CISCO UMBRELLA: QUICKLY AND EASILY STOP END USER THREATS

Montgomery College (MC) is the largest community college in Maryland, serving nearly 54,000 students on three campuses and at multiple workforce development centers. With more than 130 degree and certificate programs, MC prepares students to earn an associate degree, transfer to a four-year college or university, enter the job market, upgrade career skills, or simply enhance life through enrichment experiences.

Objective

Providing reliable applications to enable teaching and learning throughout such a large and complex institution requires a secure network and advanced cybersecurity solutions to protect online users and safeguard personal information, college resources, and intellectual property. With that objective, Networking For Future (NFF) was asked to provide MC with tools and guidance to help refine and enhance its existing security posture.

NFF focused on reducing exposure to potentially malicious websites, email phishing attacks, malware infections, ransomware and "zero-day" software vulnerabilities by implementing end-user security at the Domain Name System (DNS) layer of Internet communications. Since the DNS serves as the Internet's phonebook, all communications between user devices and applications rely on it to locate Internet resources.

Challenges

The major challenge was preventing end users from going to web sites with malicious content or malware. Other known threat risks were phishing attacks, newly seen malware (within the last 24 hours), and command and control callback (e.g., cryptomining, botnet, etc.)

Solution

NFF implemented DNS-layer security for Montgomery College using the Cisco Umbrella cloud security platform to block threats before they become attacks. With no hardware to install or software to manually update, Umbrella offers quick setup and a browser-based management interface. Umbrella was licensed to allow use by all faculty and administrative staff, classrooms and laboratories at all MC campuses. It took only a few minutes for the DNS requests of MC users to be routed to the Umbrella Global Network, enabling MC to immediately enjoy enhanced security. The addition of the roaming client expanded the threat protection coverage.

"Cisco Umbrella is a great solution because it provides protection without impacting the end user. They don't have to change their behavior. Umbrella just works.

The configuration steps were very simple, and it took only a few minutes to point our DNS traffic to the Umbrella Global Network."

Nell Feldman
Information Technology Security Manager
Montgomery College

Results

Montgomery College reports:
- With DNS layer security, Umbrella reduced malicious web site access, phishing attacks, and malware infections
- Umbrella immediately stopped command and control callback streams on several compromised workstations
- Umbrella delivers an early warning of malware intrusion
- Weekly reporting shows campus-wide Internet access protection

About Networking For Future, Inc.

Networking For Future, Inc. (NFF) is a Washington, DC based company offering a performance-focused approach to delivering transformational IT business solutions. We take pride in keeping users productive and engaged by providing business and IT teams with the solutions they need to improve their performance in a dynamic, connected world.

We are ISO 9001:2015 certified, Cisco Gold Partner, Riverbed Premier Partner, NetApp Gold Partner and hold Maryland Education Enterprise Consortium (MEEC), Cisco Virginia Association of State College and University Purchasing Professionals (VASCUPP), Fairfax County Public Schools, GSA Schedule (GS-35F-0197L) and numerous other contract vehicles. For more information contact NFF at **sales@nffinc.com**.