CASE STUDY

AMERICAN UNIVERSITY
WASHINGTON, DC

Private University Enjoys 6x Increase of Secure Remote Access with ICE License Option

American University (AU), true to its name, is spread out along ninety acres of verdant landscapes on the N.W. corner of Washington, D.C. As a private research university, they are comprised of eight schools and colleges including The Washington College of Law and School of Public Affairs. Founded in 1893 they began with a simple credo to educate and train future public servants, no doubt ready to take advantage of their proximity to the nation's Capital. Today, the school is comprised upwards of 15,000 students, employees, and adjunct support staff, with AU operating as a mid-size enterprise running 600 servers with up to 20,000 devices connected to their network.

Executive Summary

Industry

- Higher Education

Solutions

- Pulse Connect Secure (PCS)
- In Case of Emergency License (ICE)

Challenge

Provide easy, secure access while experiencing a six-fold increase in usage as the University went fully remote due to COVID-19 restrictions

Results

Adoption of MFA technology, combined with the added capacity from the ICE license provided a stable and secure full-featured platform for multiple departments across campus, including students and faculty

As Director of Information Security, Eric Weakland is tasked with coordinating and maintaining operations for the Information Security Unit, including the virtual private network (VPN) services. The university has hundreds of applications, both on and off premise, as well as a large physical data center, all of which require continuous monitoring to protect students, staff and faculty data from potential breaches and compromise.

With the recent disruptions brought about by COVID-19, AU shifted its spring and fall 2020 operations to support full remote access for faculty, staff and students; all classes are online, and only select essential workers habitually come to AU's physical campus. Over the course of working for the university for 25 years, Eric and his team have had their share of challenges in staying ahead of the security curve. Throughout the various incarnations in technology, from desktops to mobile, BYOD, and IoT proliferation, adopting best practices for security requires the ability to stay up to date on solutions, making prudent decisions on what and how to invest.

With the sudden need to scale operations and secure access due to stay-at-home mandates, Eric was able to take advantage and implement Pulse Secure's "In Case of Emergency" (ICE) licensing option.

Pulse's ICE option allows customers easy licensing for emergency activation for instant on demand capacity to address dramatic peaks in their usage. Users can gain up to eight weeks of maximum user count, per appliance, during ICE activation in addition to being able to move licenses between physical, virtual, and cloud appliances in different locations during the activation period.

At AU, they specifically use a pair of Pulse Secure PSA5000 physical appliances, including a PSA3000 as a test unit. The test unit is off-site and is used primarily for doing quality assurance on new configuration changes and as a back-up and disaster recovery VPN service should their main cluster and data center lose connectivity.

Pulse Secure®

Taking a Layered Approach to Security

With thousands of records containing PII (Personally Identifiable Information) AU maintains stringent security protocols to protect the data it is entrusted with. With thousands of students online, accessing University resources from more than 170 countries, Eric and his team must stay one step ahead of the persistent attacks on its community, trying to gain access via malicious emails (phishing attacks). To help manage and reduce the compromise of passwords and credentials, they added an additional layer of security by implementing Duo's multifactor authentication (MFA) with Pulse's VPN.

Requiring MFA has reduced the number of breached accounts used to send spam from the AU network. Having the ability to deploy an MFA solution seamlessly on the Pulse VPN has helped neutralize the risk of stolen passwords, while hardening the ability to connect to their network, thus further protecting AU's threat landscape.

Host Checker Functionality Rocks

One of the Pulse Connect Secure (PCS) features that gets used on a regular basis is its Host Checker function. As a client-side agent, it performs endpoint checks on hosts that connect to PCS. It can check hosts for endpoint properties using a variety of rule types, including rules that check for and install advanced malware protection; predefined rules that check for antivirus software, firewalls, malware, spyware, specific operating systems, third party DLLs, ports, processes, files, registry key settings, and the NetBIOS name, MAC address, or certificate of the client machine.

Being able to create and customize rule sets including creating different profiles based on user types—whether users are students, faculty, or internal IT staff that needs access to critical data—Host Checker automatically remediates non-compliant endpoints by updating software applications that do not comply to corporate security policies.

Security as a Cultural Shift

Implementing and deploying security solutions goes beyond simply installing hardware and software. In many cases, working democratically across departments (with varying degrees of accessibility to sensitive data) requires communication and transparency when discussing user expectations. No one wants disruptions to connectivity or being denied access to data or systems.

As such, Eric and his team have taken a "default deny" or deny-by-default policy approach which means unless one specifically allows something, one denies it. This approach helps prevent malicious activities and accidental leakage of traffic by restricting the traffic to only known sources, and only to those protocols, ports, or services that are permitted and necessary to maintain operations. Applications and endpoints are identified and used to develop sets of rules and controls to restrict access.

To help communicate and clear up perceptions about more stringent security policies, like "default deny" Eric met with campus partners to answer questions and develop consensus on security protocols. Providing users with hard data and forensics around potential Indicators of Compromise (IoCs), malicious attack patterns, and general abnormal network activity laid the groundwork for cross-functional adoption without pushback.

Why Pulse Secure?

"There's no reason for everybody's desktop in their office to be reachable from Russia. So that's why we adopted a VPN model where, as we moved applications to be better protected from the Internet at large, we could still enable our customers in a very friendly way to get access to the resources they need."

"What I've been most impressed with is that it was able to scale up sixfold and still maintain a usable user experience and throughput. Man, I'm impressed!"

"I think the thing that makes my job so interesting is that I, number one, love the fact that I'm supporting a mission at a nonprofit that I can believe in: the goal of educating students while staying secure and compliant."

- Eric Weakland, Director of Information Security

Moving to the Cloud with a Zero Trust Mindset

As a private university, AU is 95% tuition-dependent, meaning investments in technology tend to lean more conservative vs. bleeding edge. Targeting Software-as-a-Service and cloud services will allow the Enterprise Security Unit the flexibility to pay-as-they-go and turn cloud services on or off as needed. Adopting Zero Trust principles such as "Principle of Least Privilege" allows Eric and his team to make incremental changes to their existing security policies to take proverbial "baby steps" in their security journey. Luckily, having a partner like Pulse Secure provides them with the solutions, personnel, and expertise to help get them there.

Pulse Secure®

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
(408) 372-9600
info@pulsesecure.net
www.pulsesecure.net

ABOUT PULSE SECURE

Pulse Secure, LLC offers software-defined Secure Access solutions that provide visibility and easy, protected connectivity between users, devices, things and services. The company delivers suites and a SaaS platform that uniquely integrate cloud, mobile, application and network access control for hybrid IT. More than 24,000 enterprises and service providers across every vertical rely on Pulse Secure to empower their mobile workforce to securely access applications and information in the data center and cloud while ensuring business compliance. Learn more at www.pulsesecure.net.

linkedin.com/company/pulse-secure
www.facebook.com/pulsesecure1
twitter.com/PulseSecure
info@pulsesecure.net

VERSION 11052020