

CASE STUDY

Retailer Improves Security With SD-WAN and Simplifies Operations at 740 Stores Nationwide

In 1988, Batteries Plus opened its first retail store in Green Bay, Wisconsin. At the time, the company was responding to a relatively new market need—specialty batteries for a growing assortment of electric and electronic devices used by consumers and businesses.

The company expanded rapidly almost from day one, embracing franchising in 1992 to accelerate its geographic reach. Today, Batteries Plus Bulbs' 740 physical stores and its e-commerce site offer access to more than 60,000 types of batteries, lightbulbs, and accessories—and the expertise to help customers choose the right product. Since 2014, the brick-and-mortar locations have also offered smartphone and tablet repair services.

Vice President and CIO Michael Lehman is a two-decade veteran of the company, having arrived in early 2000. "At the time, we had five IT employees for 120 stores," he recalls. "And our data center consisted of a single server."

Today, the IT team consists of around 75 people, providing development, service desk, and infrastructure services to headquarters and to the corporate and franchised stores. Given the unique needs of its market niche, the company has built its own custom applications for its e-commerce site and point-of-sale infrastructure as well as a sophisticated cross-reference tool that shows which batteries fit which devices.

Enhancing Cybersecurity

While in-house development is a key part of Batteries Plus Bulbs' strategy, Lehman's team does not hesitate to use third parties to perform specific functions or to supplement the internal team during specific projects. Cybersecurity is one area where the company has relied on service providers for close to a decade. "Franchisees want secure and compliant systems, and we do not want to pretend that we have the in-house expertise to make that happen," Lehman contends.

Two years ago, Batteries Plus Bulbs' contract with its managed security service provider (MSSP) was coming up for renewal, and the team knew they needed to update the way they approached security.

"We engaged our legacy provider eight years ago, at a time when retail organizations were scrambling to meet new security requirements," Lehman recalls. Specifically, versions 2.0 and 3.0 of the Payment Card Industry Data Security Standard (PCI DSS), released in 2010 and 2014, introduced new, more stringent standards for merchants.

The company's arrangement with the legacy MSSP was limited primarily to management of the firewall solution, leaving Lehman's team to deploy and manage other point products to protect their infrastructure. These included intrusion



"We can take a more proactive stance to managing security. This gives us confidence that we are equipped to manage security threats for the next 5 to 7 years."

– Dan Dugan, Vice President of Information Technology, Batteries Plus Bulbs

Details

Customer: Batteries Plus Bulbs

Industry: Retail

Location: Hartland, Wisconsin, USA

Partner: Leeward Business Advisors

Business Impact

- Full visibility of the entire security architecture from a single pane of glass
- Flexibility to bolster specific security elements in the future with integrated solutions

prevention system (IPS) and antivirus tools. In addition to the hassle of managing the solutions in-house, the team had limited visibility into the company's overall security posture. "Many elements of our security architecture were in their own silo," Lehman remembers.

Finding a Broad Solution Provider

The team determined that the best approach was to partner with a single service provider that could provide as many network and security operations functions as possible. Ideally, the software and hardware used by this provider would be integrated as well. "Unlike last time, we had a defined idea of what we wanted," Lehman says. "So, we decided to do a smaller, more directed proof of concept (POC), focusing primarily on the hardware selection."

Batteries Plus Bulbs selected Fortinet as its hardware provider over another vendor. To manage this relationship, the company selected Fortinet Partner Leeward Business Advisors, a Wisconsin-based consultancy that takes a broad, strategic approach to designing technology solutions for businesses of all sizes.

LeewardBA won the contract for a number of reasons. "They took the time to understand our business and put together a thoughtful proposal that was a value add for us," Lehman relates. "They also provided a superior solution at a really good price."

Specifically, Batteries Plus Bulbs appreciated the fact that LeewardBA has both security operations center (SOC) and network operations center (NOC) capabilities and uses the fully integrated security solutions of the Fortinet Security Fabric. "The Batteries Plus Bulbs team saw the value in our broad capabilities," says Michael Polzin, CEO at LeewardBA. "Our ability to dynamically support the desktop infrastructure, switching, and the wireless infrastructure in addition to the SOC was a huge advantage."

Deploying Comprehensive Security

The LeewardBA solution is built on FortiGate next-generation firewalls (NGFWs) installed at each store. The FortiOS operating system underlying the NGFW technology also enables all other Fortinet Security Fabric solutions—including third-party solutions developed by Fabric Partners—to be seamlessly integrated. All Fortinet solutions are backed by comprehensive, artificial intelligence (AI)-enabled threat intelligence from FortiGuard Labs. And LeewardBA has access to other sources of threat intelligence that have also been integrated into the Security Fabric.

One welcome feature of the FortiGate NGFWs is Fortinet Secure SD-WAN functionality, which the company uses to connect its 740 stores to the headquarters. This robust software-defined wide-area network (SD-WAN) technology enables the company to safely use the public internet to scale network traffic, rather than relying solely on expensive multiprotocol label switching (MPLS) circuits. "Managing this part of the solution enables LeewardBA to ensure network performance as well as security," says Jason Klein, CTO for LeewardBA.

Now, every store has both landline and LTE connections, and Fortinet Secure SD-WAN automatically shunts traffic from the landline to LTE as needed. This has been a boon for Batteries Plus Bulbs, as Infrastructure Architect Jason Thelen explains: "Today, we have stores fail over seamlessly between the primary connection and the cellular backup, and most times they don't even realize the switch has been made."

Another feature of FortiGate NGFWs that Batteries Plus Bulbs is taking advantage of is intent-based segmentation. "For PCI compliance reasons, our register network is separated from the rest of the infrastructure," Lehman explains. "Being able to take advantage of the dynamic trust models in the FortiGate makes this segmentation even more robust."

Business Impact (contd.)

- Assured network performance at 740 stores due to Secure SD-WAN solution
- Scalability to meet future security needs
- Solution was cost neutral compared with prior solution while delivering vastly better performance and security

Solutions

- Fortinet Secure SD-WAN
- FortiAP
- FortiManager VM
- FortiAnalyzer

LeewardBA also manages instances of FortiManager VM and FortiAnalyzer on behalf of Batteries Plus Bulbs. “These tools enable us to provide centralized management from a single pane of glass, detailed reporting, workflow automation, and trends analysis,” says Klein. “This enables the in-house team to get a complete picture of their security posture at a glance, at any time.” The centralized management also enables consistency, according to Thelen. “We can push out uniform policies to every single store,” he says, “everything from whitelisting and blocking URLs to different network segmentation policies to provide PCI security.”

Consolidating Disparate Security Functions

Batteries Plus Bulbs was also able to integrate many additional security functions that were previously siloed into an SD-Branch solution based on Fortinet. For example, FortiAP wireless access points replaced a legacy solution that never worked very well. “Our prior solution was cobbled together, and while better than nothing, left a lot to be desired,” Lehman relates. “It is really nice to have secure, integrated wireless protocols.” From a security angle, Thelen notes, “SD-Branch truly allows you to embrace a zero-trust methodology. Some people find that a scary thing. But when your switches, APs, and firewalls are all integrated, it becomes an easier concept to swallow. Zero-trust is where everybody should be going.”

Batteries Plus Bulbs also elected to subscribe to the FortiGate Unified Protection (UTM) Bundle, which gives the company access to security services like advanced malware protection, web filtering, IPS, and application control—enabling the company to retire several point products. “They are using just about every element of their UTM package, and they love that it is all visible from one place,” Klein reports. Thelen concurs, adding, “We rely heavily on the [FortiGate] UTM. We definitely sleep better at night knowing that it’s all baked into the product.”

In addition to the consolidation accomplished to date, the FortiOS platform and the Fortinet Security Fabric provide the flexibility to add myriad additional security features in the future—all seamlessly integrated with centralized visibility and control. “The flexibility and scalability of the solution was a big selling point for Batteries Plus Bulbs,” says Peter Van Opens, a client success manager at LeewardBA.

Starting To See Tangible Benefits

The deployment was rather complex, given the number of point products being retired and the number of separate franchise groups Lehman’s team supports. Batteries Plus Bulbs and LeewardBA moved at a deliberate pace and recently completed the rollout. “We are now working on final fine-tuning for this project and planning for next steps,” Klein says. And while specific results are not available yet, the company is beginning to see benefits.

Perhaps the most visible benefit to Lehman’s staff was a greatly increased level of visibility of the company’s security posture and infrastructure. “We were often in the dark with our prior solution,” Lehman remembers. “Our prior MSSP did not provide us with actionable insights about what risks we faced or what we could do about them.”

“Now we have security information by glancing at a screen, and we can drill down to any level of detail we need,” says Dan Dugan, vice president of IT for Batteries Plus Bulbs. “We can take a more proactive stance to managing security. This gives us confidence that we are equipped to manage security threats for the next 5 to 7 years.”

Another benefit is the flexibility of the Fortinet solution. “I was pleased with the many ports the Fortinet devices have,” Lehman says. “This gives us the flexibility to add services in the future without having to rearrange the infrastructure.”

One example of this flexibility is that stores have been able to set up a separate wireless protocol specifically for testing smartphones and tablets that are brought in for repair. “We need to isolate customer devices from company devices,” Lehman explains. “So, it is prudent to be able to have a dedicated testing protocol.”

“These tools enable us to provide centralized management from a single pane of glass, detailed reporting, workflow automation, and trends analysis. This enables the in-house team to get a complete picture of their security posture at a glance, at any time.”

– Jason Klein, CTO, Leeward Business Advisors

Controlling costs is another benefit of the LeewardBA/Fortinet solution. “This wound up being a cost-neutral project,” Lehman relates. “When we set up the security infrastructure eight years ago, franchisees starting paying a cybersecurity fee that they had not paid before, and this was frustrating for many of them. The new solution does not increase their fees, yet it delivers much more robust security and performance.”

Finally, Batteries Plus Bulbs now has a scalable solution that makes adding additional security products and services very easy. “Having a single provider gives us economies of scale, and we know that services we add later will be compatible,” Lehman asserts. “Some of what will happen in the future is unknown today, but we have the depth and breadth in our security architecture to provide protection from whatever comes along.”

Looking to the Future

“We have recently transitioned to a new point-of-sale solution,” Lehman says. “With that complete, we are looking to move forward with the next steps of our security roadmap. Some possibilities include sandbox analysis using FortiSandbox to detect zero-day threats, FortiAuthenticator to provide secure authentication, and the newly released version of the Security Fabric. Whatever we do next, we know we’re in good hands with LeewardBA and Fortinet.”

“Our ability to dynamically support the desktop infrastructure, switching, and the wireless infrastructure in addition to the SOC was a huge advantage.”

– Michael Polzin, CEO,
Leeward Business Advisors



www.fortinet.com

Copyright © 2021 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 General Counsel, 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.