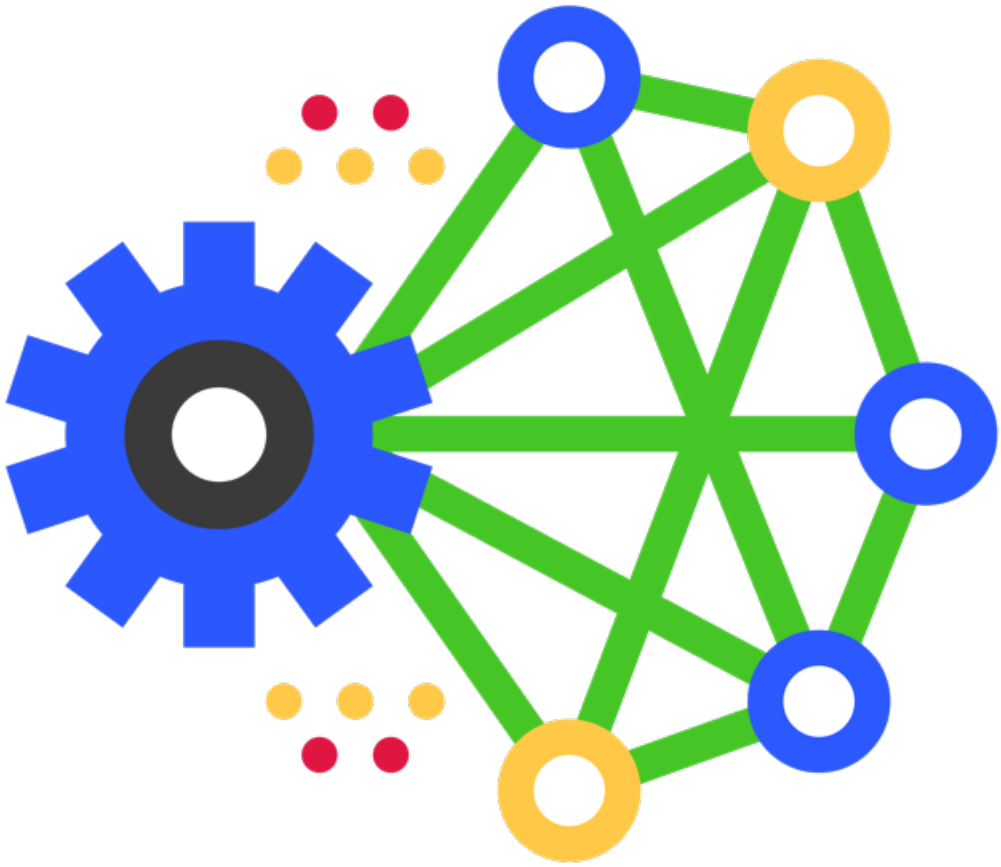
NETENRICH

The Netenrich Guide to Cybersecurity Mesh Architecture (CSMA)

Implementing an open architecture for security — and all digital operations



The Netenrich Guide to Cybersecurity Mesh Architecture (CSMA)

Implementing an open architecture for security — and all digital operations

The security industry is at a turning point. Infrastructures are becoming more and more complex because of an increase in remote workers and enterprise cloud workloads. Meanwhile, cyberattacks are ubiquitous, and data breaches are soaring.

According to Ponemon Institute and IBM's Cost of a Data Breach Report 2022, 83% of organizations experienced more than one data breach in 2021, and 45% of threats were cloud based. Worse, the average cost of a breach hit an all-time high of US$9.44 million in 2022, up 12.7% in just two years and with an average time of 277 days to identify and contain.

The status quo is unsustainable

Today's security tools and services, many of which are self-described "next-gen" versions of solutions developed decades ago, are not designed to address the enormous complexities, dynamism, and scale of current infrastructure and threat landscapes. The Cost of a Data Breach Report 2022 also found that the average midsize enterprise runs 45+ security tools — not including those for monitoring applications, the network, and cloud operations. Many of these tools are great at what they do, but they simply weren't developed with current use cases in mind.

Dynamic, complex environments and increasingly sophisticated, relentless threat actors are here to stay. Current approaches to cybersecurity aren't sufficient to address these issues.

Enter cybersecurity mesh architecture (CSMA)

Recognizing this need for change, research and advisory firm Gartner®, Inc. coined the term Cybersecurity Mesh Architecture, or CSMA, to describe a new approach, and estimates that by 2024, CSMA "will reduce the financial impact of individual security incidents by an average of 90%."[1]

What is CSMA?

According to Gartner report Top Strategic Technology Trends for 2022: Cybersecurity Mesh:

> 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 multicloud 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.[1]

[1]Gartner, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Felix Gaehtgens, James Hoover,et al., October 18, 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved

Figure 1: Cybersecurity Mesh Layers

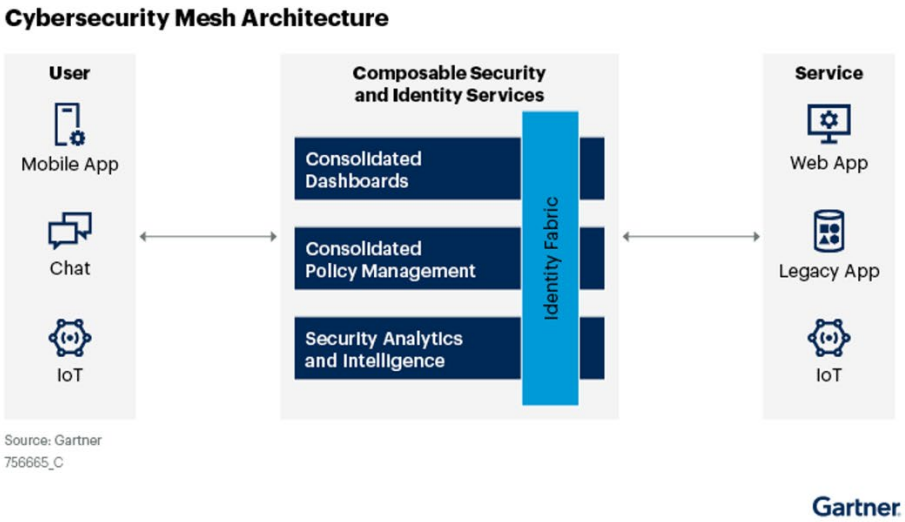


Figure 1: Source: Gartner, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Felix Gaehtgens, James, Hoover, et al., October 18, 2021.

At Netenrich, we developed Resolution Intelligence Cloud as an integral component of successful CSMA implementations. Highly scalable, with an open architecture that encompasses not only security but all digital operations, Resolution Intelligence Cloud is a cloud-native platform for managing secure operations: across security and digital operations, at scale.

CSMA creates opportunities to improve security

According to Gartner, CSMA creates several opportunities for organizations, including[2]:

1. It "provides a foundational support layer that enables distinct security services to work together to create a dynamic security environment."
2. It "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 multicloud environments."
3. It "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."

[2] Source: Gartner, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh", Felix Gaehtgens, James Hoover, et al…, October 18, 2021

4. “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.” [4]

Resolution Intelligence Cloud: At the Apex of CSMA

Here’s how Resolution Intelligence Cloud fulfills these opportunities (and more) for enterprises and service providers.

No security tool is an island.

CSMA addresses critical problems affecting enterprise security. According to a Gartner report, “Attackers don’t think in silos, but organizations often deploy siloed security controls.”[4]

Cybersecurity point products are at a stage of diminishing returns. As IT environments continue to grow beyond the network perimeter, and threats continue to increase in volume and success, you simply can’t manage security with siloed technologies. Threat actors thrive on finding gaps between the silos.

The new approach leverages today’s tools and new ones to come in an open architecture in which they work together, getting rid of the siloes and enabling a common operational view from which to manage and control security.

CSMA is not prescriptive, rather it’s a framework that helps organizations ensure they have the security coverage they need — with the tools they have, optionally augmented by others that fill gaps. This interoperable, open architecture “enables distinct security services to work together to create a dynamic security environment.” Organizations can thereby avoid inefficient duplication and, most importantly, close gaps that increase vulnerability.

Resolution Intelligence Cloud pulls together data from all of your security and digital ops telemetry tools — including those for hybrid-cloud and on-premises infrastructures — to establish a common operational picture. That’s a lot of data. Resolution Intelligence Cloud uses Google Chronicle as its security data lake to enable speed and search at Google scale. It then applies advanced data analytics, machine learning, and automation to proactively find and fix vulnerabilities and identify and respond to threats far faster.

Dynamic security environments require agility and scalability.

CSMA assumes complex and fast-changing infrastructure and security environments. You can’t buy new tools and hire enough people to manage them to cover everything — now or in the future — so you must be smart about your approach and assume a dynamic environment from the outset.

Dynamism requires scalability, which is critical for addressing three key concerns:

1. The growth and changing nature of attack surfaces.
2. The growth and sophistication of attacks.
3. The growth of your business.

Using security data analytics and machine learning, Resolution Intelligence Cloud correlates and contextualizes telemetry data at scale to detect patterns over time in data from all security sources. It automates responses, reduces noise, and identifies threats that are most risky to the business based on impact, likelihood, and confidence. In essence, it transforms findings into intelligence — related alerts, users, assets, etc. — that teams can act on before critical issues or business disruption occurs.

Collaboration is key to better, faster incident response.

Similar to how organizations have often deployed siloed security controls, they've also kept security operations centers (SOCs) siloed from the rest of digital operations. This longstanding division, where SOCs focus on detecting, investigating, and responding to threats while digital operations focus on meeting the daily operational needs of the business, is past its expiration date. It's time to break down these silos to avoid duplicated efforts (extra costs) and coverage gaps (extra vulnerabilities).

CSMA provides a cleaner, more collaborative approach that breaks down these siloes so teams can respond better and faster to incidents.

Resolution Intelligence Cloud can sit at the apex of CSMA — providing the common operational picture, analytics, insights, and resolution capabilities that security and operations teams need to work best together.

Resolution Intelligence Cloud applies data analytics, machine learning, and automation to reveal critical, risky situations from the flood of noisy alerts so your teams can collaborate on what matters most and take a more preventive approach to mitigating risk. Anticipating and responding to risky situations helps reduce negative business impact.

With Resolution Intelligence Cloud, security analysts can also instantly create "war rooms," where they can pull in the right experts and stakeholders — other SOC analysts, IT, heads of business units, and/or third parties — to share insights and discuss appropriate actions for a swift resolution to the most critical, confirmed issues.

Gain time to focus on high-value activities.

Another opportunity CSMA presents is freeing security analysts from low-level, repetitive tasks so they can focus on more important ones.

Resolution Intelligence Cloud does so in multiple ways:

- Boosts efficiency and effectiveness with automation plus the information and insights analysts need at their fingertips.
- Reduces alert noise, typically by 80-90% or more.
- Presents highly curated, contextual data — like related alerts, asset, and user data, saving investigation time, with details just a click away.
- Prioritizes risky situations and incidents based on a risk score aligned to the business, based on likelihood, impact, and confidence, so analysts focus on what matters most.

With this approach, organizations don't need to hire more information security experts or train junior staff to perform basic monitoring and triage tasks. For hybrid operations, where personnel may be

responsible for the entire ops gamut — NetOps, CloudOps, SecOps — there's also an opportunity to improve security proficiency.

Achieve operational excellence with convergence of security and digital operations teams.

The beauty of CSMA is that organizations can apply it to both their security *and* digital operations — in essence, transforming it into an *operational* mesh architecture and using that as a basis for secure operational excellence.

As described in Netenrich CEO Raju Chekuri's Dark Reading commentary Better Together: Why It's Time for Ops and Security to Converge, operations and security organizations share two main goals:

1. **Availability**: Ops teams ensure business systems and information are readily available to all who need access. Security teams ensure the right data is available to the right people at the right times on the right devices.
2. **Risk**: The operations view of managing risk focuses on keeping systems up and running, avoiding downtime and poor performance, and supporting business productivity and efficiency. Security organizations view risk in terms of avoiding data loss, manipulation, and damage to the business.

The most effective — and cost-effective — way to achieve these goals is by converging digital operations and security, enabling them to work together with a common operational picture, shared data, and the right tools that interoperate.

Ready to start your CSMA journey?

Fortunately, this smart and practical open architecture doesn't require an expensive, painful rip and replace. At Netenrich, we're here to help with Resolution Intelligence Cloud. Learn more about CSMA from this Gartner report, or request a demo or use-case session with one of our experts to chart your course of action.

About Netenrich

Netenrich boosts the effectiveness of organizations' security and digital operations so they can avoid disruption and manage risk. Its Resolution Intelligence Cloud is a native-cloud data analytics platform for enterprises and services providers that need highly scalable, multitenant security operations and/or digital operations management. The platform uses Google Chronicle as its scalable, fast security data lake. Resolution Intelligence Cloud transforms security and operations data into intelligence that organizations can act on before critical issues occur. More than 3,000 customers and managed service providers rely on Netenrich to deliver secure operations at scale.

NETENRICH
www.netenrich.com