CISCO UMBRELLA: QUICKLY AND EASILY STOP END USER THREATS

Objective
Montgomery College wanted to reduce malicious web site, phishing attack, malware infection, zero-day, and command and control callback threats by extending end user security to the DNS layer.

Pain Points
The major pain point 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
The Cisco Umbrella Proof of Performance showed the number of web sites that could be blocked was unlimited. While Umbrella was in its initial monitor mode, it detected several cryptocurrency mining instances on workstations. Switching Umbrella to blocking mode instantly stopped the command and control data streams.

Networking For Future (NFF) activated 3,120 FTE Umbrella licenses to cover administrative staff, faculty, classrooms, and laboratories across three county-wide campuses. It took only a few minutes for Montgomery College to point their DNS traffic to the Umbrella Global Network. The addition of the roaming client expanded the threat protection coverage.

Results
Montgomery College reports:

- It took less than five minutes for the Montgomery College IT team to point DNS traffic to the Umbrella Global Network
- By extending security to the DNS layer, Umbrella reduced malicious web site access, phishing attack, malware infection, and command and control callback threats
- When Umbrella was switched from monitoring to blocking mode, it immediately stopped command and control callback streams on several compromised workstations
- Umbrella provides early warning of malware coming into the environment, with no extra work for the IT team
- Weekly reporting instills a sense of comfort that campus-wide Internet access is protected

"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

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.