CASE STUDY

Unified cybersecurity across global operations

Manufacturing services leader, Flex, unified its cybersecurity approach, including 20,000 at-home workers, with Palo Alto Networks Prisma Access and Cortex XSOAR solutions.

IN BRIEF

Customer

Flex

Industry

Manufacturing

Country

United States of America

Featured products

Cortex XSOAR, Prisma Access, Threat Prevention, URL Filtering (PAN-DB), WildFire®

Organization size

2,795

Website

www.flex.com

Challenge

Enable a unified approach to defend against cyberthreats with strong network security and the ability to extend central security policies to remote workers.

Requirements

- Assures consistent security policies on the network and for remote users
- Supports Zero Trust security posture with microsegmentation and content-level identification
- Enables rollout of secure remote access to 20,000 users in seven days with zero downtime
- Automates correlation of threat information for faster investigations and response
- Prevents malware spreading from home users to the corporate network
- Allows vital procurement and logistics work from home to help factories make ventilators during pandemic

Solution

Palo Alto Networks Prisma™ Access secure access service edge (SASE), Cortex™ XSOAR security orchestration and automated response.

Customer overview

Flex is the manufacturing partner of choice that helps a diverse customer base design and build products that improve the world. Through the collective strength of a global workforce across 30 countries and responsible, sustainable operations, Flex delivers technology innovation, supply chain, and manufacturing solutions to diverse industries and end markets.

Summary

Providing manufacturing services for diverse companies across many industries, Flex required advanced cybersecurity not only to protect its own digital assets but also to segment and secure network resources associated with its customers whose products Flex manufactures. The company deployed the Palo Alto Networks network security platform in answer to these requirements. The company also needed to modernize remote access for its global locations accessing regional data centers and cloud services. When the demand for secure remote access became urgent during the global COVID-19 pandemic, Flex enlisted assistance from Palo Alto Networks Diamond Innovator partner, Armature Systems, and rolled out Prisma Access worldwide in seven days, enabling 20,000 employees to securely work from home and support critical business operations without disruption. With Prisma Access, Flex applies consistent security policies across its network and global workforce, preventing malware from spreading either from home users to the network or laterally across the network. This has been crucial for enabling Flex to maintain essential manufacturing services during the pandemic, including retooling factories to make ventilators.

More sophisticated cyberthreats demand more advanced security

For more than 50 years, Flex has provided innovative manufacturing solutions for companies of all sizes, across many diverse industries. While Flex may not be a household name, the company manufactures many of the brand-name products recognized around the world—from consumer and lifestyle products to medical devices, and automotive components to technology infrastructure, for enterprise and industry applications. Flexibility is designed into the Flex business model, and it extends to the company's manufacturing operations in every corner of the world.

Cybersecurity is essential for any business in the digital age, but for Flex, it is especially important to safeguard the data and intellectual property of its diverse customers as well as its own digital assets. For years, Flex relied on traditional firewalls for network security. As cyberthreats became more sophisticated, however, the company recognized the need for next-generation cybersecurity capabilities. This led Flex to Palo Alto Networks.

Flex already had an established relationship with the company as a manufacturer of Palo Alto Networks Next-Generation Firewalls. Having a mix of point products for intrusion detection, URL filtering, and sandboxing, Flex saw an opportunity to consolidate on Palo Alto Networks.

Friedrich (Fritz) Wetschnig, chief information security officer and vice president of enterprise IT at Flex, says, "Primarily, we wanted to use the next-generation firewall capabilities that Palo Alto Networks provides, like content-level identification, because it was necessary for us to get more granular control on our network. The second thing was we saw an opportunity to consolidate from three vendors to one by taking advantage of Palo Alto Networks' platform approach to cybersecurity."

> Prisma Access is simple for the user—that was a tremendous help for us. It's not a big deal for people to use. We were looking for an easy, stable client and the ability to apply centralized security policies. Prisma Access matched all those points. If you can bring up a secure remote access solution for 20,000 people in seven days, I think that shows we made the right choice.
>
> **– Friedrich (Fritz) Wetschnig, Chief Information Security Officer and Vice President of Enterprise IT, Flex**

Microsegmentation provides foundation for zero trust

Flex brought in local trusted network and security partner, Armature Systems, to assist with the initial deployment of the Palo Alto Networks platform and migration from the legacy solutions. As a Diamond Innovator partner with Palo Alto Networks, Armature also had the depth of expertise to then leverage the capabilities of the platform to support Flex's microsegmentation requirements. This was central to securing internal cross-network traffic and isolating network resources associated with each of the customers whose products Flex is manufacturing.

Wetschnig notes, "Microsegmentation is important if you want to prevent attackers from lateral movement across the network. It's the basis for our Zero Trust strategy. Our goal is to make it so, whenever people need to access resources, they can only access them based on certain conditions and with context to know it's legitimate at that point in time."

Modernizing remote access turned critical when COVID-19 hits

Having embraced the Palo Alto Networks platform approach to cybersecurity, Flex also worked with Armature to modernize remote access for the company's global operations. Historically, Flex relied on a traditional hardware-based VPN solution to connect users in its worldwide locations to regional data centers and out to cloud resources and SaaS applications. With growing network traffic pushing the capacity limits of the VPN appliances, Armature recommended the cloud-based Prisma™ Access secure access service edge (SASE) solution for more efficient direct access to the cloud and data centers, with virtually infinite scalability.

The plan had been to roll out Prisma Access after Flex closed its books for the end of the fiscal year at the end of March 2020. However, with news that the COVID-19 pandemic would likely force shutdowns around the world, the company shifted gears to expedite the rollout.

Gus Shahin, Flex's chief information officer, explains, "When we saw the Chinese New Year extend into a lockdown, we felt the pressure. Most of our factories were considered essential and could remain open, but our indirect workforce would need to work from home. These are the people who handle critical aspects of the business, including procurement and logistics. Our financial staff were especially important as we were approaching the fiscal year close. We needed to make sure they had full, uninterrupted access to our financial systems, and it was clear our old VPN solution would not hold up."

The enterprise IT team went into emergency mode. Flex engaged Armature for assistance once again and deployed teams of engineers around the world to deploy Prisma Access, pushing out clients to 20,000 end users and setting up service connections regionally. The team started on a Monday, and by the following Monday, they had Prisma Access turned up and everyone switched over from the old VPN with zero downtime.

Wetschnig recalls, "Our original timeline was to roll out Prisma Access in about six to eight weeks. We ended up doing it in seven days. When the lockdown was announced in China, and the people at our biggest service center needed to work from home, we were prepared."

> At the end of the day, a large part of our business is procurement. Our end users are mostly buyers. How we bring in materials and components and put them all together to ship out a finished product is extremely important. With our people securely working from home using Prisma Access, they could still support those processes and allow us to quickly ramp up for the new demand presented by COVID-19.
>
> **—Gus Shahin, Chief Information Officer, Flex**

Enabling vital procurement and logistics work from home

Closing the company's books for the fiscal year was just one important business need for enabling staff to work from home. As a manufacturer, Flex was also quickly enlisted directly in the COVID-19 battle by retooling some of its operations to make ventilators. In a testament to the company's operational agility, Flex set up six new ventilator programs within a few weeks when such a move typically takes manufacturers 18 to 36 months.

Shahin comments on the value of having staff able to work successfully at home during this critical time. "The ability for our people to work from home was absolutely a factor in enabling that shift to manufacturing ventilators. At the end of the day, a large part of our business is procurement. Our end users are mostly buyers. How we bring in materials and components and put them all together to ship out a finished product is extremely important. With our people securely working from home using Prisma Access, they could still support those processes and allow us to quickly ramp up for the new demand presented by COVID-19."

Advanced security extends to at-home workers

With 20,000 people working from home, the security of all those remote connections is a top priority. Wetschnig points out that the difference Prisma Access brings, as compared to traditional VPN, is that it extends the next-generation security features of the Palo Alto Networks platform to every remote endpoint. Users can only connect to Flex's data center or SaaS applications by passing through the same full inspection of the next-generation firewalls, as if they were directly connected to the Flex network. "The difference comes down to the kind of security policies we can apply with Prisma Access—the traffic analysis, threat prevention, URL filtering, and segmentation. For a security person, that's what really counts."

One of Wetschnig's biggest cybersecurity concerns is the potential for malware, contracted at home, then spreading back to the corporate network. He says, "In a home environment, we don't have any control of the network. People are on all kinds of sites, kids are playing computer games, and you have to put your corporate assets in such an environment. That's where Prisma Access was very comforting for us because of all the security features it provides. It gives us confidence that no cyberthreat from home will move to our corporate network."

Wetschnig adds, "Prisma Access is also simple for the user—that was a tremendous help for us. It's not a big deal for people to use. We were looking for an easy, stable client and the ability to apply centralized security policies. Prisma Access matched all those points. If you can bring up a secure remote access solution for 20,000 people in seven days, I think that shows we made the right choice."

Accelerating incident response with automation

The successful rollout of Prisma Access has further strengthened the partnership between Flex and Palo Alto Networks. Flex recently acquired Cortex™ XSOAR, the extended security orchestration, automation, and response platform from Palo Alto Networks. The IT and security teams at Flex will use Cortex XSOAR to intelligently correlate threat indicators and determine if an incident is an attack, and then automate specific response actions based on the nature of the threat.

Shahin notes, "The automation provided by Cortex XSOAR is expected to help Flex reduce the number of tickets, and close tickets faster with more efficiency. This will free up valuable resources and cycles for both SecOps and IT."

The successful rollout of Prisma Access and the automation opportunities enabled by Cortex XSOAR have further strengthened the 15-year partnership between Flex and Palo Alto Networks. This long relationship, most recently with each company a customer of the other, has cemented the trust and confidence both Flex and Palo Alto Networks have in each other, which promises many more years of successful partnership.

Shahin sums things up: "Palo Alto Networks is an important partner to Flex. We have plans to use more of their solutions in the future."

> The automation provided by Cortex XSOAR is expected to help Flex reduce the number of tickets, and close tickets faster with more efficiency. This will free up valuable resources and cycles for both SecOps and IT.
>
> **—Gus Shahin, Chief Information Officer, Flex**

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com