CASE STUDY

Fortinet Brings Security, Efficiency, Performance, and Stability to a Global Manufacturer's Network

Based in Sweden, Alleima leverages advanced materials technologies to build high-end components for a wide range of industries. The company manufactures market-leading metal products, from umbilical tubing and aerospace titanium tubes to heat-resistant ultra-fine wire for electronics and medical devices to precision strip steel products used in razors, knives, and scalpels.

"We have contracts with some very large companies, both in the U.S. and abroad," explains Chris Lubinski, network security engineer. "As a global organization, we are subject to a number of compliance frameworks. If we failed to meet even one of these frameworks, we would lose business."

"To ensure we effectively protect our data and systems—and remain compliant around the world—we have very tight security frameworks," Lubinski adds. "We take network security very seriously."

Maintaining airtight security is an ongoing challenge for Lubinski and his colleagues. Alleima operates out of 52 locations globally. Some of these are small sales offices, while others are campuses consisting of several buildings. In total, the network serves around 100,000 endpoint devices, and its network and security team includes just four full-time staff, supported by a handful of Swedish contractors.

In Need of a Single Pane of Glass

In September 2022, Alleima was carved out from Swedish manufacturer Sandvik. Before the divestiture, network efficiency was not optimal. "We might have seven different systems that all did the same thing but for different geographic regions," Lubinski says. "End-users might need to access the network via VPN or via a proxy service or a WLAN [wireless LAN] controller, depending on where they were located. This environment was very cumbersome to manage and assisting end-users with network or security issues meant relying on the users to provide information about their configuration that they often had difficulty finding."

As Alleima prepared to separate from Sandvik, Lubinski's team was tasked with building a new networking and security infrastructure from the ground up. "We decided to look for a single pane of glass, one system that would give us all the information we need in one place," he says.

Another criterion was tight network segmentation. "We are rapidly approaching an environment where office and OT live in the same building," Lubinski says. "We need to segment OT and office networks so they can coexist safely. But at the same time, remote administrators need to be able to assist with both office- and OT-related issues. There are not many next-generation firewalls that can do what we were looking for, but FortiGates can. On top of all the IPS [intrusion prevention system] and security profiles that we need, FortiGates enable us to set up VDOMs [virtual domain object models].

Alleima

"Fortinet makes awesome products, and I love installing them. They make my job easier while also improving my team's ability to secure and support our many sites."

Chris Lubinski
Network Security Engineer,
Alleima

Details

Customer: Alleima

Industry: Manufacturing

Headquarters: Sandviken, Sweden

Business Impact

- Response time for security events reduced from two weeks to 30 minutes
- Network performance and stability vastly improved
- Production issues no longer bring down the entire network
- Security improvements possible without expanding staff
- User support requests fulfilled in 90% less time
- Minutes, rather than hours, to deploy and configure new network devices

"I was a proponent of Fortinet because I had used Fortinet switches and access points in the past," he continues. "I explained to my colleagues in Sweden that I have worked with many different vendors, and I have never had a bad experience using Fortinet equipment. Once we all agreed to move to Fortinet for the LAN and local connections, we decided to use Fortinet for SD-WAN as well."

Fortinet Secure SD-Branch Brings Big Improvement in Network Visibility

Alleima began rolling out FortiGate NGFWs on the network edge in locations around the world. Each FortiGate is supported by the FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle. "Fortinet Secure SD-WAN is our perimeter, via HA [high availability] stacks of FortiGates in every site," Lubinski says.

"All our U.S. office locations also have a FortiGate HA stack that handles the LAN and internal segmentation, and routes outgoing traffic to the SD-WAN FortiGates," he adds. "Some of our SD-WAN hubs assist with services such as SSL inspection, IPS, and antivirus. In other cases, the SD-WAN handles so much traffic that we offloaded those services to the LAN FortiGates."

Alleima's Americas businesses are now in the process of transitioning to FortiSwitch secure Ethernet switches and FortiAP access points. "It makes sense to manage the switches and APs [access points] through our firewalls," Lubinski says. "We can go into a FortiGate and easily see both the SD-WAN and the LAN, so we can get a complete view of a particular location, from the LAN connection all the way out to the other side of the globe."

Lubinski's team uses the FortiManager security management platform anytime they need to roll out new devices. FortiAnalyzer, the Fortinet Security Fabric, analytics, reporting, and response platform, produces reports that Lubinski's team uses to understand any security events that occur on their Fortinet network. And the FortiSIEM security information and event management is deployed as a SaaS solution. It collects data from all of Alleima's security data sources, including the other Fortinet solutions, detecting incidents and generating alerts when necessary. "We drive a lot off of FortiAnalyzer and FortiSIEM," Lubinski says. "We work with an external SOC [security operations center] that alerts us to issues we need to handle. We also receive reports from FortiGuard Labs about new threats, and reports from FortiSIEM about unusual behaviors on the network. When we get any of these alerts, we take up the issue, using FortiSIEM and FortiAnalyzer to investigate."

This approach has dramatically reduced the time to resolution of any security event. In the legacy Sandvik environment, Lubinski says, "It would usually be a couple of weeks before we even heard about an incident. Now, we are getting that information right away, and we can start investigating within a half hour of the issue being detected. We have a much faster response time and are more aware of what is happening on our network."

He adds that the Fortinet-driven security environment has improved communication between Alleima's internal IT team and the staff of its external SOC. "Information travels a lot faster now, and we are all able to make that full connection across both LAN and WAN, which we could not previously do," Lubinski says.

Business Impact(cont.)

- Six hours to roll out entire Fortinet infrastructure to a new site vs. 24 hours previously
- Port configuration changes completed on the day of the request vs. wait of five to seven business days in legacy environment
- Minimized training required to manage network security

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiManager
- FortiSIEM
- FortiAnalyzer
- FortiEDR
- FortiClient Endpoint Management Server
- FortiAuthenticator
- FortiMail

Services

- FortiGuard AI-Powered Security Services Unified Threat Protection Bundle

"It makes sense to manage the switches and APs through our firewalls. We can go into a FortiGate and easily see both the SD-WAN and the LAN, so we can get a complete view of a particular location from the LAN connection all the way out to the other side of the globe."

Chris Lubinski
Network Security Engineer,
Alleima

World-Class Endpoint Protection That Is Easy to Manage

Alleima's Fortinet deployment extends beyond the LAN and SD-WAN solutions. The company has also rolled out FortiClient Endpoint Management Server (EMS), FortiEDR endpoint detection and response, and FortiAuthenticator for user authentication. "In our previous environment, our VPN services were a nightmare to deal with, so as we deployed Fortinet Secure SD-WAN, we added Fortinet's VPN capabilities as well," Lubinski says. "FortiClient EMS has proved a great addition to our network."

FortiClient EMS offloads its logs in to FortiSIEM and FortiAnalyzer. By offloading logs in to FortiAnalyzer, Lubinski's team can easily manage and support their assigned regions, benefiting from a uniform approach across the company. The familiar user interface (UI) of Fortinet products further simplifies this process, reducing the learning curve and enabling the team to deploy and support new solutions quickly. This streamlined operation improves efficiency and ensures the team can respond to incidents and support requests quickly and accurately.

"Because FortiAnalyzer has everything from every device, it is easy for our small team to manage," Lubinski says. "We each use FortiAnalyzer to support our assigned region, and if a country that does not have its own network security specialist needs assistance, we can easily help because of the uniform approach across the company. The UI is so similar across Fortinet products that it is easy to sit down in front of a new solution and figure out what to do," Lubinski says. "You do not need to take a course to understand how these products work. Typically, a walkthrough with someone who knows how to use a Fortinet solution gives you everything you need to get your job done."

> *"Management at remote Alleima locations has been very complimentary of the Fortinet infrastructure. Their connections are much faster and more stable, and our response time for their support tickets is around tenfold quicker. Everyone at Alleima is much, much happier now."*
>
> **Chris Lubinski**
> Network Security Engineer,
> Alleima

Alleima is extending its use of FortiAuthenticator, which it installed around the time of the divestiture from Sandvik. "In the past year, we have started setting up our radius and tying FortiAuthenticator directly to FortiManager so that we have a template for configuring clients for each site," Lubinski says. The team is also increasingly digging into FortiEDR alerts. "FortiEDR does a great job of flagging suspicious endpoints, processes, and activities," Lubinski adds. "If FortiEDR has not seen something before, it flags and blocks it, then sends us an alert so we can figure out whether it is a threat."

Finally, Alleima uses the FortiMail email security solution to protect mission-critical applications and traffic. "We use FortiMail for any systems that need to be available 24×7×365 without a hiccup," Lubinski says. "So, it is in use day in and day out, but not for all Alleima communications across the globe."

Dramatic Efficiency Improvements Accelerate End-User Support

Lubinski says his favorite aspect of the Fortinet Security Fabric is its efficiency. "Fortinet makes awesome products," he says, "and I love installing them. They make my job easier while improving my team's ability to secure and support our many sites. A prime example is rolling out new network devices. To deploy APs in our legacy environment, we needed to install and configure them one at a time, which the team's deep familiarity with Fortinet terminology and user interfaces (UIs) streamlines their support of other business divisions.

"The UI would take hours. But with the Fortinet suite, all we do is plug them into the network."

Launching an entire site is similarly accelerated. "In our previous environment, we would plan on at least 24 hours of actual work by the networking team for a site migration," Lubinski says. "Now, we have cut that down to six hours of total work time to have a site up and running. We just plug the devices into the network, and the FortiGates automatically populate with the correct settings.

"We have much shorter turnaround times for all kinds of network support activities," he adds. Thus, his team can resolve user support requests much faster than it could a few years ago. "For instance, we used to have a week-plus turnaround time to change a port from one VLAN [virtual LAN] to another," Lubinski reports. "I handle about 15 of those each week, and I would send them to another team, which would take five to seven business days to make the change. Now, I manage them myself, and I complete port configurations on the same day, as many as are needed."

These efficiencies enable Alleima to operate globally without adding staff to the networking and security teams. Better yet, the U.S. group worries less about other teams' upcoming vacations. "Sweden takes long summer vacations, so we lose many of our headquarters' staff from June till late July or even August. Before, we would put in issues in May and hope they got to them before June. Now, because we can troubleshoot and resolve issues ourselves, Sweden's summer vacation does not lead to network hiccups for us." Plus, the increased visibility into network traffic gives Lubinski's team better leverage in negotiating contracts with internet service providers.

One more benefit: The Fortinet infrastructure has eliminated network performance and reliability issues that were prevalent in the prior environment. "Our industrial equipment needs massive amounts of electricity, and production issues can result in a power shutoff," Lubinski says. "In the past, that would bring our network down as well. When we built our Fortinet architecture, we bought switches with dual power supplies, and we gave a lot of the Fortinet devices their own dedicated circuits. So, we now have a network that does not go down even if we lose power to a building."

Continuing to Expand the Fortinet Security Fabric

Next, Alleima is looking to shift to a Fortinet-driven zero-trust network access model. In addition, Lubinski is exploring options for pulling FortiAnalyzer reports into Microsoft PowerBI so that business units can view network security at their sites. He wants to provide easy access to answers such as: How many incidents has the facility experienced in the past year? How many people have clicked on phishing links? What is the return on network infrastructure investments?

Beyond these plans, Lubinski adds, "We are looking to expand our Fortinet Security Fabric connections wherever that makes sense." His team is considering adding the FortiNAC network access control solution in 2025, as well as FortiMonitor, which would give managers outside of IT easy-to-access information about the activities of specific endpoints.

"Management at remote Alleima locations has been very complimentary of the Fortinet infrastructure," Lubinski says. "Their connections are much faster and more stable, and our response time for their support tickets is around tenfold quicker. Everyone at Alleima is much, much happier with the global network and security infrastructure we now have."