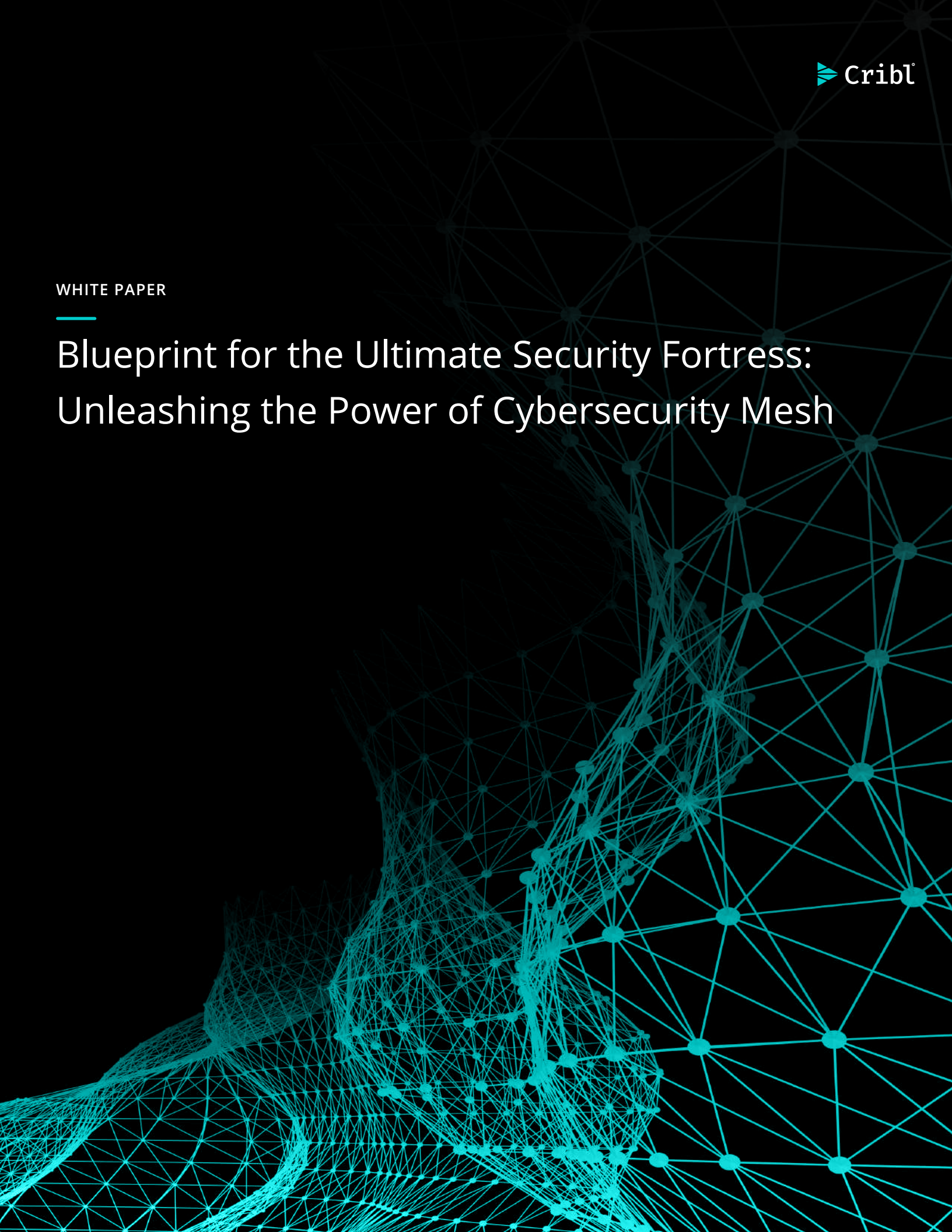
Cribl

WHITE PAPER

Blueprint for the Ultimate Security Fortress: Unleashing the Power of Cybersecurity Mesh



Blueprint for the Ultimate Security Fortress: Unleashing the Power of Cybersecurity Mesh

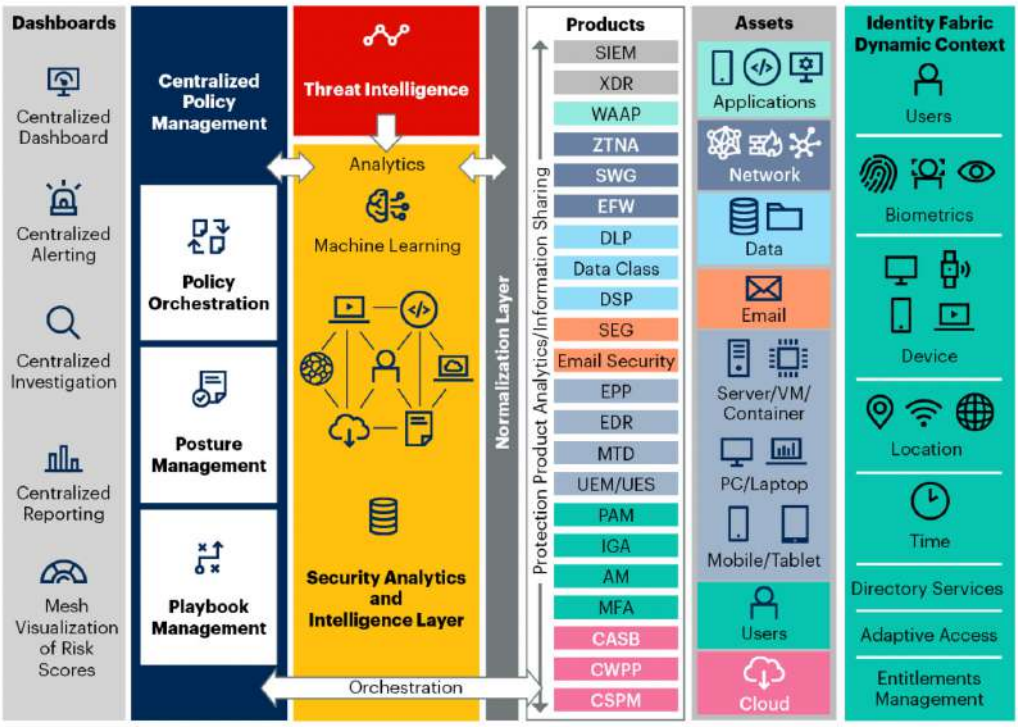
Cybersecurity Mesh Architecture (CSMA) is a concept that aims to transform isolated security data silos into a cohesive ecosystem of tools and controls to protect the modern enterprise. The strategy focuses on integrating various security tools by consolidating data sources and using high-quality enrichment and data normalization to enable more effective collaboration and correlation.

Implementing a CSMA offers several benefits, including:

- *Enhanced detection capabilities through complete access to data;*
- *Increased response efficiency through access to higher-quality data;*
- *Consistent management of policies, postures, and playbooks; and*
- *Adaptive, granular access controls*

Collectively, these improvements bolster security within modern enterprises, where computing resources are widely distributed, yet security tools often remain isolated and disconnected. The conceptual architecture of the CSMA is represented in Figure 1 below sourced from a 2022 Gartner® report titled – The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA).

Cybersecurity Mesh Architecture Reference



Source: Gartner
Note: Products included in the diagram are not all of the products that can be included but an example list of possible tools that protect assets
754315_C

Core Components of CSMA

Cybersecurity mesh is well-suited for contemporary computing environments, emphasizing scalability, interoperability, and composability. The four core components of CSMA include:

- *Security analytics and intelligence*
- *Distributed identity fabric*
- *Unified policy and posture management*
- *Integrated dashboards*

These components enable various security controls to collaborate, each contributing distinct capabilities to the architecture.

SECURITY ANALYTICS & INTELLIGENCE

As businesses generate and accumulate vast quantities of data, managing the sources and their outputs presents increasing challenges for security teams. Solutions in this component collect, aggregate, and analyze telemetry and other security data, drawing information from numerous existing security tools. By employing security information and event management (SIEM), endpoint detection and response (EDR), network detection and response (NDR), and security orchestration, automation, and response (SOAR) solutions, this layer unifies telemetry from disparate tools. Subsequently, intelligence can be applied to the data, potential threats analyzed, and necessary threat responses triggered.

IDENTITY FABRIC

This component offers identity and access management services, which are crucial for implementing a zero-trust architecture (ZTA) and, consequently, a zero-trust security policy. Key capabilities within this layer include:

- ***Identity Lifecycle Management:*** *Automating and streamlining the management of user identities, access privileges, and activity monitoring for employees, contractors, and other stakeholders.*
- ***Externalized Authorization Management:*** *Separating policy management from the application lifecycle and delegating access control to an external decision point.*
- ***Identity Proofing:*** *Verifying user identity during account creation or upon detection of suspicious activity.*
- ***Adaptive Access:*** *Controlling user access to resources based on real-time factors such as location and device type.*
- ***Entitlement Management:*** *Granting, enforcing, and administering fine-grained access entitlements across various platforms, devices, network components, and applications.*

UNIFIED POLICY, POSTURE, AND PLAYBOOK MANAGEMENT

To manage and enforce consistent security policies across diverse and distributed environments, solutions in this component translate policies into context-specific rules and configuration settings. These tools may also manage and orchestrate playbooks and (in some cases) provide dynamic runtime authorization services.

INTEGRATED DASHBOARDS

Although many security solutions claim to offer a comprehensive view of the security ecosystem, it remains to be seen whether any have genuinely achieved this capability. This component consolidates information from various sources, enabling security teams to respond rapidly to security events. The ultimate goal of integrated dashboards is to reduce alert fatigue and enhance overall security operations by intelligently parsing and filtering data.

91% OF IT AND SECURITY TEAMS SURVEYED RELY ON THE SAME INFORMATION, DATA, AND TOOLS.
CRIBL: THE STATE OF SECURITY DATA MANAGEMENT 2022

Building a CSMA: Getting Started

The objective of constructing a CSMA is not to purchase a single solution encompassing all layers and capabilities. Instead, it outlines the layers necessary to ensure existing security solutions can integrate, forming a mesh that is more effective than its individual components. To initiate the development of a CSMA, follow these steps:

1. *Assess current tools to determine their alignment with CSMA principles to determine which tools have the flexibility required to meet future demands.*
2. *Streamline security platforms where feasible. For example, if multiple versions of a tool exist within a single category, it is more efficient to consolidate them before introducing integrations.*
3. *Ensure future security solution investments align with long-term CSMA objectives. Seek vendors with advanced APIs, integration capabilities within security partner networks, and compliance with modern security standards.*
4. *Allocate more resources to independent security analytics technologies to optimize existing tools, gain control of data, and manage costs effectively. Aim to evaluate solutions that apply data and analytics principles to security information.*

Advantages of Integrating Various Security Tools

Historically, security architecture approaches assumed IT and security teams maintained physical control over the majority of an organization's assets. Today, digital assets are dispersed across numerous locations, vendors, and providers, both on-premises and in multiple clouds. As modern enterprise becomes more distributed, security must be treated as a collaborative ecosystem. Integrating various security tools, information, and storage allows organizations to select solutions tailored to their unique needs. This strategy is more often more effective than attempting to make a single-vendor solution, which may not offer the scope or scale of tooling necessary for future innovation.

ENHANCED VISIBILITY AND COVERAGE

Insights vary from one tool to another based on factors like its programming language, logging capabilities, and whether it uses open-source or proprietary code. Similarly, some tools excel at defending against specific threats, while others offer more general protection. Organizations that want to adopt a cohesive cybersecurity strategy can start by integrating these disparate security tools. This enables security teams to utilize a single management console to view and respond to alerts from all sources rather than managing multiple tools with separate interfaces and reporting systems. It also helps to eliminate potential blind spots by providing a comprehensive overview of enterprise security coverage.

ADAPTABILITY TO A CHANGING THREAT LANDSCAPE

Security tools are typically purpose-built for the detection of specific types of threats. Firewalls, for example, block traffic from known malicious IP addresses, but intrusion detection systems detect unusual patterns within the network traffic. By integrating these tools, organizations can develop an architecture that rapidly identifies and adapts to an ever-evolving threat landscape—leveraging multiple sources of data grants security teams access to more robust and complete incident information, accelerating incident response, root cause identification, and appropriate action. This adaptability increases the likelihood of preventing, detecting, and stopping threats before they cause serious damage.

92% OF SECURITY PROFESSIONALS CITED THE ABILITY TO COLLECT, ANALYZE, AND ROUTE DATA AS DIRECTLY IMPACTING THEIR WORK. CRIBL: THE STATE OF SECURITY DATA MANAGEMENT 2022

REDUNDANCY FOR IMPROVED RELIABILITY

In addition to providing enhanced visibility, an effective architecture ensures visibility into the infrastructure overlaps, providing multiple sources for each critical data point. This way, if one tool fails to identify an issue, another detects it. This enhances the overall effectiveness of the security mesh and provides necessary redundancy for critical operations. Finally, the security mesh approach permits the addition of solutions that fulfill specific security requirements, improving overall reliability and the ability to respond quickly to emerging threats with the latest tooling (provided the tools satisfy the CSMA interoperability prerequisites). This adaptability prevents the accumulation of technical debt by allowing security architecture to be updated in stages.

EMPHASIZING INTEROPERABILITY

For CSMA to be effective, its principles must be applied to all unique digital assets within an organization. This provides critical visibility as enterprises move towards ZTA and must verify not only that users are authenticated, but also authorized for access to each service. As a best practice, opt for applications that support interoperability, with new applications adhering to standards that facilitate seamless integration with security and identity tools.

CSMA benefits from extending existing standards, adopting emerging ones, and incorporating new standards:

- *Existing standards: JSON Web Tokens (JWT), FIDO2, SAML 2.0, OAuth 2.0, OpenID Connect (OIDC), SCIM 2.0, and RADIUS.*
- *Early adoption standards: Open Policy Agent (OPA) and Secure Production Identity Framework for Everyone (SPIFFE).*
- *Emerging standards: Continuous access evaluation protocol (CAEP), which is defined by the OpenID Shared Signals and Events Working Group, and Demonstration of Proof-of-Possession (DPoP), which uses sender-constrained tokens to fight token theft and reuse.*

CREATING COHESIVE DATA SOURCES

Ensuring the sources of data within an organization can work together is vital to successful CSMA implementation. The number and type of data sources in modern security are vast and growing. They include telemetry, endpoint, network, firewall, data lake, object store, and many others. To collect these data streams, most organizations utilize multiple monitoring tools with dedicated agents, which can create information silos and blind spots. Integrating and leveraging data and intelligence from various sources enhances overall security.

Increased visibility and control over data offer significant security improvements, represented in Figure 2:

Figure 2 Survey results.

BY 2024, ORGANIZATIONS THAT ADOPT A CYBERSECURITY MESH ARCHITECTURE TO INTEGRATE SECURITY TOOLS, SO THAT THEY WORK TOGETHER AS AN ECOSYSTEM, WILL REDUCE THE FINANCIAL IMPACT OF INDIVIDUAL SECURITY INCIDENTS BY 90%, ON AVERAGE.

GARTNER: HOW TO START BUILDING A CYBERSECURITY MESH ARCHITECTURE

MAKE SMARTER SOFTWARE PURCHASES

When making buying decisions, focus on integration and interoperability. Rapid technological advancements mean use cases and security tools emerge quickly, but may become obsolete just as fast. Attackers also leverage advanced technology, resulting in rapidly evolving tactics. Organizations must develop a flexible security architecture capable of keeping pace with this evolution by investing in infrastructure that is adaptable and capable of integrating with the security ecosystem of today, as well as tomorrow.

UTILIZE TOOLS FOR INTEROPERABILITY

In cases where interoperability isn't natively supported, tooling can help bridge the gaps in a CSMA. Software capable of collecting, routing, transforming, and enriching data can help overcome challenges associated with siloed or malformatted data. This capability is essential for organizations with existing infrastructure that need to create a systemized plan for modernization.

Best Practices for Building an Adaptable CSMA

As an emerging area, cybersecurity mesh architecture will undoubtedly mature and evolve over the coming years. Developing the four layers of a CSMA facilitates a mesh of security controls across technological environments, centralizing configuration and management (see Figure 3). These layers enable enhanced detection, more adaptive and granular access control, greater policy and management consistency, and more efficient incident responses. Emerging specifications and standards can be leveraged by conducting an asset protection inventory and assessing existing security tools based on their integration capabilities, real-time risk scoring, and advanced analytics.

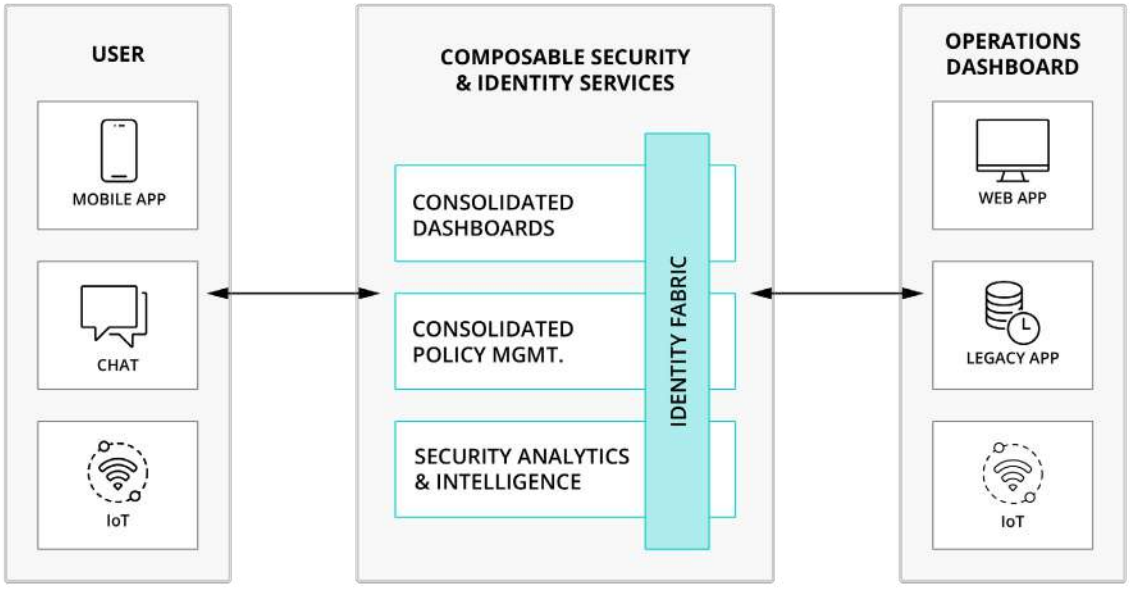


Figure 2 Composable Security and Identity Services

CRIBL'S STATE OF SECURITY DATA MANAGEMENT 2022 REPORT SUGGESTS THAT MOST ORGANIZATIONS' DATA MANAGEMENT STRATEGIES ARE NOT SUSTAINABLE LONG-TERM DUE TO THE LARGE VOLUMES OF INGESTED DATA AND NUMEROUS TOOLS FOR DATA VISIBILITY AND CONTROL.

FREQUENT TESTING AND COMPREHENSIVE MONITORING, INTELLIGENCE, AND ANALYTICS

Security and identity tools are increasingly powered by machine learning and artificial intelligence to identify risks and alleviate the burden on security teams facing relentless attacks. Regularly evaluating the organization's cybersecurity mesh architecture ensures alignment with security goals and helps pinpoint areas needing tool additions, integration updates, or new data sources.

Monitoring and observability are crucial for understanding an organization's environment. Monitoring ingests well-known data to answer specific questions, while observability discovers and comprehends application and infrastructure behavior based on generated data. The vast amounts of data organizations produce, collect, and store present challenges as data is delivered to diverse destinations, including time-series databases, logging analytics platforms, SEIMs, and APM systems.

Each destination requires unique data formatting and optimization, which may only be valuable in certain destinations or based on other signals. By removing data from silos and creating a centralized pipeline encompassing all observability data processing, teams gain greater data control, analysis capabilities, and intelligence application. A centralized observability pipeline allows data filtering, enrichment with additional context, sensitive data redaction, routing data from a single source to multiple destinations, and leveraging low-cost storage for full-fidelity data accessible when needed.

CSMA Enhances Security Through Adaptability

Cybersecurity mesh architectures present a potent new framework for developing a strong and flexible security infrastructure, one which is vital in today's highly distributed settings. Contemporary technology stacks depend on extensively distributed technologies and are unmanageable and challenging to monitor effectively, using traditional tools that divide data and environments into separate silos. Siloed security solutions have limited orchestration capabilities, impeding their ability to detect anomalies. In an exceptionally complex and distributed infrastructure, a CSMA offers increased visibility and coverage by:

- *Unifying security analytics and intelligence within a single layer*
- *Establishing a single identity fabric for enterprise-wide utilization*
- *Consolidating policy, posture, and playbook management*
- *Generating unified dashboards, enabling security teams to have comprehensive visibility across their ecosystem*

As the industry continues refining and setting standards, CSMAs provide the necessary adaptability for organizations to establish a robust, integrated, and interoperable system tailored to each organization's unique needs. Moreover, it fosters ongoing innovation by incorporating the ability to integrate new tooling and solutions into the security mesh at any given time, providing critical flexibility in a rapidly evolving world.

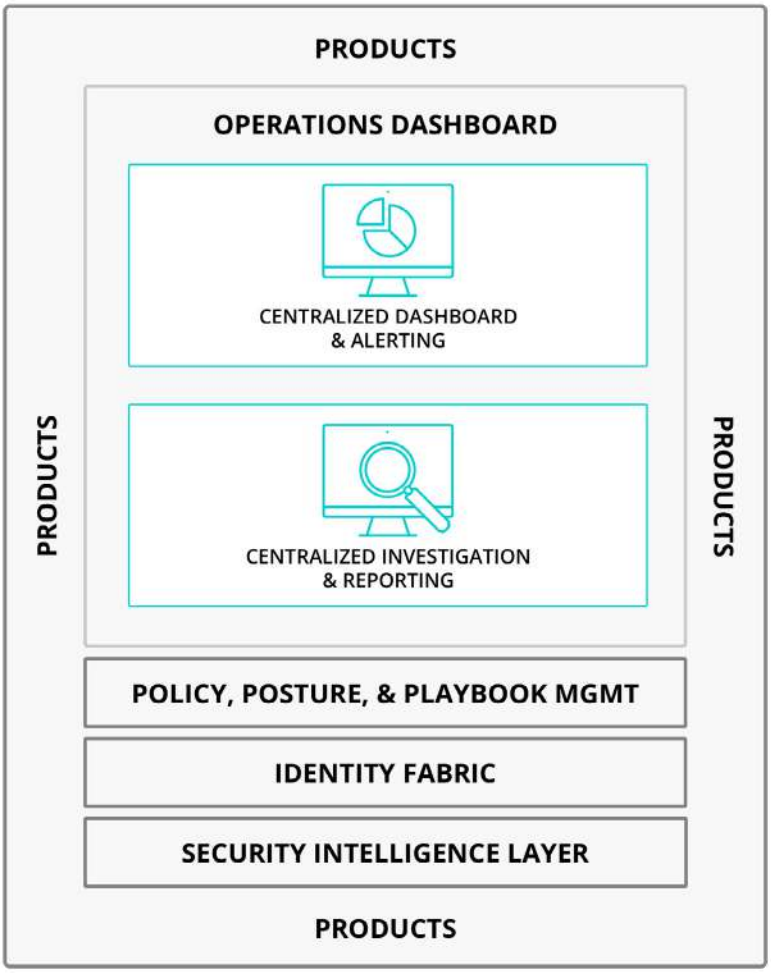


Figure 4 The Cybersecurity Mesh Architecture

ABOUT CRIBL

Cribl makes open observability a reality for today's tech professionals. The Cribl product suite defies data gravity with radical levels of choice and control. Wherever the data comes from, wherever it needs to go, Cribl delivers the freedom and flexibility to make choices, not compromises. It's enterprise software that doesn't suck, enables tech professionals to do what they need to do, and gives them the ability to say "Yes." With Cribl, companies have the power to control their data, get more out of existing investments, and shape the observability future.Founded in 2018, Cribl is a remote-first company with an office in San Francisco, CA. For more information, visit **www.cribl.io** or our **LinkedIn**, **Twitter**, or **Slack** community.