CASE STUDY

Sanmina Revs Up Security, Profitability, and M&A Strategies with Zero Trust for Users and Workloads

Sanmina is a leading integrated manufacturing solutions provider serving the fastest-growing segments of the global Electronics Manufacturing Services (EMS) market. A recognized technology leader, the Fortune 500 enterprise provides end-to-end manufacturing solutions, delivering superior quality and support to Original Equipment Manufacturers (OEMs) across multiple sectors.

VPNs hinder digital transformation

During its ongoing cloud transformation to support advanced Industry 4.0 manufacturing practices, Sanmina confronted a data security challenge.

"We'd already adopted zero trust principles and had started to re-architect our systems," explained Matt Ramberg, Vice President of Information Security at Sanmina. "But we realized we couldn't achieve zero trust using traditional virtual private network [VPN] technology. We needed an access solution appropriate for a modern, perimeter-less world."

Adopting ZPA addresses the zero trust need

A respected global electronics manufacturer, Sanmina focuses on delivering excellence in performance, flexibility, and technology that exceeds customer expectations for industrial, medical, defense and aerospace, automotive, communications networks, and cloud solution OEMs in 20 countries on six continents.

Like many enterprises, Sanmina's workforce of more than 35,000 was increasingly mobile and remote, particularly in the wake of COVID-19, making zero trust access imperative.

"On any given day, we have several thousand people working remotely and they need to access tens of thousands of assets," Ramberg said. "Using VPNs was an outdated practice that actually increased cybersecurity risks by creating attack surfaces."

CHALLENGE

Replace outdated VPN technology with an AI-powered zero trust solution to reduce attack surfaces and secure application access

SOLUTION

- Zscaler Private Access™ (ZPA™)
- Zscaler Internet Access (ZIA)
- Zscaler™ Zero Trust Exchange™

OUTCOMES

- Eliminated attack surfaces and mitigated risk by replacing traditional VPN and web gateway technology with an AI-powered zero trust platform
- Delivered high-performance private and public application access that significantly improved user experiences
- Improved M&A processes to support strategic growth initiatives
- Reduced security updates from days to a few minutes
- Gained a scalable, expandable platform for continued security innovation in a modern, perimeterless world

After evaluating multiple options, Sanmina decided to expand its **Zscaler Zero Trust Exchange** platform capabilities by adopting **Zscaler Private Access (ZPA)**.

"Our due diligence revealed that Zscaler's global presence, with data centers worldwide, made ZPA the most resilient choice," said Manesh Patel, CIO for Sanmina.

Easily making users and devices invisible to threats

A fundamental building block of the Zero Trust Exchange, ZPA connects users and devices with applications, rather than connecting them to the network. Unlike VPNs, which create back doors allowing threats to enter, ZPA makes users and applications invisible to external threats and also prevents lateral threat movement by enabling enterprises to limit user access based on the applications they need.

When a user attempts to access an application, identity and device posture are verified using Zscaler Client Connector software installed on the end user device. To enable access to private applications, whether on site or in a cloud environment, Zscaler App Connector is installed at an application's location. App Connector is a lightweight virtual machine (VM) that brokers the secure connection between private applications and the Zscaler Zero Trust Exchange.

In Sanmina's case, Client Connector was already deployed as it's also the enabling agent for the company's previous adoption of **Zscaler Internet Access (ZIA)**. The inaugural component of the Zero Trust Exchange, ZIA protects users and devices accessing the internet and cloud-delivered SaaS applications, including the Sanmina-developed **42Q** cloud manufacturing execution system (MES) that is well-regarded in the industry.

"Like ZIA, deploying ZPA was very easy—especially compared to traditional VPNs—and enabled us to implement a least-privileged access model," Ramberg said. "We set up policies for accessing applications within the solution and then added users to each policy, based on their job requirements."

Fully inspecting encrypted traffic advances protection

Sanmina was also concerned that their VPNs were not protecting them from threats embedded within encrypted traffic. Using ZPA, they can fully inspect all encrypted traffic between users and applications, as well as protect internal applications against security vulnerabilities.

"Whether it's enabling remote access or spotting potentially malicious activity, ZPA helps save us time and headaches," Ramberg said. "It's easy having visibility and control we need in a single place as there is no context-switching."

> "With the Zero Trust Exchange platform, employees experience high-performance access and the company considerably enhances data security. That's a win-win for our entire enterprise."
>
> **– Matt Ramberg**
> Vice President of Information Security
> **Sanmina Corporation**

Better experiences and less complexity boosts profitability

According to Ramberg, the returns on Sanmina's Zero Trust Exchange investments have quickly added up. "We've received overwhelmingly positive feedback from business users," he said. "Unlike legacy appliances, which bogged down device performance and required authenticating multiple times a day, users report experiencing fast, seamless, high-performance access for both private and public applications."

From the company's perspective, Sanmina has considerably enhanced its security posture. "It's a win-win for our entire enterprise," Ramberg said.

In addition, deploying ZPA enables Sanmina to safely extend private application access to external constituencies. "We can grant access to customers, suppliers, vendors, contractors, and anyone who needs access to Sanmina resources without their devices touching our network," Patel said. "They gain the access they need while we maintain security. It's tremendous."

Further, IT administration expenses are considerably reduced compared with acquiring, configuring, managing, and updating traditional VPNs and web gateways. "We had multiple physical appliances spread across the globe, each of them requiring their own configurations, rules, patches, updates, and maintenance contracts," Ramberg said.

"With the Zero Trust Exchange we've eliminated physical appliances and their related pain points, which reduces complexity and contributes to profitability," he continued. "Now, we can swiftly and easily make changes that instantaneously flow to every facility globally. What once took us hours, or days, to complete across all of our locations now takes less than five minutes."

Exceptional Industry 4.0 security IT/OT on shop floors

As an industry pioneer in deploying Industry 4.0 practices and Industrial IoT (IIoT), Sanmina also applies its Zero Trust Exchange platform to protecting its manufacturing technologies. This includes 42Q as well as leading solutions for enterprise resource planning (ERP) and product lifecycle management (PLM).

"Our ZIA deployment uses policy-based routing that ensures virtually every plant-level web application traverses the Zero Trust Exchange platform prior to accessing the internet," Ramberg said. "We're also using the Zero Trust Exchange to protect IT/OT environments at our manufacturing facilities."

> "ZPA improved our M&A security posture and increased our agility as well."
>
> – **Manesh Patel**
> CIO
> **Sanmina**

Expediting M&A processes for greater agility

From a strategic growth perspective, Sanmina appreciates the role ZPA plays in upping its M&A game.

In the past, VPN technology forced Sanmina to place acquired users directly onto its corporate network to give them complete application access. "That was a scary proposition because we wouldn't know whether their security solutions were properly updated or even sufficiently robust enough to meet our specifications," Ramberg said.

Using ZPA, Sanmina can create policy groups for each acquired company and limit its users to only accessing the resources within a specific group. "ZPA was instrumental in assisting us with two recent acquisitions," Ramberg said. For each acquired company, the process of creating policy groups and deploying ZPA to all users was less than an hour.

"In other words, ZPA not only improved our M&A security posture but it increased our agility as well," Patel said.

Deterring industry ransomware attacks

Creating a holistic zero trust environment by combining ZIA and ZPA is also netting significant risk reduction benefits.

For example, industry peers recently have been plagued by ransomware that the Zero Trust Exchange platform has helped Sanmina prevent. "In our industry, one characteristic of recent attacks is that the malware communicates with a newly-created URL," Ramberg explained.

"Zscaler enables blocking newly-created URLs by default and, had there been an attempt on one of our facilities, our Zero Trust Exchange solution would have alerted us, permitting the infected device to be isolated and quarantined instantly."

Strategic shift creates immeasurable value

By utilizing the AI-powered threat intelligence built into the Zero Trust Exchange, Sanmina can also shift professional resources to higher value projects. "The platform's combination of intelligence and an intuitive management interface allows us to turn day-to-day administration of Zscaler over to our operations teams," Patel said.

"This frees our highly-skilled security professionals to focus on strategic goals rather than tactical tasks," he added. "The value from becoming more strategic is immeasurable."

> "Overall, the benefits of Zscaler have been phenomenal and our experience completely positive. To put it simply: Zscaler's solutions just work."
>
> **– Matt Ramberg**
> Vice President of Information Security
> **Sanmina Corporation**

Workload, visibility, and deception innovations underway

Moving forward, Sanmina plans to continue expanding its Zero Trust Exchange platform. The company recently began adding workloads to the platform by adopting the **Zscaler Workload Posture**, which secures cloud configurations and access permissions across multiclouds. Sanmina is also evaluating **Zscaler Workload Segmentation**, which stops lateral movement of threats to prevent application compromise and data breaches, for enhancing the security of manufacturing processes.

In addition, Sanmina is currently evaluating **Zscaler Digital Experience (ZDX)**, for gathering and analyzing granular telemetry and application performance data to improve user experiences, and **Zscaler Deception**, for proactively detecting threats by populating environments with decoys that are hidden from valid users.

Regardless of how Sanmina evolves its Zscaler platform, the results thus far have been seismic. "Although security has historically been the department of 'n-o,' deploying the Zero Trust Exchange has enabled us to turn that around and become the department of 'k-n-o-w,' Ramberg said. "Overall, the benefits of Zscaler have been phenomenal and our experience completely positive," he added. "To put it simply: Zscaler's solutions just work."

Contributing to net-zero goals

Sanmina's technology leadership extends to partnering with providers like Zscaler that help the manufacturer further its Environmental, Social, and Governance (ESG) goals, including reducing carbon emissions 40% by 2030 and becoming net-zero by 2050. As Zscaler powers its global data centers and offices with **100% renewable energy sources**, the partnership helps Sanmina move closer to its ESG targets while advancing its zero trust journey to protect employees, systems, and data.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com