Updated February 2025

The Journey to a Self-Protecting Network

The future belongs to networks that protect themselves

Contents

We've digitally transformed – what's next?

Over the past decade organizations have invested over $14 trillion[1] to digitally transform themselves. We have deployed many new technologies at scale to deliver competitive advantage by improving the customer experience and lowering costs. A key part of this transformation has been the rapid evolution of our security and networking infrastructure.

To support this evolution, the web became our network, as we moved our data and applications to the cloud. We successfully transformed branch connectivity with direct internet access. As remote and hybrid work took the world by storm, we enabled our employees to connect from anywhere in the world to anywhere in the cloud. And our network edge became a million devices.

We have arrived today at a point where our networks and security are fundamentally intertwined – networks are the lifeblood of our digital business, and we need to ensure they are secure and reliable. As we move forward into the next phase of transformation, we face both challenges and opportunities in how we evolve our network and security infrastructure to fix current constraints and meet future needs.

Today's security and network challenges

Our objective is clear: how can we capture the productivity and agility benefits that come with ongoing digital transformation without compromising security, resilience, or performance? Despite the advanced capabilities we've delivered in our network and security infrastructure, there is more work to do if we are to continue our progress in the face of the challenges described below.

Security is a race against time

Threat actors are leveraging automated tools and AI-driven techniques to target, accelerate, and scale their attacks. In contrast, organizations often rely on slow and manual processes for detecting and responding to security events, relying on a limited pool of human experts to address a wide array of threats. This dependence on human intervention means our defenses are often unable to keep pace with the advanced attacks we encounter today, leaving organizations vulnerable during critical moments. The following dynamics lie at the root of this situation:

Cyber threats are faster, stealthier, and more dangerous than ever before
The rapid evolution of cyber threats showcases a disturbing combination of increased speed and sophistication. Examples of recent threat advances include:

- **Internet-scale exploitation –** Mass internet scanning technology allows threat actors to remotely identify and attack newly discovered vulnerabilities and common misconfigurations in internet-facing hosts in less than five minutes.
- **Faster and better phishing –** Gen AI tools are making it ridiculously easy, cheap and fast to create highly convincing phishing emails that are harder to spot, and significantly more dangerous.
- **AI-powered attacks –** Attackers are using AI to automate the search for targets, identify key personnel within organizations, and craft personalized phishing messages with high accuracy, increasing the likelihood of successful deception.
- **Compromises harder to detect –** Sophisticated threat actors can often maintain a long-term presence in their target environments for months at a time, without being detected, allow them to spread within a digital environment and compromise more devices than ever before.

[1] Statista, "Spending on digital transformation technologies and services worldwide from 2017 to 2027," 2024

[2] "Gartner Forecasts Global Information Security Spending to Grow 15% in 2025," Gartner, August 28, 2024

We are getting breached more than ever, despite huge security investments

Our cyber attack surface has expanded dramatically over the past five years, now encompassing our cloud estate, millions of devices at the edge, and mobile and remote workers, in addition to our internet-facing infrastructure. Yet despite spending more than $180 billion this year on information security[2] to protect ourselves, we continue to experience record highs in terms of data breaches[3]. This leaves us with a number of challenges as we attempt to diagnose and correct this problem, including:

- ✓ **Bespoke security infrastructure –** Every CISO today is forced to create his or her own customized security fabric built out of a set of point products that need to be manually integrated and often do not communicate effectively with one another. This patchwork approach not only increases complexity and the potential for misconfigurations but also escalates costs without delivering the desired security outcomes.
- ✓ **Manual alert triage and response –** Manual elements of such processes can lead to delays in threat detection and mitigation, giving attackers more time to exploit vulnerabilities. In environments where automated attacks trigger alert storms, security teams become overwhelmed, struggling to prioritize genuine threats. The sheer volume and complexity of security data exacerbates the issue, making it difficult for analysts to differentiate between real threats and false positives. As they sift through excessive information, crucial context can be missed, leading to delayed responses or the misprioritization of threats.

Our networks are too complex and costly

Today's network infrastructure is becoming more complex and costly due to fragmented connectivity and the abundance of security and management tools, leading to increased operational costs for integration, monitoring, and maintenance. Specific challenges include:

- ✓ **Fragmented islands of connectivity –** Organizations now operate a mix of on-premises infrastructure, private and public cloud environments across their WAN, LAN, cloud, and data center networks. Added to this, many organizations are starting to connect IoT devices to their infrastructure as well. Each of these network segments has its own set of security risks, protocols, management tools, and performance metrics, leading to a highly fragmented network landscape.
- ✓ **Product sprawl –** A proliferation of point products that get “bolted on” to the infrastructure is another driver of networking and security complexity. On the security side, organizations often pursue a multi-layered “defense in depth” strategy, adding multiple specialized security point products into the network to address various threats. The problem exists equally on the networking side with bolt-on acceleration, observability, and other products. The challenge is that each of these products comes with its own unique management console, policy framework, data repository, and operating environment that must be managed and maintained. This complexity drives up operational costs, as organizations must invest in even more advanced tools, skilled personnel, and ongoing training to keep pace with evolving threats and network requirements.
- ✓ **Fragile networks –** Maintaining network resilience in the face of high complexity and single points of failure presents significant challenges for organizations today. As networks grow more intricate due to the integration of diverse technologies, cloud services, and IoT devices, identifying and troubleshooting bottlenecks, latency and outages has become increasingly difficult. This complexity can obscure potential single points of failure, where the malfunction of one component may lead to widespread disruptions. Additionally, recovery efforts can be hampered by the multitude of interconnected systems, making it challenging to pinpoint the source of an issue and implement timely fixes.

We have massive data, but limited insight

Our systems generate terabytes of logs, metrics, and alerts daily, capturing every nuance of network traffic, security events, and system performance. However, despite this wealth of information, our ability to analyze and derive meaningful conclusions is often limited. This disparity is a common challenge in today’s data-driven environment, where the sheer volume of data collected far exceeds our capacity to effectively interpret it, rooted in the following three problems:

[3] "2024 Data Breach Investigations Report," Verizon Business, 2024.

Fragmented data
Historically, extracting insights from fragmented and inconsistent security and networking data lakes has been challenging. The crux of the issue lies in the quality and cohesiveness of the data we gather. In our attempts to create a comprehensive view of our network and security posture, we often resort to cobbling together a cloud data lake that ingests telemetry from a myriad of disparate network and security point products. This approach results in a sparse matrix of information that, while extensive, loses its detail and value as the data is normalized.

Alert storms
Data overload can result in alert storms that overwhelm analysts and administrators. With terabytes of logs and metrics generated daily, the sheer volume of alerts can make it difficult for teams to prioritize and respond effectively. As a result, critical security threats or network inefficiencies may go unnoticed, while the constant flood of notifications and false positives leads to alert fatigue. This further complicates their ability to maintain an accurate, real-time view of network health and security, reducing overall operational efficiency.

Weak signals
Critical insights can become buried within the noise, making it difficult to identify patterns that indicate potential security threats or network inefficiencies. The fragmentation of our data sources and systems further exacerbates this problem, complicating efforts to correlate information across different platforms and hindering our ability to achieve a holistic understanding of our infrastructure's health and security.

Taking security and networking to the next level

To move past the challenges above - sophisticated security threats, high levels of complexity and cost, and limited insight – we need a fundamentally different approach. We can’t continue to do the things we’ve been doing and expect a different or better result. Throwing more point products at the problem has reached the point of diminishing returns, and we can’t get any faster or more secure by adding more people.

Instead, we need to adopt a new approach that transcends the limitations of our legacy infrastructure and leverages advanced technologies to deliver a more secure, performant, and resilient network. We need to rethink our approach to networking and security in two fundamental ways:

Total automation

The second part of this approach to deliver a step-change in our security and networking is to apply “total automation”. Legacy approaches to detecting, troubleshooting, and fixing network and security issues no longer scale. In today's fast-paced digital environment, responding to breaches and outages manually means that the damage is already done. Adding more people or layering on additional products won't speed up response time or improve efficiency.

The future of networking and security lies in creating self-protecting networks that leverage advances in artificial intelligence (AI) to operate efficiently and securely with minimal human intervention. Several key insights underlie this approach:

- ✓ **We are in the age of AI –** Over the past five years, AI has evolved into a scalable and reliable operational tool that can support both security and network operations. AI's ability to analyze massive volumes of data in real time and deliver highly accurate insights in real time is transformative.
- ✓ **It’s all about the data –** To fully harness the potential of AI in network security, we need to focus not just on the technology but also on how AI processes and utilizes data. While anyone can implement open-source AI algorithms, high-precision autonomous operations require high quality, contextually rich and detailed data. In particular, this high-quality data can be provided by a unified platform, but is much harder to deliver from a disparate set of bolted-together products. A unified platform consolidates all network and security data into a single, comprehensive data lake, ensuring structural consistency that allows AI to operate with unmatched efficiency. As a result, AI can deliver precise, actionable insights across the entire network, significantly enhancing both performance and security.

Radical simplification

The first step is to eliminate complexity by consolidating network and security into a single, unified platform. This approach enables us to connect all our disparate network and security islands, reducing the sprawl of point products that currently burden our system. By converging multiple point products into a converged platform, we can dramatically reduce both cost and complexity, streamlining operations and enhancing overall efficiency. This specifically translates to a couple of key imperatives:

- ✓ **Converge security and networking into a unified platform –** Imagine the simplicity and radical transformation if all of our network and security infrastructure operated from one console, one policy set, one data lake, and one operating system. This would mean having one policy that is defined once and applied universally across the entire network, eliminating inconsistencies and ensuring comprehensive security measures are uniformly enforced. A single data lake capturing detailed, consistent telemetry would provide a powerful centralized repository for data analysis, improving visibility and enabling more effective use of AI and machine learning for proactive threat detection and network optimization. With one operating system governing the entire infrastructure, we would achieve unparalleled coherence and manageability, making our network not only simpler but significantly more resilient and responsive to emerging challenges.
- ✓ **Bridge the islands of connectivity** – In the future, our network infrastructure must break down our current silos, and span across WAN, LAN, data center, and cloud environments. Rather than each of these network segments operating its own network and security stack, a single platform across these areas will offer immense value by fostering a more cohesive and efficient operational environment, with enhanced visibility, collaboration, and security. This consolidation would reduce the complexity associated with managing multiple point products and fragmented systems, allowing for streamlined processes and improved response times to incidents. Furthermore, a connected infrastructure enables better data sharing and analysis, facilitating proactive threat detection and informed decision-making. Ultimately, bridging these islands enhances overall resilience, enabling organizations to respond more effectively to evolving challenges and optimize their resources for greater operational efficiency.

A unified platform is not the same as "single vendor"

While all unified platforms are single vendor, not all single vendor platforms are unified. A unified platform integrates all components from the operating system up, streamlining network and security management by reducing reliance on multiple point products that can create operational burdens. By consolidating functionalities into a single management console, organizations can enforce universal policies, ensuring consistent security measures across the network.

In contrast, a single-vendor platform may NOT be unified in this same sense. Often, vendors have acquired multiple products and "bolted" them together via APIs, but the underlying products still operate on different foundations and fail to achieve true operational streamlining. With multiple management consoles and policy repositories, fragmented data management, and an incomplete view of network health, many of these "single vendor" solutions fail to deliver the visibility and operational benefits promised.

In addition, there is often a negative impact on innovation for vendors attempting to unify their "single vendor" platforms. The development effort required to refactor and rebuild multiple disparate products onto a common platform is significant, and there are numerous historical examples of the innovation slowdown that occurs as vendors attempt to make this shift.

The future belongs to self-protecting networks

To achieve this level of simplification and automation, we require resilient and adaptive networks that are smart enough to identify, predict, and respond to issues autonomously, without the operational necessity of constant human intervention. Whether it's detecting and responding to threats in real time, or predicting and routing around network bottlenecks, the future belongs to networks that protect themselves.

The two key capabilities of such a self-protecting network are **self-healing networking** and **self-defending security**. These capabilities require an AI-powered infrastructure that self-manages both network performance as well as security.

A "self-healing" network for resilient connectivity and performance

In terms of network resilience and performance, a self-protecting network should be "self-healing". This represents a transformative approach where the network infrastructure can autonomously detect, predict and respond to network latency and outages. Key capabilities include:

- ✓ **Continuous data collection and baselining –** Network health and performance data is continuously collected in real time from across the entire network infrastructure and stored in a unified data lake accessible by monitoring, analytics, and AI tools. This approach baselines normal network behavior as a foundation for anomaly detection and predictive analysis.
- ✓ **Anomaly detection and prediction –** Comprehensive real-time observability is essential to monitor for anomalies against baseline data to identify or predict issues such as increased latency or packet loss. This also provides network administrators with detailed insights into network operations, health, and performance.
- ✓ **Diagnosis and recommended corrective action –** Once anomalies are detected, automated diagnosis tools quickly determine severity and root cause. This rapid diagnosis is followed by the development of corrective plan of action to bring the network back into its nominal state. Example recommended actions might include rerouting traffic, adjusting bandwidth, or isolating compromised segments.
- ✓ **Automated remediation with "human in the loop" –** AI can power automated recovery and repair processes that follow a corrective plan of action. However, organizations will need to determine how much autonomy to allow in these decisions and will likely need to build up trust in AI-generated recommendations. It is critical to provide a "human in the loop" capability that provides human oversight until IT staff determine what level of trust can and should be granted for autonomous decisions.
- ✓ **Predictive modeling –** Predictive modeling plays a crucial role in optimizing network performance proactively. By analyzing historical data and identifying patterns, predictive algorithms can forecast potential issues before they occur. For example, if a specific route consistently shows increased traffic at certain times, the network can preemptively re-route traffic to avoid congestion.

SASE is a good vision that doesn't go far enough

The concept of Secure Access Service Edge (SASE) has been a step in the right direction to reduce our infrastructure complexity and cost, but it doesn't go far enough. Today's SASE approach securely connects our remote workers, branch and campus offices directly to the internet via a combination of SD-WAN and SSE. What's needed is an approach that extends the principles of SASE to every user, device, and location across our entire LAN, WAN, data center, and cloud estate. This strategy, which we call "Universal SASE," aims to unify and simplify the design and operation of an organization's entire network and security infrastructure.

Universal SASE can provide comprehensive security and connectivity for all network segments, creating a cohesive and streamlined infrastructure. This approach will enhance security by applying consistent policies across all areas and reduce complexity and operational overhead by consolidating management under a single framework. The vision of Universal SASE is to provide a truly integrated network that supports the diverse and dynamic needs of modern enterprises.

A “self-defending” network for real-time defense against threats

In terms of network security and threat detection, a self-protecting network should be "self-defending". This represents a transformative approach where the infrastructure is built on a Zero Trust foundation to ensure universal secure access, and autonomous threat and data protection leverages machine learning and AI to identify security anomalies and block threats and data breaches in real-time.

- ✓ **Zero Trust foundation –** Zero Trust represents the future of cybersecurity, emphasizing that every user and device must be continuously authenticated and authorized before accessing network resources. In a self-protecting network, this concept must extend to all users and devices, regardless of their location—whether remote employees or on-premises users. Integrating the principle of "least privilege access" further enhances this framework, ensuring that users are granted only the minimum level of access necessary to perform their roles. This combination of "never trust, always verify" and least privilege significantly reduces the risk of unauthorized access and potential breaches, creating a more robust security posture.
- ✓ **Intelligent threat and data protection at the edge –** With the rise of IoT, cloud, and edge computing, the network attack surface has dramatically expanded. The goal of intelligent threat protection is to use AI-powered tools and technology to better identify and block threats from entering our networks, and to better identify and block sensitive data from leaving our networks. AI is being applied in a number of ways from advanced malware and exploit identification, to sensitive data identification and control.
- ✓ **Autonomous threat detection inside the infrastructure –** AI-powered threat detection leverages machine learning and AI to identify anomalies and stop potential threats inside our trusted network, in real-time. A self-protecting network applies advanced AI technologies to detect subtle indicators of compromise that traditional security measures might miss, by identifying weak threat signals in massive volumes of telemetry. Once a threat is detected, automated and real-time incident response mechanisms are activated, enabling the network to respond swiftly and effectively to mitigate the threat. Adaptive micro segmentation within the network reduces the risk of lateral movement and enhances overall security posture.

  In addition, adaptive security measures ensure that the network's defense mechanisms evolve in response to emerging threats, maintaining a high level of security. The integration of machine learning and AI not only enhances the network's ability to detect and respond to threats, but also enables continuous learning and improvement, ensuring that the network remains resilient against an ever-changing threat landscape.

The self-defending network’s time has come

The dream of a self-defending network has some history. Cisco first introduced the concept of a "self-defending network” back in the early 2000s, with a vision to enhance network security by integrating various security measures directly into the network infrastructure, enabling it to automatically detect and respond to threats. While this concept emphasized the need for networks to be proactive and intelligent, Cisco was never able to effectively deliver on the vision, because the enabling technologies looked dramatically different back then. Most important, the infrastructure was fragmented, and the era of artificial intelligence had not yet arrived.

Today, AI has matured into a powerful tool that can provide real-time insights, predictive analytics, and automated responses to security threats. The combination of a unified platform and advanced AI capabilities enables modern networks to operate more efficiently and securely. This integration allows for a comprehensive, cohesive approach to network security and management, dramatically improving the ability to defend against sophisticated cyber threats and ensuring optimal network performance.

Conclusion

> *“Nothing is more powerful than an idea whose time has come.”*
>
> — Victor Hugo

As organizations face the dual challenge of enhancing network security and performance amidst increasing complexity and evolving cyber threats, the further evolution of network and security infrastructure is essential. Too many organizations today grapple with fragmented architectures and an overwhelming volume of data, which impedes effective network optimization and threat protection. To overcome these obstacles, a paradigm shift towards a unified platform is necessary, facilitating radical simplification and enabling AI-driven self-protecting networks. The vision of self-protecting networks is to autonomously identify, predict, and respond to issues, thereby ensuring resilience against threats while enhancing operational efficiency. Ultimately, embracing this approach will empower organizations to navigate the complexities of today’s digital landscape and secure their future in an increasingly interconnected world.

About Versa

Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security. Versa is privately held and funded by investors such as Sequoia Capital, Mayfield, and BlackRock.

About VersaONE™

VersaONE seamlessly integrates security and networking to securely connect all users, devices, workloads, and networks through a unified platform. Powered by AI, the VersaONE Universal SASE platform enhances data protection and defends against cyberthreats while delivering an exceptional digital experience. As the cornerstone of Versa’s product portfolio, which includes Unified SASE, SSE, Secure SD-WAN, and Secure SD-LAN, it incorporates Zero Trust security at every edge and utilizes AI for advanced threat detection, network optimization, and real-time response. VersaONE simplifies network management with a unified console, ensures consistent policy enforcement with a unified policy engine, and delivers comprehensive visibility via a unified data lake. The platform offers organizations a robust, adaptive infrastructure that supports global connectivity, reduces complexity, and enhances security.

For more information, visit https://www.versa-networks.com and follow Versa on LinkedIn and X (Twitter) @versanetworks.

VERSA

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054, +1 408.385.7660, info@versa-networks.com, www.versa-networks.com

© 2025 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and VOS are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners. Part# WP_SELFPROTECTNET-01