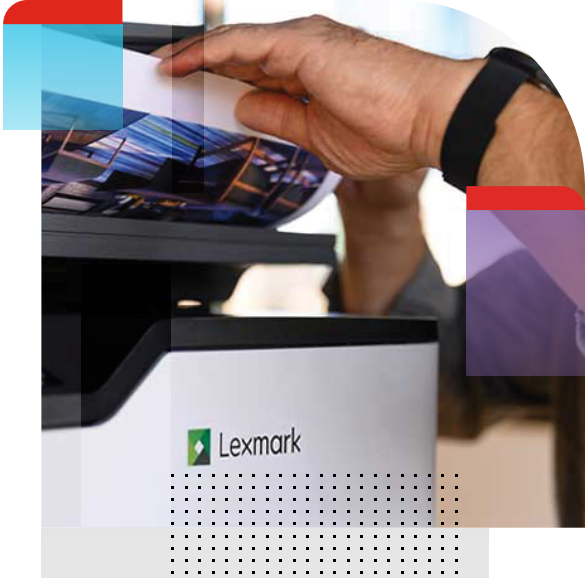
CASE STUDY

Lexmark Cuts WAN Costs in Half While Shoring up Its Global Security



Lexmark's business is built on eliminating IT burdens for companies whose core competencies lie outside the tech sector. The Lexington, Kentucky–based organization provides printer hardware, accessories, services, and other enterprise solutions to customers across more than 170 countries worldwide.

And just as the company is focused on solving customers' imaging and document creation challenges so that customers do not have to, the Lexmark IT team is committed to streamlining access to systems and connectivity for their internal customers—Lexmark's business and development groups. Ensuring that security is both effective and transparent to end users is a key objective.

"We have several thousand employees spread across multiple sites throughout North and Latin America, APAC [Asia Pacific], and EMEA [Europe, Middle East, and Africa]," explains Tony Arcuri, security architect at Lexmark. "Like most companies, we have a concern that somebody might infiltrate our network and deploy ransomware or get access to sensitive information. "And then, of course, there are supply chain concerns," he adds. "Since we handle a lot of manufacturing, we need to make sure that the technology we build are safe and secure."

Cutting Connectivity Costs in Half

To that end, Lexmark began rolling out FortiGate Next-Generation Firewalls (NGFWs) several years ago. From headquarters to the company's various global data centers, sales offices, and manufacturing facilities, "the FortiGates were originally installed as edge firewall devices for outbound traffic," Arcuri says. "Since then, they have evolved into a lot more than that."

The first step in this evolution was a transition of the company's internet connectivity. Previously, all Lexmark sites connected to the corporate global wide-area network (WAN) via multiprotocol label switching (MPLS). But Lexmark saw an opportunity to significantly reduce connectivity costs, while also boosting network security.

"We looked into what it would take to replace MPLS with FortiGates using an internet-based ADVPN [auto-discovery virtual private network] solution," Arcuri says. "We use a multi-cloud hybrid approach and we decided to implement virtual FortiGate firewalls in all our environments. FortiGates are a good solution for us because we can use centralized tools and our operations team can manage security in these different clouds through the same FortiGate platform."

The Lexmark team built out private networks using cloud-based FortiGate NGFWs in each geographic region—EMEA, APAC, and North America—serve as the hubs in the WAN's new hub-and-spoke architecture. The local physical FortiGate

Lexmark™

"We cut our WAN connectivity costs in half. We are saving hundreds of thousands of dollars a year by navigating away from MPLS."

– Tony Arcuri,
Security Architect, Lexmark

Details

Customer: Lexmark

Industry: Technology

Location: United States

Business Impact

- Minimized risk that ransomware or other cyber threat will be successful
- Minimal staff time required to maintain security infrastructure across multiple locations around the world
- WAN connectivity costs cut in half vs. prior MPLS solution
- Improved security on technology products developed internally and deployed to Lexmark customers

NGFWs in each Lexmark location then connect to the hubs via Internet Protocol security (IPsec) tunnels with VPNs layered on top. This architecture connects the company's dispersed locations and securely connects users to cloud resources.

It has also enabled Lexmark to eliminate its MPLS connections, for substantial cost savings. "We cut our WAN connectivity costs in half," Arcuri says. "We are saving hundreds of thousands of dollars a year by navigating away from MPLS."

Security and Efficiency in Equal Parts

Next, the team turned on the load-balancing capabilities in the FortiGate NGFWs. "The FortiGates provide an easy path for redundancy and high availability," Arcuri says. "Most of our sites have two or three ISPs [internet service providers], and the FortiGates route traffic to the best choice so that we are using all the available circuits and not saturating any of them."

Finally, Lexmark is now configuring the FortiGates to provide virtual local-area network (VLAN) segmentation. "So, we will segment our server VLANs, which will segment out sensitive environments such as manufacturing facilities," Arcuri says. "The FortiGates provide us with a zero-trust platform and enable us to get more details on the type of traffic."

Arcuri says these WAN improvements have boosted Lexmark's security posture. "We are confident in the security we have achieved through our Fortinet solutions," he says. "When we stand up a FortiGate or put access layers or firewall policies in, and we put web filters in, or we turn on certain security profiles, we are confident it is going to work."

Solutions

- FortiGate Next-Generation Firewall
- FortiAnalyzer

"FortiAnalyzer is very easy to use. It is simple to move around and get to the data we need to see in order to make the right decisions. We have worked extensively with another vendor over the years, and the usability of the Fortinet solutions is far superior."

– Tony Arcuri,
Security Architect, Lexmark

Easy Visibility Simplifies Security Management

The Lexmark team leverages FortiAnalyzer, Fortinet's Security Fabric analytics and automation solution, to transform the FortiGates' data into enhanced management visibility. "We use FortiAnalyzer all the time," Arcuri says. "If we are investigating a security incident, or we are trying to set up new infrastructure services, and we need to figure out what the traffic profile looks like, we turn to FortiAnalyzer."

He cites an example: A developer might come to the security team complaining about a site they cannot access. "We will research using FortiAnalyzer and find out that it is something like a reverse proxy or reverse shells," Arcuri says. "Then we can push back against what they are doing, since we want to lock down those technologies to make sure we are pushing only the most secure solutions out to customers." Ultimately, he adds, the FortiAnalyzer investigations help his team ensure the products they are providing to customers are as secure as possible.

This level of visibility was much more difficult to achieve in Lexmark's legacy environment. Arcuri says, "FortiAnalyzer is very easy to use. It is simple to move around and get to the data we need to see in order to make the right decisions. We have worked extensively with security management tools from another vendor over the years, and the usability of the Fortinet solutions is far superior."

A Partnership for the Long Term

COVID-19 struck when Lexmark was in the midst of establishing its hub-and-spoke WAN architecture. The remaining MPLS connections meant "Lexmark was not in the best position to support a fully remote workforce," Arcuri says. "We had to make some quick design changes to our global infrastructure to support working from home. We deployed them quickly, with FortiGates essentially serving as our WAN routers."

Within one month of employees shifting to remote work, Lexmark's network operations team was able to migrate 85% of the company's MPLS-connected sites and partners to the new internet-based ADVPN WAN. The sites and partners that remain

on MPLS—either because the transition is time-sensitive or because the location simply cannot support the requisite internet circuits—will be migrated over the next few years.

Now, the Lexmark team is evaluating FortiAP wireless access points and FortiSwitches to move Fortinet security and ease of management to the Lexmark LAN edge. "Theoretically, having a Fortinet infrastructure throughout would give us a lot of capabilities to manage security and network controls all the way through the stack," Arcuri explains. "In contrast, if we mix and match LAN infrastructure and WAN infrastructure, we might lose a lot of that functionality. It is a good idea to have some diversity in your technology stack, from both a business and technology perspective, but there would be significant benefits to having a Fortinet stack throughout our LAN."

That decision has yet to be made. For now, Arcuri is enjoying the dramatically simplified security throughout Lexmark's WAN. Basically, he says, "we set it up, and it just always works. It functions like we expect it to, so nobody has to keep a close eye on it." For a company focused on reducing customers' technology-related headaches, that "set it and forget it" mentality is the sign of a truly successful solution.

"The FortiGates provide an easy path for redundancy and high availability. Most of our sites have two or three ISPs, and the FortiGates route traffic to the best choice so that we are using all the available circuits and not saturating any of them."

– Tony Arcuri,
Security Architect, Lexmark

July 15, 2022 1:44 PM
1595255-0-0-EN