CASE STUDY

Ice Manufacturer Consolidates onto the Fortinet Security Fabric to Freeze Out Attackers

Ice manufacturing is an industry that tends to fly under the radar, but some companies in the sector have a storied past. Bridgetown, Ohio–based Home City Ice was established in 1893 to provide home delivery of block ice before the invention of the modern refrigerator. Fast-forward 130 years, and Home City Ice now uses turbo icemakers to hard-freeze highly purified water. Its process freezes the water in motion, which allows any remaining impurities to run off and results in ice chunks that last longer than those created through other processes.

Consumers across the Midwest, as well as in eastern states including New York and Florida, experience the benefits of this process when they buy bags of ice from grocery stores, gas stations, or other retailers. Instead of becoming solid blocks, Home City Ice bags are filled with distinct individual pieces.

"Our turbos have big metal plates that water moves across," explains Stuart Carlisle, network architect. "It freezes onto the plates as it moves. Then, at a certain point, the machines add slightly warmer water, which causes the ice to break off the plates. Augers crush it up into the little nuggets consumers are familiar with, and a separate machine seals it in the bags."

The company has grown rapidly through acquisitions in recent years, with annual revenue reaching $200 million in 2020. "We now have 80 manufacturing plants, plus about 75 satellite distribution facilities, which are essentially remote iceboxes in the middle of nowhere," Carlisle says. "Our trucks store ice in those terminals for delivery to distant retail outlets."

Like most businesses today, Home City Ice prioritizes data security. A successful attack or data incident could take down the network and damage the business infrastructure. "We do not have a lot of proprietary company information, but we have customer information that we do not want to lose," Carlisle emphasizes. "If there was a successful incident, we would face both a financial hit and a reputational impact."

Consolidation of Capabilities a Competitive Advantage for FortiGate

More than a decade ago, Home City Ice needed a new solution for failover of internet links. The IT team deployed FortiGate Next-Generation Firewalls (NGFWs), which had a cellular network interface, as backup for the network routers. The company continued using the firewalls it already had in place, which were from a different vendor. Over time, however, the market landscape changed.

The legacy firewalls reached end of life, and turning to the FortiGates for their inspection, networking, and firewall capabilities made sense. "We were using a third-party intrusion prevention system [IPS] and separate VPN concentrators," Carlisle says. "We decided to move to everything to the FortiGates, which offered a single license for all their features, including wireless."

"We have not experienced any major incidents in more than a decade with Fortinet, and between FortiAnalyzer and FortiSIEM, we have clear visibility to what is happening. When something does require security response, we can see it and react very quickly."

Stuart Carlisle
Network Architect
Home City Ice

Details

Customer: Home City Ice

Industry: Consumer Goods, Manufacturing

Headquarters: Bridgetown, Ohio

Number of Secure SD-WAN Locations: 150

Home City Ice standardized on FortiGate NGFWs with the FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle. Now the company has two high availability (HA) pairs protecting the network edge in each of its two data centers, where all the company's servers reside in a virtual environment. FortiGates also secure the perimeter of many of the company's terminals, sales offices, and other remote sites. Fortinet Secure SD-WAN provides load-balancing capabilities in these locations.

"Our network is private MPLS, and all network traffic is backhauled to the data centers, so the data center FortiGates secure it," Carlisle says. Those FortiGates also protect networked IoT devices, such as programmable logic controllers (PLCs) that manage the icemaking equipment.

In addition to securing the perimeter, the data center FortiGates manage internal network segmentation. Previously, Home City Ice used the FortiGate NGFWs in conjunction with VMware NSX for microsegmentation of its virtual environment. But the organization is moving away from NSX. "We are experimenting with using FortiGates without NSX for microsegmentation," he says. "It will work similarly to what we had, but will not be managed the same." Meanwhile, a FortiGate VM is securing access to resources in the company's small Microsoft Azure cloud environment.

Carlisle manages the FortiGates in the on-premises data center, remote offices, and the Azure cloud through the FortiManager security management platform. "FortiManager keeps all our security policies synchronized across our locations," he says. "If I need to add policies to allow or block specific traffic, it makes sense to change them in a central location and push them out to all the appropriate devices. FortiManager makes that simple to do." The FortiAnalyzer security analytics solution pulls logs from the other Fortinet products, giving Carlisle a single location for monitoring security networkwide.

Building a Full Suite of Fortinet Security Fabric Solutions

Since deciding to standardize on FortiGate NGFWs, Home City Ice has incrementally transformed most of its network to the Fortinet Security Fabric. All the company's locations provide Wi-Fi through FortiAP secure access points. "The biggest reason we transitioned to FortiAPs is the ease of deployment," Carlisle reports. "Being able to control the access points from the FortiGate makes the wireless network less expensive and easier to manage."

FortiSandbox gives Home City Ice advanced, AI-powered sandboxing anytime the FortiGates detect a threat, and the FortiSIEM security information and event management solution consolidates information about security issues throughout the network. The FortiWeb web application firewall (WAF) provides advanced web application and API protection, securing inbound internet traffic to Home City Ice's web servers and giving the company an extra layer of defense in the case of a web-based attack.

FortiNAC handles network access control for Home City Ice. "FortiNAC helps us enhance security in the physical layer at the point of connection," Carlisle says. "It ensures that devices physically cannot access our network unless they are approved. It can also recognize and categorize systems—such as IoT devices, managed workstations, even unmanaged devices and BYOD [bring your own device]—and put them in the right granular network segment. That makes it much easier for me to stay on top of network segmentation since it's dynamically adjusted, versus doing all this statically and manually."

Business Impact

- Zero major incidents in more than a decade on a network with 150+ locations
- Successful penetration testing demonstrates security effectiveness
- Smaller staff can manage network because of efficiencies in the Fortinet Security Fabric
- Lower total cost of ownership throughout the network

Solutions

- FortiGate Next-Generation Firewall
- Fortinet Secure SD-WAN
- FortiManager
- FortiAnalyzer
- FortiAP
- FortiSandbox
- FortiSIEM
- FortiWeb
- FortiNAC
- FortiAuthenticator
- FortiToken
- FortiClient Enterprise Management Server
- FortiEDR

Services

- FortiGuard AI-Powered Security Services Unified Threat Protection Bundle
- FortiGuard Managed Detection and Response Service

The FortiAuthenticator network and user identity authentication solution ensures that only approved users can access the network, supported by FortiToken for multi-factor authentication (MFA). "We have been using FortiAuthenticator for a long time," Carlisle says. "Today, we are using it for MFA privileged access on all our nodes. Everybody in IT and certain executives use FortiToken MFA to connect. In addition, FortiAuthenticator is our authentication toolbox for monitoring and changing authentication mechanisms from one service to another."

FortiClient Enterprise Management Server (EMS) provides antivirus and vulnerability scanning on all Home City Ice endpoints, as well as offering zero-trust network access (ZTNA) proxies for remote connectivity to the network. At the same time, the FortiGuard Managed Detection and Response (MDR) Service, based on the FortiEDR endpoint detection and response solution, prevents threats from reaching company systems.

"FortiEDR is our final layer of defense," Carlisle says. "We really like how FortiEDR inspects libraries and executables, blocking events before they happen. And, since we are a small team, having the managed service is especially useful because the FortiGuard team has eyes on FortiEDR at all times, especially during evenings and weekends when internal staff are not available. Using FortiEDR on top of FortiClient gives us confidence that we can quickly catch, block, and deal with whatever threats arise.

"We have so many layers of security," Carlisle continues. "The ecosystem Fortinet offers, in which all the solutions communicate with one another, gives us layer after layer trying to prevent attacks. For example, if FortiEDR needs to isolate a threat, it can work with FortiNAC to understand the physical location of the compromised device, not just the logical isolation on the VLANs [virtual LANs], and leverage FortiNAC to quarantine the compromised device, closing the loop on the threat response. Another example is that threat information from FortiSandbox can be shared amongst all the different FortiGates and the FortiClient EMS."

"The ecosystem Fortinet offers, in which all the solutions communicate with one another, gives us layer after layer trying to prevent attacks."

Stuart Carlisle
Network Architect
Home City Ice

"The Fortinet solutions are intuitive. The interface is easy to use, and the GUI means we do not rely on the command line. Because the Fortinet solutions overlap in their terminology and layout, once you know one, they all become a lot easier to use."

Stuart Carlisle
Network Architect
Home City Ice

He adds that the IPS and web filtering services within the FortiGates UTP bundle are particularly valuable in keeping resources secure. "We rely heavily on category filtering in IPS to filter and act on network traffic and sniff out threats, as well web filtering which allows us to manage access to the website—blocking, restricting, and filter out bot-like behavior," Carlisle says. "Signature updates from FortiGuard Labs are key, and we bucket everything that FortiGuard lists as threats by using threat feeds within FortiSIEM. The FortiGates automatically block potential threats right away."

Highly Effective Security Managed by a Smaller Staff

The Fortinet Security Fabric gives Home City Ice a solid, interconnected security fabric for automating threat response, as well as one place to turn if an issue arises. Plus, the similarity between solutions makes the entire infrastructure easier to manage. "The Fortinet solutions are intuitive," Carlisle says. "The interface is easy to use, and the GUI means we do not rely on the command line. Because the Fortinet solutions overlap in their terminology and layout, once you know one, they all become a lot easier to use."

Carlisle believes the integrations and familiarity across the Fortinet Security Fabric are also reducing the total cost of ownership of Home City Ice's network. "Running solutions from a bunch of different vendors, like we used to do, increases the labor needed," he says. "If we still used a hodgepodge of vendors, we would need a bigger staff because all the systems would be more cumbersome to learn and manage. That gives Fortinet a significant cost advantage."

Even more important, he believes the Fortinet Security Fabric is effectively protecting Home City Ice. "We have not experienced any major incidents in more than a decade with Fortinet, and between FortiAnalyzer and FortiSIEM, we have clear visibility to what is happening," Carlisle says. "When something does require a security response, we can see it and react very quickly."

Perhaps most telling, Home City Ice recently engaged a third-party firm to perform penetration testing on its network. “It was funny, because they struggled with both the external and internal pen tests,” Carlisle says. “They could not do anything. We had to explicitly change our security posture over and over so they could connect to the network to run tests. We ended up making exceptions to our firewall and other product rules to let them in, but FortiSIEM still blocked them.”

Now Home City Ice is evaluating the FortiSASE secure access service edge solution and FortiSwitch secure Ethernet switches. “I have used a different vendor’s switches for many years, and it would be hard for me to move away from that, but we are considering potentially moving to FortiSwitches,” Carlisle says. “We have one to evaluate, so we will see what happens. Because of the tight integration across the Fortinet ecosystem, when we need a new solution, it makes sense to look at the Fortinet Security Fabric first.”

“Running solutions from a bunch of different vendors, like we used to do, increases the labor needed. If we still used a hodgepodge of vendors, we would need a bigger staff because all the systems would be more cumbersome to learn and manage. That gives Fortinet a significant cost advantage.”

Stuart Carlisle
Network Architect
Home City Ice

FORTINET

www.fortinet.com

Copyright © 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 5, 2025 2:27 PM / CS-68-0-0-EN