# Securely Supporting a Diverse and Open Environment at Texas A&M University at Qatar

Texas A&M University at Qatar works to serve Qatar, helping to achieve its National Vision 2030 by enriching its greatest natural resource – its people. Guiding the institution's way is a strategic plan which blends the goal of Texas A&M's Vision 2020 with the Qatar National Vision and includes four strategic imperatives – teaching and lifelong learning, research, engagement, and organizational excellence. This branch campus of Texas A&M University has graduated more than 840 Aggie engineers who are currently making a difference in the development of the State of Qatar, the region, and the world.

The Texas A&M at Qatar campus attracts students, faculty, and staff from around the globe, leading to tremendous diversity in devices, applications, and user requirements. "Any higher ed institution must support an open learning environment, which means we are far less restrictive with the types of apps students or faculty can run – they have considerably more freedom than users at most enterprises – and that lack of control makes security more challenging," says JD Lewis, enterprise technologist at Texas A&M at Qatar. "I spent 10 years at the main campus in College Station where we also have a diverse population, so I appreciate the importance of being open. However, here we encounter apps that are common in Asia and Europe that pose additional security risks in our environment."



## Executive summary

**Customer name:**
Texas A&M University at Qatar

**Size:**
500+ students and 450+ faculty and staff

**Industry:**
Higher Education

**Location:**
Education City, Doha, Qatar

**“Cisco gives us the visibility and flexibility to identify and stop threats faster which is particularly challenging and important when you’re dealing with a wide range of devices, apps, and users in an education and research environment”**

**JD Lewis**
Enterprise technologist at Texas A&M at Qatar



## Meeting the requirements

As the hardware was aging at their branch campus, including their previous Cisco firewalls, Texas A&M at Qatar had an opportunity to upgrade multiple pieces of hardware from access, to the data center, to security. Lewis and his team evaluated competing products from several vendors and found that the Cisco Firepower 4110 Series NGFW with Firepower Threat Defense met all their requirements, beginning with enhanced **visibility and flexibility**.

“Our main objective was to find a solution that would offer greater visibility into our traffic,” said Lewis. “We recognize that no solution is capable of preventing all risks or threats, but Cisco offered visibility that would allow us to track a file that retroactively appears to be malicious. That, in combination with the deeper visibility we gain from Snort were big selling points, particularly since our team is already familiar with Snort.”

As with every security organization, **budget constraints** were a big consideration. “We were looking to spend our resources efficiently,” said Lewis. “Cisco offered flexibility with the number of interfaces and integrated security capabilities which made us confident that whatever deployment we chose it would meet our requirements and evolve with us.”

Being a small shop, **well-defined and intuitive management** of the enhanced feature set was significant. The streamlined and workflow-based firewall management of the Firepower Management Center solved this challenge. Yaser Mansour, security analyst at Texas A&M at Qatar, explains, “Some of the products we reviewed involved assembling multiple, different hardware appliances to make a complementary and comprehensive solution. With Firepower Threat Defense these capabilities are combined, along with the management piece with the Firepower Management Center. This makes manageability and visibility seamless.”

And finally, Cisco offered **in-country support** from a local Cisco representative. “Often vendors are either flying in-country to provide support or using a local VAR,” said Lewis. “This isn’t the case with Cisco – they have a local Cisco support team that allows them to be very responsive and engage with us.”

Since deploying the Cisco Firepower NGFW, the security team at Texas A&M at Qatar has found that a holistic approach to security makes it easier to take advantage of interoperability between solutions. With streamlined management and integrated capabilities, they’re blocking threats before they enter the network and more quickly stopping those that do slip by defenses.

## Blocking threats

The Cisco Firepower NGFW is continuously updated with the latest protections from the built-in threat intelligence provided by Cisco Talos and the Texas A&M at Qatar security team's own custom signatures. Mansour adds, "We know and trust the Talos team behind the product. Having really smart people doing the research, understanding the techniques, feeding the signatures, gives us a lot of confidence in our ability to defend against attacks. The ability to include our own custom Snort and Open AppID signatures to address emerging threats in our extremely diverse environment was really important too."

Cisco Umbrella also allows them to proactively block threats faster. "With Cisco Umbrella there's really not much effort to have the service up and running," says Mansour. "The visibility provided by Cisco Umbrella serves as a threat-enriched passive DNS repository. It is possible to quickly gain insights and make informed response decisions whether proactively or reactively based on the threat."

## Mitigating the impact of attacks

The team also utilizes AMP for Networks on the NGFW appliance allowing them to inspect files as they traverse the network and continuously monitor for malware. "Security is about layered defenses and if something passes through the firewall, AMP for Networks as part of Firepower Threat Defense can retrospectively tell us that a file is bad," says Mansour. "We can go back in time, know where the file went, the systems affected, and rapidly make decisions about remediation."

The Firepower Management Center is central to being able to take action quickly. Mansour explains, "Managing all our appliances from a centralized view and aggregating data from appliances in different locations across the network was easier than I thought. This makes reporting easier too because you can aggregate and mesh the data. We're doing all of that in one place."

## Effectively blocking ransomware

These capabilities were demonstrated in action during a recent attack where having Cisco Security solutions in place effectively blocked a ransomware campaign denying more than 1,000 attempted deliveries of the malware before it reached the end user. "There was a spike in Necurs botnet activity delivering Locky ransomware," Mansour explains. "The Cisco NGFW blocked the malicious attachments in transit before they even hit our email appliances. Witnessing the visibility and fast response by the product in a real-time situation was awesome."

This is a single example of multiple campaigns that have been identified and prevented through the Cisco NGFW with Firepower Threat Defense and the security intelligence feeds provided by Talos.

**"Security is about layered defenses and if something passes through the firewall, AMP for Networks as part of Firepower Threat Defense can retrospectively tell us that a file is bad. We can do analysis and take action in 3 days as opposed to 3 months later when someone tells us we have a bad machine in our network"**

**Yaser Mansour,**
Security analyst at Texas A&M at Qatar

Mansour adds, “In the past one of the things that has been generally difficult to deal with is BitTorrent traffic – it is very challenging to see and block. Now we can apply detection and prevention based on application and traffic types.”

## A secure and open future

With the Cisco solution Lewis and his team have been able to eliminate downtime and identify and stop threats before they become incidents – improving their ability to support faculty, staff, and students.

“The rapid response to threats, allowing us to look at traffic from different perspectives and devise remediation based on the data we are seeing, is really powerful – we can enable, disable, or do whatever we need to do,” says Mansour. “Also, because we’re familiar with the Snort and Open App ID engines, whenever we see a threat with no signature available, we can write our own, and upload it to the appliances through the Firepower Management Center giving us visibility into previously undetected patterns.”

The quality and timeliness of reporting has been an invaluable tool to use with leadership. “During the most recent ransomware campaign, having reports that clearly demonstrate these were the threats and the number of threats that were inbound and denied access, makes it easier to justify budget,” Lewis explains.

With Cisco’s security architecture in place, the security team at Texas A&M at Qatar is now migrating from Cisco ACS to Cisco Identity Services Engine (ISE) to take advantage of the additional features including user tracking and security tags. The diverse requirements of research require flexible access methods with enhanced protection features to ensure standards for campus security. The team is also looking at Cisco Stealthwatch to gain additional visibility at various levels of the network architecture.

“By maintaining an open environment we can use the tools we choose,” said Lewis. “Cisco gives us the visibility and flexibility to identify and stop threats faster which is particularly challenging and important when you’re dealing with a wide range of devices, apps, and users in an education and research environment. We’ve been very happy with our Cisco support team and the Cisco NGFW with Firepower Threat Defense which has lived up to everything it promised during the evaluation.”

## Products and services

- Cisco Firepower NGFW with Firepower Threat Defense – 4100 Series
- Cisco Advanced Malware Protection
- Cisco Firepower Management Center
- Cisco Umbrella
- Cisco Identity Services Engine
- Cisco Nexus Data Broker



C36-739198-00 06/17