INDIANA WESLEYAN UNIVERSITY

Located in Marion, Indiana, Indiana Wesleyan University is the largest private university in the state, with 10,000 students enrolled as of 2022. Indiana Wesleyan University offers more than 80 undergraduate degrees and 57 graduate degrees, including 9 doctorate degrees.

Original article posted in **ITPro Today** on Sep 06, 2022:

Every organization has a responsibility to protect valuable resources and keep employees safe, but colleges and universities have even more to protect – students. Yet it can be a tough balancing act to keep students safe while respecting their privacy.

Universities must protect student data, which means **complying with various privacy and security regulations**, like Gramm-Leach-Bliley for financial aid data, PCI for credit card payments, and even General Data Protection Regulation for students who come from the European Union. Universities also aim to protect students from visiting inappropriate sites or downloading malicious files.

For Indiana Wesleyan University, the gaps in its ad hoc approach to security became apparent about five years ago. That's when the evangelical Christian university hired its first CISO.

When Michael Madl took the job, he evaluated the security controls that were in place, what was working, and what needed to be done. Madl immediately noticed the **proliferation of shadow IT**, largely due a culture that enabled faculty and staff to use the tools that suited them best instead of those sanctioned by the university. If, for example, a faculty member insisted on storing data in Dropbox when the university had standardized on Microsoft, cybersecurity and compliance issues could emerge. With that in mind, Madl took a full inventory of data assets, devices, networking systems, and software.

Over the next few years, Madl tightened security and privacy across campus resources. He upgraded firewalls to next-generation Palo Alto firewalls and added extended detection and response, behavior analysis, and an external security operations center to oversee a centralized security information and event management system. He also upgraded the university's **network access control** (NAC), providing wireless NAC to students to limit where they could and couldn't go online.

YOU CAN'T PROTECT WHAT YOU CAN'T SEE

One issue Madl quickly noticed was a lack of visibility into traffic or data entering or leaving the network. Even the firewalls, which had basic URL filtering and some DNS sinkhole technology, didn't provide enough visibility into what was happening on endpoints. Yet the ability to see the traffic was critical for filtering content and deploying controls rapidly.

When looking for new technology, Madl first considered the obvious choices from vendors like Cisco and Cloudflare. They have effective filtering technology, but the products proved too expensive for a university strictly funded by enrollment, he said. More research led him to DNSFilter, a content filtering technology designed to block online threats and inappropriate content. It was a much more affordable option and would meet the university's needs.

The DNSFilter tool could address the university's two groups of users, employees and students, differently. For employees, the university's small IT team pushed an agent out via its **mobile device management** system on all employee devices – phones, laptops and desktops. The agent alters the DNS settings on the host, funneling everything through the DNSFilter cloud. The agent then converts the DNS settings to point to DNSFilter for any query the machine makes – web queries but also other programs installed on the machine that point home, like anti-virus. This helps Madl's team not only from a web traffic perspective; it identifies traffic from anything on the device that "phones home" and makes an internet connection.

Through that agent, DNSFilter can enforce compliance and safety policies. Employees have access to the internet except for malicious and inappropriate sites. DNSFilter also helps to ensures that employees use university-sanctioned software and tools like VPNs and file sharing.

Madl highlighted AppAware as a particularly useful DNSFilter feature. AppAware detects and blocks risky applications, which has helped put controls on the applications used by employees.

Protecting students is a little trickier since the university doesn't want to infringe on personal rights and preferences. Because of that issue, the DNSFilter instance for students doesn't install agents on endpoints. Instead, the university uses DNSFilter controls at the firewall, edge, and directory/DNS levels to prevent users on its network from accessing malicious and adult sites. As students access the internet, they cross the university firewall and are assigned an IP address for the network, along with DNS settings. If the site can't connect to the internet for any reason, it is forwarded to DNSFilter, which applies the appropriate policies.

SECURITY PROGRAM CONTINUES TO EVOLVE

The insights that DNSFilter generates have been instrumental in keeping the university safe.

For example, the dashboard enables the IT staff to drill down to specific users to determine if the endpoint is actually attempting to communicate with a malicious server. When the dashboard flags something as infected or compromised, the team can use the tool to validate what they are seeing and determine if it ties to a domain.

> **"MADL HIGHLIGHTED APPAWARE AS A PARTICULARLY USEFUL DNSFILTER FEATURE. APPAWARE DETECTS AND BLOCKS RISKY APPLICATIONS, WHICH HAS HELPED PUT CONTROLS ON THE APPLICATIONS USED BY EMPLOYEES."**