CASE STUDY

Lean Security Team Achieves 24x7 Monitoring and Response with Fortinet SOC-as-a-Service

Murata Machinery USA aims to stretch the boundaries of automation, dramatically improving efficiency for manufacturing customers across various market sectors. Its machine tool division makes equipment such as lathes, press punches, and laser cutters. Its textile division builds machines used in making fabric. Its logistics and automation group produces systems underlying automated warehousing. And its clean-factory division supports the manufacture of microchips, batteries, and other products that require a sterile environment.

Although the company's four divisions operate independently, they share services, including HR, accounting, and IT. The OT machines on the factory floor arrive from Japan preprogrammed and do not connect to the corporate network. Still, Murata's six-person IT staff—including two help desk employees—have their hands full.

"Murata Machinery USA has six facilities throughout North America, and about half of our employees never come into one of those brick-and-mortar locations," explains Bill Konecy, IT manager. "They are in the field and at customer sites around the world at all times. We have a very lean IT team supporting about 550 end-users and 1,000 endpoints, plus 2,000 customer servers that we manage. So, we use technology to improve our efficiency."

Customer Experience Breeds Trust in Fortinet Solutions

When Konecy joined Murata eight years ago, the different divisions were all running different security solutions. "We did an assessment of the infrastructure and found a lot of systems that needed to be upgraded," he says. "Step one was improving our firewalls to build a better buffer between our network and the outside world."

The team researched firewalls, looking at third-party research and customer reviews. "We liked everything we read about Fortinet," Konecy says. "The more we explored, the more we felt that FortiGate Next-Generation Firewalls [NGFWs] would be a great fit for Murata Machinery USA. They are a very high-quality product at a reasonable price." The company replaced all its legacy firewalls with FortiGates equipped with the FortiGuard AI-Powered Security Services Enterprise Protection Bundle.

Konecy's team was immediately pleased with the NGFWs' usability. "We wanted to configure all our firewalls and switches through one pane of glass," he says. "We initially just focused on the quality of the FortiGates, but after we had standardized on them, we decided to migrate to FortiSwitch secure enterprise switches and FortiAP access points as well."

Now, all six Murata sites are protected by FortiGate NGFWs, with FortiSwitches for routing and FortiAPs for wireless connectivity. The IT team uses FortiManager to centrally manage all its FortiGates, FortiSwitches, SD-WAN, and FortiAPs through

muratec
A MURATA MACHINERY BRAND

"Thanks to the increased visibility that we have with the FortiGuard SOC-as-a-Service, we get a much clearer picture of what happened if there is an incident. So, we can more easily educate the impacted user on how to avoid a similar situation in the future."

Bill Konecy
IT Manager,
Murata Machinery USA

Details

Customer: Murata Machinery USA

Industry: Manufacturing

Location: Charlotte, North Carolina

Number of Users: 500

Business Impact

- Top-quality security, around the clock, through 24×7 monitoring and alerting
- Faster investigation and response to security threats
- More thorough end-user education around security risks, via better visibility to incidents

a single pane of glass. This consolidated view of security networkwide enables Murata to build great consistency and tighter security policies across the entire Fortinet Security Fabric. FortiClient provides VPN access, while FortiAuthenticator and FortiToken handle user authentication. FortiEDR provides endpoint detection and response to further secure the company's client and server systems. Murata also selected the FortiGuard MDR Services, a powerful tool providing visbility and insights into the data provided by FortiEDR.

A series of virtual LANs (VLANs) minimize unnecessary traffic between network segments, and the IT team has begun implementing zero-trust network access (ZTNA) via the FortiSwitches. "We have built certain rules into the firewalls to restrict movement as much as possible," Konecy says. "We do need some traffic between VLANs, but it is very limited. And VPN users are restricted in what they can see and interact with, depending on their role."

Konecy adds, "We are so happy with the products and services we get from Fortinet. If we want to add new security capabilities, we reach out to Fortinet and ask whether they have anything that can meet our needs. If they do, we usually go with it. We have learned over time to trust Fortinet solutions."

FortiVoice Saves up to 30 Hours a Month for IT Staff

That is exactly how Murata learned about and decided to transition to the FortiVoice secure unified communications platform and FortiFone handsets. "We had an old PBX [private branch exchange] system that was built in the 1980s," Konecy says. "It did not connect to our network, and it did not have modern security features. We had an incident where an attacker compromised the system, and when we called the vendor, they said they could wipe and rebuild it, but they could not guarantee the same thing would not happen again. We realized we needed a modern phone system that we could protect within our walls."

When he reached out to his Fortinet representative, Konecy learned about FortiVoice and FortiFone. His team deployed the system three years ago and has not looked back. "FortiVoice was a huge leap forward in efficiency," he says. "The archaic system we had was very time-consuming to support. Installing a single phone took a couple of hours. By contrast, when Murata merged with a Canadian business last year, I deployed about 30 phones and extensions in less than an hour. I planned for the phone system rollout to take all day. We started shortly before lunch and were finished when we went to lunch."

Better yet, many day-to-day system changes no longer require IT involvement. "Before, changing an extension because someone moved from one desk to another took 30 minutes because we had to reprogram the phone," Konecy says. "Now, they just pick up their phone, plug it in wherever they are going, and it works."

Overall, the IT team's phone-related support volume has dropped to "next to nil," he adds. "Prior to moving to FortiVoice, we spent 20 to 30 hours a month handling help desk tickets for the phone system. Today, if we get a call about the phones, it is generally a user wanting help with a feature they have not used in the past, like call forwarding. The IT team spends less than an hour a month on phone support."

24×7 Security Monitoring and Better Guidance for Network End-Users

Two years ago, Murata decided to further streamline security management by adding the FortiAnalyzer Cloud log management and analytics platform to its

Business Impact (cont.)

- Avoidance of hiring more staff members for the same level of coverage without the SOC-as-a-Service
- Happier end-users because of better education on security risks
- 20–30 hours per month saved by eliminating most phone system support
- Accelerated resolution of any issues through consolidation of security infrastructure with one vendor

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiManager
- FortiClient
- FortiAuthenticator
- FortiToken
- FortiEDR
- FortiVoice
- FortiFone
- FortiAnalyzer Cloud
- FortiSASE

Services

- FortiGuard MDR Forensic OnDemand Service
- FortiGuard AI-Powered OT Security Services
- FortiClient Forensic Service
- FortiGuard AI-Powered Security Services Enterprise Bundle
- FortiGuard SOC-as-a-Service

product mix and engaging the FortiGuard Security Operations Center-as-a-Service (SOCaaS) for 24×7 security monitoring.

"We have one security administrator who is responsible for protecting systems not only in North America, but also in Ireland, Israel, and time zones around the world," Konecy says. "We wanted to increase visibility into threats to our infrastructure, but we do not have the personnel to monitor and respond around the clock. When Fortinet introduced us to their SOC-as-a-Service, we could immediately see the benefit."

Konecy sold corporate management on those benefits. "My argument was: 'There are threats out there 24×7, and if one gets through in the middle of the night, it might shut down production. What would such an incident cost us in terms of our reputation and future business? That is something we probably do not want to find out.'" His pitch was successful; Murata moved forward with a proof of concept of the Fortinet SOCaaS. Fortinet security experts monitored Murata's network day and night, notifying the IT group anytime an issue needed their attention. "We were impressed with the proof of concept," Konecy reports.

> *"Using the FortiGuard SOC-as-a-Service frees up time that we would otherwise be spending monitoring everything. To have the same level of coverage without using the SOC-as-a-Service, we would have to add two or three more staff members, minimum."*
>
> **Bill Konecy**
> IT Manager,
> Murata Machinery USA

Along with the FortiGuard SOCaaS, Murata deployed the Forensics Service for FortiClient and FortiAnalyzer Cloud. "The SOC-as-a-Service team alerts us anytime they see something funny," says Security Administrator Justin Evans. "The dashboard gives us a lot of information about what is going on and how they found it. For example, it gives us names and IP addresses to help us pinpoint where to look. Then we use FortiAnalyzer, FortiSwitches, FortiClient Forensic Service, or a third-party security tool to look at it. On average, we investigate about one issue every day."

As an example, he describes a situation in which a Murata user was trying to access nefarious websites. "The SOC-as-a-Service notified me of that activity and explained the risk," Evans says. "I used the information to block those sites, not just for that user but for all our users. We learned quite a bit through that experience."

This approach also enables the IT team to educate end-users, which helps improve the company's security posture. "Thanks to the increased visibility that we have with the FortiGuard SOC-as-a-Service, we get a much clearer picture of what happened if there is an incident," Konecy says. "We do not see only that something nefarious got downloaded, but what the user clicked on, where it redirected them, and why that is a problem. So, we can more easily educate the impacted user on how to avoid a similar situation in the future."

Lean Team Avoids Adding More Staff for Security Monitoring

The managed service is not necessarily reducing the time Evans spends managing security, but "we now have nonstop coverage," he says. "I am the only one monitoring security events internally, and I am only here eight hours a day. I sleep better at night knowing that we have experienced analysts at my back, watching the logs when I am not available."

It also enables the Murata team to respond more quickly when a security threat does emerge. "Using the FortiGuard SOC-as-a-Service frees up time that we would otherwise be spending monitoring everything," Konecy says. "When something does happen, we have time to concentrate on our response. To have the same level of coverage without using the SOC-as-a-Service, we would have to add two or three more staff members, minimum."

Another benefit of the SOCaaS relationship is that the FortiGuard analysts identify best practices Murata can use to improve network security. For instance, Konecy says, the FortiGuard team recommended leveraging the ZTNA capabilities in the company's FortiSwitches. "Having access to that expertise and learning is great," Konecy says. "Our communications with the FortiGuard SOC-as-a-Service team helps us keep up with the current threats. We could get this information elsewhere, but having it served up in an easy-to-digest format makes it less time-consuming to access than if we had to go out and find it on our own."

Konecy adds, the SOCaaS "allows us to do more with less" while providing excellent security and exceeding end-user expectations. "With FortiGuard SOC-as-a-Service, we are protected inside and out. That means we can put more time into supporting our internal users—not only sitting down to fix a problem, but also training the user on how to prevent it in the future. I have heard a lot of great things about how much better the service provided by IT has become."

Always-on Security for a Hybrid Workforce

Recently, Murata extended its Fortinet infrastructure by purchasing the FortiSASE secure access service edge solution for enhanced security across its remote workforce and cloud applications. The company is transitioning a lot of resources to the cloud, which has made cloud security a top priority across the IT team. A thorough due diligence process revealed FortiSASE as the best solution to meet Murata's needs.

FortiSASE has a global network of points of presence (POPs) that can guarantee secure access to cloud services anywhere in the world. Its upcoming integration with FortiEDR promises to provide end-users with a consistent user experience. And for network and security administrators, FortiSASE offers full visibility and easy troubleshooting through integrated digital experience monitoring. It also comes with a forensics service for investigation of any issues at the endpoint level. Plus, FortiSASE integrates tightly with Murata's SOCaaS to give Konecy and his team complete control over, and visibility into, the company's networking and security architecture.

Ultimately, utilizing so many solutions within the Fortinet Security Fabric simplifies life for Konecy and his team. "When we had a mix of different products, if there were an issue, we would get the runaround trying to get it fixed," he says. "Sometimes solving a problem is a multistep process—maybe changes need to be made on both the firewall and the switches, for example. When we were dealing with multiple companies, each would blame issues on the other. We might spend three hours on the phone with the switch vendor, only to be told we needed to talk to the firewall people again."

"I cannot overstate how much we simplified network management by moving to a single provider [Fortinet] and a single management solution [FortiManager] for our key solutions," he continues. "If we think there is an issue with a switch, but it turns out to be something with the authentication tool, we call one place, and they get somebody to help us. We do not get passed from company to company, and we do not start the process over every time another vendor gets involved." Any issues that arise are resolved much more quickly. "It is also a huge timesaver."

March 14, 2025 4:42 AM / MKTG-1086-0-0-EN