algosec

Secure application connectivity.
Anywhere.



State of Network Security 2026

Cisco Live Las Vegas Edition

June 2026

State of Network Security 2026

Cisco *Live*! Edition

From Tool Sprawl to Unified Control

Hybrid networks are entering a new era: **less expansion, more consolidation**. After years of adding firewalls, cloud tools, SD-WAN, SASE, and AI capabilities, enterprises are now focused on **unifying visibility, automating policy, and regaining centralized control**.

Based on insights from **504 security, network, and cloud professionals across 28 countries**, the 2026 report shows one clear shift: **resilience now depends less on how many tools an organization deploys, and more on how well those tools work together.**

Why This Matters for Cisco Users

Cisco Users are building and operating the environments where this shift is happening: hybrid clouds, distributed users, SD-WAN fabrics, SASE architectures, Zero Trust programs, and AI-ready infrastructure.

The message for network and security leaders is clear:

The future of network security is unified, automated, and policy-driven.

Key Trends for Cisco-Centric Environments

1. Firewalls are being rebalanced

Organizations are split between expanding multi-vendor environments and consolidating vendors. **30% plan to expand to multi-vendor firewalls**, while **24% plan to consolidate**. The winning model is not single-vendor everywhere, it is **centralized control across diverse enforcement points**.

2. Cloud security is now a platform decision

55% of organizations select cloud platforms primarily based on security, ahead of cost, performance, and flexibility. Cloud strategy and security strategy are now inseparable.

3. Policy consistency is the new cloud security challenge

For the first time, **consistent policy enforcement across cloud and on-prem environments** has overtaken visibility as the top cloud security challenge. This is especially relevant for organizations running Cisco alongside public cloud firewalls, private cloud, and SASE controls.

4. SD-WAN is now foundational

SD-WAN has moved from optional to essential, with only **21.1% reporting no SD-WAN solution**. Cisco remains a major player at **30.7% adoption**, close behind Fortinet at 31%. The differentiator is no longer connectivity alone , it is **integration with security and orchestration platforms**.

5. SASE is becoming standard

Non-adoption of SASE dropped from **40% in 2025 to 27.5% in 2026**. Enterprises are moving from pilots to operational models, increasingly favoring integrated approaches that combine access, connectivity, and cloud-delivered security.

6. Zero Trust is still hard to execute

Zero Trust adoption remains steady, but maturity is limited. **31% are still learning**, and only **19% report full implementation across cloud, on-prem, and SDN**. The barrier is not belief, it is execution across hybrid infrastructure.

7. AI is shifting from hype to operational use

AI is now both a threat and a defense priority. **65% of organizations have adapted their strategies for AI-powered attacks**, while the highest-impact AI use case is **hybrid network visibility and risk prioritization**.

8. Automation maturity is rising

54% of organizations now report moderate or high automation in network security management. The focus is shifting from faster changes to **policy assurance, compliance tracking, and risk-based automation**.

9. Teams and tools are consolidating

Only **19% of organizations still operate in silos**. Meanwhile, **75% have consolidated at least some security tools or policies under a single platform or management layer**. Shared tools are becoming the foundation for shared accountability.

What Cisco Live Attendees Should Take Away

The next phase of network security is not about adding more point solutions. It is about making existing infrastructure work together through:

- **Unified policy control** across Cisco, cloud, firewall, SD-WAN, and SASE environments
- **Automated change and risk analysis** to reduce manual work and prevent misconfigurations
- **Consistent enforcement** across hybrid and multi-cloud networks
- **Shared visibility** for cloud, network, and security teams
- **AI-assisted operations** focused on visibility, cleanup, and risk prioritization

Bottom Line

The 2026 network security mandate is simple:

Consolidate control. Automate policy. Secure the hybrid network as one environment.

For Cisco Live attendees, this is the practical path forward: connect security, networking, cloud, and application teams around a shared operating model, and turn complexity into control.