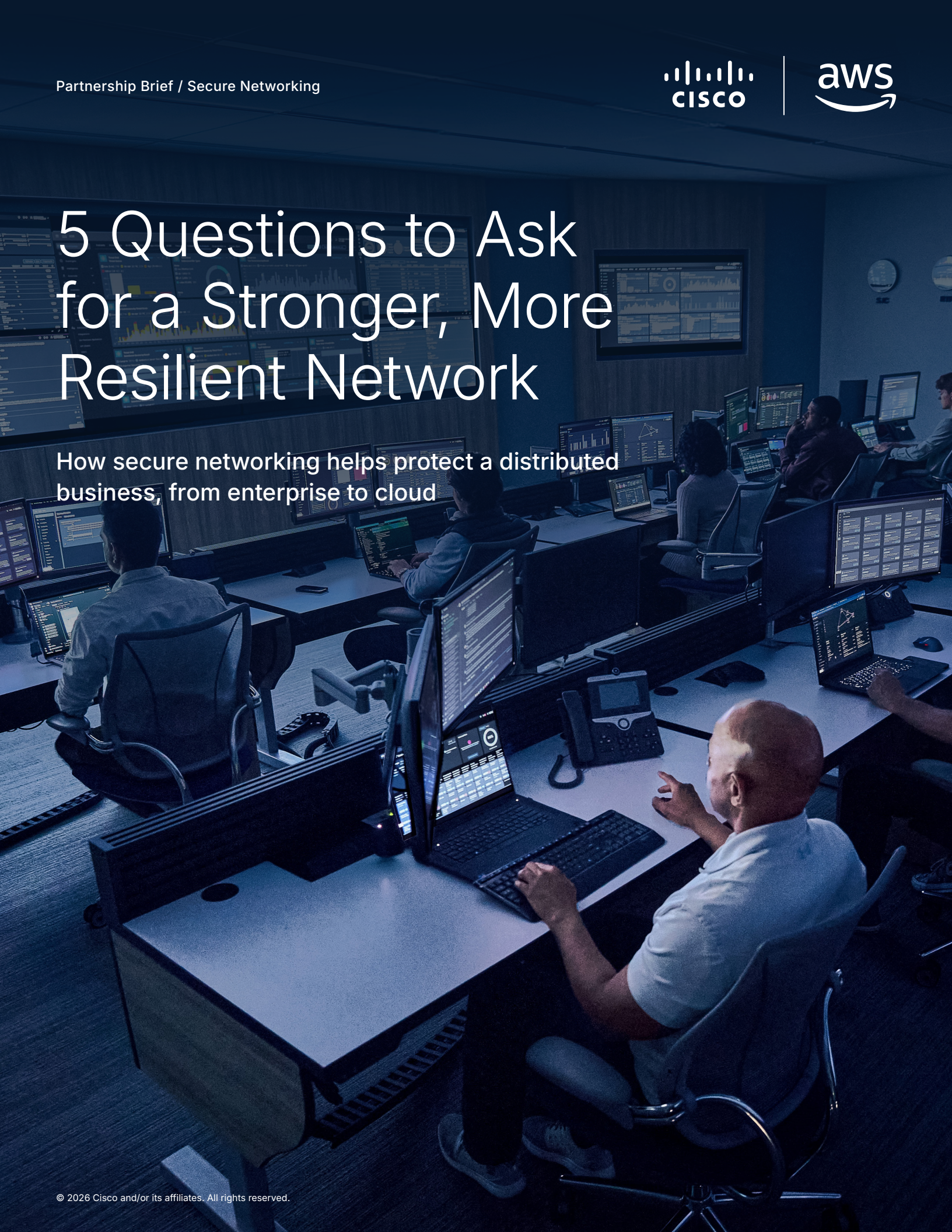
5 Questions to Ask for a Stronger, More Resilient Network

How secure networking helps protect a distributed business, from enterprise to cloud



© 2026 Cisco and/or its affiliates. All rights reserved.

Your network already goes everywhere your business does.

It connects people to applications, branches and data centers to the cloud, workloads to data, and devices and AI agents to the many far-flung resources they need. Your network keeps information moving and experiences running across an increasingly distributed business.

All of that depends on connections you can trust. And because your network is already carrying the business, it's also one of the most powerful places to protect it.

Secure networking recognizes that security isn't separate from the network's job—it's part of how a resilient network does its job. Rather than add defenses after the fact, you can fuse security in, making it an inherent part of how your network operates: verifying who and what connects, applying policy wherever traffic flows, containing threats before they spread, and giving teams the context to see what's happening and act quickly when something goes wrong.

Cisco and Amazon Web Services (AWS) bring that idea to life from core to cloud, making security part of the foundation everything else depends on. The result is a network better prepared for anything you need it to do next.

Keeping your business connected and protected raises some important questions. Here's how Cisco and AWS help answer five of the biggest:

1. **How do I protect users, applications, and data when they're everywhere?**
2. **How do I keep the network ready for everything our business asks of it?**
3. **How can I keep security and policy consistent across enterprise and cloud?**
4. **How do I stop a compromise from spreading?**
5. **How do I know what's happening across my environment and where I need to act?**

© 2026 Cisco and/or its affiliates. All rights reserved.

How do I protect users, applications, and data when they're everywhere?

The traditional perimeter was built for a world where users, applications, and data lived exclusively within the enterprise. Today's world looks a lot different: Work happens across branches, remote locations, devices, SaaS applications, data centers, and cloud environments. Protecting it all can feel like a tall order.

But keeping security consistent across all those connections comes down to a simple idea: Set the standard, enforce it wherever your business operates, and verify continuously.

That starts with changing what determines trust. Instead of assuming something or someone is safe simply because of where they connect, Zero Trust uses identity and context to dynamically determine who and what should have access to which resources, and under what conditions. (Increasingly, those identities include AI agents—more on them later.)

Cisco and AWS help put that model to work across enterprise and cloud, so the expectations don't change from one environment to the next. Cisco SASE (secure access service edge) helps make this practical across a distributed business by bringing networking and security together to protect access wherever the users and applications are. AWS identity and networking controls help apply the same principles to applications, workloads, and data across your AWS environments. The result: consistent security policy, enforced wherever your business goes.

Taken together, that means more flexibility to put people, apps, and workloads where they make the most sense. Security becomes something that can scale with the business instead of something that has to be built around it.

How does SASE help?

SASE is a prime example of networking and security working together. It combines the job of connecting users to applications with the job of protecting those connections. Because security is cloud-delivered in this model, inspection and enforcement can happen closer to where users connect and applications live. That means traffic can take a more direct route when it makes sense, rather than requiring a detour just to pass through security controls.

For a distributed business, that can mean faster, simpler access while still applying the protections each connection needs.

Industry recognition

Cisco was named a Leader in the 2026 IDC MarketScape for Worldwide SASE.[1] IDC cited strengths including architectural flexibility, identity integration, AI capabilities, and threat visibility.

[1]IDC MarketScape: Worldwide Secure Access Service Edge 2026 Vendor Assessment, July 2026

© 2026 Cisco and/or its affiliates. All rights reserved.

How do I keep the network ready for everything our business asks of it?

The network has always been a place where business ambition meets operational reality. AI is the latest example: 75% of organizations say they're more confident in their AI strategy than in their network's ability to deliver it.[2] In fact, AI has already driven a 34% increase in network traffic, and organizations broadly deploying AI expect traffic to triple within three years.

Meeting that kind of demand will take more than capacity. Whether a business is scaling AI or just scaling up, the network has to keep up without compromising security or resilience. And the more the business asks of its network, the more important those qualities become.

This calls for a network that can adapt as your business does. Cisco and AWS bring together deep networking expertise and global infrastructure to create a secure, resilient foundation across enterprise and cloud. Cisco SD-WAN integrates with AWS Cloud WAN and AWS Transit Gateway, connecting campus, branch, and data center environments with applications and workloads on AWS. As conditions and demands change, connectivity can adapt to help keep applications and critical operations running smoothly.

Whatever comes next—AI-powered or otherwise—that foundation gives your business more room to move.

[2]Cisco and Foundry, "No time to wait: The accelerating impact of AI on campus and branch networks," June 2026

450%

more network traffic can be generated when a task is performed by an AI agent rather than a human[3]

[3]Cisco, "The Impact of AI on Wide Area Network Traffic," May 2026

What about post-quantum security?

Network readiness also means preparing for emerging security requirements. Powerful quantum computers could eventually break some of the encryption methods widely used today. Because sensitive data can be captured now and stored for future decryption, organizations with long-lived data need to act before that capability arrives. Post-quantum cryptography (PQC) uses new cryptographic standards designed to withstand these attacks.

Cisco and AWS are already putting PQC into practice, with support continuing to expand across their portfolios. Examples include:

- **Cisco:** Cisco 8000 Series Secure Routers
- **AWS:** Amazon CloudFront, AWS Identity and Access Management, AWS Key Management Service, Amazon S3

© 2026 Cisco and/or its affiliates. All rights reserved.

How can I keep security and policy consistent across enterprise and cloud?

Security policy only works if it holds up everywhere your business operates.

But when each of those places comes with separate controls and management points, keeping protections aligned becomes a job of its own. A policy change in one place may not make it to another. Adding new environments can mean still more rules to configure. And every new control is something else to monitor and maintain.

Fusing security into the network helps simplify the job. Instead of relying on separate security checkpoints for each environment, your business can apply policy across the places traffic already moves. That means security can be enforced where it's needed, without requiring teams to manage every enforcement point as a separate operation.

Here's what a distributed layer of defense looks like in action: Cisco Hybrid Mesh Firewall extends firewall enforcement across enterprise and AWS environments. Unified management helps teams keep policy aligned across those enforcement points. Within AWS, AWS Network Firewall protects traffic across cloud environments, and AWS Firewall Manager helps govern those protections across virtual private clouds (VPCs) and accounts. The protections may live in different places, but teams can still manage them as part of a coordinated security approach.

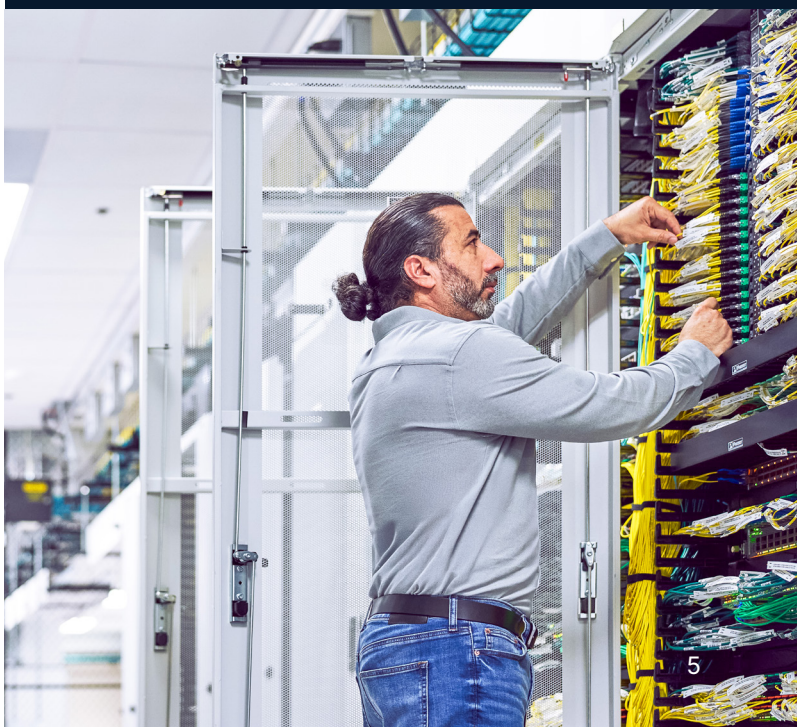
That coordination matters as your environment expands. Instead of starting from scratch with every new location or workload, you can extend protections consistently without multiplying the work of managing them.

Distributed enforcement's next test: AI agents

AI agents cover a lot of ground in a hurry. To complete a single task, an agent might move between applications and tools, call APIs, access sensitive data, and take actions across different environments, all at machine speed.

That makes strong safeguards essential throughout the agent's journey. Zero Trust and least-privilege policies help determine what an agent should be allowed to access and do, while guardrails set boundaries around its actions. Distributed enforcement helps make those rules stick wherever the agent operates, limiting its reach and containing its activity when needed.

The more autonomy you give agents, the more important it becomes to make sure your security policies can keep up.



© 2026 Cisco and/or its affiliates. All rights reserved.

How do I stop a compromise from spreading?

The reality is that no defense is perfect. When something does get through, what matters next is how far it can go. An attacker who gains a foothold in an on-premises workload may try their luck tapping sensitive data in the cloud. An AI agent that falls into the wrong hands may have permission to access a host of apps, systems, and data sources.

However it starts, this kind of lateral movement can turn one compromised resource into a much bigger problem—particularly in a distributed environment.

Segmentation seals off those paths instead of leaving an open landscape for threats to roam. Identity-aware controls make that containment more precise, limiting access based on who or what is connecting and what it should be able to reach. And with distributed enforcement, there are more chances to stop a threat in its tracks.

Cisco Hybrid Mesh Firewall extends enforcement across enterprise and AWS environments, so suspicious activity can be contained closer to where it happens. Within AWS, virtual private cloud segmentation provides another line of defense, restricting which cloud resources can communicate with one another and where a threat can go next.

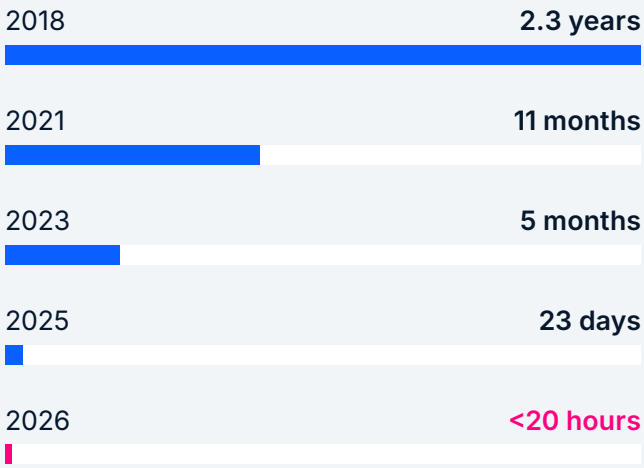
Together, these capabilities stack the odds in your favor: containing threats earlier, limiting the blast radius, and keeping the rest of your business moving.



The fast-moving case for containment

Attackers are exploiting vulnerabilities faster than ever. That makes limiting what happens after a compromise even more critical.

Average time from vulnerability disclosure to confirmed exploitation:[4]



[4]Zero Day Clock (zerodayclock.com), based on 3,529 CVE-exploit pairs from CISA KEV, VulnCheck KEV, and XDB

© 2026 Cisco and/or its affiliates. All rights reserved.

How do I know what's happening across my environment and where I need to act?

Troubleshooting a distributed environment can feel like detective work, with clues scattered across networks, cloud services, applications, and user experiences. Each team has a few pieces of evidence, but no one sees the whole picture amid the flood of alerts.

The key lies in connecting those clues. But identifying likely root causes, spotting potential security risks, and seeing what's actually affected is only half the job. Teams also need to know where to act, what to do next, and whether their actions truly fixed the problem.

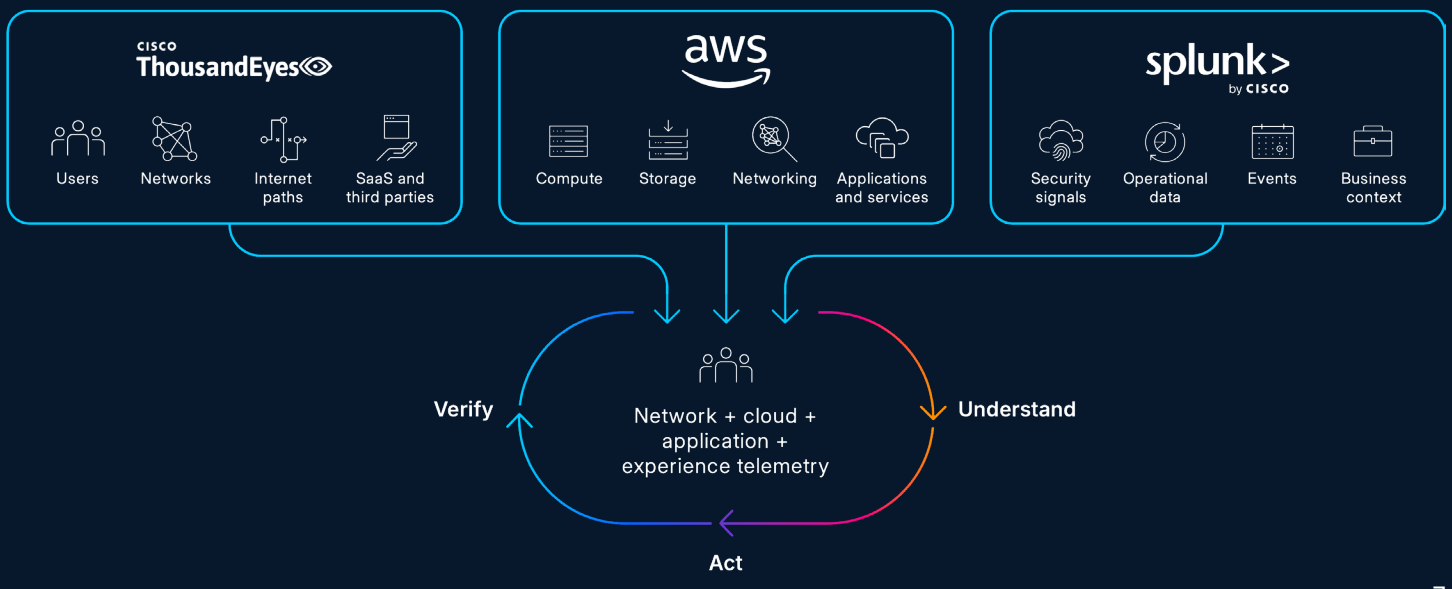
Cisco and AWS help bring the fuller picture into focus. Cisco ThousandEyes provides visibility into network paths and digital experiences, including connections beyond your own infrastructure. Splunk adds broader operational and security context, while AWS telemetry provides insights into the health, performance, and activity of cloud resources and services. These capabilities help teams connect the dots across enterprise and cloud, so they can spend less time searching for answers.

And NetOps and SecOps teams don't have to put those insights to work alone. Cisco Cloud Control brings AI agents into the mix through AgenticOps, helping teams zero in on issues, determine what to do, and act within established guardrails. Agents can also verify the results, feeding them back into a continuous cycle of monitoring, action, and assurance. Each finding sharpens the picture, helping teams weed out anomalies and focus on keeping their environments secure and performing at their best.

4,100

monitoring alerts and events are generated by the average organization every day, about half of which are network-related[5]

[5]Cisco, "Cisco AI Research: AgenticOps Scaling Quickly in the Enterprise," September 2026



© 2026 Cisco and/or its affiliates. All rights reserved.

Protection that goes wherever your business does

Your network connects everything your business depends on. But there's little value in all that connectivity if you can't protect what moves across it. Likewise, there's little value in security that gets in the way of what your business needs to do.

Connectivity and protection aren't separate ambitions anymore. They're two parts of the same job.

Cisco and AWS help put that approach to work across enterprise and cloud, making security part of how the network operates. You can build on familiar Cisco networking and security capabilities, extend protections and visibility into AWS environments, and use automation to take some of the manual work out of keeping everything running securely. The result is more room to connect, scale, and innovate without adding a new layer of complexity at every turn.



Trust the infrastructure: Build a secure, resilient foundation that keeps critical operations running across enterprise and cloud



Protect every flow: Apply consistent, identity-aware security to protect connections and contain threats wherever traffic moves



Assure every experience: Connect insight to action to resolve issues faster and keep applications, networks, and experiences performing at their best

See business value sooner

Cisco and AWS also help simplify the operational side of secure networking, from deployment and management to procurement and billing. Explore Cisco networking and security solutions on AWS Marketplace.

And learn more about our partnership at cisco.com/go/aws.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)