Breaking Down Silos with Secure Networking

Three Secure Networking Pillars to Enable Digital Resilience

Contents

Overview

IT and business leaders are feeling the pressure to deliver secure, reliable, and connected experiences for their customers and workforce in a time of great technological and economic volatility. While returning to the office is a priority for many organizations, nearly half of the workforce continues to work from anywhere[1]—requiring IT to ensure secure access for their people and devices. This hyper distribution also transcends to an organization's complex infrastructure comprised of SaaS applications, data, and workloads all running simultaneously in on-prem, cloud, and third-party environments.

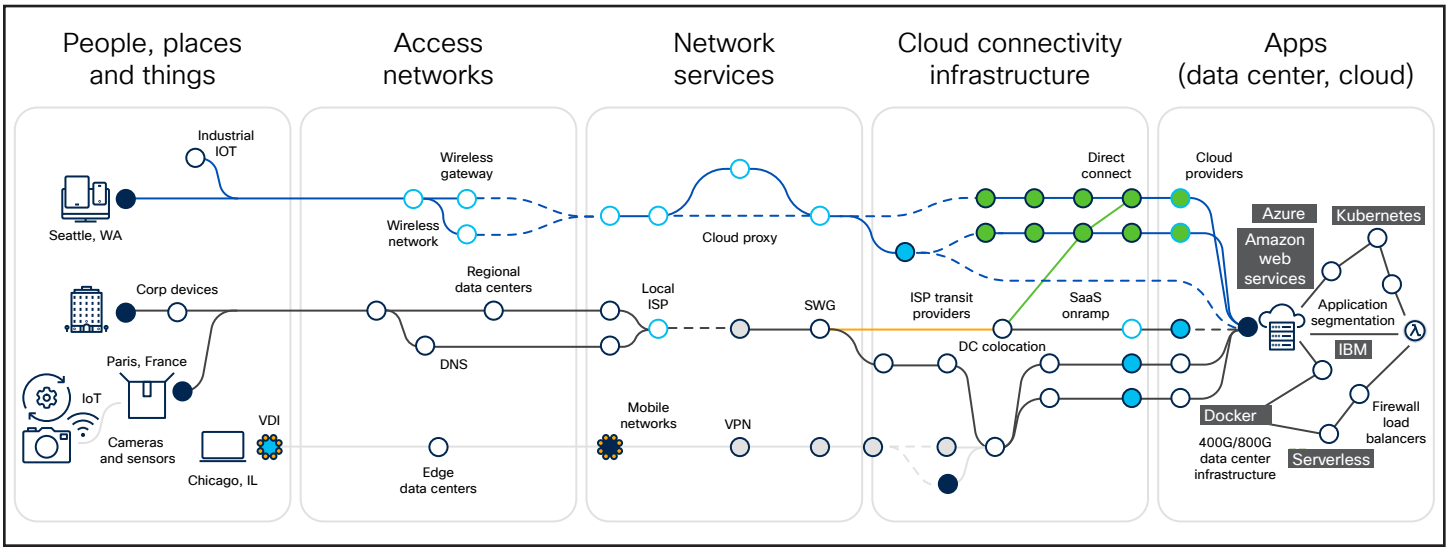

Figure 1. Complex IT infrastructure.

Compounding this infrastructure complexity is that of one's IT organization with siloed NetOps and SecOps teams—each having their own set of tools and priorities resulting in separate policies, Network Operations Center/Security Operations Cener (NOC/SOC), centers of excellence, etc. This disjointed operating model can lead to significant delays in detecting and remediating vulnerabilities, costing organizations both time and money. With the average time to detect and contain a breach being 258 days and costing organizations $4.88 million[2] these inefficiencies are unacceptable and unaffordable.

And while AI promises accelerated automation of business and IT processes to alleviate growing skills shortages, being able to master these innovations is proving challenging with only 13% of companies feeling ready to capture AI's potential today.[3] This challenge is not shared by bad actors who are reaping AI's benefits through cleverly orchestrated phishing, deepfake, and ransomware attacks.

Coupling these challenges with the increasing pressure for IT to meet the needs of business leaves little margin for internet and network downtime. IT and business leaders recognize the need to provide more reliable digital experiences and increase their infrastructure's overall digital resilience—the ability to prevent, detect, recover, and respond to events that have the potential to disrupt business processes and services. A cohesive and comprehensive secure networking strategy is foundational in providing this digital resilience.

[1] ESG SSE Survey, June 2023. [2] Cost of Data Breach Report, IBM, 2024. [3] Cisco 2024 AI Readiness Index.

What is secure networking?

Secure networking refers to the practice of protecting the integrity, confidentiality, and availability of data and resources throughout the end-to-end network. Its hallmark is a platform-led approach calling for the integration of security measures into networking solutions to ensure that the network is protected from unauthorized access, misuse, or theft. Involving the implementation of various technologies, policies, and procedures, secure networking is essential for maintaining the security of data transmitted over the network and ensuring that only authorized users and devices can access network resources.

This practice not only calls for an integrative approach of network and security technologies and processes but also requires a cultural shift between siloed NetOps and SecOps teams into a unified NetSecOps approach. This shift is top of mind for many IT leaders. Forty-two percent recognize integrating network and security as a key area requiring the most significant improvement to meet business objectives.[4]

Secure networking also delivers greater digital resilience by giving organizations the ability to recover quickly from disruptive shocks and ensure continuous operation.

Key pillars of a comprehensive secure networking strategy

Establish trust. At the heart of an organization's secure networking strategy is the adoption of a Zero Trust Architecture (ZTA) framework, which requires strict verification for every user and device trying to access resources on a network, regardless of whether they are inside or outside the network perimeter. This approach is a sought-after standard because it minimizes the risk of breaches by taking a role-based access approach. This approach eliminates implicit trust, and continuously validates every access request. By segmenting and establishing policies by role, organizations can ensure the right access to the right devices and data for the right user. By applying the ZTA framework, the highest level of infrastructure access security can be ensured while also delivering best-in-class user experiences.

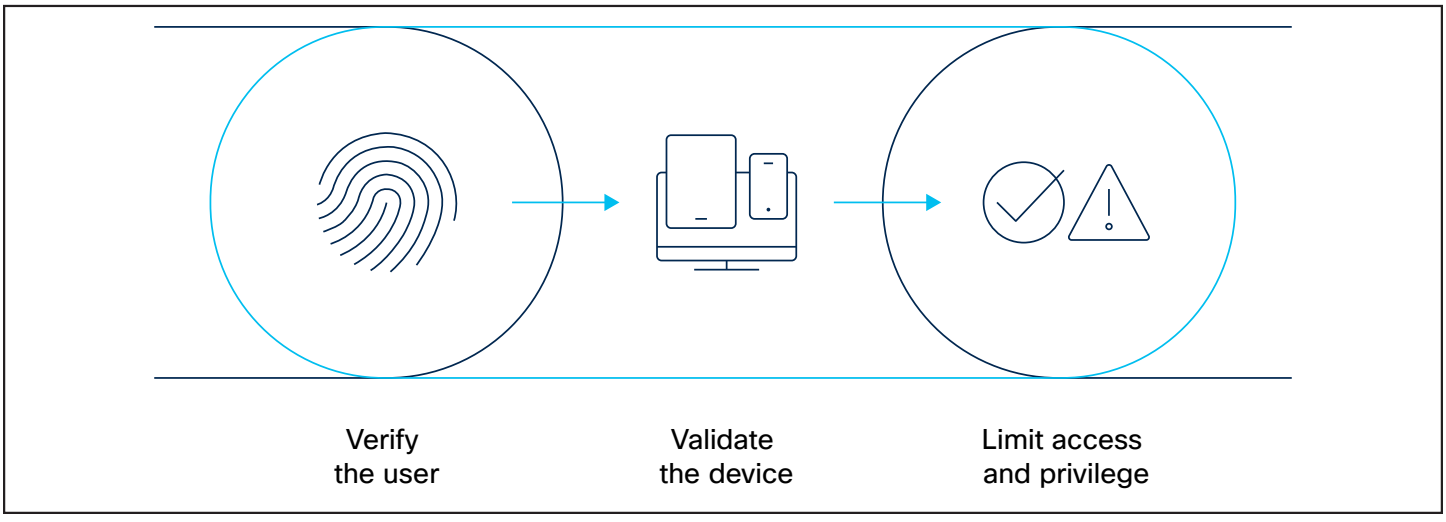

Figure 2. ZTA framework requires user verification, device validation, and role-based access.

4 Cisco 2024 Global Networking Trends Report.

Fortify security with AI. Bad actors are leveraging generative AI to host more sophisticated and efficient attacks, putting proprietary company and customer data at risk. A recent Harvard Business Review study showed that 60% of respondents recently fell victim to an AI-automated phishing attack, and these attacks were made 95% more cost-efficient due to AI-powered automation.[5]

Conversely, AI can also be used for good in secure networking through AI-enabled endpoint recognition, segmentation, and policy management, which allows organizations to identify potential performance and security issues and proactively address them. AI can also be applied to cloud-enforced security controls including Cisco Secure Service Edge (SSE) and Cisco Secure Access Service Edge (SASE) to help IT teams make smarter zero-trust access decisions and better defend against identity-based attacks. Additionally, AI capabilities can provide a stronger and more consistent security posture, allowing network security to be tackled at machine scale, not just human scale.

Bring NetOps and SecOps together. Taking a cue from DevOps, organizations are beginning to see the need to converge NetOps and SecOps to streamline operations, achieve greater operating consistency, and reduce risk. By aligning teams, tools, and workflows into a comprehensive NetSecOps approach, IT can simplify operations, increase collaboration between IT teams, and ensure a consistent set of security policies across different environments.

This convergence supports a more integrated and efficient approach to managing both networking and security challenges, particularly in a distributed and cloud-centric infrastructure. Here are some ways organizations can start aligning these two disparate teams:

1. **Increase collaboration and communication:** Encouraging Net/Sec IT and OT teams to work together to define anomalies, understand industrial processes, and set criticality levels for potential impacts.
2. **Sharing tools and platforms:** Look for best-of-breed solutions with clear integration between network and security solutions to provide a complete view of the cyber kill chain, integrating IoT/OT into existing IT/SecOps and SOC tools.
3. **Gain end-to-end visibility and assurance:** Increasing visibility across the infrastructure to ensure secure access and simplify operations by adopting integrated solutions to provide unified visibility across operational domains, helping break down silos and reduce friction among teams.

By aligning network and security teams, tools, and processes, organizations can streamline operations, achieve greater consistency, and mitigate risk.

5 “AI Will Increase the Quantity — and Quality — of Phishing Scams,” Harvard Business Review, 2024.

Benefits of secure networking

Implementing a secure networking strategy is crucial for organizations to address the risks associated with a complex and hyper-distributed infrastructure in an AI-prevalent world. A secure networking strategy helps simplify network and security management, reduce cybersecurity threats, improve user experience, and reduce complexity and costs.

It ensures consistent identity, policy, visibility, and enforcement across the enterprise, providing secure and resilient connectivity to applications. By converging networking and security, organizations can safeguard the network with always-in security, deliver the best networking experience based on a zero-trust framework, and simplify management with one suite of solutions—enhancing one's cybersecurity posture and overall operational efficiency.

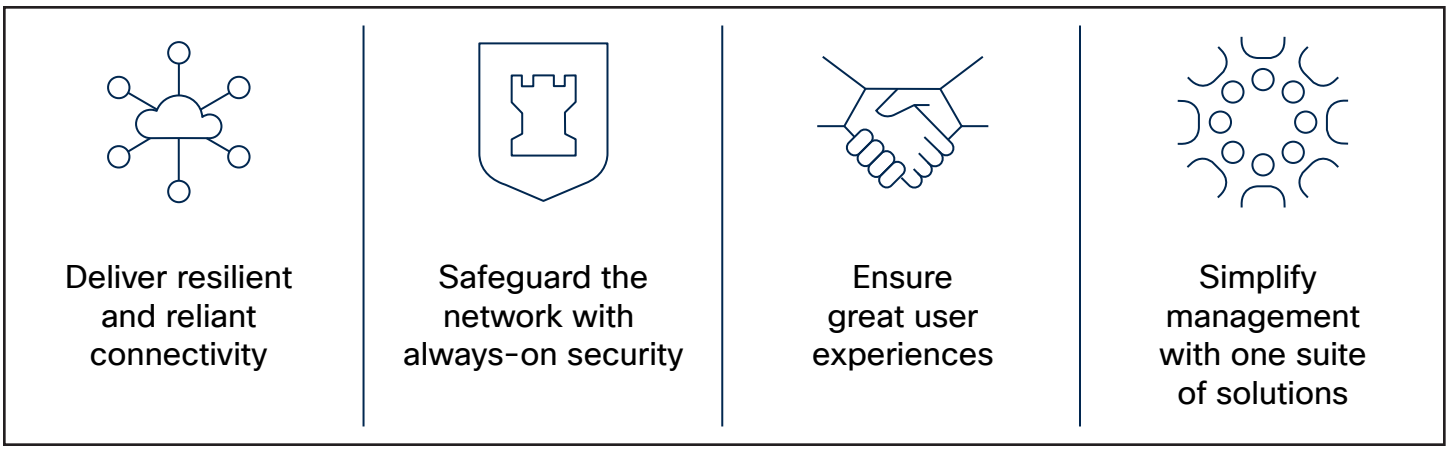

Figure 3. Benefits of secure networking.

Advance secure networking with Cisco

With the industry's most complete end-to-end suite of networking and security solution, only Cisco has the breadth and depth of telemetry, technology, and expertise to speed your secure networking adoption. Celebrating 40 years in delivering unparalleled network connectivity, Cisco solutions deliver the best protection across your unique domains by combining the power of AI-automation and zero trust, common policy enforcement at every user touchpoint.

Our networking and security solutions work in harmony, delivering comprehensive visibility, protection, and connectivity across diverse environments. Start on your secure networking journey with Cisco today to decrease downtime and increase network reliability for greater digital resilience.

Learn more

Experience how secure networking solutions from Cisco are empowering organizations with secure and seamless access to the internet and SaaS applications, as well as corporate applications, assets, and resources.

- Secure Networking on Cisco.com.
- Secure Networking Solution Overview

C11-4981040-00 04/25