Protecting 24/7 Food Manufacturing Across Four States

The customer summary

Customer name
SugarCreek

Industry
Food Manufacturing

Location
North America
Security Challenge
• Upgrade security posture from zone-based stateful firewall
• Provide centralized policy management and visibility everything and everyone accessing the network through a single pane of glass console
• Enable network segmentation to isolate each vendor’s manufacturing equipment

Solution
• 18 Cisco Firepower 2110 NGFW (HA pairs) with Firepower Threat Defense
• 2 Firepower Management Center (HA)
• Next-generation intrusion prevention, AMP for Networks subscriptions
• AMP for Endpoints
• Umbrella
• AnyConnect VPN
• Identity Services Engine (ISE)

Results
• Improved security posture across the board with Cisco Integrated Security Architecture
• Reduced day-to-day security management tasks such as provisioning new equipment with centralized Firepower Management Center
• Gained complete visibility into the network so that the team could monitor all activity and potential threats and focus on actual alerts and not correlating alerts across disconnected devices

SugarCreek is an innovative, diversified and flexible food manufacturer helping some of the industry’s largest and best known companies develop Brandworthy Food Solutions. SugarCreek’s authentic culinary expertise helps drive innovation. Their in house expertise in everything from food trends and marketing to packaging and logistics makes the company an ideal partner for new food product development – including bringing scale to sous vide.

SugarCreek employs over 2,000 people in six manufacturing facilities and serves clients across North America. With its roots in bacon products, SugarCreek has expanded its food manufacturing with customizable sous vide food products for the quick service restaurant market.

The 20-person IT department oversees operations across all six manufacturing facilities, and the vendor data center that services the nearly 3 dozen vendors that supply and service the food manufacturing equipment. In addition, the IT team led by Todd Pugh, also support the corporate data center servicing corporate finance operations, personnel records, accounting, and customer data.

SugarCreek’s food manufacturing facilities are located across 4 midwestern states. Each operation is supported by skilled industrial engineers that co-develop ready to cook protein food products with their customers. They start out testing food concepts in test kitchens that are equipped with the latest restaurant scale cooking and refrigeration equipment so that once a recipe is perfected, it is the then scaled for mass manufacturing within the plant.

The highly-automated food preparation and packaging equipment at each facility is connected via redundant cabling and Wi-Fi to minimize manufacturing downtime in case of failure in one of the routes. The entire IT infrastructure has redundancy built-in to maximize uptime for their 24-7 operations. Manufacturing equipment is maintained and serviced by scores of globally-based 3rd party vendors. These vendors troubleshoot malfunctioning equipment on the manufacturing floor either from the centralized vendor data center in Indianapolis or indirectly via clientless VPN.
Upgrading the legacy security solution
Cisco ISR routers outfitted with zone-based firewalls and Cisco Identity Services Engine (ISE) and Cisco ASA 5545 comprised the legacy security solution at SugarCreek. ASA firewalls protected the data center. ISE and ISR routers limited access of each vendor to their specific equipment only. With more vendors and manufacturing techniques coming on line constantly, the team needed to work more efficiently. The wanted a solution that would improve their security posture so that “they would not be one of those companies in the news that got attacked by ransomware and did nothing about it”.

In addition to next-generation firewall features, top criteria for the new security solution was centralized policy management and visibility into everything and everyone accessing the network through a single pane of glass console. IT Director, Todd Pugh and Senior Network Administrator Wes Dawes began selecting options to improve security across their organization.

Evaluation
The team evaluated Palo Alto firewalls with Vigilant Cyber Systems against Cisco’s latest Firepower 2110 series NGFW. Each solution had similar capabilities with NGFW features and a single pane of glass management console. SugarCreek was very impressed with the integration of Firepower Threat Defense firewall functions with ISE, AnyConnect VPN, NGIPS, AMP for Networks and AMP for Endpoints within the Firepower Management Center (FMC).

The visibility FMC provides into malware blocked from user’s laptops was phenomenal. Todd experienced it first hand when he downloaded a file from email and it disappeared from his desktop. Not believing his eyes, he tried it again. Once again it disappeared. When he heard that the CIO experienced the same thing, he knew that AMP was doing its job.

It came down to making a decision. Todd and Wes knew capabilities and features were important but the time it would take to train staff on unfamiliar products and the potential impact of ongoing support with multiple vendors also were important. Considering the integration of multiple security solutions with existing Cisco equipment that the IT team was already quite experienced with, it became clear that even with similar capabilities across competing products, Cisco’s integrated security architecture all backed by Talos threat intelligence and one-vendor support would tip the scales in Cisco’s favor.

The Solution
The SugarCreek team decided on the Cisco integrated Firepower solution. To maintain the redundant capability, SugarCreek chose to deploy 9 Firepower 2110 high-availability pairs with NGIPS and AMP for Networks subscriptions and Umbrella at each of their sites. The NGFWs are managed centrally with an HA pair of Firepower Management Center appliances located at the corporate headquarters, that are also accessible

“We’re able to monitor the health of all devices in the network so we know when something’s failing and we’re able to isolate and fix those problems before they become disasters.”

Wes Dawes
Senior Network Administrator, SugarCreek
remotely when Wes and his team are at satellite facilities. At each remote site, traffic traversing each operation is routed through Firepower 2110 appliances to both inspect for threats and to gain visibility into what information was moving across the network.

They also chose to deploy AMP for Endpoints and Cisco AnyConnect integrated with Umbrella secure internet gateway on all users’ laptops to keep users safe from risky internet sites even while they are off the corporate VPN.

Saving administrative time
With all of the Cisco tools that SugarCreek use: Firepower Management Center, Firepower Threat Defense NGFWs, the Cisco ASAs that run the Firepower Threat Defense software as well as AMP for networks and endpoints and ISE, the team has put together a solution that makes things simple to manage. Administrators can write sets of rules that apply across the entire network, rather than focusing on individual devices, which saves an enormous amount of time. What took one person a week to manage previously, now takes only hours.

Cisco Firepower with AMP has made it easier for SugarCreek to manage security in multiple ways. The IT team no longer has to go out and look for definitions or updates and make sure that they get pushed out through AMP for networks and endpoints. Everything’s done in the background, automatically in the cloud.

Administrators are now able to monitor everything from the Firepower Management Center, where they can pool all the intelligence in one place, identify threats more quickly and isolate real threats to stop them before they become widespread.

With the new visibility that SugarCreek has gained with the AMP products, they see things that they never saw before in their log files. And that’s not because it didn’t exist, it’s because they didn’t have the benefit of Talos threat intelligence integrated across Cisco Firewall, AMP for network and AMP for Endpoint. HTML-type attacks through browsers are now visible and the great thing is not only that it allows the administrators to see those, but it tells them that it’s caught those attacks and it’s blocked them. Cisco security products do all this work for the SugarCreek IT team.

Cisco Identity Services Engine (ISE) with Cisco ISR routers, round out the complete security architecture. With so many vendors accessing SugarCreek’s manufacturing operations, it is imperative that the IT team created a virtual network for each vendor’s food manufacturing equipment. The entire network is segmented using ISE to isolate the sous vide operation from the packaging operation from the bacon cooking process or flash freeze to prevent Introduction of a virus or ransomware virus from percolating across the entire manufacturing line with devastating financial effects.

Deployment results
SugarCreek worked with Cisco Gold Partner Presidio to help with the installation and set-up of the new Firepower security solution. The original estimate of 200 hours was whittled down to less than 100 hours with 24-7 phone support from Cisco’s expert FTD Customer Assistance Team who helped with introducing the myriad new capabilities available with FTD. The new security solution has been up and running for over 8 months now with hardly a hiccup.

“We can write sets of rules that apply across the entire network, rather than focusing on individual devices, saving us an enormous amount of time.”

“It gives us peace of mind knowing that we’re stopping a lot of that stuff that we believe used to come through our environment.”

Wes Dawes
Senior Network Administrator, SugarCreek