Swinburne University of Technology Meets Its Essential 8 Mandate

Profile:
Swinburne is a public university with campuses across Melbourne, Australia, and Malaysia. It was established in 1908 with a commitment to provide and transform education through strong industry engagement, social inclusion, a desire to innovate, and above all a determination to create positive change.

Location:
Melbourne, Australia

Industry:
Education

Website:
http://www.swinburne.edu.au/

Solutions:
- Ivanti Workspace Manager
  - Ivanti Application Control
  - Ivanti Environment Manager
- Ivanti Patch for Windows
- Ivanti Xtraction

Benefits:
- Comply with the ASD's Essential 8 and Top 4 cyber security strategies
- Apply proportionate security controls
- Reduce malware risk
- Patch hundreds of servers rapidly

The Perimeter Has Moved

With geographically dispersed students across its Australian and Malaysian campuses, as well as online who are digitally savvy and socially connected, Swinburne University needed to protect its critical infrastructure and financial, statutory, and personally identifiable information (PII) while empowering academic freedom.

Meeting this challenge required changing conventional security thinking. Steven Cvetkovic, Chief Information Security Officer at Swinburne, said, "The perimeter has moved. It's not about keeping the baddies out at the fence line anymore with just firewalls. The perimeter is now the individual user. We're only as strong as our weakest link, so we had to refocus our whole energy and mindset on what that means."

Meeting the Essential 8

Following a risk assessment, Swinburne determined that following the Australian Signals Directorate's (ASD) Essential 8 recommended cybersecurity mitigation strategies would help ensure the strongest form of defense against a cyber attack. Thomas Duryea Logicalis (TDL) assisted Swinburne in finding the solution that would help it achieve those standards and the objectives underlying them while reducing overrun and costs.

Products from the Ivanti security portfolio provided the best end-to-end solution to help address the Essential 8 strategies. The Top 4 strategies recommended by the ASD—deploying application whitelisting, patching operating systems and applications, and minimizing administrative privileges—help mitigate at least 85 percent of targeted cyber intrusions.[1]

- Ivanti Application Control provides capabilities to protect against malware infection in desktop and server environments with application whitelisting and granular privilege management.
- Ivanti Patch for Windows ensures Windows operating systems and third-party applications are patched efficiently.
- Ivanti Environment Manager (EM), helps Swinburne address additional Essential 8 controls by disabling untrusted Office macros and hardening user application configurations. EM can block web browser access to Adobe Flash player, web ads, and untrusted Java code on the Internet. Flash, Java, which are popular ways to deliver malware to infect computers.

1 Top 4 Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirements Explained, Australian Signals Directorate, July 2013 https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

With Ivanti's solutions Swinburne can apply proportionate security controls, dialing them up or down to suit the individual user and safeguard academic pursuits.

Pinpointing Risks and Patching Vulnerabilities

With Swinburne's input, Ivanti also developed a dashboard around the ASD Essential 8 to give the university insight into security issues.

"Ivanti Xtraction is a powerful tool that provides access to the real-time data that matters most to us. We can link it to both our Ivanti patching solution and User Workspace Manager, to pinpoint where the risks and issues are we need to act on, and share relevant, real-time reporting metrics with stakeholders," said Cvetkovic.

The Swinburne information security team can also easily report on compliance with the ASD Essential 8 standards and determine where it needs to focus attention and resources.

For patch management Swinburne now uses Ivanti Patch for Windows to identify vulnerable clients and servers and apply patches rapidly. During the WannaCry outbreak, Swinburne was using standard Microsoft systems to determine where updates should be applied. This approach failed to identify all the systems that needed patching, so the university had to develop its own scripts to hunt those down.

"Ivanti enabled us to deep dive into our environment to identify which of our 500+ servers need patching – in a very short time frame compared to some of our counterparts," said Cvetkovic. "The team can quickly and easily deploy patches across a variety of operating systems. They no longer need detailed knowledge of all the operating systems in our environment to apply a patch, and they can patch multiple operating systems from a single console. We can meet our patching requirements in less time, which frees the team up to take on other projects."

A Customer-focused Approach

Swinburne chose Ivanti not only on the strength of its solutions, but also on being a trusted advisor to its customers.

"They're very focused on the customer as opposed to the sale. Their unified IT approach ensured we could go through a seamless change management process and quickly define a best-practice approach for achieving the necessary transformation."

Summing up the results to date, Cvetkovic said, "We're there to support academic freedom and enable users to do their jobs, while also providing that backend layer of security. Having visibility into the entire landscape and the tools at hand to balance security with user needs makes it easier to meet both objectives."

www.ivanti.com

1.800.982.2130

sales@ivanti.com

Copyright © 2018, Ivanti. All rights reserved. IVI-2144 02/18 CW/JR/DL/LB/DL