CISCO
SECURE

Case Study
Public

Organization:
Deakin University

Headquarters:
Burwood, Victoria, Australia

Users:
64,000 students and 12,000 staff at four Australian campuses and offices in three other countries

Industry:
Higher education

How a higher education institution built a mature security program from the ground up

"Given the Cisco technologies we have implemented and integrated through SecureX threat response, the processes we have built around them, the people we have trained and upskilled to use these technologies and capabilities, and the awareness campaigns we launched and worked on with users, we have managed to elevate our maturity significantly and improve our security posture."

– Fadi Aljafari, Information Security and Risk Manager, Deakin University

CISCO The bridge to possible

Objective:

Deakin University needed to improve its outdated security posture and transform security from ad hoc processes to a mature program.

Deployment:

Cisco SecureX

Cisco Umbrella

Cisco Secure Endpoint (formerly AMP for Endpoints)

Cisco Secure Email (formerly Email Security)

Cisco Secure Firewall (formerly Next Generation Firewalls)

Cisco Secure Access by Duo (formerly Cisco Duo)

Impact:

- Decreased investigation and response time from more than a week to an hour for some incidents.
- Reduced response time to malicious emails from an hour to as fast as five minutes.
- Increased NIST framework compliance from 20% to 68%, with a target of 85% by 2022.
- Improved government audits from 20 findings and 90 open or overdue items to zero findings and no overdue items.

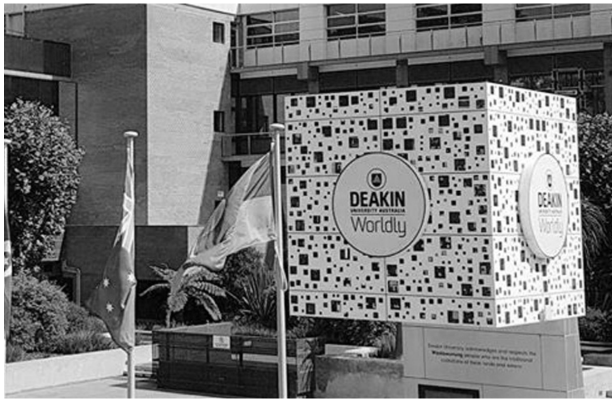
Weak security posture due to patchwork technology and processes

One of Australia's largest universities, Deakin University serves more than 64,000 students and 12,000 staff at four Australian campuses, as well as offices in three other countries. The university also has a strong research component, with influential partners in the commercial and government sectors relying on Deakin to conduct research that solves a variety of problems. A few years ago, the university embarked on a digital transformation journey and became renowned for driving innovation and enabling a globally connected education. But Deakin didn't have a solid security foundation to support its digital initiatives.

"We are a small team, coming from a very low-maturity security function and ad hoc processes here and there," explains Fadi Aljafari, information security and risk manager at Deakin University. "We didn't have a reliable security capability or any sort of architecture for our security offering."

With as many as 100,000 devices and users connecting to the network each day, threats slipped through the cracks and Deakin lacked the ability to efficiently investigate and respond to security incidents. Additionally, it performed poorly in government audits. At one point, Deakin's audits had 20 findings and 90 open or overdue items. And the university environment–with heterogeneous devices and applications as well as researchers' need for seamless access to potentially riskier websites–posed additional challenges.

"A lot of the university security practices were outdated and needed to be uplifted," Aljafari says. "The university recognized its responsibility toward protecting its customer data. This information needs to be treated with confidentiality and the level of integrity that our students and research partners expect from the university."



A seamlessly integrated security architecture

The security team needed integrated security solutions that simplified and accelerated threat detection and response, enabled them to quickly find the root cause of threats, and automated workflows to allow for threats to be blocked automatically. As a small team, however, they didn't have the resources for complex architecture deployment, integration, and management.

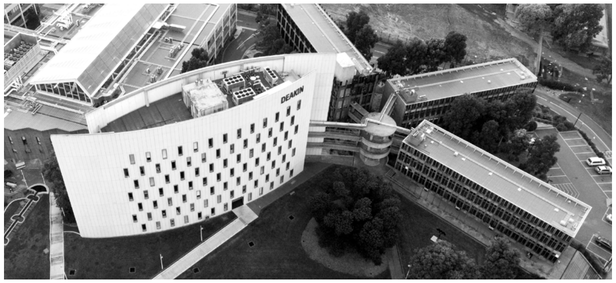
Deakin University chose Cisco for its comprehensive suite of solutions that are easily integrated and provide turnkey interoperability. The team began building out an architecture with Cisco Umbrella, Cisco AMP for Endpoints, Cisco Email Security, and Cisco Firepower 9300 next-generation firewalls. As they added new solutions, they could identify security weaknesses and develop a defense-in-depth, integrated approach to information security. And with Cisco SecureX threat response integrated with all of their Cisco Security products, analysts have unified visibility and can investigate threats from a single console.

"With Cisco SecureX, you get a single pane of glass and you don't need to worry about manually integrating your anti-malware solution with your firewall, with your network monitor, with the network segmentation, with email security," - Aljafari says.

In June 2020, the team got to see SecureX threat response in action when the country's prime minister announced that Australian organizations across a wide range of sectors–including government, higher education, and critical infrastructure–were being targeted by a sophisticated, state-based actor.

"As events unraveled, we discovered that he was talking about an alert that was sent to us a week before the PM publicly talked about this issue," Aljafari says. The Deakin team had already acted on that alert. Previously, it would have taken at least a week to investigate, but SecureX drastically shortened the response time. **"Using the security products from Cisco, in one hour we were able to search all our network and block all the indicators of compromise from a single application (SecureX threat response). We didn't even need to switch screens."**

The team confidently reported to university executives and the board that they'd already blocked the threat a week earlier. "It provided them with good assurance that cybersecurity is working and efficient," Aljafari says. "They're more satisfied that they made the right investment in Cisco as the technology partner, and they have a level of assurance that their cybersecurity investment is giving them value."



A mature security program and improved posture

Thanks to the seamless integrations and easy-to-use technologies, analysts have better tools without switching between consoles. **SecureX also works with Deakin's SIEM solution.** **"This saves a significant amount of time for analysts to do their job and they can solve more incidents more quickly and with a level of certainty that might not be there if these products weren't integrated,"** Aljafari says. One example is responding to malicious emails—what used to take an hour now has an average response time of 15 minutes, and it can be as fast as five minutes.

Deakin University transformed security from a provisional approach into a mature, comprehensive program that enables the small team to stay ahead of threats and mitigate threats that previously went undetected—all without negatively impacting users. One of the wins, Aljafari notes, is that last year's audit of the university resulted in zero findings and there are now no overdue items. He is also pleased with improvements in Deakin's compliance with the NIST cybersecurity framework and Australia's ACSC Essential Eight Maturity Model. After implementing Cisco solutions, Deakin went from 20% compliance with NIST to 68%, with a target of 85% by 2022. Likewise, the university raised its ACSC model maturity level for most of the strategies on mitigating cybersecurity incidents.

"Given the Cisco technologies we have implemented and integrated through SecureX threat response, the processes we have built around them, the people we have trained and upskilled to use these technologies and capabilities, and the awareness campaigns we launched and worked on with users, we have managed to elevate our maturity significantly and improve our security posture," Aljafari says.

He is looking forward to the next step in the partnership with Cisco—implementing the SecureX orchestration capabilities for workflow automation. Another priority, after the deployment of Duo multi-factor authentication (MFA) for staff last year, is to expand Duo MFA to student accounts and to roll out Duo Beyond to check endpoint security posture.

Aljafari feels that as a security partner, Cisco provides Deakin with access to tools, top-notch technology, advice, and insights into the market and threats, along with technology that addresses previously unsolvable problems. **"The most important outcome that we have achieved so far is that security is now a trusted function.** We can tell people what we do for the organization—not what we do for security but what we do for Deakin," Aljafari says. "We have a team who understands where we need to improve and we can deal with threats from a risk-management perspective."