On lists of industries facing the highest risk of cyberattack, car dealerships do not typically appear at the top. That is an oversight, according to Shane Williams, director of IT for White Family Dealerships, which operates in 18 locations across Ohio, Wyoming, and South Dakota.

“Car dealerships are a gold mine of customer information, so we need to follow security protocols similar to those that banks follow,” he says. “If we experienced a successful breach and had not done enough to prevent it, we would face substantial fines from the FCC [Federal Communications Commission]. It would also damage our brand.”

White Family Dealerships is committed to securing customer information and to meeting requirements of both regulators and the auto manufacturers whose vehicles it sells. These run the gamut from Land Rover and Porsche to Chevy, Dodge, and Ford. “Each manufacturer has its own philosophy about what cybersecurity we need,” Williams says. “We periodically provide them with information on our email and perimeter security, antivirus, and even physical security. Some of them then make surprise visits to dealerships, to verify that we are actually doing what we claim we are doing.”

In the Market for Lower Cost, Improved Ease of Use

The challenge for Williams is that he and two other staff members manage an IT, network, and security infrastructure that spans three states. Previously, White Family Dealerships contracted with a third party to oversee its network security and dealership management system (DMS), but that was not ideal.

“If I needed to make a change or to check on anything, it was a long process,” he says. “I would call, then be put on hold forever. In the end, I might get a support person who did not understand what I was asking.” Williams was also spending a good deal of time on the road. “Two or three times a week, I would need to drive to a dealership to troubleshoot, install updates and patches, or add equipment. All in all, a lot of my time was wasted in that environment.”

When one automaker began encouraging dealerships to contract with a specific managed security service provider (MSSP) to install and run FortiGate next-generation firewalls (NGFWs), Williams reconsidered White Family Dealerships’ IT environment. The third-party
service provider offered him only limited visibility into network security, and the idea of single-pane-of-glass management was appealing. For both cost and control reasons, he wanted to bring management of all network and security infrastructure in-house.

“The goal was to add security and increase business continuity,” Williams says. “Time without network services is money lost. Especially since the beginning of COVID—with more and more people shopping and doing business over the internet—maximizing uptime for our network infrastructure has become critical.” He also saw an opportunity to reduce connectivity costs by replacing the multiprotocol label switching (MPLS) connections between the dealerships and company headquarters with software-defined wide-area networking (SD-WAN).

Williams quickly found Fortinet solutions to be an attractive option. The company’s approach to security-driven networking converges networking and security to enable network firewall, SD-WAN, and SD-Branch solutions, managed through a single pane of glass. Fortinet Secure SD-Branch provides WAN with industry-leading security at the network edge, to improve user experience and reduce overall cost. It also extends the benefits of SD-WAN throughout the enterprise branch, enhancing security and simplifying management across the local-area network (LAN), end-user systems, wireless and direct internet connections, and any Internet-of-Things (IoT) devices the company is using.

White Family Dealerships liked the price of SD-WAN networking, as well as the fact that security is built into all the components of Fortinet Secure SD-Branch. In addition, Williams says, “Ease of use was a major decision factor. I was familiar with other security and networking vendors; I was even certified in another vendor’s solutions. But I was impressed with the simplicity of the Fortinet interface, which makes it quicker and easier to accomplish the same tasks.” Another consideration was the tight integration among NGFWs, switches, and access points. “One of the things I like best about the Fortinet platform is the integration of all these different components,” Williams adds.

Fortinet Security Fabric Brings Excellent Visibility

White Family Dealerships deployed a FortiGate NGFW, FortiSwitch switches, and FortiAP access points to provide wireless connectivity for each dealership and company headquarters. To start, the NGFWs provided network connectivity via Internet Protocol security (IPsec) virtual private network (VPN) tunnels on the legacy MPLS connections. Within a year, however, the company turned on Fortinet Secure SD-WAN in each dealership’s FortiGate to implement security-driven networking across all the company’s network edges.

“This creates a much simpler approach to the WAN,” Williams says. “Traditional IPsec mesh would have become unmanageable over time, because it does not scale. Previously, adding our 18th site would have required adding a VPN connection at each of our 17 existing sites, plus adding 18 connections at the new site, to create a complete mesh.

Now, we are managing a single VPN tunnel at each location.”

The company also deployed the FortiEDR endpoint protection, detection, and response solution to protect machines companywide. White Family Dealerships had experienced a couple of minor incidents that highlighted for Williams the need for a stringent endpoint solution. “The human factor is the biggest security risk, in my opinion,” he says. “I can put all kinds of firewalls in place, and then an individual might be duped into clicking on a phishing email. The way the FortiEDR platform functions within the operating system kernel gives me peace of mind.”

Williams’ small team uses FortiManager and FortiAnalyzer virtual machines (VMs) to oversee threat detection and response activities across the network. “FortiManager is a powerful part of the Fortinet Security Fabric and one of my favorite tools for managing our network
Better Security That Saves Time and Money

The transition from MPLS to SD-WAN has significantly reduced operating expenses for White Family Dealerships. "MPLS is expensive," Williams says. "By replacing the MPLS infrastructure with SD-WAN, we’re saving around $120,000 a year. We expect to achieve a return on our investment [ROI] in about three years." Williams’ team is also saving a substantial amount of time, mostly on travel among the company’s locations. As an example, he says, when he needs to add a FortiSwitch in a dealership, he can simply ship it to the location.

"Most of our dealerships have an employee who can plug in the wires for us," Williams says. "So, we can provision the switch in FortiManager before we ship it, and when that local person plugs it in, the switch will download the appropriate configuration. Since we implemented FortiManager early in the process, we were able to make a lot of the networking and security changes in our SD-Branch rollout from a central location, versus logging into every device in person at the dealership."

Remote deployment of devices is especially beneficial because the company is in growth mode. "Our owners are always on the lookout for opportunities to add another dealership to the portfolio," Williams says. "We have standardized our dealer infrastructure and put together an onboarding kit. It includes Fortinet Secure SD-WAN, FortiSwitches, and FortiAPs. That means we can get acquisitions tied into our corporate network fast and with very little strain on IT resources."

Now, White Family Dealerships has begun installing a second FortiGate NGFW at each location for high availability, and a FortiExtender device to provide internet connectivity in case the SD-WAN connection fails. This business continuity solution is already in place at the dealerships with the highest turnover (and, therefore, the largest potential revenue hit from system downtime).

The SD-Branch solution meets the cybersecurity requirements of all the auto manufacturers White Family Dealerships works with. It also provides the level of security the company requires. "These days, people are continuously trying to break into our network," Williams says. "Years ago, the bad guys ignored car dealerships, but cybersecurity is becoming a bigger threat for us. Our Fortinet Secure SD-Branch solution helps me sleep better at night."