# Technical Insights: Architecting Cybersecurity Mesh — Preparing and Selecting Capabilities for the Future Using CSMA

Richard Bartley



Gartner®

# Your security architecture has hit a brick wall.

# You need to modernize!




Gartner®

# Pivoting to cybersecurity mesh brings new opportunities




Gartner®

# But .....
# What do you mean?




Gartner®

# Agenda

1. Limits of today’s security capabilities
2. New architectural principles
3. Pivoting with new requirements
4. Specifying new capabilities
5. Minimum viable architecture




Gartner®

# Agenda

1. Limits of today's security capabilities
2. New architectural principles
3. Pivoting with new requirements
4. Specifying new capabilities
5. Minimum viable architecture




Gartner®

# Current State

**Sources**

- SIEM
- XDR
- PACS
- SCRM
- PKI/Secrets/HSM/KMS
- LI
- WAAP
- MAST/SAST/DAST/ASPM
- ZTNA
- SWG/EFW
- DDoS
- NDR
- DLP
- Data classification
- DSP
- SEG/MTD
- Email security
- CPSPP
- UEM/UES
- EPP
- EDR
- MTD
- EAM
- PAM/AM
- IGA
- UEBA
- ITDR
- CASB/SSPM/SSE
- CWPP/CSPM
- CNAPP

**PROBLEM**
Limited log information

**PROBLEM**
No common API/ data standards

**PROBLEM**
No cross-communications between point solutions

**PROBLEM**
Fixed architecture

**Security information and event management**

**Security orchestration, automation and response**

**PROBLEM**
Analysis after the fact

**PROBLEM**
Need more effective analytics functions

**PROBLEM**
Solution doesn't support zero trust principles

**PROBLEM**
Cannot detect zero day attacks

**Actions**




Gartner®

# Lost Opportunities

- We’re not using point tools to the maximum extent.
- We’re not using threat intelligence well.
- We need to be proactive.
- We need to repurpose, reassign, commission and decommission tools.

# Agenda

1. Limits of today's security capabilities
2. New architectural principles
3. Pivoting with new requirements
4. Specifying new capabilities
5. Minimum viable architecture




Gartner®

# Build From New Fundamental Principles

- Maximize visibility
- Normalize data formats
- Use open standards and protocols
- Rigorously apply zero trust architecture
- Score risks in the context of all other risks
- Model for prediction using external insights
- Map identity context to all assets
- Enable real-time actions




Gartner®

# Agenda

1. Limits of today's security capabilities
2. New architectural principles
3. Pivoting with new requirements
4. Specifying new capabilities
5. Minimum viable architecture



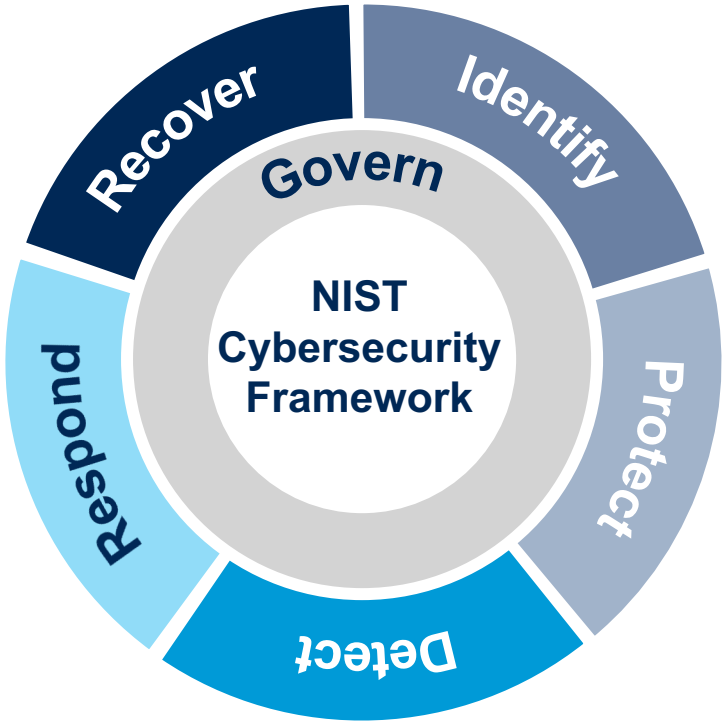

Gartner®

# Choose Point Tools to Meet Security Needs

## Security attributes

| | |
|---|---|
| Business enabled | Auditable |
| Architecturally open | Measured |
| Access-controlled | Flexibly secure |
| Detectable | Monitored |
| Flexible | Compliant |
| Authorized | Automated |
| Authenticated | Protected |
| Controlled | Extensible |
| Future-proof | Trustworthy |

## Security framework




## Point products CSMA aligned
(Subscriber/contributor)

- PACS
- SCRM
- PKI/Secrets/HSM/KMS
- LI
- WAAP
- MAST/SAST/DAST/ASPM
- ZTNA
- SWG/EFW
- DDOS
- NDR
- DLP
- Data classification
- DSP
- SEG/MTD
- Email security
- CPSPP
- UEM/UES
- EPP
- EDR
- MTD
- EAM
- PAM/AM
- IGA
- UEBA
- ITDR
- CASB/SSPM/SSE
- CWPP/CSPM
- CNAPP
- XDR
- SIEM




Gartner

# Conceptual Architecture to Fulfill the Principles

Map identity context to all assets

Normalize all data formats

Model for prediction using external insights

Enable real-time actions

Maximize visibility

Use open standards and protocols

Score risks in the context of all other risks

Rigorously apply zero trust architecture

**Visual-ization and UI**

**Policy and control**

**External sources & sinks**

**Security intelligence & data analytics services**

**Orchestration functions**

**Normal-ization service**

- PACS
- SCRM
- PKI/Secrets/HSM/KMS
- LI
- WAAP
- MAST/SAST/DAST/ASPM
- ZTNA
- SWG/EFW
- DDoS
- NDR
- DLP
- Data classification
- DSP
- SEG/MTD
- Email security
- CPSPP
- UEM/UES
- EPP
- EDR
- MTD
- EAM
- PAM/AM
- IGA
- UEBA
- ITDR
- CASB/SSPM/SSE
- CWPP/CSPM
- CNAPP
- XDR
- SIEM

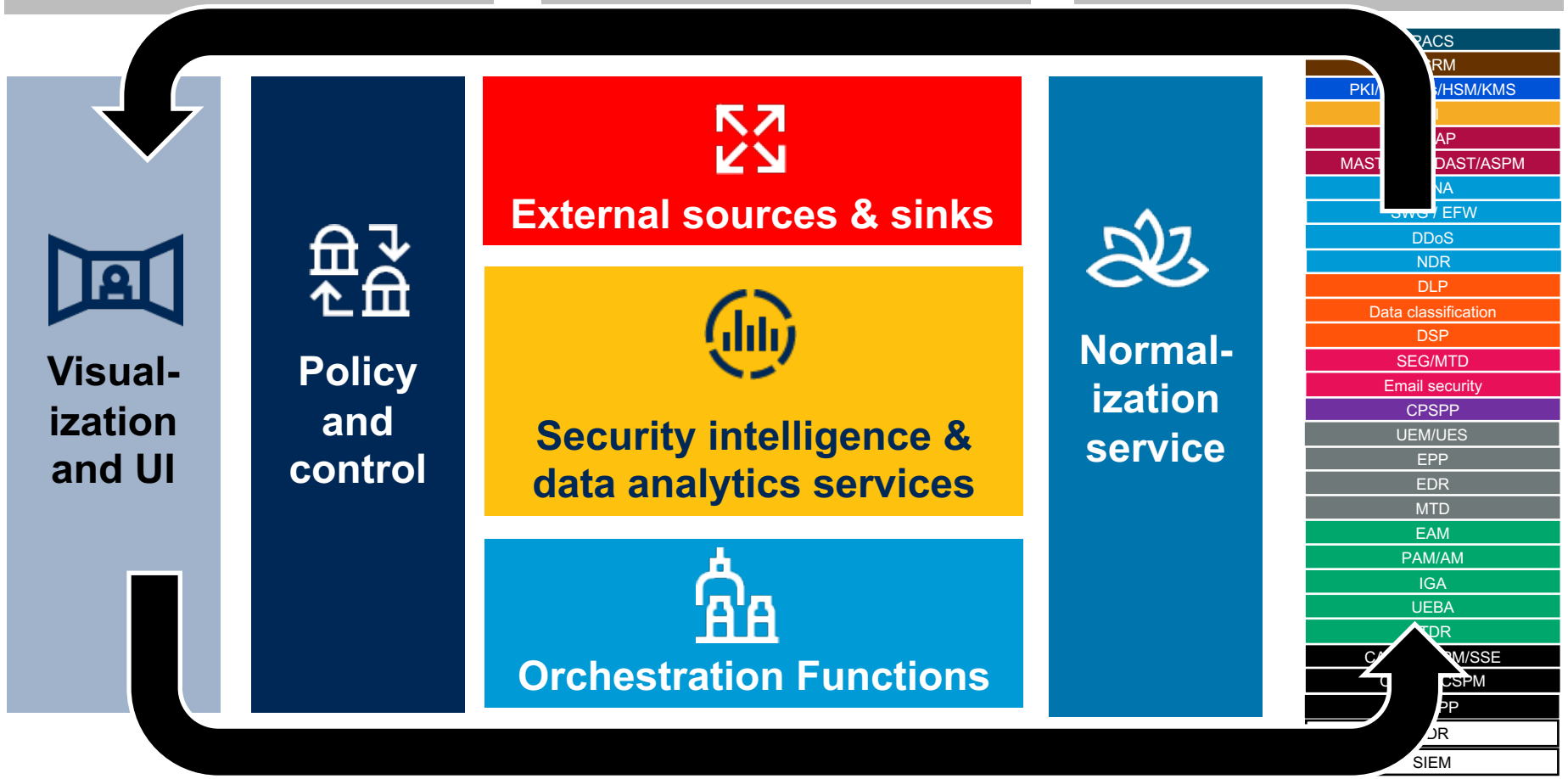
**IT assets and data**

**Identity services**

Gartner®

# Conceptual architecture to fulfil the principles

- Map identity context to all assets
- Normalize all data formats
- Model for prediction using external insights
- Enable real-time actions
- Maximize visibility
- Use open standards and protocols
- Score risks in the context of all other risks
- Rigorously apply zero trust architecture




Gartner

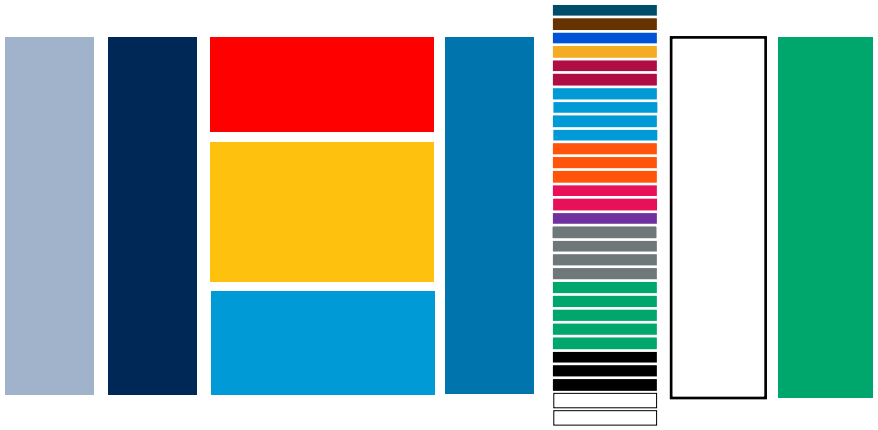
# Agenda

1. Limits of today's security capabilities
2. New architectural principles
3. Pivoting with new requirements
4. Specifying new capabilities
5. Minimum viable architecture



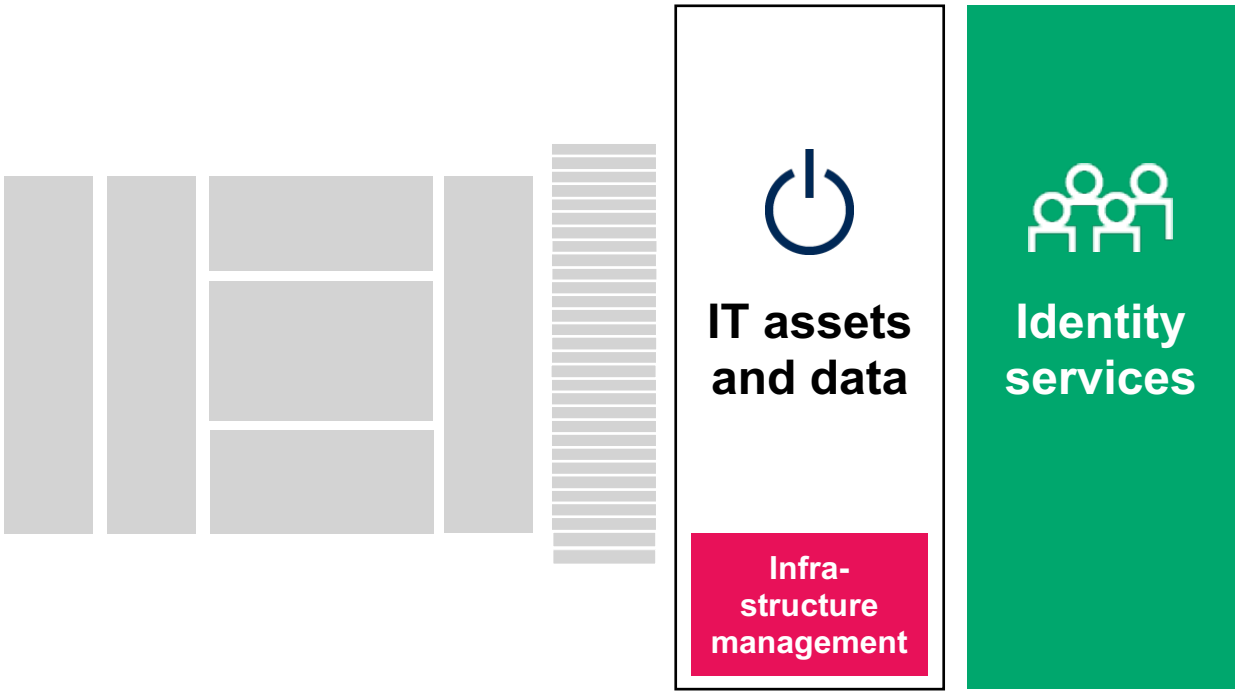

Gartner®

# New Requirements — Overall Architecture



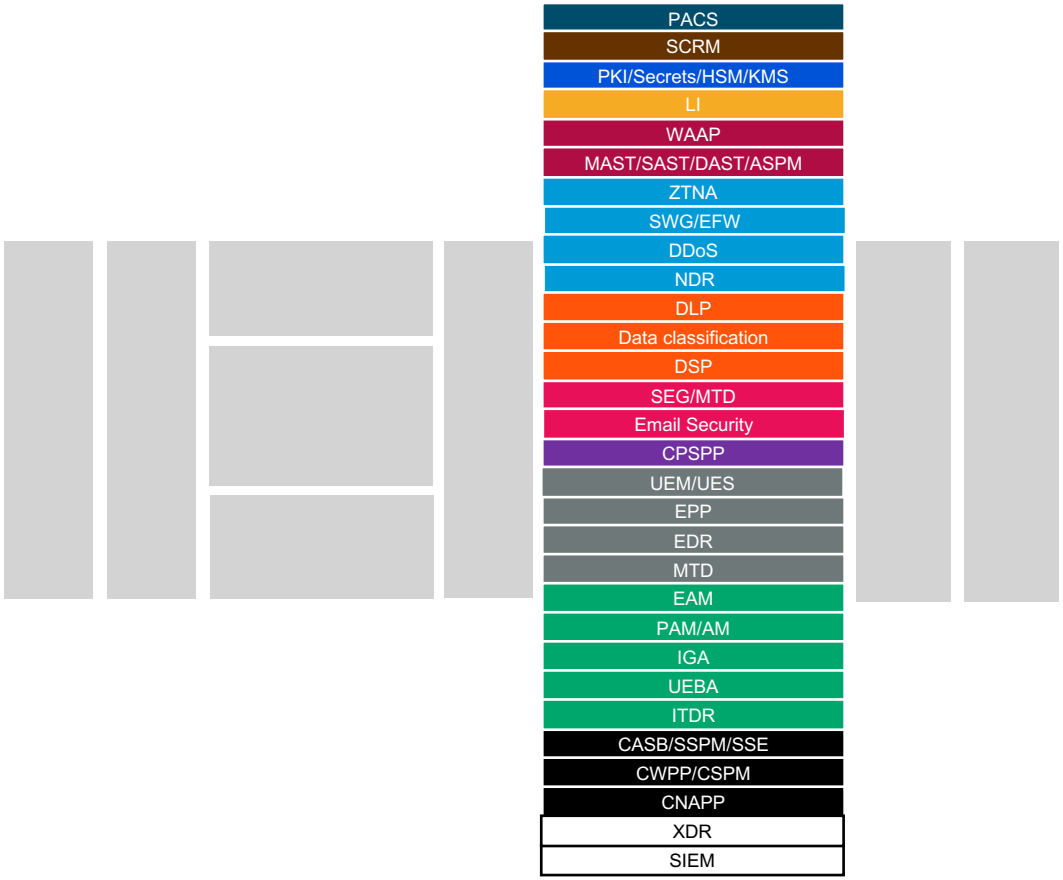
- Use normalized data analytics as the core of the architecture.
- Extract meaning data from more sources and scope accordingly.
- Select mesh architecture location to maximize access to data.
- Identify user communities early to support maximum utility and functionality.

# IT Assets and Identity




- Ensure future mesh architecture covers IT and data landscapes.
- Modernize identity services prior to any next steps.
- Must have foundational as well as advanced capabilities including:
  - Real time adaptive access
  - Discovery and ownership
  - Continuous session management
  - Encryption and trust
  - Policy enforcement
  - Entitlement management

# Security Tooling

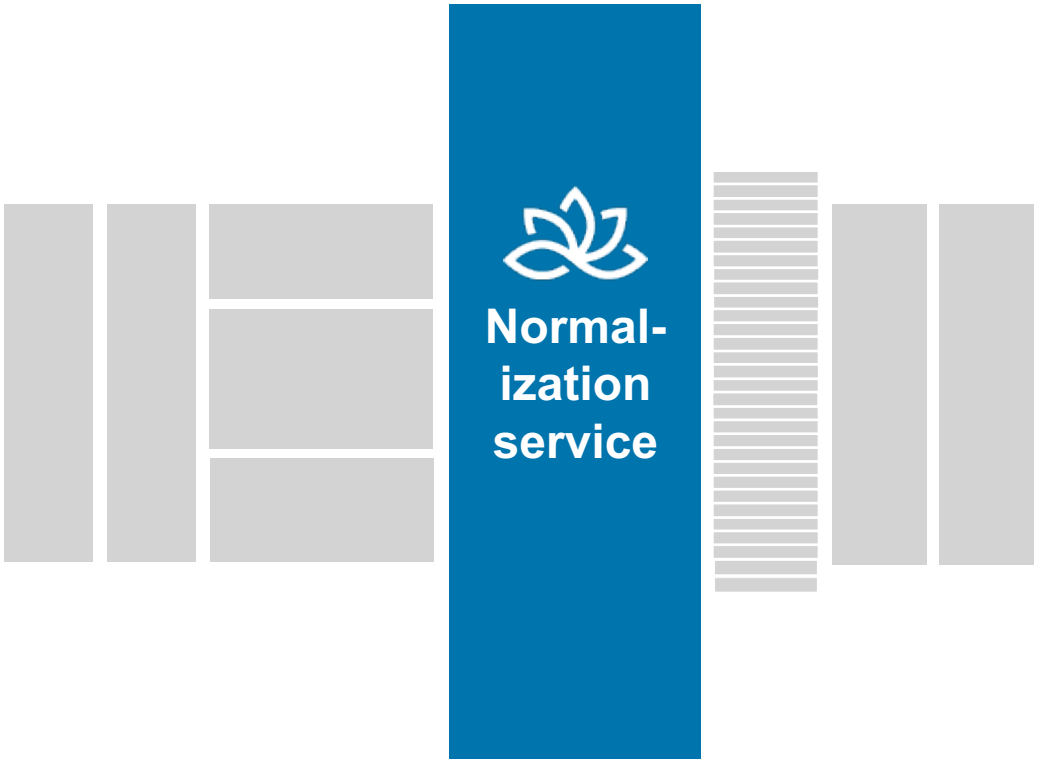



- Key requirements for these tools:
  - — Published APIs for integration
  - — Use common industry standards in their field (e.g. SCAP, OAuth, STIX, SARIF, OCSF)
  - — Localised information sharing between tools
  - — Architected to provide defense-in-depth compensating controls




Gartner®

# Normalization Service

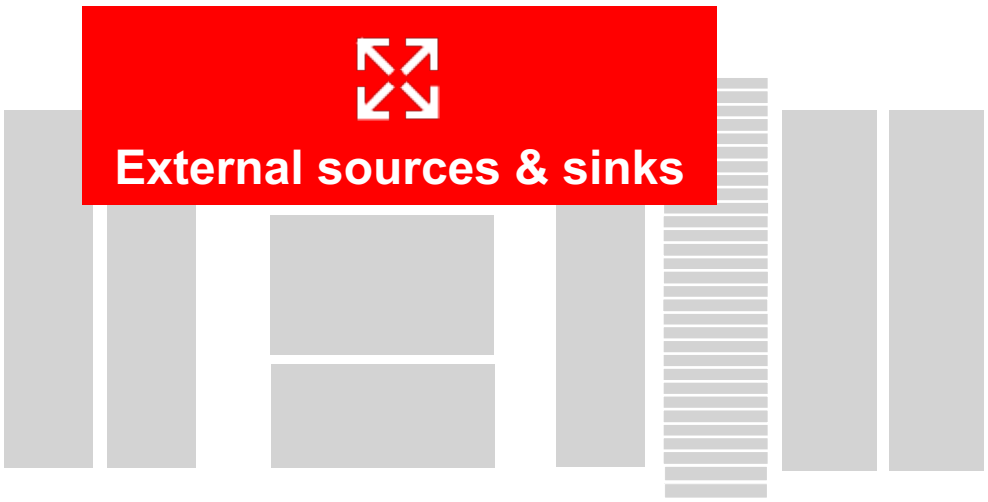



- Normalization translates all feeds from security tooling and external sources into the same format for data analytics.
- Select new schema frameworks like Open Cybersecurity Schema Framework (OCSF) or Elastic Common Schema (ECS)
- Seek to normalize locally by tools and pass data directly to data stores but create a central normalization service for all others.




Gartner®

# External Sources and Sinks




- Identify key enrichment sources to directly enhance data analytics.
- Select feeds that will augment insights from your security tools:
  - — Identify new IT vulnerabilities and pattern vulnerabilities
  - — Identify attack paths
  - — Define possible attack mechanisms that sensor data can be mapped to.
  - — Identify non-security feeds that could help risk scoring with context (e.g., news, social media feeds)

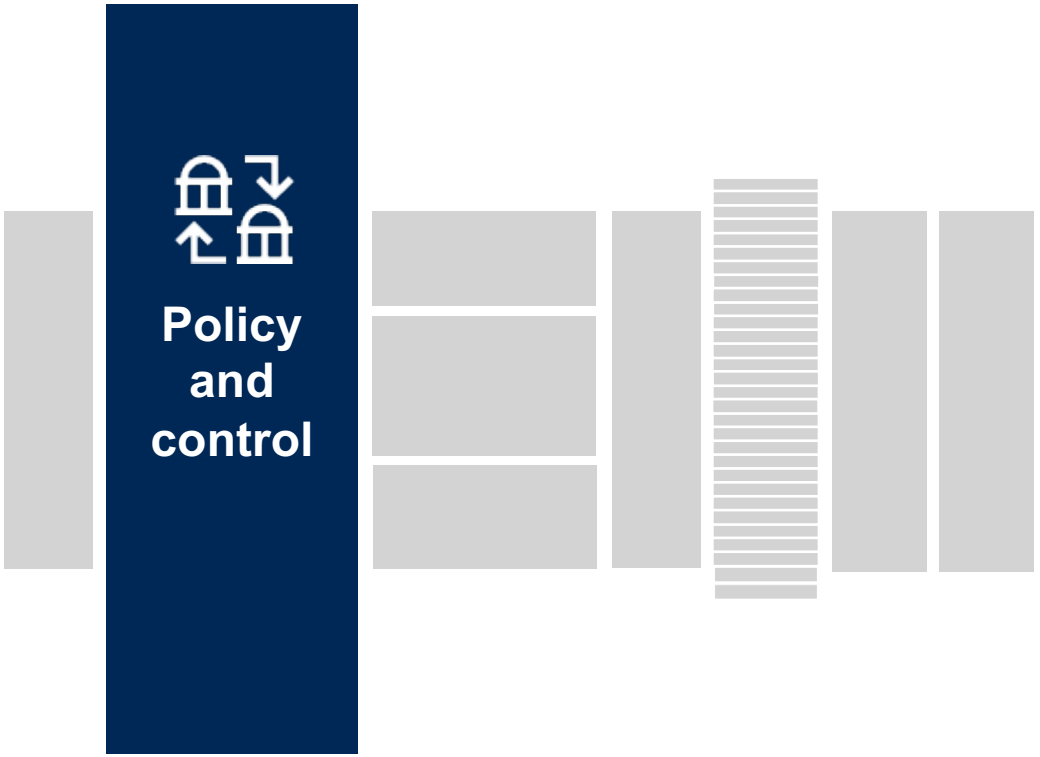



Gartner®

# Security Data Analytics and Intelligence


- Layered service model:
  - — Data analytics and AI/ML platform
  - — Data governance and processing
  - — Data lake
- Create a versatile platform to:
  - — Identify and map IT entities across enterprise
  - — Real-time risk modeling and scoring
  - — Perform what-if analysis
  - — Identify and predict malicious behaviors
  - — Assess security tool effectiveness

# Policy and Control




- Governance function to define what actions should be taken based on risks.
- Policy and control needs for actions:
  - — Ability to define technical policy and standards, then orchestrate it
  - — Assign business logic for boundaries based on risk appetite, risk acceptance and thresholds
  - — Posture assessment and mapping of IT assets and security tooling
  - — Running playbook of actions for the orchestration layer to perform.

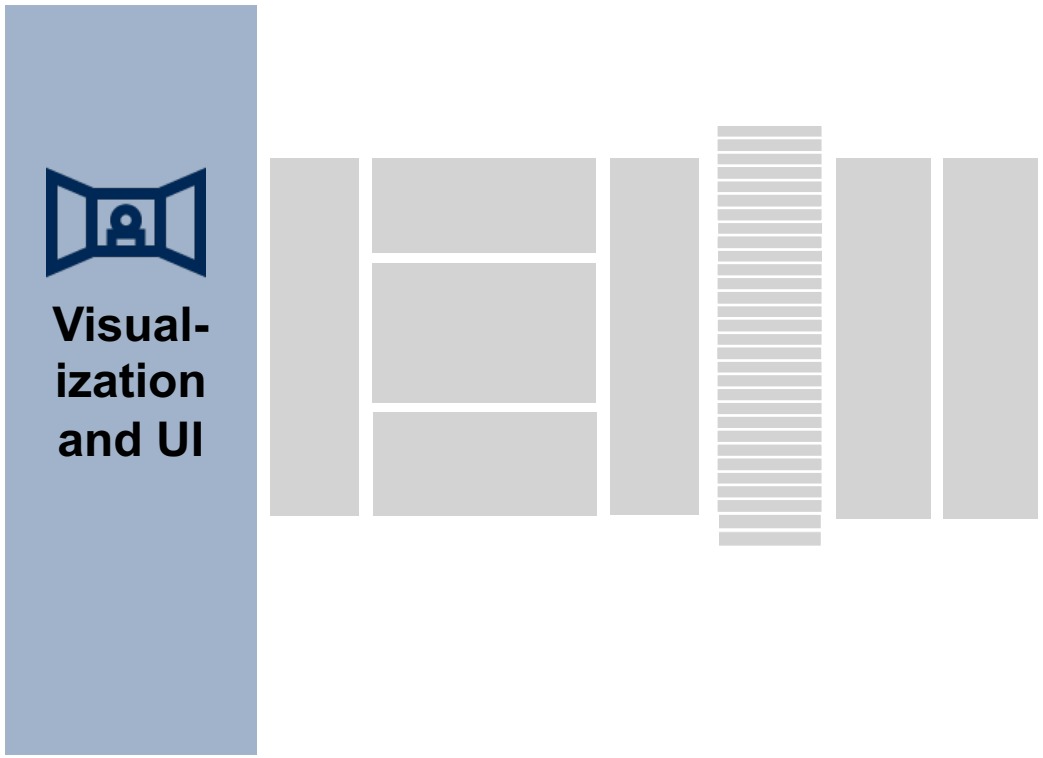



Gartner®

# Orchestration Functions


- Orchestration provides the output.
- Use two-way API integration with security tooling. Integrate directly with IT platforms (cloud management, Kubernetes, workload management tools).
- Survey and identify potential tool capabilities to directly act on IT.
- Select orchestration actions by identifying and prioritizing specific risks.

# Visualization and UI




- Identify user communities and design dashboards and UIs:
  - — SOC team need new ways including VR/AR/haptics to support risk identification as well as deep dive investigation and hunting
  - — Data security analytics team need UI for model construction, maintenance and risk scoring
  - — Leadership and risk functions need top-level UI visibility
  - — All need interactive ways to work and visualize data in real time

# Agenda

1. Limits of today’s security capabilities
2. New architectural principles
3. Pivoting with new requirements
4. Specifying new capabilities
5. Minimum viable architecture

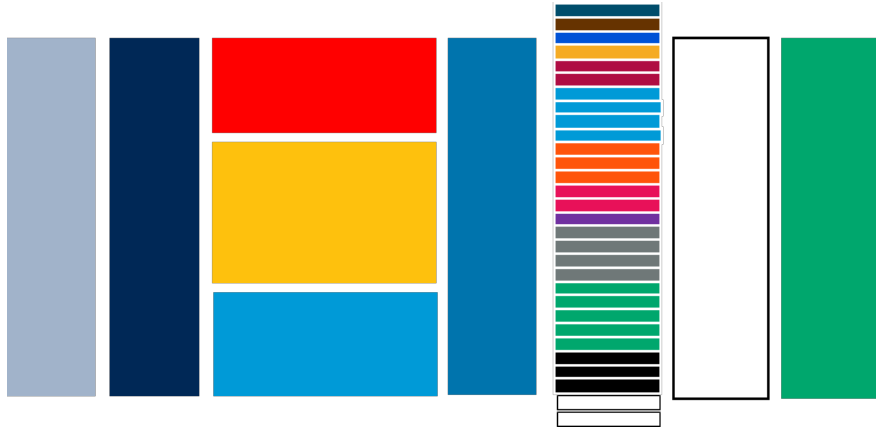



Gartner®

# Quickest Path to a Minimum Viable Architecture

1. Survey and use existing security feeds from your security tools

2. Implement a data lake to receive feeds (with normalization)



3. Acquire and implement attack path analysis tools

4. Engage AI/ML tools to support analysis and querying

## Then build out from here …




Gartner®

# Building out CSMA — options

## Approach 1: Build your own

- Define specifications for CSMA requirements
- Identify a minimum set of security tool and IT integrations
- Define risk models for the analytics team to construct
- Define UI needs for stakeholders

Selection considerations:

- Skills: data analytics team, integration, UI, governance and technical policy, security risk, IAM
- Cost of build/ownership

## Approach 2: Vendor integration

- Map requirements to vendor capabilities
- Identify security tools that are supported
- Compare vendor roadmap to your planned needs
- Seek out vendors with open interfaces for third-party integration

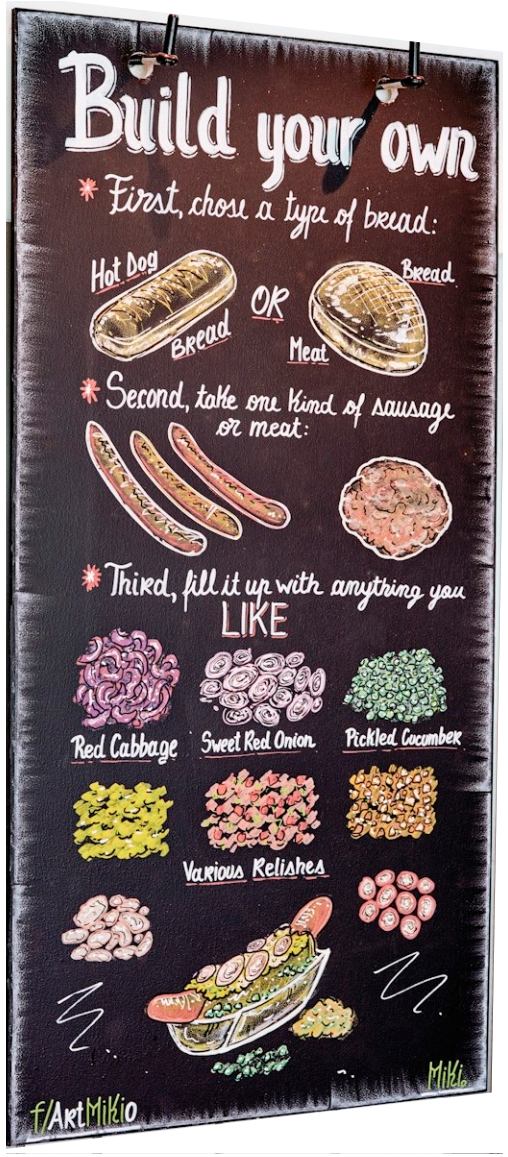
Selection Considerations:

- Offered capabilities vs. requirements
- MSSP approach?
- Significant blind spots and gaps?




Gartner®

# Build Your Own Cybersecurity Mesh Architecture




- Your existing IT and security tools are the foundation
- Modernize your IAM capabilities
- Build a data analytics platform with normalization ingress capabilities, integrate compatible security tooling and IT functions.
- Choose external security feeds for augmentation
- Define technical policy to handle risk mitigation actions
- Build outbound integrations with security tooling and IT functions



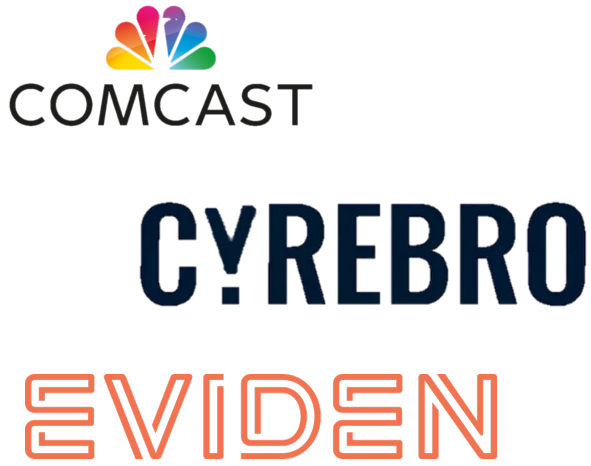

Gartner®

# Start With a Vendor Integrated Solution

## Building Blocks


## Vendor Platform


## Managed Service







Gartner

# Recommendations

- Anticipate your CSMA by selecting point security tools which have good integration and use of open standards for data sharing.
- Define clear requirements for each CSMA area.
- Decide whether to build this yourself or work with a small number of vendors or MSSP.
- Skill-up! Either way you will need security analytics expertise as well as upskilling your current security operations team to take full advantage of CSMA.

# Cybersecurity Mesh Architecture (CSMA) V3.0

## Operations

### Work bench

100 Overall risk

AR/VR Mesh Visualization of Entities Risks

Generative AI Interface

Predictions of attack

SOC Team

### Situational Awareness

Centralized operations Dashboard

Centralized Alerting

Centralized investigation

Centralized reporting

Businesss, executive and board context

Business Teams

## Policy, posture, & playbook management

**Policy management**

- Security policy standards, i.e., zero trust, ISO, CIS, CSA, NIST, etc.
- Policy settings management

**Posture management**

- Posture standards
- Config/policy drift management

**Playbook management**

- Playbook creation
- Playbook registration
- Action repository
- Business logic rules
- Automated response

### Business logic rules

- Business boundaries
- Business risk acceptance
- Thresholds requiring action
- Models to map security to business
- Business impact Quantification (business priority, financial)
- Addressing cyber liability

### Automated Response

- Pen tests, AST, DAST, SAST
- Realtime scanning
- Honey pots
- Deception tools
- Security awareness training
- Cyber resiliency service
- Software updates
- Security tool replacement
- Scripts
- Configuration changes
- Infrastructure configuration
- Resets based upon version
- Forensic investigation

## Predictive Sentiment Monitoring

- Dark Web
- Brand Reputation
- Social Media
- Activism

## External Feeds

- Finance/Fraud
- News
- HR
- Travel
- Help Desk

## External Threat Intelligence

- CSV/Vulns
- Attack Chains
- MITRE
- Anonymized CSMA
- Security Threat Feeds

## Security Intelligence

Real time Entity & Risk scoring/dynamic context

100 Overall Risk

Analytics aggregation

AI Safety

Machine Learning & Generative AI

Environment Risk Models

Zone Defense

Third-Party Risk Models

Security Product Performance Reliability

Infrastructure Version Control

What if scenario modeling (Probability)

Behavioral Patterns

Anomalies IOCs, Incidents

Product register

Historical records

### Exposure Management Tool box

- Attack surface measurement
- Attack chain mapping
- Asset inventory
- Vulnerability measurement modeling
- Red vs. blue team
- War gaming
- Breach and attack simulation
- Control/monitor/response validation
- Chaos engineering

## Adversarial Intelligence

Sandboxed ongoing Hacker AI generating Attacks

Machine Learning & Generative Malicious AI

Attack Chains, Darkweb Threats, Security Threat Feeds

## Integration/Standards/API Integration

Intel Feeds

Behavior

Incidents

Registration

Inventory

Asset -> Entity

## Protection product analytics/Information sharing

### Point Products CSMA Aligned (Subscriber/Contributor)

- SIEM
- XDR
- PACS
- SCRM
- PKI/Secrets/HSM/KMS
- LI
- WAAP
- MAST/SAST/DAST/ASPM
- ZTNA
- SWG/EFW
- DDoS
- NDR
- DLP
- Data classification
- DSP
- SEG/MTD
- Email security
- CPSPP
- UEM/UES
- EPP
- EDR
- MTD
- EAM
- PAM/AM
- IGA
- UEBA
- ITDR
- CASB/SSPM/SSE
- CWPP/CSPM
- CNAPP

## Entity/Assets

- Physical
- Supply chain
- Cryptography
- Location
- Applications/API
- Network
- Data
- Messaging
- IOT/OT
- Server/VM/Container/ Serverless
- PC/Laptop
- Mobile/Tablet
- Operating Systems
- Users/entities
- Cloud

## Infrastructure Management

Asset Inventory and Tagging

Systems/ Config/Patch Management

Dev/Test/ Preprod/ Production Management

Development Pipeline

## Identity Fabric

- Users
- Authentication
- Devices with proximity
- Location
- Date & Time
- Other contextual attributes and signals
- BYO

- Identity storage
- Identity onboarding
- Policy enforcement
- Encryption & trust
- Identity governance and life cyle
- Discovery & ownership
- Continuous session management
- Directory services
- Real time adaptive access
- Entitlements management

## Discovery, Orchestration & Automation