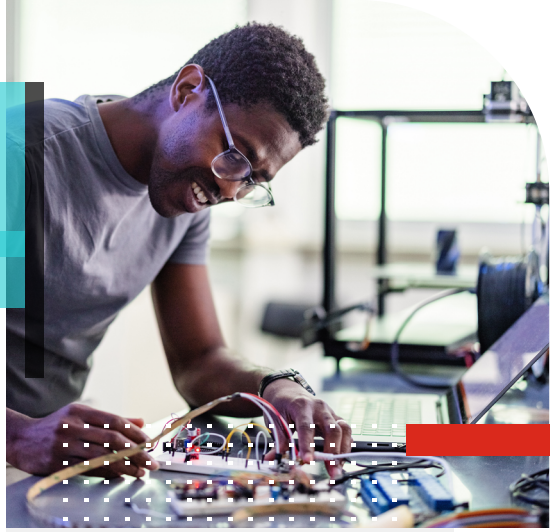
CASE STUDY

Metro Tech Network Team Can Manage More Devices with 88% Less Staff Effort and Lower TCO



Skilled tradespeople, such as plumbers, electricians, welders, and carpenters, are in such high demand these days that North American companies frequently struggle to fill open positions. The shortage of these skilled workers is impacted as more young people choose to attend college, as well as an aging workforce.

Oklahoma City's Metro Technology Centers are helping mitigate this problem. The school was established in 1979 to provide career and technical education for Oklahoma City residents. Today, it does so through a network of four large campuses and four additional sites, with programs funded by prospective employers and property taxes.

"We offer multiple hands-on programs ranging from welding, plumbing, and electrician training to STEM [science, technology, engineering, and math] and biosciences courses, including real-world training at a couple of local hospitals," explains Dr. Indrit Vucaj, director of information technology and data management for Metro Tech. "We serve approximately 1,900 high-school students, who come to one of our locations for part of the school day, and about 35,000 adult students, who participate in either full-time programs or on-demand industrial training."

All these programs rely heavily on technology, so a successful cyberattack or data breach of the Metro Tech network would have a huge impact. "We provide our students with the latest and greatest tech," Vucaj says. "The downside is that an attack might render our students unable to learn for a while."

He also continues that they "must comply with an assortment of state and federal statutes around data governance and network security," he continues. "There is also a serious risk of reputational damage. Less technology protection around our data vector means less reliability and institutional trust for our stakeholders. We might also suffer from falling enrollment rates if prospective students saw our campuses as less attractive. We protect our network because it is the right thing to do—and by doing so, we avoid the serious consequences of a prospective attack. It is a medium we take very seriously and rely on the best to prevent such consequential protection. "

Fortinet Firewalls Are a "Game-Changer"

Several years ago, Metro Tech's network security was hampered by a landscape of misconfigured products. The school had firewalls, switches, and access points from three different providers. And it became encumbered upon the IT staff to configure work instead of strengthening posture. "We had to have different people specializing in different areas of networking, and we would still sometimes need to turn to an MSP [managed service provider] for assistance," Vucaj says. "Keeping the network running took a village, and basically, the complexity of the environment created incompatible and vulnerable systems."

"The Fortinet Security Fabric mesh has consolidated and elevated our security utilization by fourfold. It has been quite impressive. I have been particularly impressed with how well the FortiAPs work. That has improved the speed and reliability of our Wi-Fi, enabling teachers and students to access curriculum and other resources much more quickly with fewer issues and an always reliable amount of uptime."

Dr. Indrit Vucaj
Director, Information Technology and Data Management,
Metro Technology Centers

Details

Customer: Metro Tech

Industry: Education

Headquarters: Oklahoma City, Oklahoma

Vucaj and his colleagues began shopping for a new solution set. Their two most important criteria were ease of management and cost. "We were looking for the most comprehensive suite of products that we could find at a fair price point, and we wanted to minimize the effort required for network management," he says. "Of all the vendors we evaluated, Fortinet was by far the best, especially in reducing time dedicated to managing the network. One key factor was that all Fortinet products are native to Fortinet standards. That reduces the complexities of trying to make the solutions work."

In 2020, Metro Tech rolled out Fortinet solutions throughout its LAN. FortiGate Next-Generation Firewalls (NGFWs) protect the network edge at each of the school's eight locations, with a high-availability (HA) pair of FortiGates at the two largest campuses. For additional protection, the school internally segments its network into many virtual LANs (VLANs) to prevent threats from moving laterally using FortiSwitch secure Ethernet switches. This is particularly crucial in areas of the school that rely heavily on OT and IoT devices.

"The internal segmentation within the FortiGates has been a game-changer for us," Vucaj says. "For example, we have a lot of very high-end audiovisual [AV] equipment that needs to be on the network. Instead of changing our network settings to accommodate this gear, we gave it its own VLAN. Now the AV team can manage the complexity of their systems without putting the rest of the network at risk."

Another example involves Metro Tech's "building-sized" airplane simulator. "For security reasons, and because the FAA requires it [Federal Aviation Administration], we have to run the plane simulator on its own network segment," Vucaj explains. "And then, a third example is our wellness center. The instructors use videos in some dance classes, which they record or livestream. We segmented off the wellness center, then within that VLAN, we further segmented to separate the dance studio. Now, people who go to the gym can hook their phone up to the guest network to play music, but they cannot watch the live stream of the dance classes. It offers quite an experience to our guests and stakeholders."

Staff Productivity Soars as Total Cost of Ownership Falls

FortiSwitch secure enterprise switches and FortiAP secure wireless access points provide switching and Wi-Fi access throughout all Metro Tech locations. Vucaj is pleased with the tight integration among the LAN solutions.

"The Fortinet Security Fabric mesh has consolidated and elevated our security utilization by fourfold. It has been quite impressive," he says. "I have been particularly impressed with how well the FortiAPs work, even when positioned very close to one another. To increase bandwidth capacity, we put an access point in each classroom. That has improved the speed and reliability of our Wi-Fi relative to our legacy environment, enabling teachers and students to access curriculum and other resources much more quickly with fewer issues and an always reliable amount of uptime."

The team uses the FortiManager security management platform to schedule firewall updates and roll out policy changes to their entire environment simultaneously. "We have been very happy with FortiManager," Vucaj says. "Tasks that were previously manual and cumbersome now take us seconds.

Business Impact

- 88% fewer network staff manage nearly 3x as many network devices
- "Cumbersome" network management tasks now take 10 seconds
- Staff can fill in for one another, rather than each specializing in niche areas of network management
- One-third lower cost for more network and security devices
- Streamlined compliance with state and federal network security requirements
- Reduced risk to OT equipment such as AV devices and dance class live streams
- 32 million DDoS network attacks thwarted daily; no successful attacks over five years

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiAP
- FortiManager
- FortiEDR

Services

- FortiGuard AI-Powered Unified Threat Protection Bundle

As an example, before Fortinet, we would configure each AP separately, connect it to the network, and then install it. Now [with FortiManager], all we have to do is copy and transfer the configuration. We do this en masse, and we can deploy more APs. Before we had about eight dedicated staff across the firewalls, switches, and access points, and we relied on an MSP for some activities. Now, we can operate with only one person dedicated to networking, and we manage all the Fortinet solutions internally. At the same time, we have increased from 120 access points to about 520. That is almost four times as many devices being managed by one-eighth the number of people. Our helpdesk tickets have decreased by about 50% in the past five years. We're very pleased with the increase in our infrastructure reliability and the total lower cost of ownership," Vicaj says.

In fact, the solutions' ease of use has translated into higher staff productivity across the board. "Going with Fortinet meaningfully removed the burden from my team onto the tech stack itself," Vucaj reports. As a bonus, staff members can fill in for one another, so when one person takes a vacation, others can easily cover that role. "A lot of the knowledge is transferable because Fortinet solutions are built on industry best practices. Even if someone is just too busy to perform a certain task, we may have someone else jump in." In addition to creating a more pleasant and proactive working environment, this saves Metro Tech money.

"With Fortinet," he continues, "we could take the cost we were paying other vendors and place it into the networking and security stack. Fortinet has reduced the cost per unit, and we no longer need help from an MSP for tasks like setting up and configuring switches. Previously, we had around 150 switches, and the annual renewal of our support on those cost almost $300,000. This year, with Fortinet, we had more than 250 switches, plus 400 additional access points, and our support renewal cost is around $200,000. We can do much more with less because of the Fortinet security systems."

"We have about 32 million DDoS attacks against our network every day. It only takes one to cause a disaster, but none of those attacks has gotten through for the past five years."

Dr. Indrit Vucaj
Director, Information Technology and Data Management, Metro Technology Centers

"When we first integrated vertically to Fortinet, we intended to assess the performance and resilience of FortiGates, FortiSwitches, and FortiAPs for five years, then re-evaluate. We have thoughtfully and deliberately assessed and are jumping in even further."

Dr. Indrit Vucaj
Director, Information Technology and Data Management, Metro Technology Centers

Successfully Blocking 32 Million Attacks Each Day

Not only that, but security has improved significantly as well. "We have about 32 million DDoS [distributed denial of service] attacks against our network daily," Vucaj says. "It only takes one to cause a disaster, none of those attacks has gotten through for the past five years. We are particularly happy that the Fortinet security stack gives us insights into where and how various attacks are coming on our network."

In fact, he recounts a specific incident in which some students attempted to move from the guest network at one campus to the back-office network. "We were alerted immediately, and we shut down that specific access point, reset the connected switch, and brought it up online within minutes, all without any interruption of daily activities," Vucaj says. "One thing I really like about Fortinet is the capability to turn off individual devices. How they connect to FortiManager, we can deactivate one device without impacting another. In our previous legacy environment, we would not have seen the threat those students posed, nor could we have responded nearly as quickly."

Next, Metro Tech intends to roll out FortiGate virtual machines (VMs) in Microsoft Azure as it closes its on-premises data centers and becomes a cloud-exclusive organization. And Vucaj oversees testing the FortiExtender wireless WAN solution to provide passenger connectivity on Metro Tech buses.

"We are thinking about how we want to provide that connectivity, whether through our network or analog antenna radio waves," Vucaj says. "We are playing around with options, but one of those is to use FortiExtender to connect devices to Metro Tech's guest network. This would provide a secondary benefit, as well. Students who may not have access to the internet outside of the classroom will be able to connect wirelessly off campus and gain access to school work. We could park buses with FortiExtender Wi-Fi in certain neighborhoods so students in those areas could access the internet outside of class."

Whatever Metro Tech's decision on the bus Wi-Fi solution, Vucaj looks forward to a long and mutually beneficial partnership with Fortinet. "When we first moved to Fortinet, we intended to try the FortiGates, FortiSwitches, and FortiAPs for five years, then re-evaluate to see whether they were still the right fit for Metro Tech," he says. "Now, five years later, we have thoughtfully and deliberately assessed and are certainly not going back. In fact, we are jumping in even farther. I now require everyone on my team to pursue Fortinet certifications; that is how much I believe in the products.

"I tell people that Metro Tech relies heavily on three technology verticals. We have a primary hardware vertical that integrates with our hardware and software stack, a productivity and cloud software vertical that consolidates our data. For anything network or security, we turn to Fortinet."

Dr. Indrit Vucaj
Director, Information Technology and Data Management,
Metro Technology Centers

June 9, 2025 2:46 PM / CS-73-0-0-EN