From the Inside Out: Cisco IT's Path to Zero Trust Security

Industry:
Information Technology

Location:
San Jose, California

Organization:
- $270 billion global enterprise
- Workforce of 123,000 employees and contractors
- Operations in 300+ offices across 80+ countries

Cisco is a $270 billion global enterprise with 123,000 employees and contractors working across 300+ offices in over 80 countries. Cisco IT is the team responsible for enabling productivity, securing users, and deploying technology across the entire global organization.

"Cisco IT's goal has been to make the user authentication experience as transparent as possible – so easy that users are only prompted to authenticate when necessary. With the ZTNA capabilities of Secure Access, protecting user-to-app connectivity – whether they're in the office, at home, on the road, or in the air – has never been more straightforward."

– Rich West,
Principal Engineer, Security and Trust Organization

Architecting for Business Agility in a Complex IT Landscape

Organizations have never been more focused on finding simpler, more secure solutions to protect increasingly complex IT environments. Cisco IT is no exception. The team is responsible for securing users and deploying technology across the global organization. Like most large enterprises, Cisco IT had to adapt to the growing trend of a hyper-distributed workforce while maintaining strong security across that landscape. But supporting the shift wasn't easy; the team was working in an environment defined by extraordinary scale and complexity, including:

- 123,000 employees and contractors working across 300+ offices in over 80 countries
- 125,000 endpoints, evenly split among macOS, iOS, and Windows
- 140,000 mobile-class endpoints, primarily Apple iOS with a small percentage of Android
- 27,000 Cisco video devices
- Roughly one million IP connected things
- Continuous acquisitions – 13 between 2023 and 2025

Legacy system falls short for a zero trust world

For more than a decade, Cisco IT built and maintained a custom global system that combined networking and security – paving the way for what's now known as Secure Access Service Edge (SASE). The goal was to deliver strong security and a smooth user experience in a highly distributed environment. While the system met many early needs, it was complex, resource-intensive, and eventually couldn't keep up with Cisco's evolving workforce needs and zero trust strategy.

Challenges included:

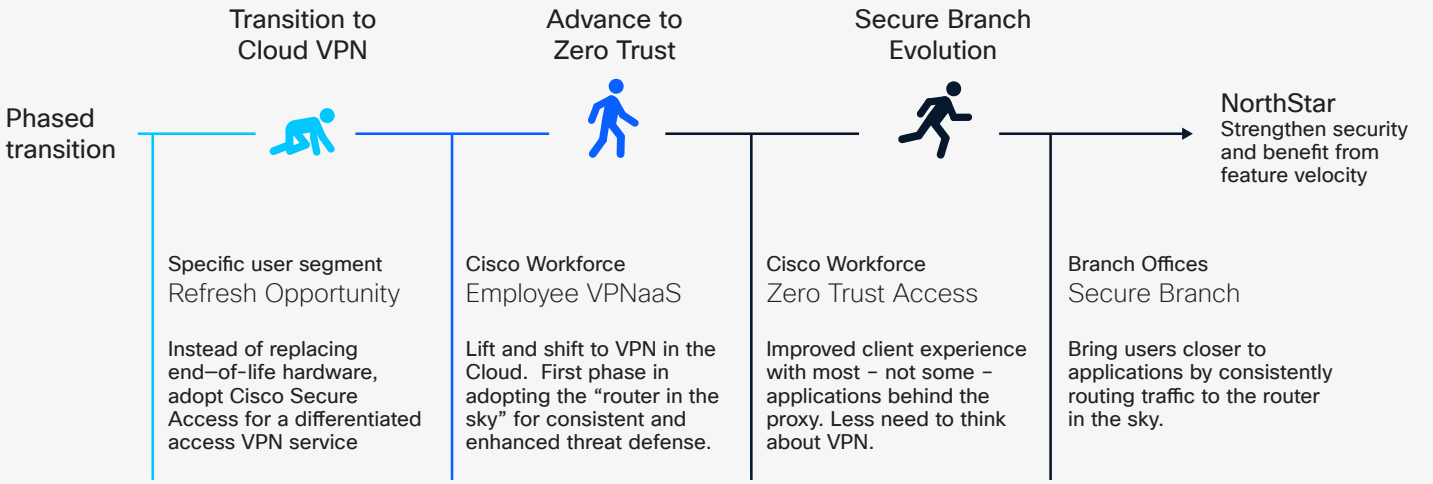
- Ensuring consistent, least-privileged user access across remote, branch, and campus environments
- Managing both managed and unmanaged devices, including IoT and OT systems without leaving the attack surface exposed
- Delivering secure access without compromising performance, especially on low-bandwidth networks
- Controlling where highly sensitive data is stored at scale, across the global environment to ensure policy management and compliance

Frictionless, Flexible, Future-Ready: Cisco IT Chooses Secure Access

Cisco IT sought a new solution to simplify IT operations, provide a seamless experience for users, streamline threat detection and mitigation, and adapt to business demands quickly. The driving force was achieving Cisco IT's "North Star" vision: centralizing traffic through the cloud, applying consistent security policies, and unifying policy management under a zero trust model.

Cisco IT partnered with the Cisco Secure Access product team to ensure the solution would address critical business challenges, as is standard when adopting Cisco's own technologies. By acting as a development partner and validating our products internally, Cisco IT gives customers confidence that these solutions can help achieve their business objectives. Specifically, Cisco IT validated that Secure Access offered a breadth of connection options, a single agent for connectivity and visibility, a better user experience, and the ability to enforce least privileged access. A variety of factors drove the decision to move forward with Cisco Secure Access, including these anticipated outcomes:

- **A better, low friction user experience:** Users can just sign on and get to work, regardless of where they are working.
- **Increased consistency:** Uniform security policies are applied across a diverse set of users and locations.
- **More effective use of IT resources:** Cisco IT can spend less time building and operating custom capabilities and more time leveraging advanced functionality.
- **Increased velocity of new features and innovation:** New capabilities and fixes can be deployed quickly, unburdened by hardware updates or patch windows.
- **Completeness of vision:** The roadmap is robust, function-rich, and unique in the industry.



A Phased Rollout Across People, Places, and Platforms

Cisco IT partnered with the Secure Access engineering team to identify must-have features required to scale and align with their zero trust approach. Secure Access's cloud-native model has enabled the teams to quickly develop and roll out new capabilities and fixes, which also benefits Cisco customers using the Secure Access solution.

Cisco IT has rolled out Secure Access in strategic phases, incrementally securing additional groups of users and iteratively implementing more functionality.

VPNaaS migration

The team has migrated the entire Cisco workforce from on-premises VPNs to VPN-as-a-Service (VPNaaS), "Since we no longer needed to replace end-of-life VPN appliances and could refocus efforts on adopting new technology, we saved IT the time it would've spent managing those appliances," said Jennifer Huber, Program Manager, Network Engineering and Operations, Cisco.

Universal ZTNA adoption

Cisco IT is currently transitioning remote users from traditional ZTNA to Cisco's Universal ZTNA, enabling more robust, granular, and high-performance least-privilege access through a simpler, faster approach.

GenAI protection

There are both risks and rewards when it comes to GenAI innovation. It's essential to identify and monitor the way in which workers leverage GenAI: is it an approved application? Are users aware of the risks that surround these tools? Cisco IT has prioritized user training and education on how to use GenAI safely and securely, reminding them of their obligations to protect sensitive data while augmenting their productivity – consistent with Cisco's Corporate Code of Conduct.

For example, Cisco IT is piloting a solution to enable deeper visibility into end user GenAI usage patterns and displaying user warning pages when a user connects to a GenAI site. As soon as the user starts engaging with the app, in-depth prompt and response data monitoring begins in Cisco Secure Access. This work will allow the team to monitor how employees are engaging with GenAI tools and identify potential risks. A second phase will focus on deeper enforcement through data loss prevention (DLP) policies specific to AI Access, a built-in integration with Cisco AI Defense.

A Modern Solution Meets Modern Demands

Since implementing Secure Access, Cisco has realized significant improvements in security, performance, compliance, and user experience.

> "By centralizing telemetry and data, Cisco Secure Access streamlines incident management, eliminating the need for teams to analyze multiple networking and security data analytics platforms and streamlining incident management – reducing mean time to troubleshoot by up to 25%."
>
> – Rich West,
> Principal Engineer, Security and Trust Organization

> "Imagine the complexity of expanding your business into new regions or moving to a different colocation facility for your VPN, branch, and internet edge. Cisco Secure Access transforms cloud edge expansion from a logistical marathon into a sprint, slashing setup times from months to mere hours."
>
> – Jon Woolwine,
> Director, Network Engineering and Operations

Unified data for faster incident resolution

By centralizing telemetry and data, Cisco Secure Access streamlines incident management, eliminating the need for teams to struggle with aggregating disparate networking and security data from multiple systems and streamlining incident management. "We've seen reductions in mean time to troubleshoot by up to 25%," said West.

Simplified policies. Stronger security.

"Previously, securing access to internal apps required maintaining several hundred individual policy lines, each tailored to specific users, applications, or scenarios," said Roel Bernaerts, Principal Engineer, Cisco. "With Secure Access, that number has dropped to just around 30 policies, easing the burden of administration, accelerating onboarding, and delivering stronger security across the organization."

Faster, seamless edge deployments

As Cisco's business has grown, IT has faced ongoing challenges managing the network and security complexities of scaling VPNs, branch connectivity, and internet edge infrastructure. By providing cloud-delivered security and networking capabilities through a unified platform, Secure Access is enabling faster, more agile and consistent expansion, without compromising on control or visibility.

"Imagine the complexity of expanding your business into new regions or moving to a different colocation facility for your VPN, branch and internet edge. Cisco Secure Access transforms cloud edge expansion from a logistical marathon into a sprint, slashing setup times from months to mere hours," explains Jon Woolwine, Director, Network Engineering and Operations, Cisco.

Deeper insights for smarter AI governance

By routing traffic through Secure Access, Cisco has significantly improved visibility into how employees are interacting with AI applications on the internet. "We can easily see who is using which AI tools, when they accessed them, how often, and how much data was transferred," explains Bernaerts. With this granular level of insight, the team can quickly respond to executive concerns about new or emerging AI apps with detailed AI usage patterns.

Unlocking Power Through Cisco Integrations

The IT group has integrated Cisco Secure Access with other core Cisco technologies, unlocking powerful synergies, boosting security, simplifying operations, and reducing user friction. Together, these solutions are delivering measurable improvements in visibility, control, and productivity.

Passwordless, frictionless, secure login at scale

Integrating Cisco Secure Access with Cisco Duo Risk-Based Authentication (RBA) and Duo Passport has enabled Cisco IT to deliver adaptive, passwordless authentication, reducing login friction, and enforcing real-time, risk-aware policies while providing a seamless access experience. In June 2025 alone, Cisco recorded 16.3 million total authentications. Thanks to using Cisco Duo:

- 92% of those logins were automatically suppressed, requiring no user login.
- 86% of the remaining interactive logins were completed using passwordless authentication.
- Only 1% of the 16.3 million authentications relied on passwords.
- 99% of all logins were phishing-resistant.

"By using Duo at Cisco, we've achieved both strong security and a great user experience—our satisfaction scores keep rising as our security team gains confidence from our enforcement capabilities." –Sarabjeet Rana, Technical Leader, IT Security, Cisco

Compliance and self-remediation cut risks and costs

Cisco is seeing measurable value from the integration of Secure Access with Cisco Duo's strong multi-factor authentication (MFA) and device trust capabilities. With over 5.76 million device health checks per month, Duo ensures that only secure, compliant devices can access corporate resources – evaluating factors like OS version, disk encryption, and password strength.

"Device health is central to our zero trust approach," explains West. "That device is where we all do much of our work – consuming and generating content, interacting with tools and data. We want to make sure that the device is both IT managed and in a healthy state – and if it's not, we can respond appropriately as a team."

Duo also allows users to self-remediate device issues, like enabling screen locks or updating OS software, without contacting IT. Each month, about 86,000 devices are brought into compliance through user prompts. This self-serve model reduces support tickets, strengthens endpoint security, and contributes to an estimated $3.4 million in annual productivity savings, along with $500,000 in reduced helpdesk costs.

At the same time, Duo enables Cisco IT to offload the burden on trusted users while more securely verifying user trust. In a recent month, 92% of 16.3 million authentications were suppressed – meaning they required no user interaction at all – using Risk-Based Authentication (RBA) to verify trust. Of the remaining logins, 82% were passwordless. "Together, RBA and passwordless authentication made 99% of our logins phishing-resistant," reports Rana.

Identity-driven access for stronger zero trust

To unify identity, access, and network enforcement, Cisco IT integrated Secure Access with the Cisco Identity Services Engine (ISE). The integration provides identity-based access control, dynamic device posture checks, and consistent policy enforcement across all access scenarios to enable a more secure, seamless, and scalable zero trust environment.

Simplified troubleshooting with AI

Integrating Secure Access with Cisco ThousandEyes has significantly mitigated risks and simplified troubleshooting by enabling AI-powered issue detection, remediation, and optimization. For example, Cisco IT can warn users about risks, monitor to prevent data leakage to GenAI tools, and monitor to decide when to block data from AI tools.

Best Practices and Lessons Learned

Throughout the Secure Access rollout, several important best practices and lessons have emerged, many shaped by challenges that required collaboration and creative problem-solving.

1. **Executive commitment is essential.** Because this was a large-scale transformation with impact across the business, strong executive support was critical to align priorities across peer teams.
2. **Cross-team collaboration is non-negotiable.** IT, networking, and security teams had to move beyond traditional silos and take shared ownership of access and security. Even within individual teams, collaboration was key to success.
3. **A mindset shift toward zero trust.** While Cisco was already on a zero trust journey, this project pushed the team to align more deeply with its principles, moving past internal debates to focus on outcomes.
4. **Cloud delivery enables faster iteration**. Not every feature Cisco IT wanted was available on day one, but Secure Access's cloud-native model allowed fixes and new capabilities to roll out quickly – far faster than the legacy approach.
5. **Centralized visibility accelerates troubleshooting.** Secure Access improved the team's ability to detect and resolve issues by providing unified visibility across users, devices, and connections.
6. **Progress with flexibility wins user trust.** To ease adoption, Cisco IT rolled out changes gradually and allowed users to opt in. This approach addressed early concerns about disruption and built confidence along the way.

A Foundation for the Future of Work

With the successful global rollout of Secure Access, Cisco IT is demonstrating what's possible when security, scale, and user experience align. The team has not only improved the company's overall security posture, but also built the agility needed to support a global, ever-evolving workforce. With Secure Access and strategic integrations in place, Cisco IT is equipped to meet the future – empowering work without limits and security without compromise.