CASE STUDY

Tier 1 Research University Leverages Next-Generation FortiGate Capabilities to Protect Students and Data

This research hospital attracts some of the best and brightest students from around the world. It is ranked as one of the top 10 best U.S. public universities and regularly receives accolades for many of its graduate and undergraduate programs.

Much of the university's renown comes from its heavy emphasis on research. A full 50% of undergraduates participate in research projects, supported by large inflows of grants. In the 2021–2022 school year alone, the university received more than $1 billion in research funding across its many disciplines.

The emphasis on and funding for scientific data also means the university must invest heavily in its cybersecurity defenses. "Oftentimes, agencies giving grants have particular security requirements," explains the data center services manager for the university. "In the past, we have seen requirements for data retention, disaster recovery, and backup policies. More recently, the requirements have extended to cybersecurity policies as well. We often need an attestation that our security environment meets the granting agency's criteria before we can submit a grant proposal."

Meeting these requirements can be challenging since the university's IT infrastructure is largely decentralized. The manager's IT team maintains the campus' core network and the two data centers where centralized applications live. But individual departments are responsible for their own equipment and their own security.

"Years ago, as cybersecurity increased in importance, we mandated that departments put all their internal systems behind firewalls, but some groups did not understand the risks and made their firewalls more porous than we were comfortable with," the manager says. "Since our IT team has security expertise, we built a Firewall-as-a-Service [FWaaS] option. For the one-third of departments that are currently using this service, we maintain and manage their firewalls."

Selecting a Next-Gen Firewall to Offer as a Service

In the first iteration of the FWaaS alternative, the university's IT team managed each department's firewalls individually. It soon became clear that centralized management of a stable of next-generation firewalls (NGFWs) would be more efficient and more secure. Deploying NGFWs would also enable the university to retire legacy intrusion prevention system (IPS) devices that were approaching end-of-life.

The team considered two NGFW vendors. "As a state institution, we follow a specific purchasing process," the manager says. "Fortinet and the other vendor were pre-vetted. We launched a proof of concept using a box from each vendor, trying them out side-by-side to determine which would be the best fit for our campus's current and future needs."

"The greatest benefit we have seen is the automatic threat protection. We are facing threats that we would not know about without the FortiGates, and even now, we do not really need to think about them because the firewalls are taking care of them. That has been incredibly valuable to us."

Data Center Services Manager

Details

Industry: Higher Education

Business Impact

- Over 2 million threats blocked daily
- Campuswide view of both zero-day and known threats
- Insight into threats that would not have been noticed by legacy security solutions
- Automated threat response secures networks without manual effort

They evaluated the alternative NGFWs across several areas of protection: their enforcement of network access policy, the effectiveness of their IPS rules in identifying known threats, the ability to customize the firewalls' threat response, the ability to quarantine external IP addresses that cross certain behavioral thresholds, and integration with third-party systems to provide closed-loop security automation. Then the team subjected both NGFWs to the same realistic test traffic.

Through this analysis, the selection team determined that FortiManager had a more intuitive interface than the competition and that its policies for dynamic IP address access denial had a simpler and more intuitive workflow. The team also preferred automation features of FortiManager because it eliminated the need for additional tools and made programming to the Fortinet API simpler.

Plus, the manager says, "The other vendor said they had an API, but they did not. By contrast, the entire Fortinet platform is built on the REST API. That made us feel comfortable as FortiManager would give us all the information and perimeters right from the GUI interface without going into APIs, whereas we were concerned that the other vendor's management console might not deliver the same functionalities in our specific setup."

Centrally Managed Security for 25 Diverse University Departments

The university deployed a pair of FortiGate NGFWs at the network perimeter in its data centers. In addition, each department that has chosen the FWaaS model has its own FortiGate NGFW, also located in one of the data centers and managed by the IT security team. "We partnered with our network operations center and located the Firewall-as-a-Service devices close to the network core," the manager explains. "All the Layer 3 traffic comes in straight from the core, then we use the VLANs created by the firewalls to distribute the Layer 2 traffic throughout campus."

Using the FWaaS, departments benefit from a standard approach to network security. The team further segments each firewall's traffic into one of at least three zones. "The university's state system's IS-3 security policy defines four protection level classifications—from P1, which is for public information, to P4, which is for information that needs the most security, such as financial and personal data," the manager says. "With our FWaaS approach, we create one security zone for the department's public-facing pages, one for its internal private traffic—whatever sits behind the firewall and needs protection, and one for all the user workstations where people are logging in and then browsing the web."

Each firewall is equipped with the FortiGuard AI-Powered Security Services Unified Threat Protection (UTP) Bundle. They chose to license the east-west firewalls with UTP, at the same level as the perimeter firewalls, to have insight into internal threats that we may be facing. This helps prevent a horizontal spread of attacks. "The fact that we have centralized threat protection and intrusion prevention is incredible," the manager says. The team uses FortiManager for unified policy deployment and timely distribution of FortiGuard security updates to all its managed FWaaS firewalls and uses FortiAnalyzer for centralized logging, visibility, and reporting.

"There have been a couple of situations where we had to research why certain traffic was not making it to its destination," the manager says. "The insights provided by FortiAnalyzer and FortiManager logs significantly simplify the process of tracing such issues. According to our security protocols, we've consistently found that the traffic that was stopped was correct."

"FortiManager is key to our entire environment," he continues. "It gives us a single pane of glass for managing all the firewalls across the 25 departments in our Firewall-as-a-Service program. We log in to one console and push the rules out from there. I can't even imagine not having this capability. FortiAnalyzer is also very helpful. Its out-of-the-box reports show us compromised systems and rules that have not been used in a certain period. So FortiAnalyzer helps us prune out the old rules, which can be difficult in a university environment."

Business Impact (cont.)

- Streamlined management activities save time for IT Security staff
- 100% accuracy in IP address blocking—no false positives
- Visibility to inactive firewall rules that need to be pruned

Solutions

- FortiGate Next-Generation Firewall
- FortiManager
- FortiAnalyzer

Services

- FortiGuard AI-Powered Security Services Unified Threat Protection Bundle

Instant Visibility into Threats Campuswide

All told, the manager says the Fortinet Security Fabric makes the university's network much more secure. "The greatest benefit we have seen is the automatic threat protection," he says. The research university is seeing over 2 million threats each day. "We are facing threats that we would not know about without the FortiGates, and even now, we do not really need to think about them because the firewalls are taking care of them. That has been incredibly valuable to us."

Since the Fortinet deployment, the university has discovered compromised workstations on various department networks. "They were sending traffic that the FortiGates were blocking on the outbound path," the manager says. "The FortiGates told us, 'This device is talking to a command-and-control center, which is probably indicative of a compromise.' So, we were able to investigate and mitigate those issues, and that is something we could not see in the past."

"Our Fortinet architecture gives us much better visibility into security events across all the different departments whose security we are managing," he continues. "And because we are managing everything centrally, we can get a bigger threat picture across the entire campus. If there is a zero-day threat, we can see whether it is localized to one department or is something that is impacting all the different departments. Then we can provide education or change our security policies as needed."

Management of the firewalls takes a lot less time now than it did in the past. "Previously, if we wanted to apply a rule to a bunch of different firewalls, we would have to log into 30 separate devices," the manager says. And having the UTP Security Services Bundle on every single firewall means we are protected from east-west attacks between the various departments."

In addition to reducing the risk of a cyberattack, the increased visibility gives university administrators more confidence to sign off on grant requests. The data center services manager also loves the scalability of the Fortinet architecture. "Adding new systems basically just involves adding a new license," he says. "Our FortiGate infrastructure is almost infinitely scalable."

> *"FortiManager is key to our entire environment. It gives us a single pane of glass for managing all the firewalls across the 25 departments in our FWaaS program. We log into one console and push the rules out from there. I can no longer even imagine not having that capability."*
>
> **Data Center Services Manager**

> *"Our Fortinet architecture gives us much better visibility into security events across all the different departments whose security we are managing. And because we are managing everything centrally, we get a bigger threat picture across the entire campus."*
>
> **Data Center Services Manager**

Now, the data center services manager and his team are exploring their options for zero-trust network access (ZTNA) and secure access service edge (SASE). Fortinet solutions are on the shortlist for both. "We foresee introducing ZTNA to provide access to certain systems within our Firewall-as-a-Service infrastructure," he says. "That is definitely on the roadmap, and the FortiEDR endpoint detection and response solution seems like a solid option. We are also curious about SASE. One of the issues we have is split tunneling vs. full tunneling. FortiSASE would allow us to full tunnel from the client to the SASE cloud, then split from there, which would be a huge security improvement."

Either option would help the research university to comply with anticipated future cybersecurity standards at the federal and state levels, as well as within their state's university system. "Fortinet has been a great partner to our university in helping us secure our Firewall-as-a-Service offering," he concludes. "We look forward to learning how we can expand our relationship with Fortinet to help us adapt quickly to whatever regulations may come down in the future."

April 14, 2025 11:10 AM / CS-59-0-0-EN