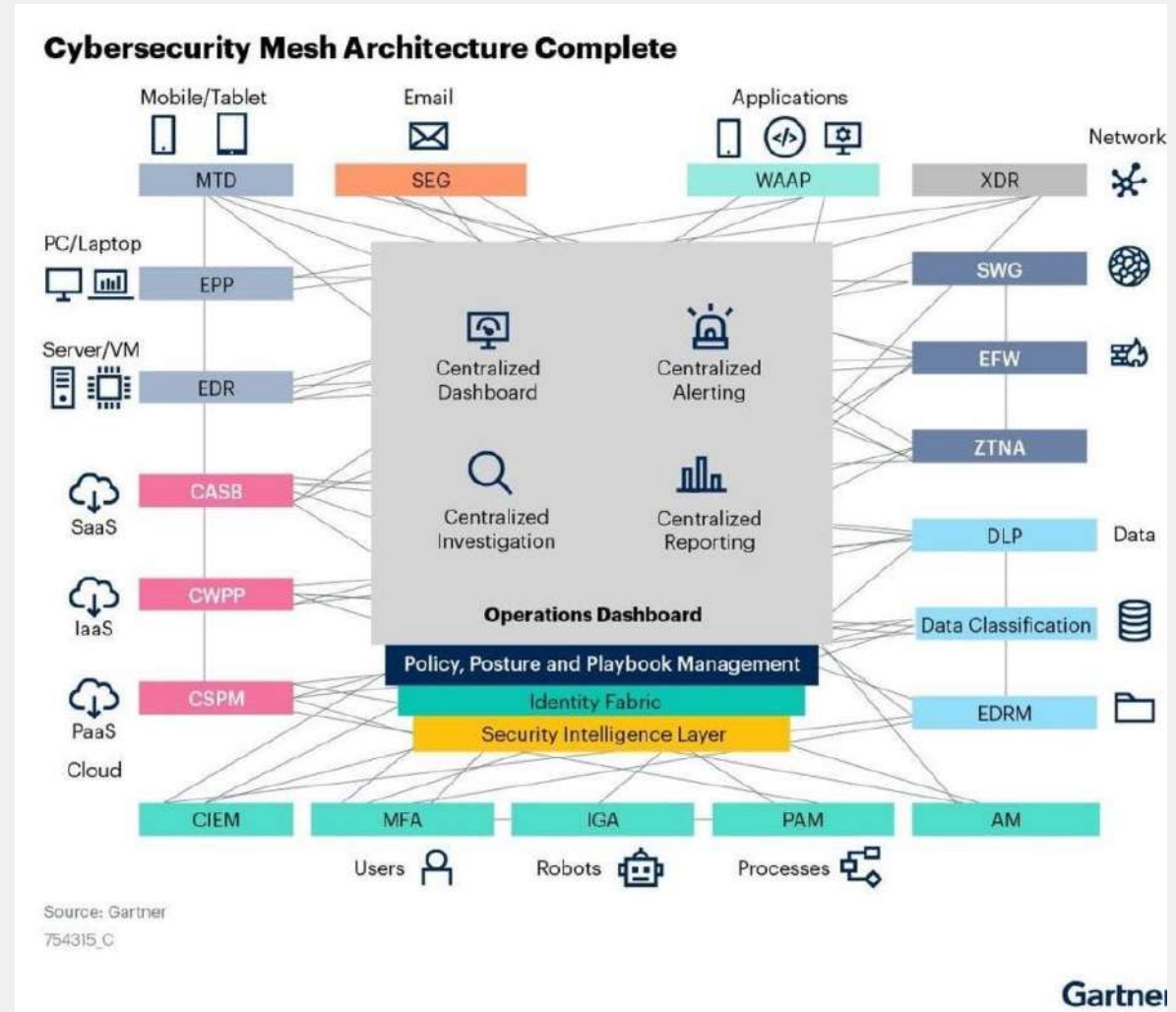


# Technology Enhancements and Digital Transformation



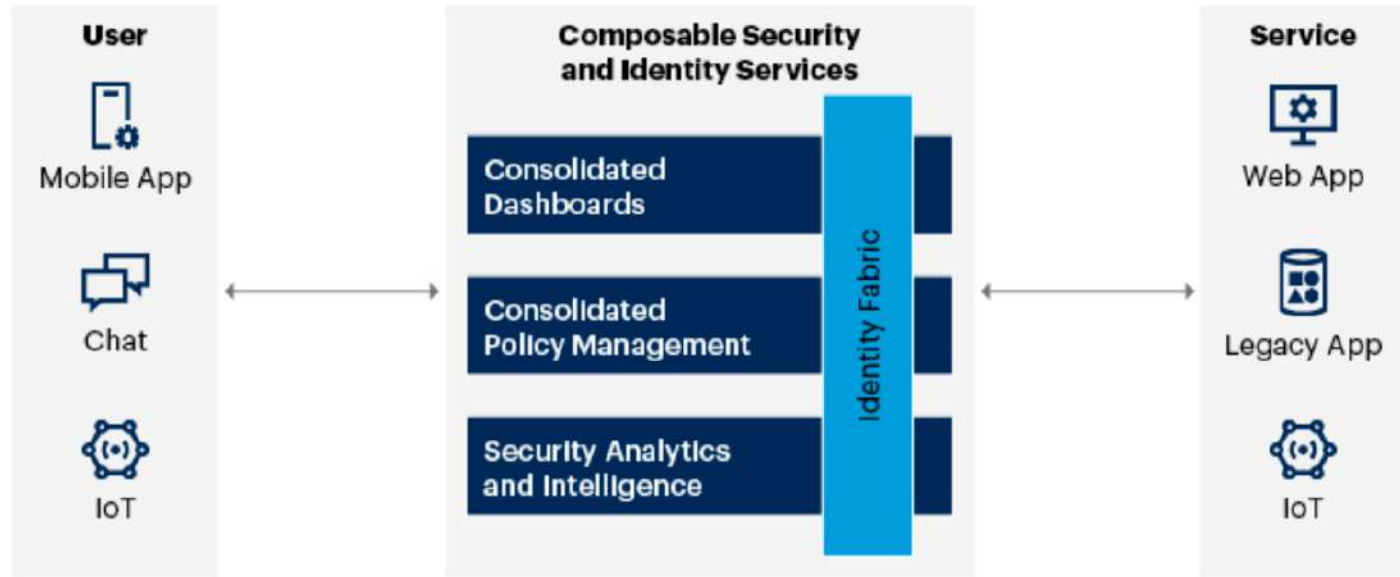
# What is Cybersecurity Mesh Architecture (CSMA)?

- A strategic approach to enhance security in distributed IT environments
- Designed for modern, distributed IT infrastructures
- security by decoupling from the traditional perimeter
- Focuses on:
  - **Identity** management
  - **Authentication**,
  - **Access Control** across multiple environments
- Offers a **scalable** and **modular** approach
- Aligns with evolving business needs for diverse IT environments



# How CSMA Works

## Cybersecurity Mesh Architecture



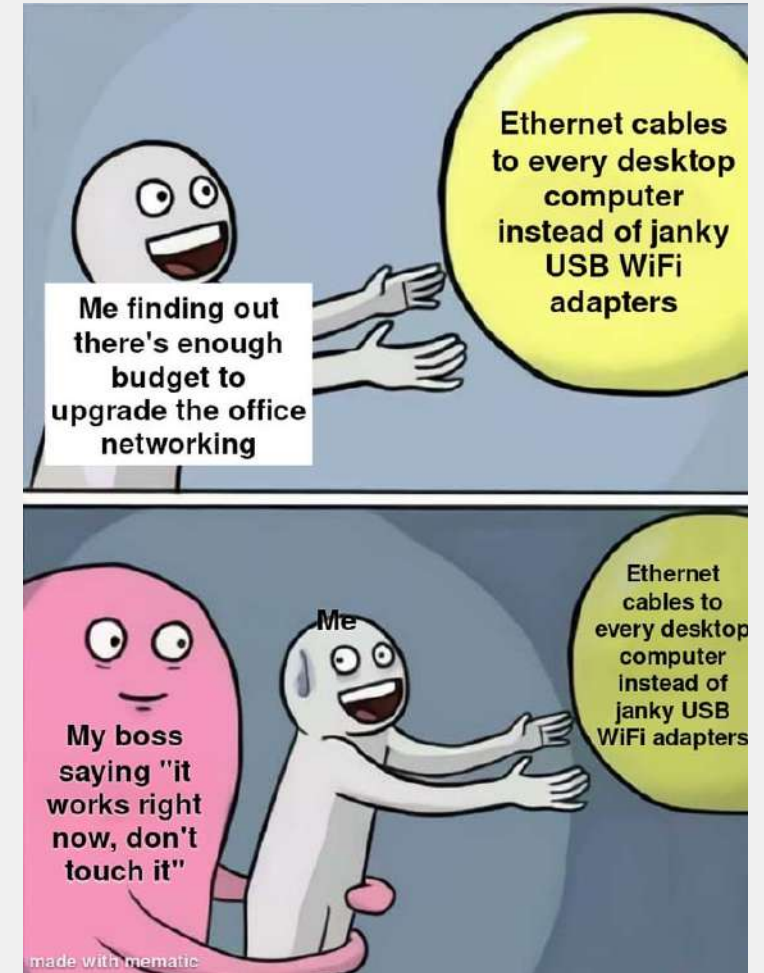
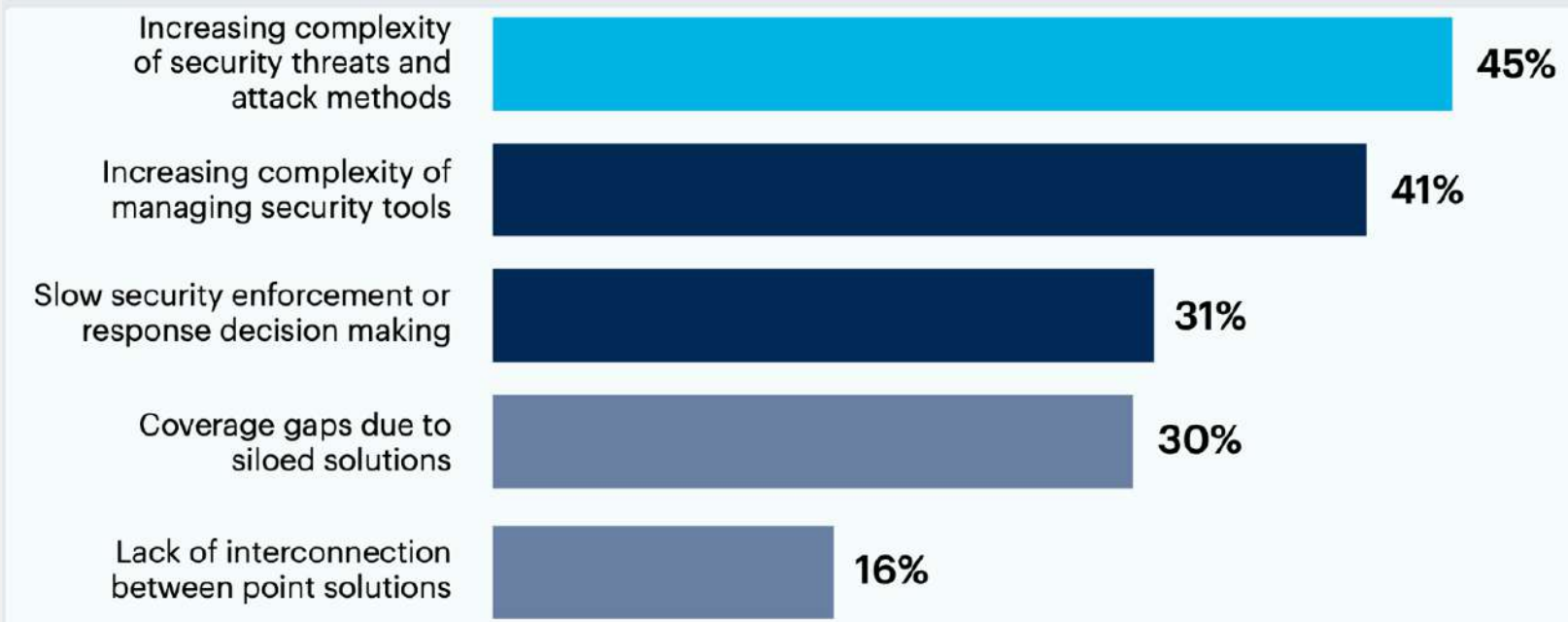
Source: Gartner  
756665\_C

Gartner

- enables organizations to implement security in a more flexible and dynamic way.
- ensures consistent policy enforcement and visibility across all assets—whether on-premises, in the cloud, or at the edge.
- uses a centralized management layer to enforce policies and a distributed architecture to apply security measures at every point of access.



# Challenge driving CSMA







# Use Case Example 1

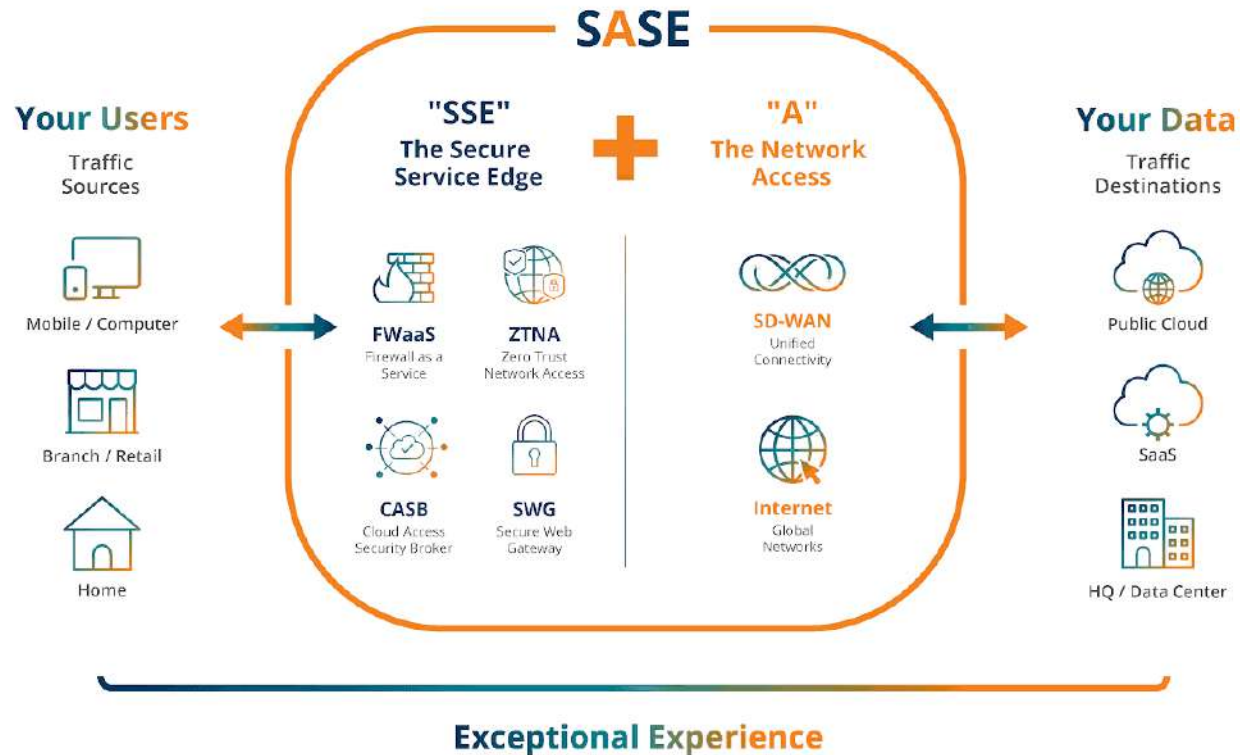
Unified/ Universal SASE





# What is SASE

Secure access service edge (SASE) is a cloud-native architecture that unifies SD-WAN with security functions like SWG, CASB, FWaaS, and ZTNA into one service.



SASE provides performance, integration, security, and management across your network for an exceptional experience for all users, applications, devices, and locations.

## Key Elements: Appliances

Key Elements:

Virtualization,

Cloud Out

Access for

5G Failover,

### • Local Compute:

- Likely Container Based, No VMs
- Self Healing, Restart
- Centralized Management, Designed for Intermittent Communications, Remote Updates

### • Local Networking and Security:

- Wi-Fi/Wireless LAN Support
- Private 5G Support
- Identity-Based Segmentation, Basic Network Access Control

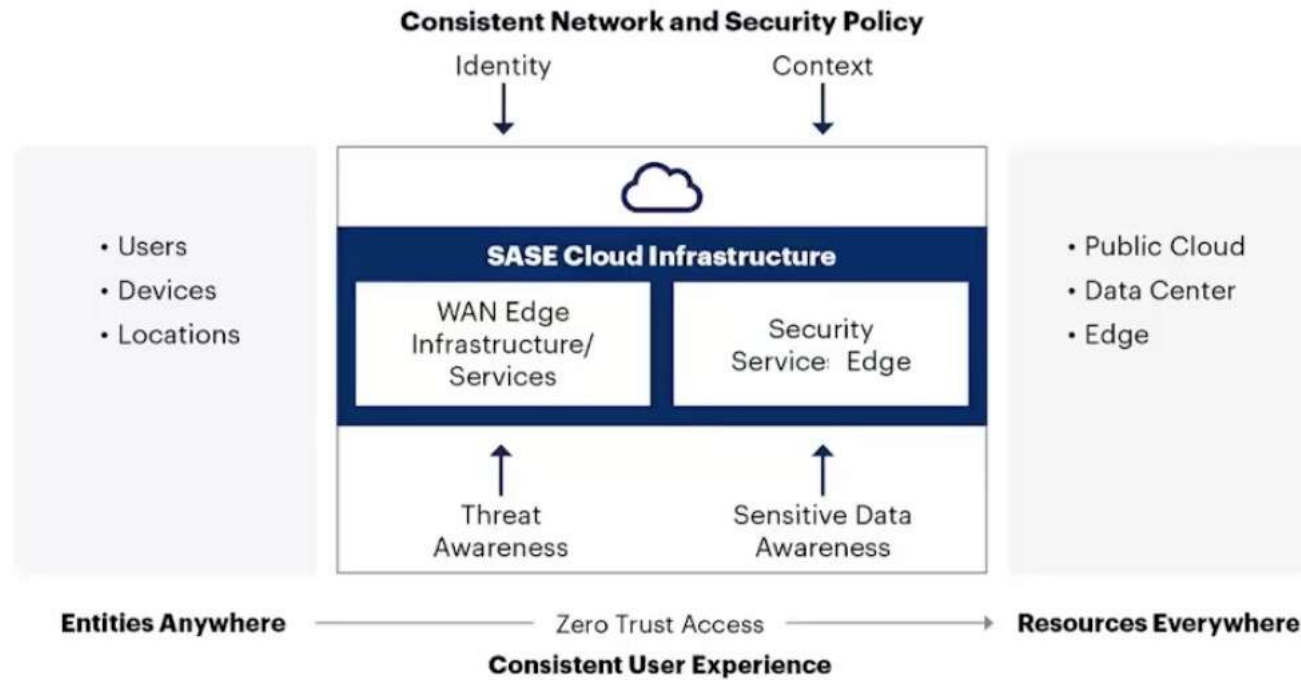
mark of Gartner, Inc. and its affiliates

Gartner



# Unified SASE

## Secure Access Service Edge



Source: Gartner

2 © 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner

## Secure Access Service Edge

SD-LAN  
Endpoint Security

Entities  
Anywhere

Ze

Uni

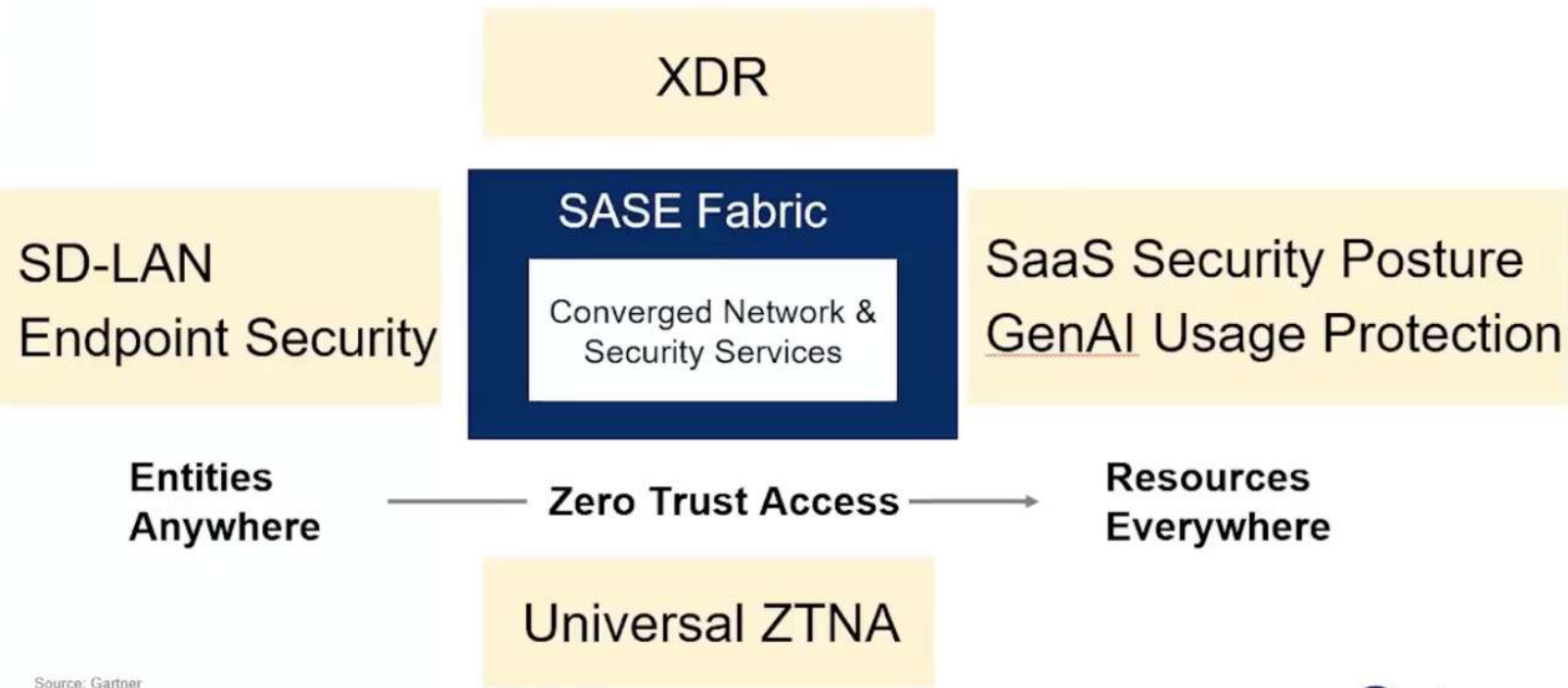
Source: Gartner

13 © 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.



# Unified SASE

## Secure Access Service Edge Expanded Use Cases



Source: Gartner

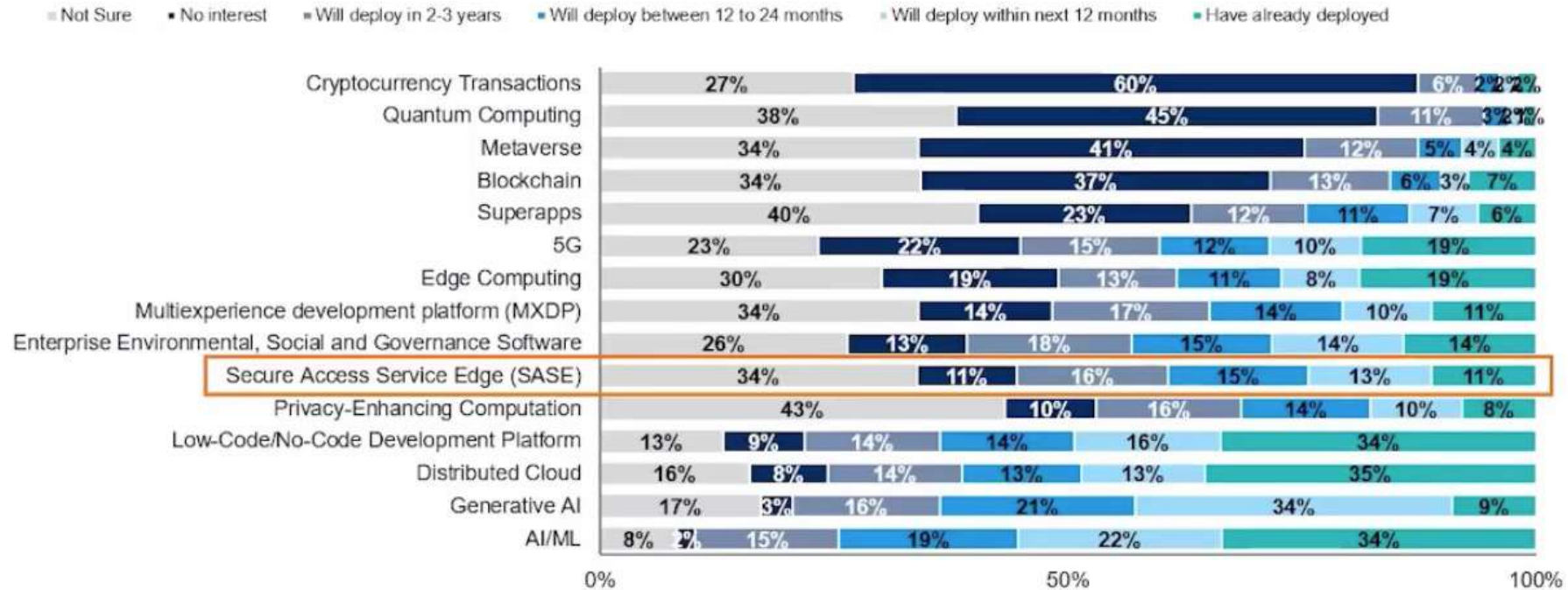
13 © 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Gartner



# CIO Trend on SASE

## State of Deployment for Emerging Technologies (see notes below) 2024 Percentage of Respondents



n = 2,443 CIOs and technology executives answering  
 Q. What are your enterprise's plans in terms of the following digital technologies and trends?  
 Source: 2024 Gartner CIO and Technology Executive Survey







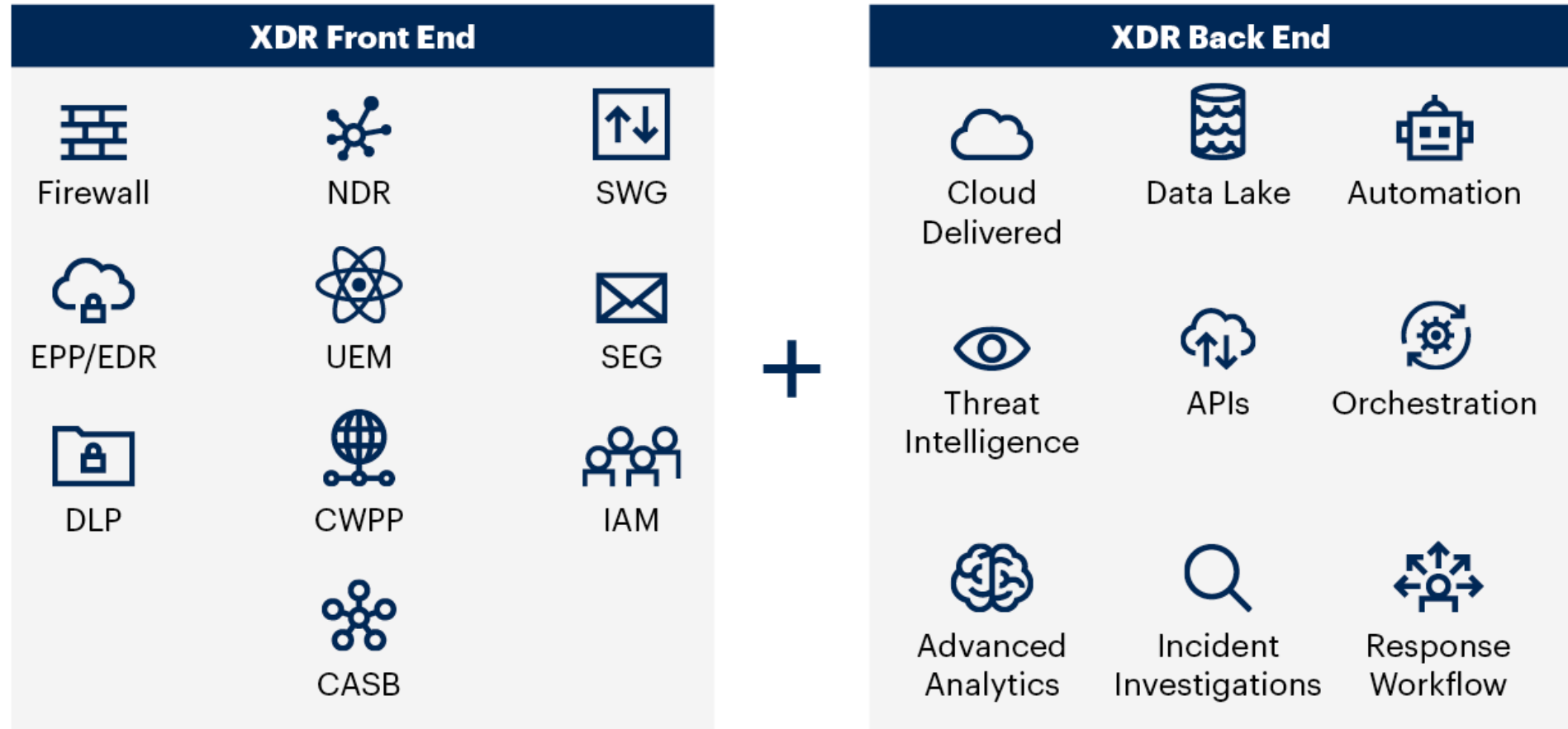
# Use Case Example 2

EDR/XDR Hype



# What is XDR

## XDR Overview

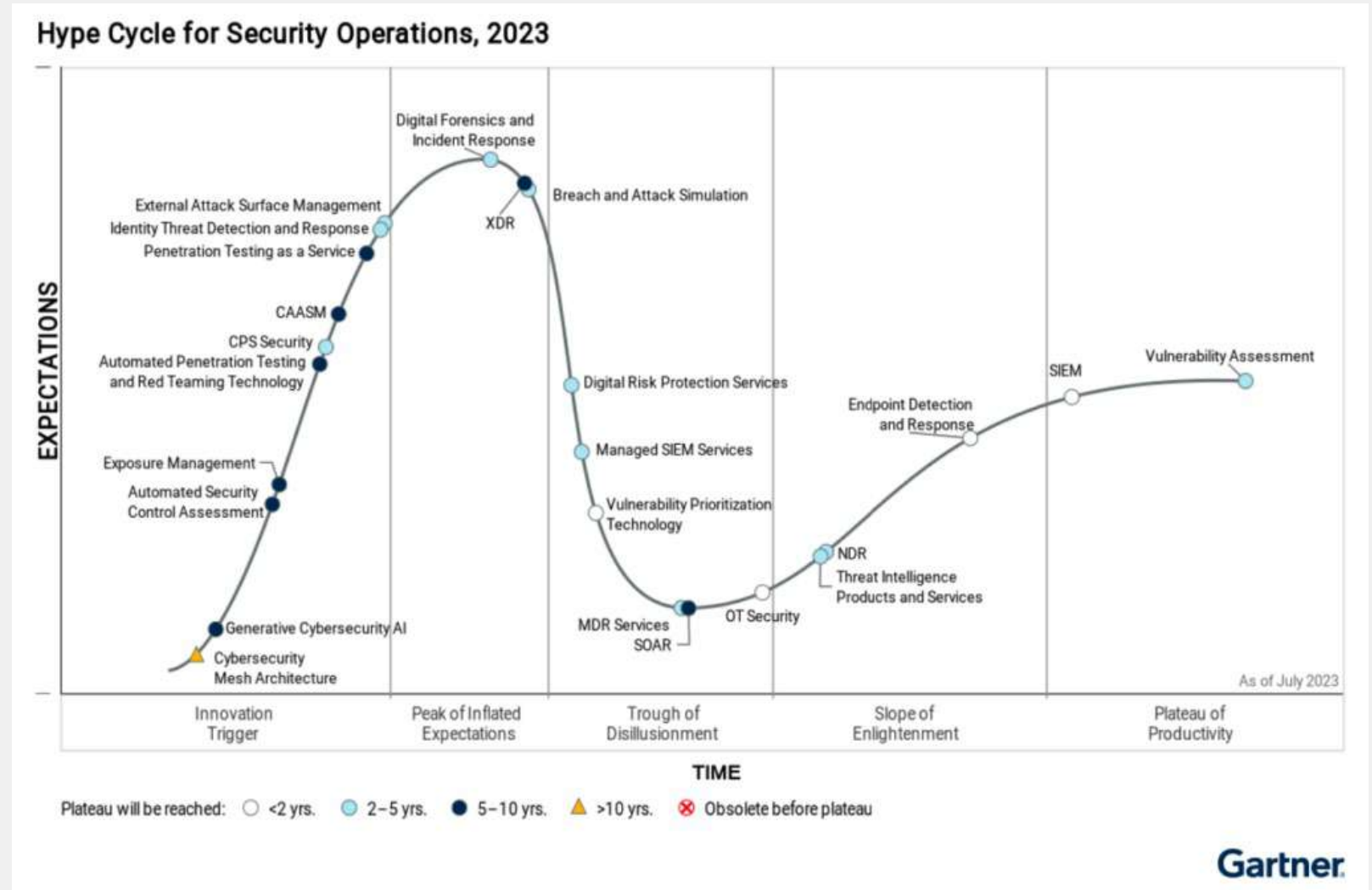


Source: Gartner  
747261\_C



# XDR Hype

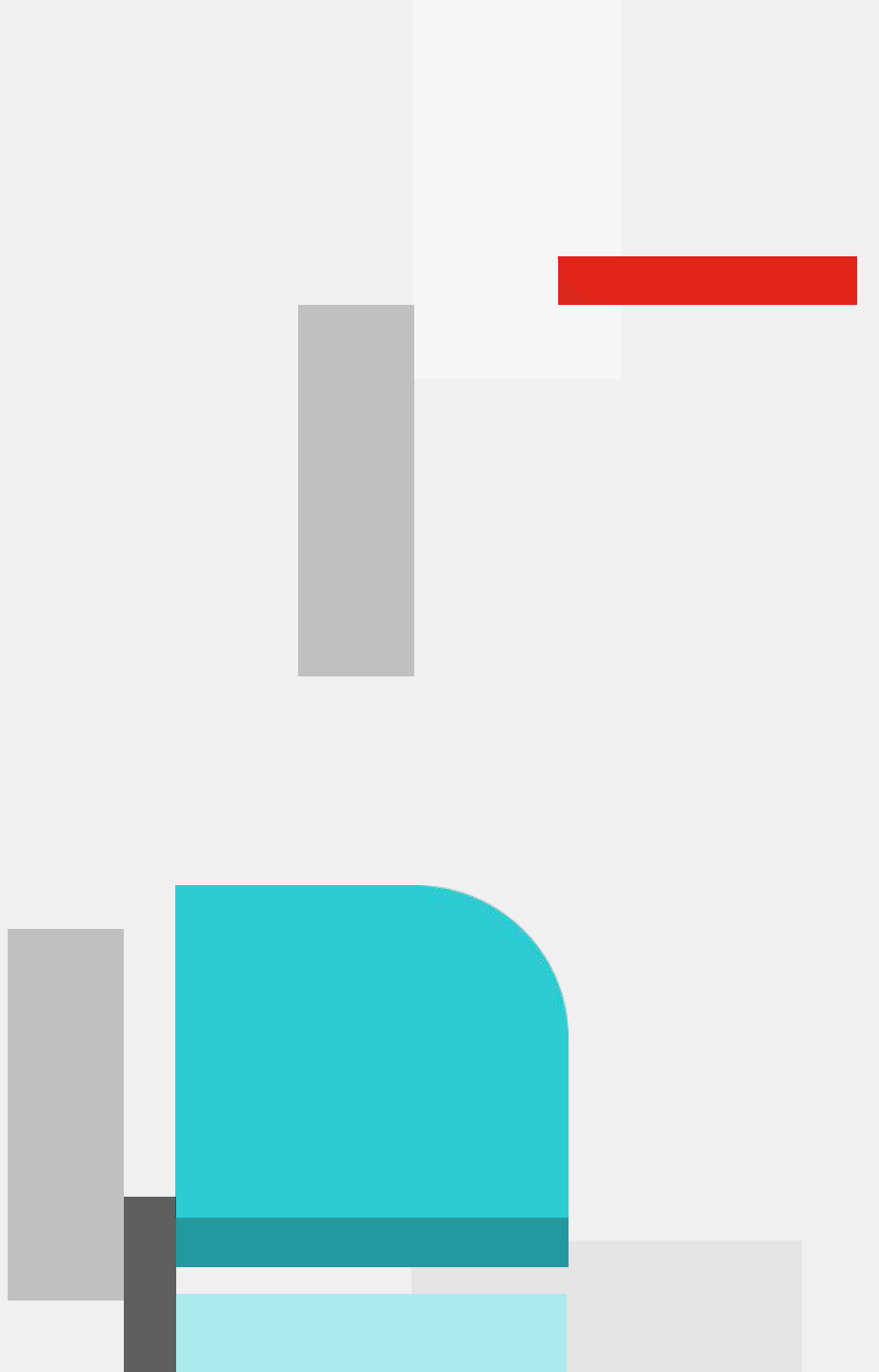


- Gartner has forecast that 40 percent of organizations will have deployed an XDR platform by 2027, up from 5 percent in 2021.
- Extended Detection and Response (XDR) is a platform that integrates and correlates data and alerts from multiple security components.





# Use Case Example 3

Cloud Service Providers





# Cloud Service Providers

Major CSPs including AWS, Azure and GCP are providing cloud native services incorporating the CSMA Architecture

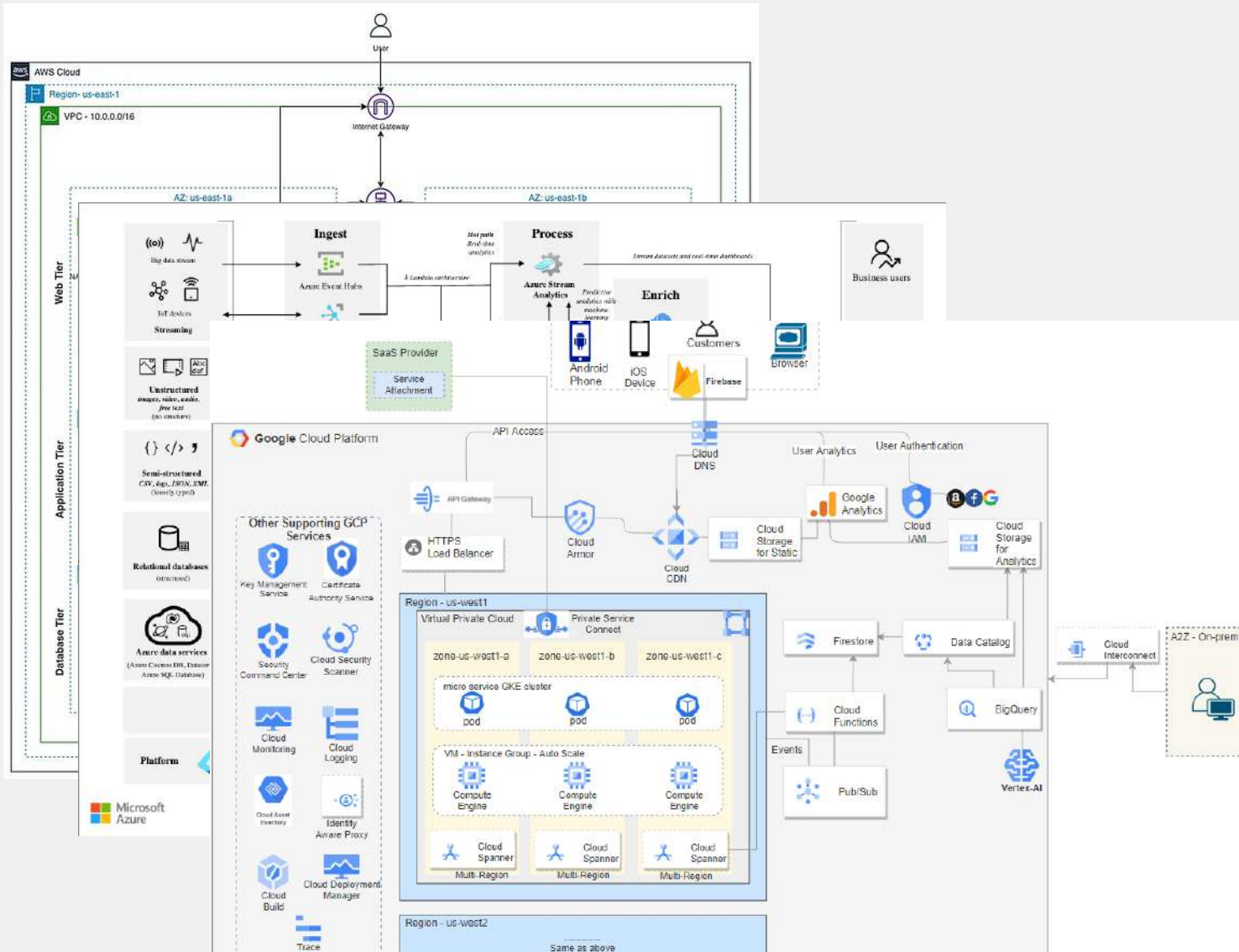
- Common policy and posture management dashboards
- Security Analytics and Intelligence
  - AWS Security Hub
  - Azure Security Center
  - GCP Security Command Center

## Identity Fabric:

- AWS Identity and Access Management
- Google Cloud Identity and Access Management
- Azure Active Directory

SERVICES	aws	Azure	Google Cloud Platform
Virtual Servers	Elastic Cloud Compute	Virtual Machines	Google Compute Engine
Serverless Computing	Lambda	Azure Functions	Cloud Functions
Kubernetes Management	Elastic Kubernetes Service	Kubernetes Service	Kubernetes Engine
Object Storage	Simple Storage Service	Azure Blob	Cloud Storage
File Storage	Elastic File Storage	Azure Files	Filestore
Block Storage	Elastic Block Storage	Azure Disk	Persistent Disk
Relational Database	Relational Database Service	SQL Database	Cloud SQL
NoSQL Database	DynamoDB	Cosmos DB	Firestore
Virtual Network	Virtual Private Cloud	Azure VNet	Virtual Private Network
Content Delivery Network	CloudFront	Azure CDN	Cloud CDN
DNS Service	Route 53	Traffic Manager	Cloud DNS
Authentication and Authorization	IAM	Azure Active Directory	Cloud IAM
Key Management	KMS	Azure Key Vault	KMS
Network Security	AWS WAF	Application Gateway	Cloud Armor

# Cloud Service Provides (AWS, Azure, GCP)



Unified Security Visibility

Distributed Security Control

Continuous Monitoring and Response

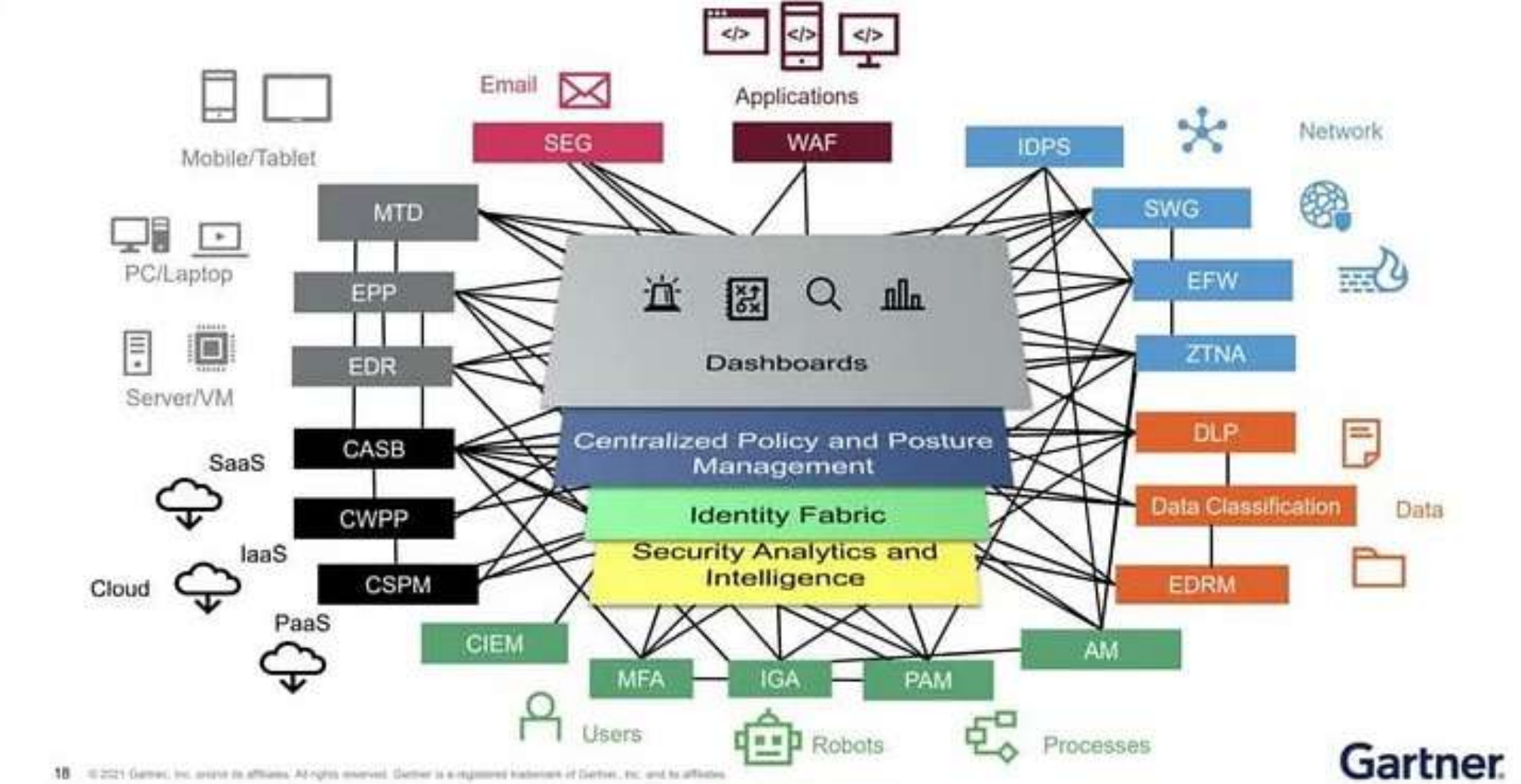




**What is common in every  
trending use cases/  
technologies ?**



# Cyber Security Mesh Architecture



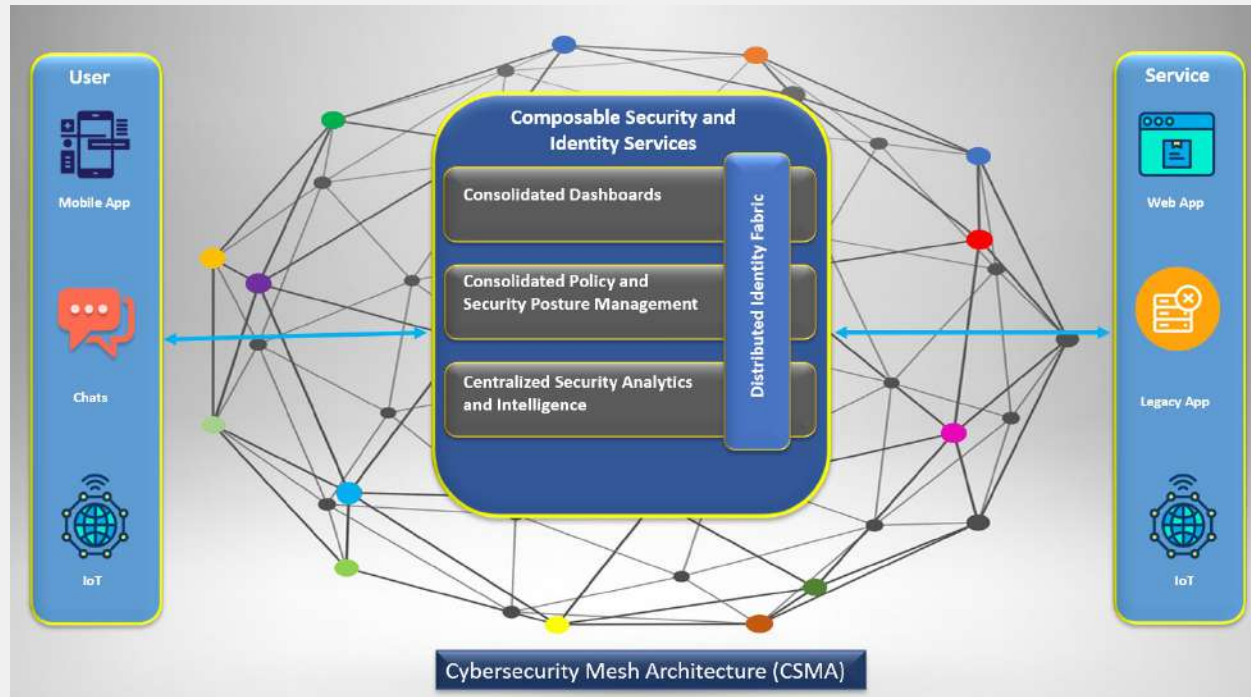
18 © 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.





# Gartner Vision for CSMA

- Gartner predicted that by 2025, 50% of organizations will have adopted some form of Cybersecurity Mesh Architecture.



<https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021>

# 2024 Gartner Peer insights

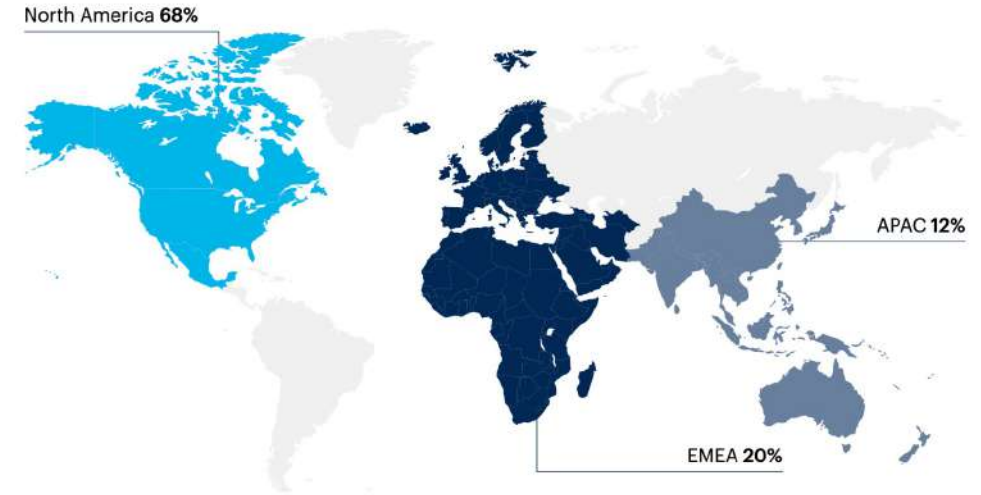
The majority are satisfied with the CSMA their orgs are building

Is your organization currently building CSMA?

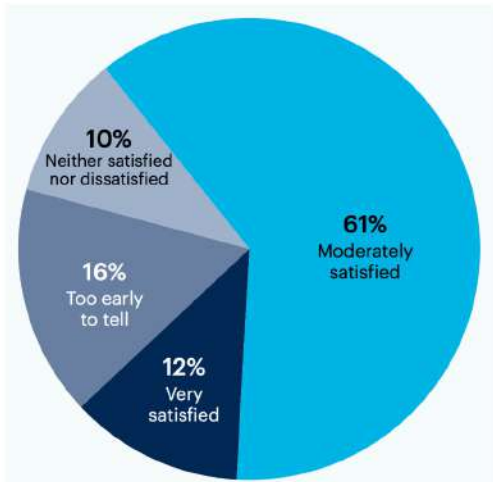


Over half (53%) of leaders are building CSMA at their organization.

n = 200



Are you satisfied with your organization's CSMA?

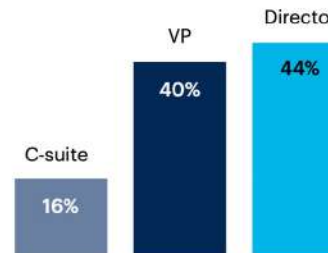


And almost three-quarters (73%) of those building CSMA feel satisfied with their organization's progress.

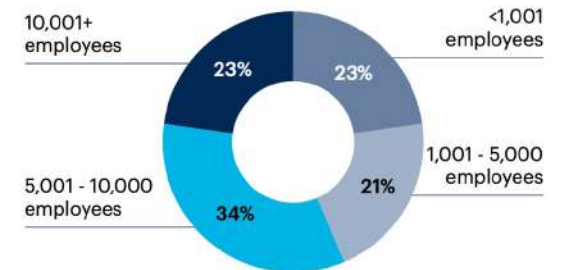
Moderately dissatisfied 0%, Very dissatisfied 0%

n = 105

Job Level



Company Size



<https://www.gartner.com/peer-community/oneminuteinsights/omi-cybersecurity-mesh-architecture-csma-guf>

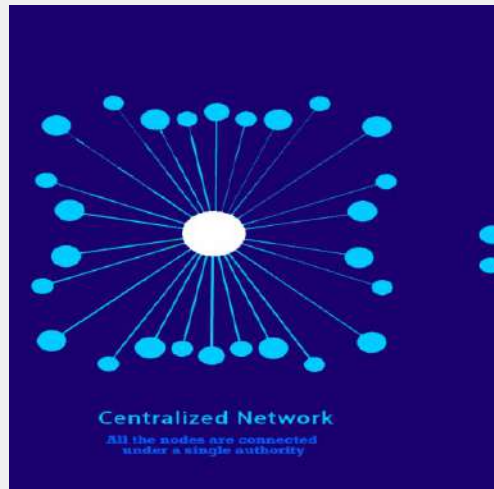


# How to Adopt CSMA

Organizations must take a phased, deliberate approach to adopt CSMA successfully.



**Assess your current cybersecurity infrastructure and identify gaps.**



**Implement a centralized security management platform to provide consistent policy enforcement.**



**Begin integrating distributed security controls at critical access points.**



**Continuously monitor and adapt to evolving security needs.**

# Avenue of Investments

<b>Avenue of Investigation</b> ↓	<b>Associated CSMA Layer(s)</b> ↓
Advanced SIEM products that are evolving toward risk-based prioritization of aggregated events and collecting more non-event-based context.	<ul style="list-style-type: none"><li>• Security analytics and intelligence</li><li>• Consolidated dashboards</li></ul>
Authorization frameworks, including dynamic authorization and policy-based entitlement management frameworks.	<ul style="list-style-type: none"><li>• Identity fabric</li><li>• Consolidated policy, posture and playbook management</li></ul>
Dynamic risk scoring of different entities (users, locations, devices, endpoints, etc.), whether as part of a point product or in a more centralized fashion.	<ul style="list-style-type: none"><li>• Security analytics and intelligence</li><li>• Identity fabric</li></ul>



Delivery of identity context to applications that require it through protocols such as OpenID Connect (OIDC) and tokens such as JSON Web Tokens (JWTs).

Also, extension of this to provide near-real-time dynamic session control.

- Identity fabric

SOAR capabilities that provide a measure of adaptive, automated response.

- Consolidated policy, posture and playbook management

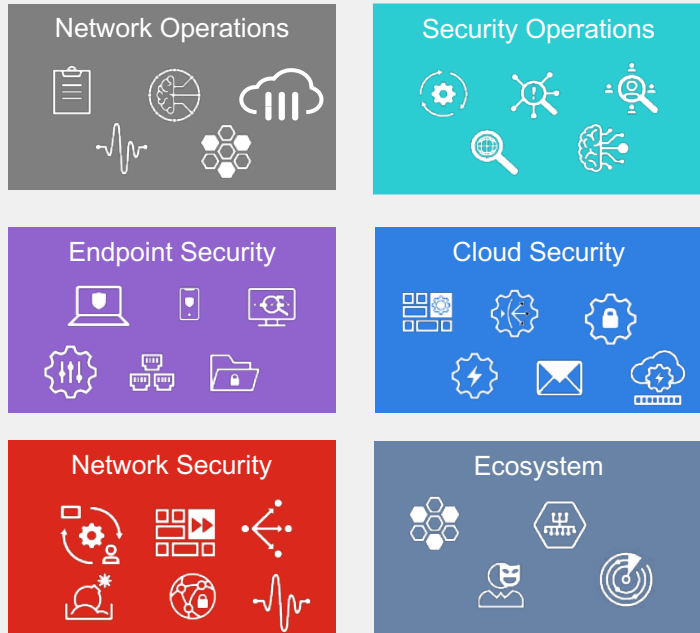




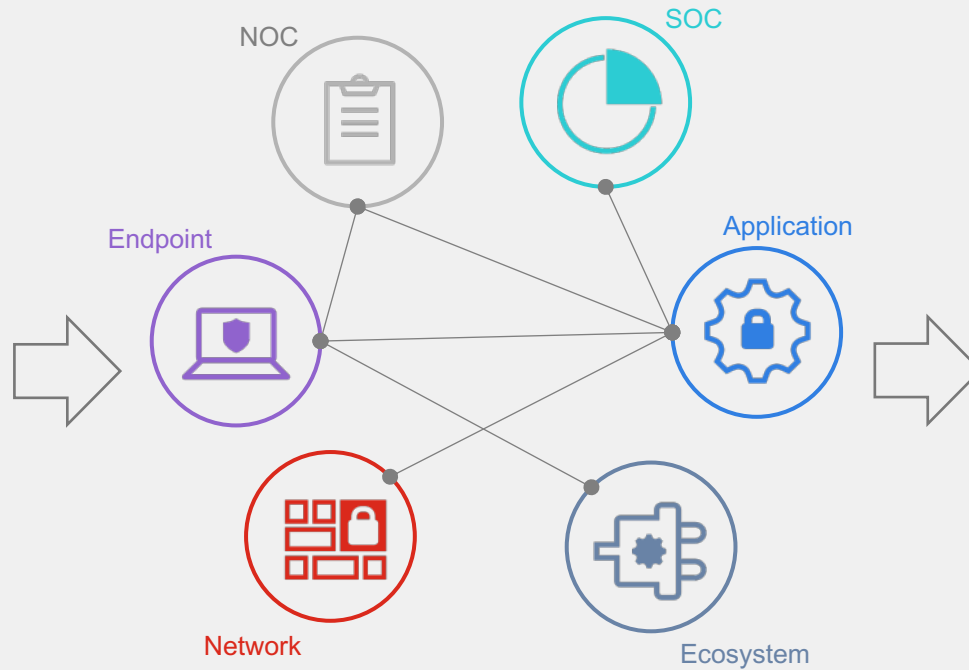
# Cybersecurity Platform Journey



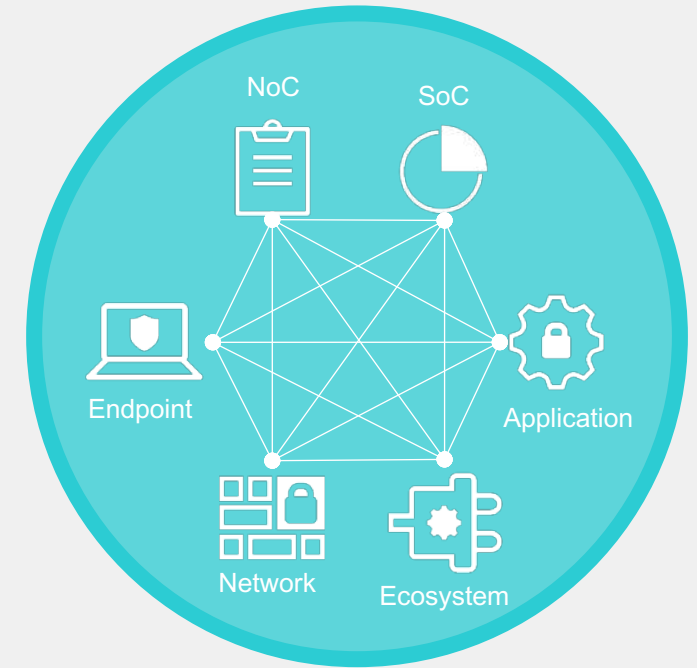
30+ Vendors



10 Vendors



2-3 Platforms



Your Journey to SOC Automation Maturity

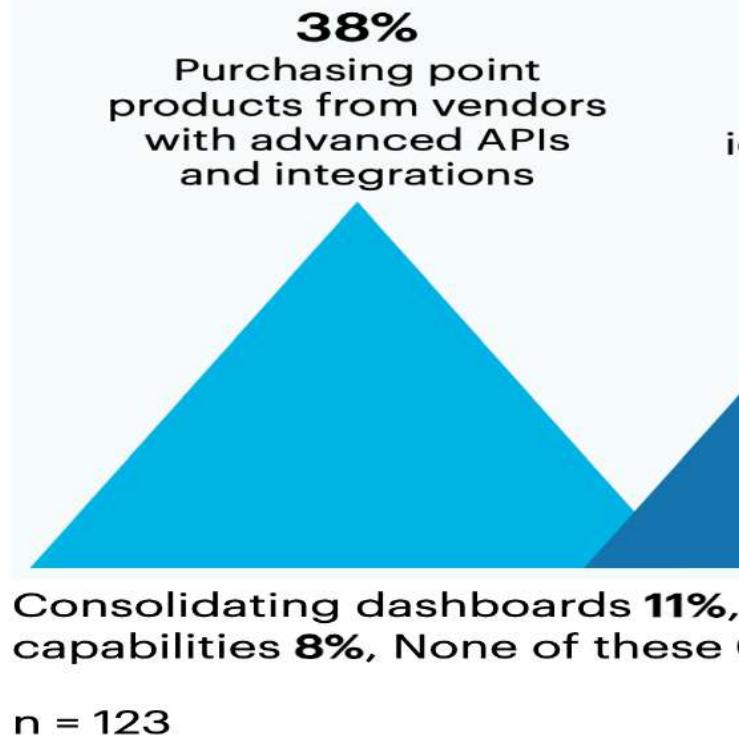


# Major Challenge in Implementing CSMA

Advanced APIs and integrations present a major challenge to building CSMA

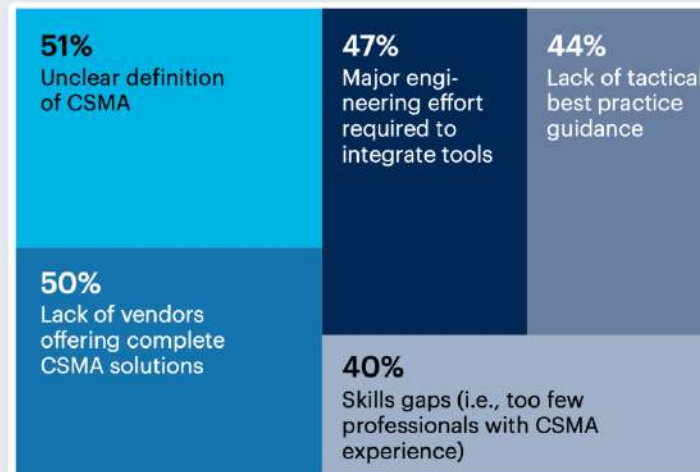
**38%** report that one of the most **difficult** aspects of building CSMA is **purchasing point solutions** with advanced APIs and integrations. About a third also find that building a common identity fabric (34%) and sourcing composable/distributed security tools (33%) are major challenges.

Which aspects of building CSMA have been most challenging?



Half of leaders say the unclear definition of CSMA (51%) as well as a lack of vendors offering complete solutions (50%) both represent key hurdles to adoption. The engineering efforts needed to integrate tools (47%) and the absence of tactical best practices (44%) are also common barriers.

What are the main barriers to CSMA?



Investment risk (i.e., introduction of industry standards may drive up cost of org's proprietary CSMA approach) **36%**, Costs **18%**, Lack of executive interest **8%**, None of these **0%**, Other **0%**

n = 200



# Conclusion

Evolving Threat Landscape vs Traditional Architecture

Cybersecurity Mesh Architecture

Key Components of CSMA

- Security Intelligence,
- Identity Fabric,
- Consolidated Policy, Posture and Playbook Management,
- Dashboards

Telemetry



**FORTINET®**