Building the future-ready network:

8 ways to power resilient, secure networking everywhere with **Cisco SD-WAN**

cisco

Modern workplaces face unique networking challenges that directly impact security

The modern workplace is a dynamic mix of corporate campuses, branch offices, and remote locations. Within this globally distributed environment, users expect a seamless, high-performance, and secure experience everywhere.

As complexity continues to rise in parallel with expectations, challenges emerge. Inconsistent performance leads to user frustration, while IT teams must deliver a uniform security posture and an excellent application experience across the entire network—from the data center and cloud to every user, wherever they may be.

Contents

A resilient, available, and high-performing network is a business imperative

$400B lost to downtime annually by the Global 2000[1]

In today's world, network downtime means you are closed for business, costing revenue and damaging your brand's reputation.

Successful businesses need a resilient network, but when complexity is baked into it—whether through application sprawl, disparate tools, hyper-automation that creates fragile dependencies, or disruptions like circuit cuts and ISP outages—resiliency and visibility are compromised. Even AI-driven processes can stall when outages strike, worsening delays. These are the cracks that lead to catastrophic downtime. That's why modern enterprises are converging networking and security: to cut through the complexity, strengthen resilience, and deliver near-zero downtime with always-on connectivity for users and customers.

There are many causes for network downtime—but it is always costly

90%
of enterprises are estimated to experience a security incident at the network edge by 2026

68%
of reported downtime issues were related to misconfiguration driven by app sprawl

70%
of enterprises run AI workloads across hybrid or multicloud environments, exposing them to network instability risks

Security issues that can impact the network are always evolving

- AI-driven attacks
- Deepfake technology
- IoT vulnerabilities
- Cloud security threats
- Insider threats
- Supply chain attacks
- 5G network vulnerabilities
- Quantum computing threats
- Data leakage via GenAI models
- Zero-day exploits

As a leader in networking and security, Cisco simplifies the journey to a future-proofed workplace

Secure, optimized access to applications from any location represents an ideal experience for the distributed workforce. But that experience is only possible when the underlying networking and security architectures enable it. Cisco is the ideal partner to chart this course. Cisco SD-WAN, with its ability to protect and optimize network traffic, paired with integrated security capabilities aligned with Security Service Edge (SSE) cybersecurity frameworks, converges security and networking as a foundation for any organization's Secure Access Service Edge (SASE).

Cisco brings the power of the network together

with industry-leading security, observability, and collaboration

31M
devices connected to our platform

886B
security events observed per day across the network

1B
clients connecting monthly

Cisco makes it easy to bring together networking and security to enable a secure, resilient, SASE-ready network.

Cisco's approach combines SSE capabilities with embedded next-generation firewall (NGFW) features. Working together, these layers deliver advanced threat protection, secure access, and granular policy enforcement at scale. Cisco SD-WAN, through tight integration with Cisco Secure Access, provides constant protection against cyberthreats, from branch locations to multicloud SaaS environments. With Secure Access integration and observability from Cisco ThousandEyes, Cisco SD-WAN helps you see and understand what's happening on your network, protect it, and deliver the performance and experience across distributed IT environments that your stakeholders expect—all in the service of achieving a securely connected and protected enterprise, everywhere.

NetSecOPEN

- Independent evaluation
- Deploy with confidence
- Trusted organization

98% Intrusion prevention (IPS) effectiveness

99% Malware detection rate

1 Integration with Cisco Secure Access for a SASE-ready network

Embracing SASE within your business

Establishing a SASE architecture within your organization streamlines cloud-based security and networking. Converging security and networking in this way not only simplifies management and operations, but with the right observability tools in place, it also gives you a more comprehensive, end-to-end picture of your environment that makes for a more resilient, secure network.

Cisco SD-WAN facilitates the journey to SASE by integrating with Cisco Secure Access to seamlessly bring advanced networking and security capabilities together. This integration is game-changing, bringing automation and consistency to IT administrators across domains to reduce complexity and deliver highly-resilient networking and security, ultimately improving experiences for end-users across locations and applications

Integrate seamlessly

Cisco Secure Access automatically connects to Cisco Catalyst SD-WAN Manager to simplify and accelerate deployment across your entire network, reducing branch office setup time to quickly protect and optimize network traffic across SaaS applications and the web. Once set up, IT administrators can manage thousands of sites from a single, centralized dashboard—allowing them to steer and secure network traffic with just a few clicks.

Underlying all of this, Cisco ThousandEyes allows your organization to consistently monitor and analyze the performance of your network and applications in context—providing end-to-end observability and a unified view. This allows your organization to easily visualize the path network traffic takes and proactively pinpoint and resolve issues to prevent outages and preserve the end-user experience.

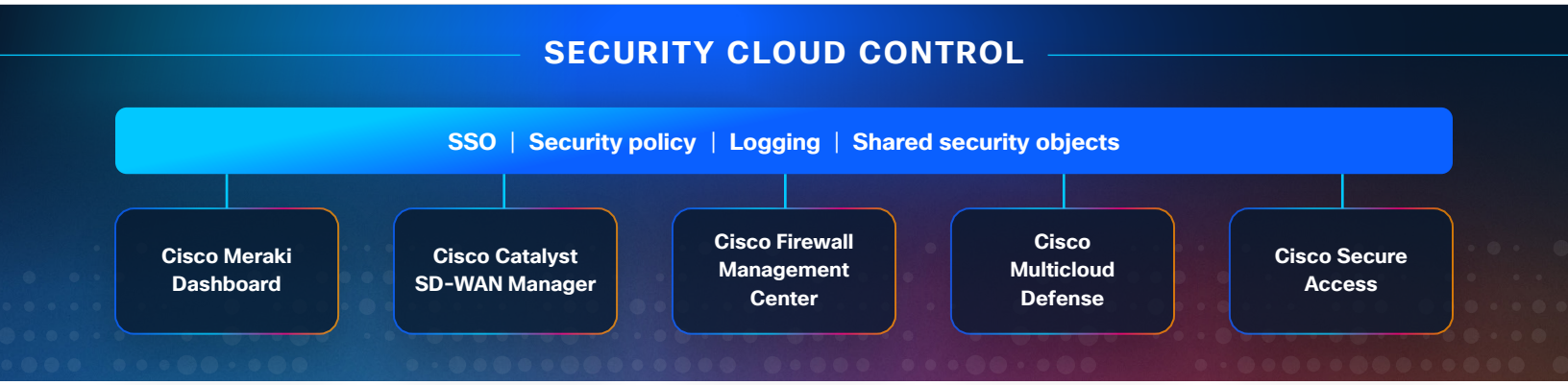
Disparate networking and security solutions

- Limited flexibility and restrictive policies, leading to performance bottlenecks, operational challenges, and security gaps
- Lack of tiered capabilities as well as scalability challenges
- Multiple management interfaces creating complexity and inconsistent policy enforcement
- Insufficient depth in networking or security features

Cisco offers seamless integration

- Flexible traffic engineering with SLA steering and ECMP load balancing
- Shared context (VRF/SGTs) between SD-WAN and Secure Access
- Hybrid security with on-box NGFW for trusted apps + SSE for others
- Automated deployment with guided workflows (SD-WAN Manager)
- End-to-end security with AnyConnect and Duo

2 Unified policy for central control and distributed enforcement



Unified policy streamlines operations

Converging networking and security functions only works if the way you manage those functions converges as well. A single, unified policy makes management simple, allowing IT teams to set and control policy in one place and enforce it everywhere. Further simplifying their processes, guided workflows and smart default settings built into the solution help IT teams make better-informed actions, more quickly, with more context. Distributed enforcement capabilities also serve to reduce mistakes from manual or inconsistent enforcement that could ultimately lead to costly downtime. The result is simpler, reliable security and compliance management across the network that empowers teams to operate effectively at the scale your business demands.

Centralized, integrated management

SD-WAN Manager plays a critical role in unifying security and network management by offering comprehensive visibility, rapid service rollout, and simplified operations—all from one centralized platform. With Security Cloud Control, organizations benefit from centrally managed unified policies that are seamlessly enforced across all distributed sites and environments, ensuring consistent protection and streamlined operations everywhere. Cisco SD-WAN is designed with robust, automated security applied across four critical planes—management, control, data, and firmware—all centrally orchestrated through SD-WAN Manager. Secure Access integrates directly with SD-WAN Manager to extend policy enforcement to the cloud, consolidating security functions and simplifying deployment and management with cloud-delivered, distributed enforcement.

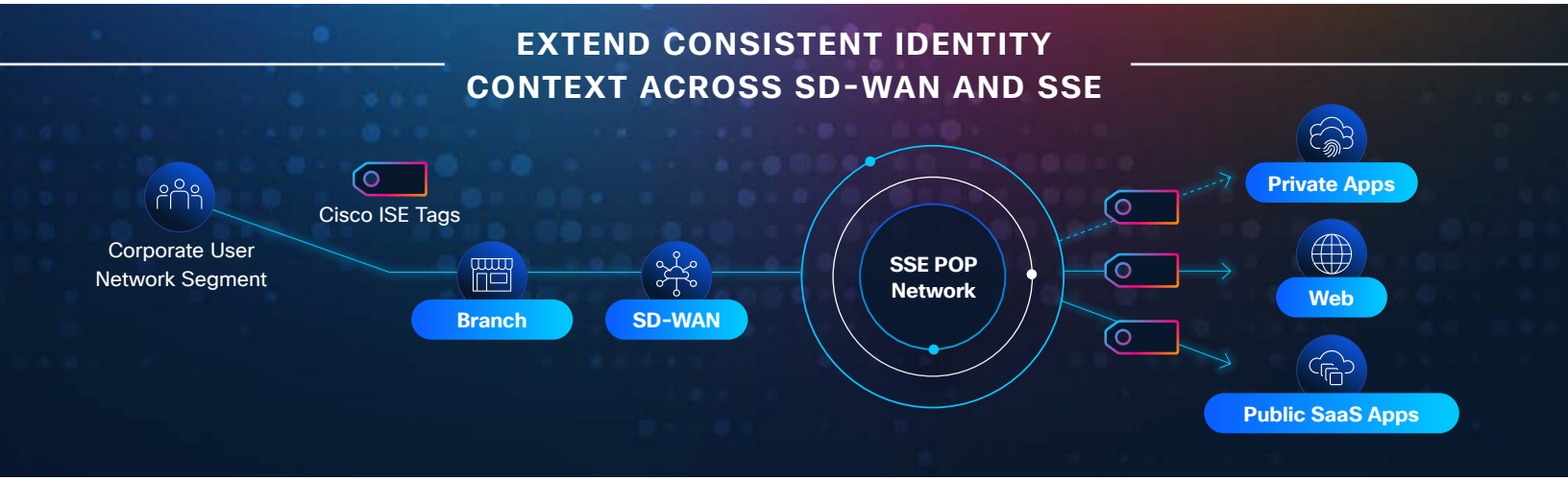
Other systems are complex and rigid

- Complex and inefficient security policy configurations heighten the risk of error
- Rigid single vendor systems force customers to replace existing investments and lose out on innovation
- Control plane activities lack robust mechanisms for device authentication and encrypted control information

Cisco offers simple, flexible solutions

- Guided workflows and smart defaults result in fewer touchpoints, streamlined policy configuration processes, and reduced likelihood of errors
- Cisco SD-WAN is designed for seamless integration with third-party solutions, protecting your existing investments while enhancing your security and network capabilities
- A centralized controller establishes and maintains encrypted connections between all SD-WAN devices in the overlay network with confidential control traffic

3 Identity-based microsegmentation to enforce zero trust policies



Provide a secure, consistent experience

Microsegmentation – the ability to create secure zones across cloud, network, and data center environments – is critical to limit east-west traffic between workloads and ensure the impact of any security or access breach is well-contained. Identity-based microsegmentation takes this a step further by tying access to the identity and attributes of a given user, device or application, rather than relying on static boundaries. This includes device posture, as employees accessing resources from managed devices can receive full access, while limiting access for unmanaged devices to maintain security. Cisco's approach to identity-based microsegmentation helps enforce zero trust policies based on user identity, device posture, and application context to provide a consistent, secure experience anywhere, anytime. Thousands of remote workers can connect to the SD-WAN fabric through their nearest branch, data center, colocation facility, or public cloud. With identity-based microsegmentation, every one of them will experience a simple, consistent user interface, helping reduce risk.

Security policies adapt dynamically

Cisco SD-WAN enables you to extend microsegmentation and identity-based policy management across Cisco Software-Defined Access (SD-Access) and non-SD-Access branches. This allows security policies to adapt dynamically based on user identity, device posture, and application context, pairing with next-generation firewall restriction to enforce least-privilege access. These features come together to drive consistent multidomain policy enforcement across your network from a single pane of glass.

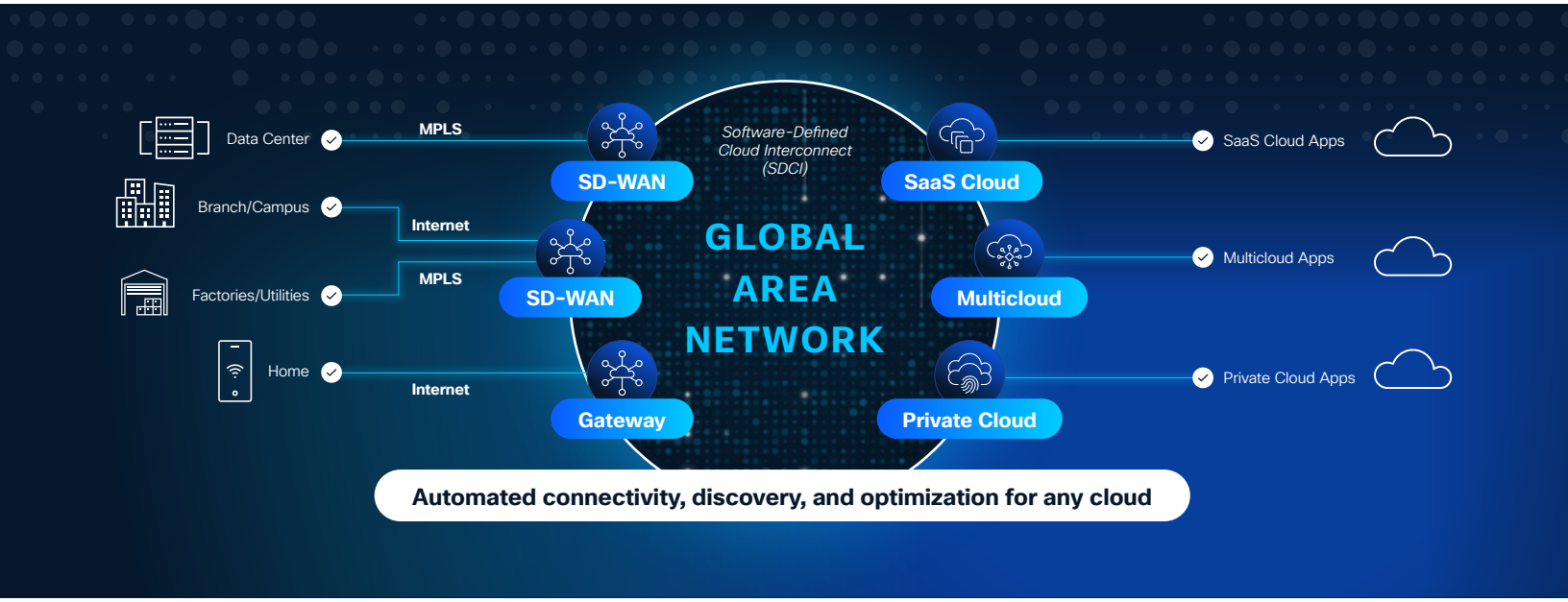
Other providers lack microsegmentation capabilities

- Expanded blast radius leaving networks vulnerable
- Reliance on static models
- Lack of integration with zero trust principles
- Limited granularity
- Scalability challenges and Insufficient visibility

Cisco SD-WAN provides centralized, granular control

- Enables microsegmentation across your network
- Provides granular control over established policies, all from a single pane of glass
- Threat radius is reduced and contained

4 Cisco SD-WAN Cloud OnRamp for simplified multicloud connectivity



Optimize user experiences

The end-user experience for any application—be it internal or external—can be heavily influenced by the application's underlying cloud services. The ideal end-user experience is seamless and consistent, but that experience can be difficult to achieve when operating in a distributed, multicloud world. Cisco SD-WAN Cloud OnRamp helps deliver the experience your stakeholders demand by providing consistent user interfaces and workflows across clouds. With granular insights into application performance and secure, cloud-agnostic connectivity, Cisco helps optimize the end-user experience for private cloud, SaaS, and multicloud applications. The SD-WAN fabric ensures end-to-end segmentation across the network, delivering precise control over traffic flows between users and services. To further optimize performance, Cisco SD-WAN Cloud OnRamp has automation in place to consistently drive minimal latency for application traffic even with custom GenAI Apps.

Automation and cloud-based security are built-in

Cisco makes it easy to automate your multicloud setup by flexibly extending SD-WAN to the cloud through internet, interconnect, or colocation environments. Paired with built-in cloud-based security, this helps unify security and networking functions in the cloud. To enhance application performance, Cisco SD-WAN uses automation and AI for traffic steering and application-aware —all to identify the most optimal IPSec/GRE tunnels to move traffic through and ensure that the end-user experience is consistent and optimized.

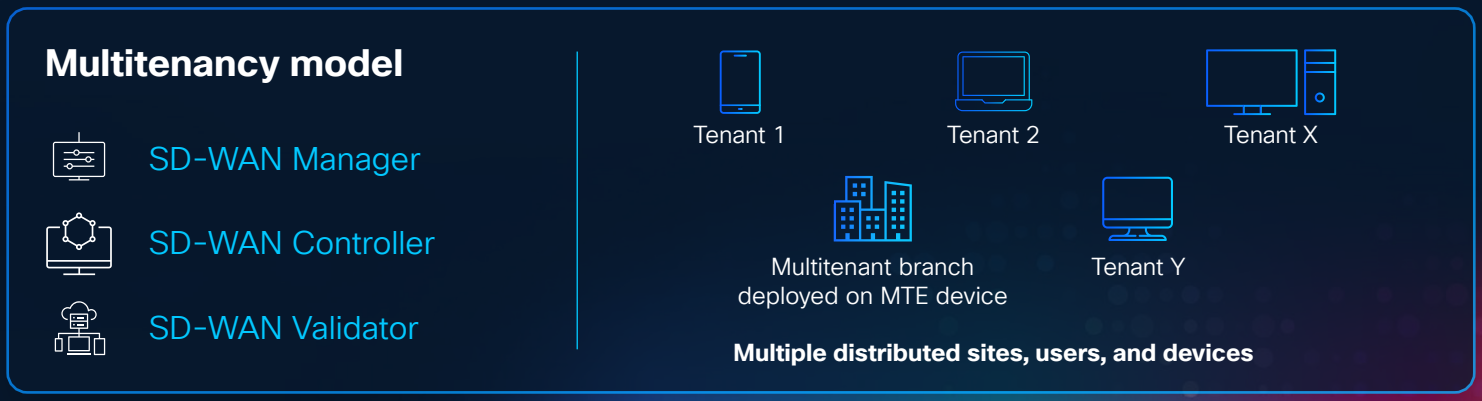
Other systems are disconnected and difficult to scale

- Immature SD-WANs struggle to scale, lacking multi-region deployments
- Cannot connect to multiple clouds
- Lack holistic integration of automation

Cisco offers scalable, integrated solutions

- Cisco is a Gartner Magic Quadrant leader in SD-WAN, scaling up to 12,500 sites and facilitating multi-region deployments
- Cisco SD-WAN Cloud OnRamp facilitates automation for multicloud environments
- Automation is built into Cisco SD-WAN to reduce latency and streamline operations

5 Advanced options for scalable, secure, and flexible SD-WAN deployments



Simplify global deployments

Multi-Region Fabric enables organizations to deploy large-scale SD-WAN architectures across multiple geographic regions while maintaining operational simplicity. By regionalizing control planes and automating inter-region policies, Multi-Region Fabric significantly reduces network complexity. Cisco's approach accelerates configuration processes and helps ensure compliance with regional data sovereignty requirements, delivering optimized performance and to secure a distributed workforce.

Future-proof legacy workloads

Cisco's Layer 2 VPN over SD-WAN solution provides organizations with a secure, cost-effective method for maintaining critical Layer 2 connectivity across distributed network environments. This modern implementation preserves essential legacy application support while reducing dependency on expensive traditional networking solutions.

Optimize resources across tenants

Multi-Tenant Edge (MTE) technology allows service providers and large enterprises to securely host multiple isolated tenants on a single SD-WAN edge device. This architecture dramatically reduces hardware expenditures and simplifies infrastructure management while maintaining rigorous data segregation between tenants. MTE's streamlined onboarding process and granular access controls make it particularly valuable for managed service providers (MSPs) and enterprises with diverse business units or customer networks.

Other solutions struggle with scale and complexity

- Limited regional support creates operational bottlenecks
- Rigid architectures cannot support multitenancy efficiently
- Lack integrated Layer 2 solutions, forcing costly workarounds
- Manual processes increase errors and deployment times

Cisco offers intelligent automation for seamless connectivity

- Simplified global scaling with automated multi-region management
- Cost-efficient multitenancy on shared infrastructure
- Future-proof connectivity with integrated Layer 2 VPN support
- Time-saving automation for faster deployments

6 End-to-end visibility and AI-powered analytics for proactive observability

Transform from reactive to predictive operations

The path taken by network and application traffic is rarely straightforward. More sensitive traffic may need to be steered through secure paths, certain elements of the network might be more congested at a given time, and not all application traffic should have the same priority in how it is handled. What's more, none of this is static, and real-time changes in the context of the network itself should impact how traffic is steered.

Cisco helps you to not only be more dynamic in steering traffic according to these real-time concerns but to actually predict the best routes for traffic to take. This is driven by end-to-end visibility and AI-powered Predictive Path Recommendations (PPR), which enable your organization to proactively determine the best paths to facilitate the best user experience with your applications.

By proactively optimizing how traffic flows through the network, organizations can reduce workarounds, performance impacts, and disruptions - preventing them before they impact users. These features are built to deliver seamless performance and consistent, predictable in-office experiences, regardless of location, even on unmanaged networks.

AIOps provides proactive insights like bandwidth forecasting and anomaly detection.

Cisco ThousandEyes powers Predictive Path Recommendations (PPR) to identify optimal paths for traffic, helping avoid disruptions and ensure availability.

To access these insights easily, users can take advantage of an interactive **AI Assistant,** further streamlining operations.

Network Wide Path Insights

Validate policy configuration

- Simulate IP traffic or reply traffic patterns
- Validate which and security policies are invoked

Event-based processing

- Trace active flows based on configured event triggers
- Analyze and determine root causes
- Resolve incidents quickly with live troubleshooting and automated remediation

Investigate user traffic

- Granular visibility into end-to-end user flows
- Investigate user experience issues and security threats

Other SD-WAN solutions lack integrated security insights

- SD-WAN solutions often have limited security insights with no integrated security monitoring dashboard
- Many AI insights run as cloud services
- Poor anomaly detection
- Lack of bandwidth optimization resulting in poor performance and availability

Cisco offers built-in visibility tools

- Cisco SD-WAN has built-in NWPI. Paired with ThousandEyes, customers have superior end-to-end visibility and security troubleshooting across networks
- Cisco is partnering with Splunk to bring some cloud functions on-prem for AI analytics, offering added flexibility
- AI-powered anomaly detection helps proactively protect against threats

7 Next-gen SD-WAN powered by quantum-safe crypto agility

Protect against future threats

The pace of technological innovation and the unprecedented access to advanced technology by bad actors calls for a more predictive security approach.

Cisco is ready when you are, with a quantum-safe SD-WAN fabric, providing greater crypto agility and protecting your network as AI-driven attacks and quantum computing threats emerge. Because these features are built into quantum-safe SD-WAN fabric, critical infrastructure and sensitive data are safe for decades to come, so you can grow securely.

Cisco plans for the future

Quantum-safe encryption and authentication help protect against future quantum attacks, keeping sensitive data and critical infrastructure safe into the future and reducing long-term upgrade costs. To smooth your transition from classical to quantum-ready security, Cisco SD-WAN offers hybrid encryption.

As more organizations prepare for quantum threats, Cisco is on the forefront of compliance standards. Cisco SD-WAN is already aligned with National Institute of Standards and Technology (NIST) security standards, helping you stay prepared.

Cisco leads the quantum security space

Developed SKIP protocol
Predates the development of ETSI API standard

Authored RFC8784
A standard adopted by all major vendors

Part of PQCA, the Linux foundation project
Together with Amazon, Nvidia, Google and others

Developed ecosystem with QKD vendors
Interoperability with major QKD vendors

Traditional security doesn't account for quantum threats

- Quantum computing is an emerging field, and many providers have yet to address the cybersecurity risks it poses
- No quantum threat protection available
- Future upgrades required

Cisco offers scalable, integrated solutions

- Cisco is quantum-ready, rapidly evolving with the threat landscape and has already developed a quantum-safe SD-WAN fabric
- Multiple deployment methods are available based on security needs
- Quantum-ready encryption is available today, reducing long term upgrade costs and keeping your data and infrastructure safe for decades as these threats emerge

8 Cisco SD-WAN is critical in building your SASE architecture

Cisco SD-WAN and Cisco Secure Access form the foundation of a strong SASE architecture – enabling secure, identity-driven access across your enterprise.

As you build your SASE architecture and move toward a future-ready, quantum-safe network, Cisco SD-WAN supports your journey with flexible deployment options. Choose cloud-delivered simplicity through templated solutions, or enable a customized approach with on-premises, private, or sovereign cloud deployments. Streamline your transformation while enhancing security and visibility through integrations with Cisco Secure Access and ThousandEyes.

Cisco SD-WAN sits at the core of an effective SASE architecture, delivering a consistent, secure experience across your network with a single, unified policy. Identity-based microsegmentation ensures enforcement of that policy.

End-to-end visibility and AIOps empower your organization to take a more proactive approach to maintaining strong, reliable performance for end-users. Cloud OnRamp automation and a quantum-safe fabric keep your organization at the cutting edge – enabling enterprise-grade experiences across cloud-based applications, while protecting your business and customers from emerging threats.

Learn more about Cisco SD-WAN

- Solution Overview
- Cisco SD-WAN Video
- Solution Demo
- Nestlé Customer Story

Networking for the future – your future