CASE STUDY

Safeguarding United Learning from the Evolving Threat Landscape

United Learning is a group of over 70 academies and independent schools across the country. Their mission statement is to bring out 'the best in everyone', and with over 45,000 students from varying backgrounds this is no easy feat. But through community days, volunteering and access to the best education, they are able to achieve just that.

United Learning makes it a priority to provide teachers with excellent professional support, and to ensure that their schools have effective technology at their disposal. In both primary and secondary schools, technology is playing an important role in enabling staff and students to teach and learn more effectively. However, the devices which connect to the school's systems are not only vulnerable to attacks, but can unknowingly introduce dangers onto the network.

The most common entryway is email, which is an access point for more than 80 per cent of incidents. This is especially true for teaching and support staff. The cyber hygiene and security practices of the staff are crucial, especially as threat actors are now mimicking the email addresses of other staff across the Group, and specific suppliers that serve the schools, to send seemingly harmless links. United Learning turned to Fortinet and TNP to help ensure their staff, students, and systems were kept safe within the context of an evolving threat landscape.

School's Threat Landscape

In education, there is the potential for every student to use a number of connected devices, each of which can be used to access a range of apps and environments. Every one of these devices is a potential entryway to the network. With the median number of SaaS apps in education at 59 and IaaS apps at 40, there are many attack vectors to keep track of.

This means that, in addition to maintaining perimeter defences and monitoring threat intelligence, IT teams must now also consider all of the ways in which cybercriminals might leverage the tools and behaviours of staff and students to gain access to the network.

The Group is part-way through a significant change in how it hosts data, with a clear focus on Cloud First, and is about to complete the first phase with all user data residing in Office365. This will help it mitigate the cost of replacing hardware on site and increase resilience and flexibility regarding how data is accessed. This is a monumental task to undertake in a sector hampered by tight spending constraints and limited in depth IT skills in the critical areas of security, especially in the cloud.

United Learning
The best in everyone™

"Using Fortinet and TNP for our security needs has not only provided us with greater control of our firewall configuration, but also with greater, easier understanding of the entire model. This is important to us, as our core focus is improving educational outcomes, not being security specialists!

Using a provider who can easily and effectively communicate what we need to do and help us implement it, means we can be certain that students and staff alike are safe online and our data and systems are secure."

James Garnett, Deputy Director of Technology at United Learning

Details

Customer: United Learning

Industry: Education

Location: United Kingdom

Solutions

- FortiGate-VM
- FortiGate 60-300 Series
- FortiManager-VM
- FortiAnalyzer-VM

Business Impact

- Increased ability to secure the connections between schools as well as the outside world
- Added ability to do a layer 7 filtering on the firewall
- Met the needs of smal primary schools to large secondary schools with broad range of devices

Ensuring Every Step Is Taken

In conjunction with TNP, Fortinet is enhancing the schools' cyber security capabilities, providing the best possible security and safeguarding solutions to keep staff and students safe. Fortinet is playing a key role in ensuring that United Learning can quickly understand impending threats, which entry points are vulnerable, and what actions need to be taken.

With a multitude of moving pieces across its 70+ schools, it was critical for United Learning to integrate advanced threat intelligence into their threat response processes. From their small primary schools, to the larger secondary schools, United Learning needed a broad range of security devices that could meet various cyber security needs across its distributed network architecture. This scenario lends itself extremely well to the FortiManager-VM platform, allowing for continuous threat monitoring and protection.

From this initial step, United Learning is looking toward more standardised reports and monitoring solutions across all 70 schools with Fortinet's help. This has already been achieved in some locations with the use of the FortiAnalyzer – Fortinet's automatic log management and real-time threat analysis system, which also provides United Learning with the use of a centralised internet filter and logging option which will contribute to reducing IT costs, as well as configuration times. FortiAnalyzer-VM is one of the first required steps in United Learning being able to centralise Web Filtering on request, while meeting the logging guidelines from the UK's Safer Internet Centre.

United Learning also wanted the ability to do a Layer 7 filtering on the firewall – allowing them to sort traffic according to which application or service it is trying to reach, and what the specific contents of that traffic are. The layer 7 filtering, along with the ability to have a secure connection between schools as well as the outside world, was established with the use of FortiGate-VM.

Securing the Cloud

United Learning was also undergoing a cloud transformation programme with the closure of their physical datacentre hosting location and the relocation of these services to Azure. To help with this, FortiGate-VM was deployed into Azure to act as an SD-WAN endpoint allowing all sites to securely access hosted services. ADVPN functionality, which allows traditional hub and spoke VPNs to establish dynamic, on-demand direct tunnels between each other, now allows clusters of schools to share services.

The overall migration was undertaken in three phases across a year to suit existing license expiries and United Learning's requirements. All equipment was pre-staged by TNP and shipped to site with remote support for the cutover being provided.

Looking Ahead

These measures implemented by Fortinet and TNP will support a highly resilient cyber programme for digitally transforming the schools. As United Learning adapts its IT infrastructure to enable digital transformation, it must also undergo a security transformation to protect against the constantly expanding attack surface.

With Fortinet and TNP, United Learning will be able to better understand their threat intelligence and deliver fast, automated responses to threats anywhere in the network while providing IT staff full visibility of security events throughout the borderless network.

November 22, 2019 3:03 PM

548513-0-1-EN

Macintosh HD:Users:rich:Desktop: • Local Work: • FORTINET EMEA:FTNT 5209 - Co branded case study x2 - 548513:United Learning Case Study - 548513 v2