Securing the Arts and Nanotechnology at VCU Arts Qatar

The customer summary

Customer name
VCU Arts Qatar

Industry
International branch campus of Virginia Commonwealth University’s School of the Arts

Location
Qatar
Challenge
• Protect student, faculty personal information as well as collaborative research intellectual property
• Keep malware out of their network
• Increase visibility and keep up to date on latest threats

Solution
• Cisco Firepower 4110 NGFW with Firepower Threat Defense
• Firepower Management Center
• Advanced Malware Protection subscription
• Next-generation Intrusion Prevention subscription
• URL filtering subscription
• Cisco Identity Services Engine (ISE)

Results
• Gained substantial visibility into threats and malware attacking the network
• Talos automatic daily threat feeds saves administrator’s time in protecting against latest threats

“Cisco’s support in deploying the Firepower 4110 exceed our expectations. We now can see how we are stopping thousands of threats every day.”

Barry Parham
Chief Technology Officer, VCU Arts Qatar

VCUarts Qatar is the international branch campus of Virginia Commonwealth University’s School of the Arts, a top-ranked art and design program in the U.S. VCUarts Qatar is celebrating 20 Years of a fruitful partnership between VCU and the Qatar Foundation. It is a partnership that underscores both institutions’ commitment to excellence, inquiry, discovery and innovation in a global setting.

Established in 1998 through a partnership with Qatar Foundation, VCUarts Qatar offers students the opportunity to earn a Bachelor of Fine Arts degree in fashion design, graphic design, interior design and painting and printmaking, a Bachelor of Arts degree in art history and a Master of Fine Arts degree in design.

A vibrant community with global reach, VCUarts promises students a lifelong passion for and conversation about the arts. As the foremost example of its commitment to global outreach and education, VCUarts Qatar presents valuable opportunities for cross-cultural exchange and connects VCUarts to the influential art and design world of the Middle East. The campus attracts renowned contributors to contemporary visual culture for speaking and teaching engagements, and hosts two major international events--the design conference Tasmeem Doha and the Hamad bin Khalifa Islamic Art Symposium.
The rich creative environment has nurtured collaborative art projects and research.

One particularly interesting research area involves a new fabric design that incorporates nanotechnology. This new fabric is not only esthetically pleasing, but will also have revolutionary features with applications from self-cleaning medical clothing to preserving cultural artifacts. Assistant Professor of Physics Dr. Khaled Saoud, and his undergraduate students have successfully synthesized nanomaterials capable of extending the lifespan of the country’s irreplaceable and fragile documents by centuries. The project, 'Preservation of Cultural Heritage in Qatar Using Nanotechnology' aims at conserving and preserving Qatar’s paper-based cultural heritage through the use of cutting edge nanotechnology. Intellectual property such as this needs to be conducted in a secure environment and VCUarts Qatar relies on Cisco for that protection.

Protecting VCUarts Qatar Research and Intellectual Property

Since 2005, the VCU Arts computer architecture has been supported with Cisco secure networking infrastructure with Cisco Firewall Services Module integrated with Cisco Catalyst 6500 Series switch served as Data Center Firewall, Cisco ASA 5500 series with IPS module and served as Perimeter/Internet Firewall. The Cisco ASA 5500 series firewall has been deployed to faithfully protect the faculty and student records and precious research data. Recently, networking engineer Michael Aguda identified some nasty malware breaches that were particularly difficult to isolate and as a result it took days to eradicate them from their network. Clearly, it was time to upgrade their security posture. With all of the great support they have received from Cisco over the years, CTO Barry Parham said “It was a no brainer” to call their trusted Cisco representative for help.
The Cisco Security Assessment

The IT team needed to clean up the malware and stop new malware from getting into their network again. The lack of visibility into potentially malicious files introduced into the environment made it very difficult to find malware and remove it from all of the systems it had infected. And with research partners, visiting artists, students, and faculty joining and leaving the network constantly, the problem was even more complex.

After a review of the network architecture, Cisco Sales Engineer, Ro’ya Hatameih identified the solution immediately. It was time to replace the trusty stateful ASA firewall with Cisco’s latest Next-Generation Firewall (NGFW). Classic stateful firewalls were designed to only inspect the state of active connections and use this information to determine which network packets to allow through the firewall. Today’s advanced threats have learned how to get through stateful inspection that is why we’ve added next-generation firewall features to the ASA to keep up with the latest threats.

To adequately support the growing number of users and traffic within the VCU Arts network, Ro’ya recommended the Cisco Firepower 4110 Series NGFW, Firepower Management Center (FMC) and a full complement of threat subscriptions. FMC will provide the deep visibility into the users, hosts, applications, files, mobile devices, virtual environments, threats, and vulnerabilities that exist in VCU Art’s constantly evolving network. Visibility is paramount, because you can’t protect what you can’t see.

Stopping Malware in its Tracks

Today, any connection to the internet via search, visiting news sites and even email can expose systems to malware. Cisco AMP can stop known malware by comparing traffic to known malware signatures delivered via daily threat updates from Cisco Talos Research. For the unknown or zero-day attacks, the team can see when the malware emerged and contain it fast. The AMP advanced malware dashboard in FMC, offers the IT team complete visibility into how files came into the network and what they have been doing since. If a file becomes malicious, they now have the tools to quickly see where it has been, how to contain it and then clean up systems that were impacted.

Protecting From Insider Threats

Another tool that Ro’ya recommended to help limit the spread of unknown threats is Cisco Identity Services Engine (ISE). By using the Secure Group Tagging (SGT) capabilities provided by Cisco ISE with TrustSec®, Barry’s team can limit user access only to systems they have a need to use, containing threats to only a portion of the network impacted. By defining user groups and where each group belongs in the network, the team will be able to streamline network access administration, threats can be localized, students will only have access to appropriate resources.

Results

With the Firepower 4110 NGFW and FMC Barry and his team are already seeing benefits. With FMC, Barry and his team are seeing thousands of attempted attacks that have been stopped by the Cisco Firepower 4110 NGFW on a daily basis. New malware infections are virtually non-existent. When new students, visiting artists, or researchers need to come on-line, they can be granted access to only the specific systems they need.

With the new Firepower 4110 Series NGFW. The VCUarts Qatar network will stay secure with the bandwidth they need to create amazing designs and preserve Qatar’s historical artifacts for another 1000 years.