College of Law

Revamping security architecture

Summary

Outcomex has implemented Advanced Malware Protection(AMP) throughout the College of Law network as a security architecture. AMP provided real time file inspection and analysis designed to protect and re mediate malicious threats. In conjunction with AMP, the security solution is comprised of Web, Email, and Network security components. As an architecture, these components provide policy driven decisions for access to the network and to the services within and outside the college.

Client

College of Law is an Australian and New Zealand based organisation providing post-graduate legal training to university law graduates and continued legal training for certified law practitioners. Their mission is to deliver innovative, practice-focused legal education and training to enhance the careers of practising professionals. Since opening in 1974, the organisation has taught over 60,000 graduates spanning across Australia and New Zealand. It now serves more than 3,000 students annually, making College of law the leader in legal education and training for professional practice across Australia.

Solution

Outcomex has implemented a security architecture that addresses the concerns and reduces the risk of security threats. Implementation consisted of multiple security solutions integrated to defend, protect, and remediate. The architecture targets the key vectors of attack; Email, Web, Network, and Endpoint.

These solutions consist of:

- Cisco Cloud Email Security with Advanced Malware Protection (AMP)
- Cisco Cloud Web Security with AMP to secure staff
- Cisco Umbrella to secure Student and Staff
- Cisco NGFW upgrade to include Firepower
- Cisco AnyConnect with Umbrella to protect roaming clients
- Cisco AMP for Endpoint
- Cisco Identity Services Engine

Opportunity

College of Law had been the victims of multiple ransom-ware attacks that heavily impacted the organisation. The security solutions coming to end of life gave College of Law the opportunity to develop a centralised vendor approach, adopting the full portfolio of Cisco content and network security product offerings. College of Law was looking for a security architecture that enables greater protection against Malware, provides them with an architecture which could be built upon, and most importantly provides visibility on issues which invade security.

Impact

Immediately after the project completion, College of Law was able to identify compromised machines within the corporate network via OpenDNS and levels of email SPAM. In addition to these, phishing emails reduced significantly by implementing better email security controls. Staff have now become more aware of potential security concerns and are more proactive in notifying IT when an issue arises. Visibility is the major key to success.