

From Legacy VPN to Cloud-First Security: How TKC has Strengthened Protection and Reduced Complexity



Industry:

Information and
Communications

Location:

Tochigi, Japan

Organization:

2,428 employees

Solution:

Cisco Secure Access

TKC Corporation delivers cloud services to over 10,000 tax professionals, their affiliated companies, mid-sized and large enterprises, and local governments – helping them drive profitability, ensure fair returns, and streamline operations. For decades, TKC has supported the growth of Japan’s economy by empowering small and medium-sized businesses. Today, in addition to its established data center operations, TKC develops and delivers innovative cloud-based solutions that enable customers to stay ahead in a rapidly evolving digital landscape.

Two years ago, TKC Corporation faced a critical turning point when they learned their decade-old VPN infrastructure would no longer be supported by the manufacturer. The IT team had only five months to find a secure, reliable replacement.

TKC had already been laying the groundwork for a zero-trust security model, and the team was actively exploring SSL-VPN options to support secure internal communications across Microsoft 365 and Azure. But they faced multiple roadblocks – especially given the sensitive nature of their work with tax professionals and local governments, where confidentiality is paramount.

- **Complex Transition:** Their existing VPN environment served more than 2,800 users across TKC and its group companies, making any transition challenging.
- **Aging System, Rising Costs:** The system itself was struggling to meet modern demands. Certificate renewals and hardware upgrades were becoming increasingly expensive. And planning, proposals, budget allocation, maintenance, and testing efforts all required substantial internal resources.
- **Network Demand Exceeds Capacity:** Surging network traffic – particularly during the pandemic – outpaced their centralized infrastructure, and TKC had to invest significantly in capacity upgrades just to maintain performance.

“With the limited timeframe before our VPN service sunset, Cisco Secure Access proved to be the ideal solution for a replacement.”



– Naoki Kanamori,
Director Corporate Management Division,
TKC Corporation

A Cloud-First Shift with Cisco Secure Access

With the clock ticking on their legacy VPN infrastructure, TKC needed a modern solution that could deliver stronger security with less complexity. “Cisco helped us realize that just having a VPN in place wasn’t enough anymore – it could actually increase our risk,” said Naoki Kanamori, Security Advisor for IT Investment Planning, Corporate Management Division, TKC Corporation. “They showed us how moving to the cloud could reduce both operational overhead and costs. After a lot of internal discussion, we agreed that Cisco Secure Access was the right choice to meet our needs within a tight timeline.”

The decision aligned well with TKC’s broader strategy of embracing the cloud. With little time to spare, the transition moved quickly and was completed within a few months. Working closely with Cisco and its implementation partner, TKC completed the full migration within their required timeframe, retiring the legacy VPN hardware in the process. “Gone are the days of complex processes like appliance procurement, site planning, and complex deployments. Being able to launch quickly made the benefits of cloud deployment – like using a cloud-based VPNaaS vs. an on-premises VPN – very tangible for us,” said Hiroyo Ichikawa, Director of IT Investment Planning, TKC Corporation.

Today, Cisco Secure Access serves as the foundation of TKC’s secure remote access strategy, simplifying IT operations through a single, cloud-managed console, unified client, centralized policy creation, and aggregated reporting. Offering extensive security capabilities, Secure Access helps TKC mitigate security risk by applying zero trust principles and enforcing granular security policies.

The cloud-based solution delivers the core capabilities of a Secure Service Edge (SSE) platform combined with Cisco’s SD-WAN to enable a scalable, best-of-breed SASE architecture. Its client-based Zero Trust Network Access (ZTNA) approach supports VPN-as-a-Service (VPNaaS) for use cases like peer-to-peer or server-initiated communication – scenarios where traditional ZTNA can fall short.

Kanamori admits that the shift to a cloud-first architecture required a mindset change. “It took time and effort to rethink traditional architectures through a cloud-first lens. We worked closely with Cisco and their implementation vendor to define the system design. For example, instead of relying on physical hardware for redundancy, Cisco Secure Access gave us logical redundancy through VPN profile functionality. It was a learning curve, but Cisco and their implementation partner helped us to fully understand the entire process.”

“Gone are the days of complex processes like appliance procurement, site planning, and complex deployments. Being able to launch quickly made the benefits of cloud deployment – like using a cloud-based VPNaaS vs. an on-premises VPN – very tangible for us.”



– Hiroyo Ichikawa,
Director of IT Investment Planning,
TKC Corporation

Stronger Security, Simpler Management, and Lower Costs

The switch to Cisco Secure Access has delivered real, measurable benefits for TKC.

Cutting Traffic - and Complexity - in Half: “With Cisco Secure Access, we now have clear visibility into our VPN traffic, all from a single cloud-based console,” said Kanamori. “Before, we needed dedicated agents just to monitor what was happening. We assumed most of our traffic was internal, but we discovered many connections were internet-facing. By auditing our network paths, we reduced traffic by 50%, which led to improved performance.”

Smarter Control, Without the Hassle: “Previously, making even minor changes to our old VPN required us to go through our vendor, which cost us both time and money,” Ichikawa explained. “Now, with the cloud-based model, our administrators can manage everything directly in the Cisco Secure Access console. We can now enhance security at a granular level - quickly update policies, monitor user activity, and even set rules by individual or department.”

Eliminating Outages and Reducing Costs: “We used to deal with multiple outages every year - along with a constant stream of updates and emergency fixes to address VPN vulnerabilities,” said Ichikawa. “With Secure Access, we have strengthened our security, significantly reduced costs, and our IT team is freed up to focus on more proactive and strategic projects that align with our executive goals.”

Looking Ahead: Building a Unified, Future-Ready Security Platform

Kanamori says TKC plans to consolidate around Cisco Secure Access and move toward a complete SASE framework. The company will transition its existing Cisco Umbrella Secure Internet Gateway (SIG) capabilities to Secure Access given the solution includes the same Umbrella features they were using in addition to other security controls like ZTNA. “By unifying our security operations in a single platform, we’ll be able to boost efficiency, respond faster to critical incidents, and simplify user operations while strengthening security and improving overall usability.”

Kanamori says they plan to leverage what they’ve learned internally to benefit their own clients. “As cyber threats continue to evolve, traditional security measures are no longer enough to safeguard our organization and our clients. We hope to apply the knowledge gained through our own implementation to enhance the services we provide to customers. We look forward to Cisco’s continued support and the delivery of even more effective, efficient solutions moving ahead.”

Explore Cisco Secure Access demos and webinars

Check out our demos, walk-through videos, and webinars to learn how to connect and protect users from anywhere they work, and how to simplify and centralize security operations.

[Watch a demo](#)