

Top Strategic Technology Trends for 2022: Cybersecurity Mesh

The rapid evolution and sophistication of cyberattacks and the migration of assets to the hybrid multi-cloud creates a perfect storm. IT leaders must integrate security tools into a cooperative ecosystem using a composable and scalable cybersecurity mesh architecture approach.

Overview

Opportunities

- 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.

Recommendations

IT leaders with a focus on [security](#) and identity and access management:

- Combat the increase in security complexity by evolving your security infrastructure to be more integrated, focusing on centralized administration and decentralized policy enforcement.
- Position the enterprise for a secure future by choosing cybersecurity technologies that ease integration via plug-in APIs that allow extensions and customization, standards support, and extensible analytics.

- Close interoperability gaps between different vendors' solutions by using current and emerging security standards.
- Deploy supportive layers for a long-term CSMA strategy by choosing a primary-vendor-led approach and filling capability gaps, or by using a best-of-breed approach from the start. Make the most of CSMA's supportive layers: security analytics, identity fabric, policy management and integrated dashboards.

Strategic Planning Assumption

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%.

What You Need to Know

This research is part of Gartner's [Top Strategic Technology Trends for 2022](#).

[Download the Executive Guide to Cybersecurity Mesh](#)

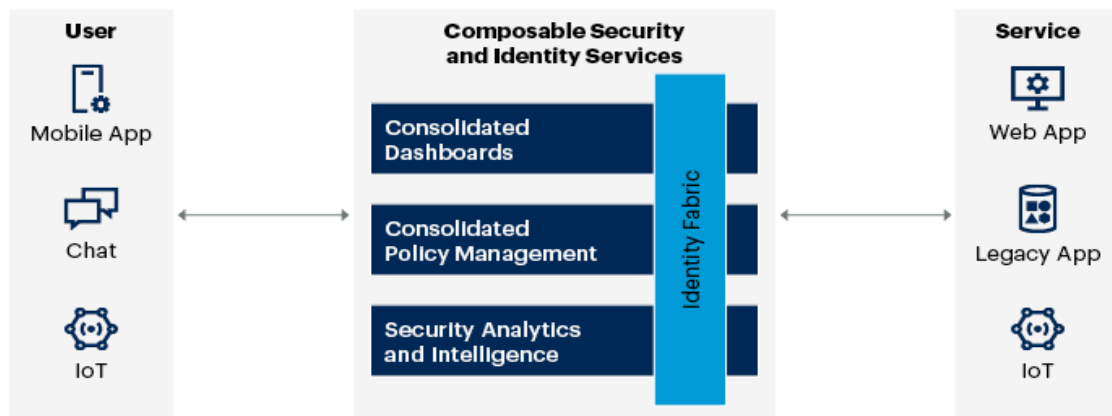
The cybersecurity mesh trend integrates security controls into, and extends them to span, even widely distributed assets. It addresses three realities affecting enterprise security:

- Attackers don't think in silos, but organizations often deploy siloed security controls.
- The perimeter has become more fragmented.
- Many organizations are adopting a multi-cloud strategy and need a consolidated security approach.

Cybersecurity mesh provides several foundational layers to act as a force multiplier when integrating different security products (see Figure 1).

Figure 1: Cybersecurity Mesh Architecture

Cybersecurity Mesh Architecture



Source: Gartner
756665_C

Gartner

Attackers don't think in silos. Ransomware and other cybersecurity attacks feature in the news daily and provide a lucrative revenue stream, or the potential for sabotage, for malicious actors. Cybercrime (especially ransomware) has led to disruptions in the physical world, particularly when it has targeted critical infrastructure. This is what happened with the Colonial Pipeline, an oil pipeline in the U.S., in May 2021.¹

A proper defensive posture requires eliminating silos and inefficiencies, both from an organizational perspective as well as within technology. This is because hackers don't think in silos. However, many organizations do, and many security tools work within their own view of the world with minimal interoperability — or even awareness — of other tools. Hackers often engage in lateral movement that uses a weakness in one area to exploit an adjacent area.

But hope is on the horizon. Some security analytics and intelligence tools already use domain-specific information across distinct security technology domains to create connections between security controls. Additionally, security standards have risen to the challenge and support the "everything, anywhere" mechanism.² However, some features from these standards are not yet commonly in use.

The perimeter has become more fragmented. Many applications and data are no longer in the company-owned data center, and users are accessing cloud-based applications from anywhere. In a traditional data center, network perimeter security was a common mechanism for controlling access. Within a distributed environment

that supports assets everywhere and access from anywhere, identity and context have become the ultimate control surface.

Many organizations are adopting a multi-cloud strategy. According to several studies,³ organizations tend to consume services from more than one cloud provider. With every cloud provider supporting a different set of policies, creating a consistent security posture across cloud providers is challenging. The huge on-premises estate of services found in most organizations only compounds the challenges. However, emerging standards and products are closing this gap.⁴

Profile: Cybersecurity Mesh

Description

Cybersecurity mesh architecture is a composable and scalable approach to extending security controls, even to widely distributed assets. Its flexibility is especially suitable for increasingly modular approaches consistent with hybrid multi-cloud architectures. CSMA enables a more composable, flexible and resilient security ecosystem. Rather than every security tool running in a silo, a cybersecurity mesh enables tools to interoperate through several supportive layers, such as consolidated policy management, security intelligence and identity fabric.

CSMA presents a collaborative approach for distributed security services to provide a force multiplier to gain a more cohesive security posture with fewer resources.

CSMA provides the foundation for people and machines to connect securely from multiple locations across hybrid and multicloud environments, channels, and diverse generations of applications, protecting all the organization's digital assets. By doing so, it fosters a more consistent security posture to support increased agility for the composable enterprise.⁵ CSMA allows security tools to integrate by providing a set of enabling services, such as a distributed identity fabric, security analytics, intelligence, automation and triggers, as well as centralized policy management and orchestration.

CSMA purposefully fosters composability, scalability and interoperability for security controls. It provides four foundational layers to enable distinct security controls to work together in a collaborative manner and facilitate their configuration and management. The four layers are:

- Security analytics and intelligence: Combines data and lessons from other security tools, and provides analyses of threats and triggers appropriate responses
- Distributed identity fabric: Provides capabilities such as directory services, adaptive access, decentralized identity management, identity proofing and entitlement management
- Consolidated policy and posture management: Can translate a central policy into the native configuration constructs of individual security tools or, as a more advanced alternative, provide dynamic runtime authorization services
- Consolidated dashboards: Offers a composite view into the security ecosystem, enabling security teams to respond more quickly and more effectively to security events

Why Trending

Existing approaches to identity and security architectures are not sufficient to meet today's rapidly changing demands. CSMA helps provide a common, integrated security structure and posture to secure all assets, whether they're on-premises, in data centers or in the cloud. CSMA enables stand-alone solutions to work together in complementary ways to improve overall security posture by standardizing the way the tools interconnect. For example, it centralizes policy management and helps move control points closer to the assets they are designed to protect.

Users, devices, applications and data have left the traditional office and data center. This means that a single network perimeter no longer exists to judge that "inside is good and outside is bad." Identity and context have become the ultimate control plane in a distributed environment that supports assets and access from everywhere. CSMA's distributed identity fabric provides trusted access by our workforce, clients, business partners and things.

Implications

Today's distributed and rapidly growing digital landscape makes complex demands requiring a new approach to security architecture. Existing architectural approaches are overly fragmented. This increases security risk and operational overhead, especially in an environment in which making good risk decisions requires orchestrating a growing number of risk signals. Adopting CSMA will lead to improved usability for both administrators and end users.

For example, today's security and identity deployments consist of multiple tools that often are not fully integrated (for example, they might be only loosely coupled by supporting federated authentication). In other cases, multiple tools may duplicate supporting functions.⁶ Operating these tools requires many separate dashboards, multiple policy administration points and maintaining many ad hoc integrations. This problem is exacerbated when new security or identity needs surface and new categories of tools are invented. There are too many separate tools with too many separate dashboards.

The CSMA approach provides IT leaders with a model that enables them to:

- Reduce deployment times and security failures.
- Increase agility and resilience.
- Focus on higher-value endeavors.

Security Product Consolidation

Many IT leaders want to consolidate their security spending and reduce complexity. According to a 2020 Ponemon Institute report, organizations deploy more than 45 security solutions and technologies on average.⁷ IT leaders want fewer vendors, with each vendor providing more and better integrated capabilities.⁸ Ideally, the offerings of large security vendors would have comprehensive and well-integrated capabilities. Realistically, however, security vendors offer some integrated capabilities at different stages of maturity and completeness. IT leaders must fill existing and emerging gaps with other security point products.

Several large ecosystem vendors (such as IBM, McAfee, Microsoft and Symantec) offer security stacks that include multiple integrated security controls that can secure traditional on-premises assets as well as cloud assets. In general, the positive outcomes from choosing a primary-vendor (not necessarily a single-vendor) approach are:

- Better integrated and centralized management interfaces and dashboards
- Consolidated (and often less expensive) licensing

However, no single vendor will have components (security controls) that are all best in class — some components will be better than others. Every [vendor](#) will have gaps in its offering that need to be filled with solutions from other vendors, or even open-source solutions. Few organizations can consolidate to a single security vendor, or

even a smaller set of security vendors.⁹ Integrating multiple security tools remains a necessity.

Integration can be achieved through a mix of open standards and interfaces, proprietary APIs, and point integrations (e.g., ad hoc integrations between vendors' tools). The offerings of some vendors can be a good starting point for building one or more supporting layers for a CSMA, and integrating further security controls in a composable manner. When gaps exist in open-standards support, or when security standards are emerging or evolving, open-source tools can be an easy way to get a head start with the latest features.

Cross-Domain Security Analytics Will Make a Real Difference

Most security analytics tools deployed are domain-specific, and organizations typically use multiple security analytics tools alongside each other, in a non-integrated manner. Several vendors now offer security tools that provide multiple analytics use cases from a single tool by using domain-specific information across different security domains, and even data from siloed analytics functions of security tools. For example, a security product may have its own native analytics engine that calculates a risk score for a particular session, user or transaction. A broader security analytics and intelligence tool could then use this risk score, applying it in a different context from that originally intended. Extended detection and response tools are one example of this trend.¹⁰

Users of these advanced technologies have tended to be organizations with a highly mature security operation, but this trend is becoming more mainstream. Gartner expects this will trickle down into smaller and less mature security organizations.

Multi-cloud

Distributed IT assets in the multicloud add to the fragmentation problem when securing assets. For example, Alibaba Cloud, Amazon Web Services (AWS), Google and Microsoft Azure use different methodologies to secure assets within their individual ecosystems. However, organizations seek to adopt a coherent security posture across the multicloud. In recent years, new technology has arisen to help with this challenge.⁴

Actions

- Prioritize composability and interoperability when selecting security solutions, and invest in building a common framework to integrate them for synergetic effects.




- Choose new tools that enable you to use standard core functions and that are designed to operate as part of a larger cybersecurity mesh, rather than another independent silo. Prioritize vendors that have opened up their policy framework, enabling policy decisions to be made outside the tool.
- Select vendors with a commitment to and track record of embracing new and emerging security and identity standards because standards compliance is becoming more important.
- Realign your organization’s security and identity vision with CSMA.
- Reprioritize your organization’s planning roadmap to use CSMA principles and connect existing projects that are now related. For example, move to a zero-trust architecture and improve multifactor authentication user experience with adaptive access.
- Transition from traditional VPNs to reliable, flexible and secure cloud-delivered, zero-trust network access integrated with an access management tool.

About Gartner’s Top Strategic Technology Trends for 2022

This trend is one of our [Top Strategic Technology Trends for 2022](#). The trends and technologies don’t exist in isolation; they reinforce one another to accelerate growth, sculpt change and engineer trust (see Figure 2). You should explore each of these trends for their applicability to your organization.

Figure 2: Top Strategic Technology Trends for 2022: Cybersecurity Mesh

Top Strategic Technology Trends for 2022: Cybersecurity Mesh

 Accelerating Growth	 Sculpting Change	 Engineering Trust
<ul style="list-style-type: none"> • Generative AI • Autonomic Systems • Total Experience • Distributed Enterprise 	<ul style="list-style-type: none"> • AI Engineering • Hyperautomation • Decision Intelligence • Composable Applications 	<ul style="list-style-type: none"> • Cloud-Native Platforms • Privacy-Enhancing Computation • Cybersecurity Mesh • Data Fabric

Source: Gartner
757234_C

Evidence

Gartner's 2020 Security and IAM Solution Adoption Trend Survey: Gartner conducted this study to learn what security solutions organizations are benefiting from and what factors affect their choice/preference for such solutions. We conducted the research online during March 2020 and April 2020 among 405 respondents from North America, Western Europe and the Asia/Pacific region. Companies from different industries were screened for having annual revenue of less than \$500 million.

Respondents were manager level or above (excluding the C-suite) and had primary involvement and responsibility in a risk management role for their organization. The study was developed collaboratively by Gartner analysts and Gartner's Research Data and Analytics team, which follow security and risk management.

Note: The results of this study do not represent global findings or the market as a whole, but reflect the sentiment of the respondents and companies surveyed.

¹ [Hackers Breached Colonial Pipeline Using Compromised Password](#), Bloomberg.

² New identity standards are emerging to support composable interoperability along new dimensions, including:

- Open Policy Agent (OPA) and IDQL for policy definition
- The OpenID Continuous Access Evaluation Profile (CAEP) of the Shared Signals and Events Framework for more consistent sharing of event signals

Additionally, adoption of security standards that foster integration between security tools, such as OpenDXL, is increasing.

³ McAfee's 2019 report [Cloud-Native: The Infrastructure-as-a-Service \(IaaS\) Adoption and Risk Report](#) contains a survey of more than 1,100 users. Of those, 76% are using multiple cloud providers. This is consistent with Gartner's 2020 Cloud End-User Buying Behavior Survey that found that just over three in four respondents from organizations that use cloud IaaS indicate that their organization works with multiple IaaS providers.

⁴ Several technologies contribute to security posture in the multicloud:

- Cloud-native application protection platforms (CNAPPs; see [Innovation Insight for Cloud-Native Application Protection Platforms](#))
- Cloud security posture management (CSPM; see [Cool Vendors in Cloud Security Posture Management](#))
- Cloud workload protection platforms (CWPPs; see [Market Guide for Cloud Workload Protection Platforms](#))

- Cloud infrastructure entitlement management (CIEM; see [Innovation Insight for Cloud Infrastructure Entitlement Management](#))

⁵ [Future of Applications: Delivering the Composable Enterprise](#).

⁶ According to Gartner's 2020 Security and IAM Solution Adoption Trends Survey, vendors' portfolios have overlapping products with a consolidation around key areas of endpoint security and network security.

⁷ [2020 Cyber Resilient Organization Report by Ponemon Institute](#), sponsored by IBM.

⁸ According to Gartner's 2020 Security and IAM Solution Adoption Trends Survey, companies have an appetite for platform vendors (Cisco, Microsoft, IBM) as they do well by offering several products under their suite.

⁹ According to Gartner's 2020 Security and IAM Solution Adoption Trends Survey, organizations pursuing a vendor consolidation strategy (that is, having fewer vendors for their security needs) have seen or expect a significant increase in information security staff and time spent on integration. Reduced spending from a vendor consolidation strategy has been a primary benefit for only 16% of organizations, while 23% said increased spending was a primary drawback. Half the organizations have seen no change in the number of security vendors, while most saw an increase in operating cost and time spent on integration.

¹⁰ [Innovation Insight for Extended Detection and Response](#).