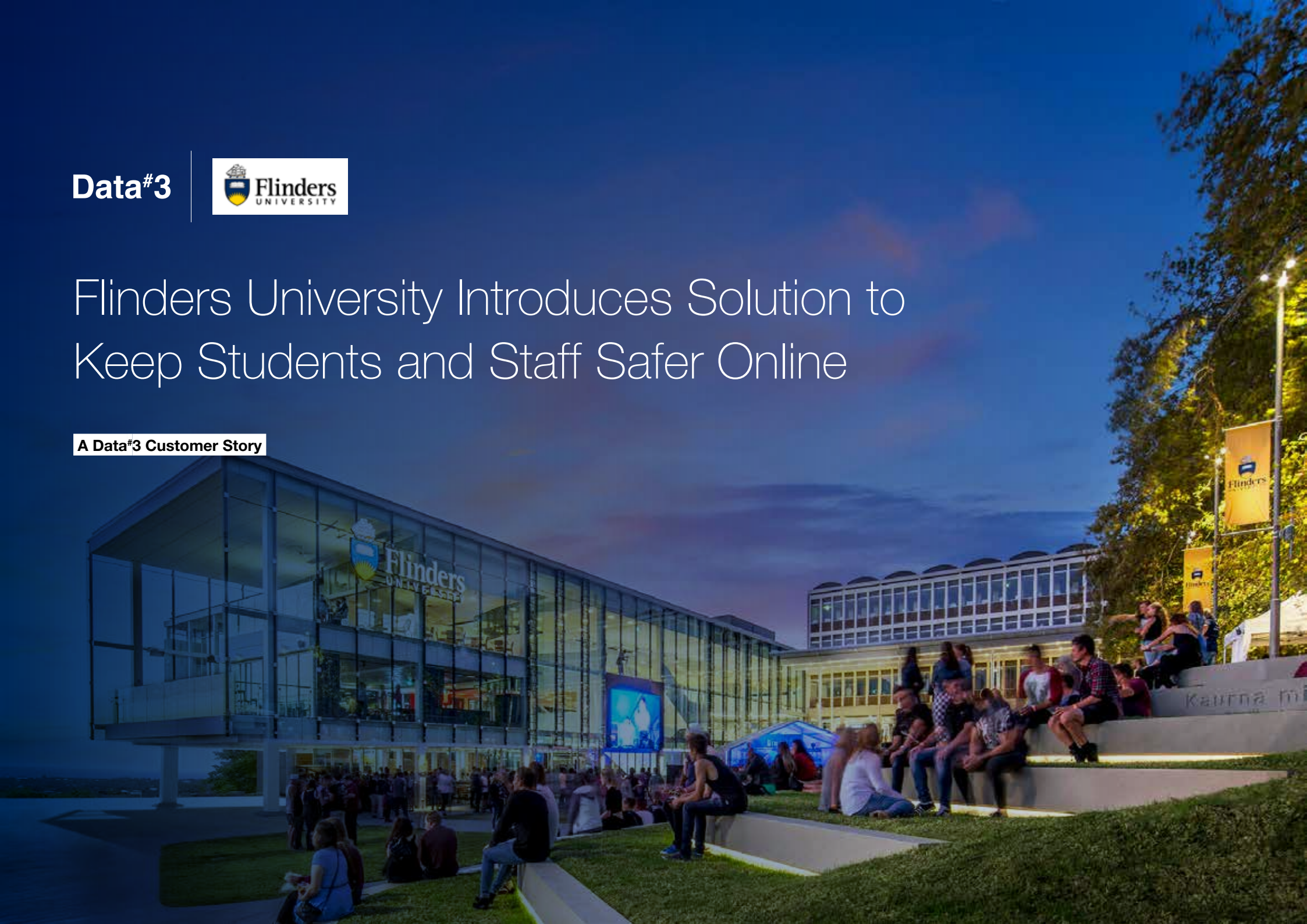
Data#3 | Flinders University

Flinders University Introduces Solution to Keep Students and Staff Safer Online

A Data#3 Customer Story



Data#3

Flinders University

ABOUT FLINDERS UNIVERSITY

Established in 1966 with a main campus in Adelaide, Flinders University ("The University") offers courses throughout regional South Australia, as well as several interstate and overseas locations.

OBJECTIVE

To gain the visibility needed to identify advanced security threats faster, and gain security incident and attack intelligence to reduce future risk.

FUN FACT

By 2022, **50%** of all SOCs will transform into **modern SOCs** with integrated incident response, threat intelligence and threat hunting capabilities, up from **less than 10% in 2015.**

Gartner (2019), Gartner Top 7 Security and Risk Trends for 2019. [Online] https://www.gartner.com/smarterwithgartner/gartner-top-7-security-and-risk-trends-for-2019/

COMMENTS

"The experience of the Data#3 team, and the local skillset, meant that we could be confident in the best outcome for the university community. Our students are safer as a result."

Aaron Finnis, Chief Information Security Officer, Flinders University.

APPROACH

Following a proof of concept, Data#3 proposed a Cisco Intrusion Prevention System (IPS) solution that met the University's needs. During the design phase, the scope of the project was extended to replace existing firewalls.

BENEFITS

- A single point of visibility of the security environment.
- Faster incident response times through real-time alerts.
- Easy identification of compromised machines.
- The IT team is equipped to address security risks resulting from compromised devices.
- Detailed Internet usage information is available to help identify trends and Shadow IT activity.
- Improved reporting accuracy on security incidents to better address threats.

TECHNOLOGY

- ☑ Cisco FirePOWER Threat Defence
- ☑ Cisco Intrusion Prevention System ("IPS")

The Background

Established in 1966 with a main campus in Adelaide, Flinders University ("The University") offers courses throughout regional South Australia, as well as several interstate and overseas locations.

Known for innovative research and quality teaching, The University views technology as a vital tool in developing career-ready graduates who will make a positive contribution to society.

The Challenge

Modern universities present an enticing target to hackers, so protecting Flinders University's 38,000 users, including 7,000 staff, is a key priority for the service-driven IT team. With ground-breaking research in science, medicine, and even autonomous submarines-mapping the ocean, safeguarding intellectual property is also a pressing concern. It takes constant effort to stay ahead of cybercriminals.

Dealing with a highly complex environment is part of daily life for the IT team, and The University must face off against increasingly sophisticated online threats. Chief Information Security Officer, Aaron Finnis, said that the trend is for hackers to target individual users as a method of access.

"We have many types of on-campus users, from staff and students to affiliated organisations and casual tutors, connecting via 2,000 wireless access points," said Finnis.

"With this many concurrent users, we lacked the visibility to see threats quickly enough."

The University had a strong security program already in place, with an identity-driven security architecture making access conditional, but it was determined that more could be done to address threats faster. Increasing visibility and using next-generation security intelligence would alert IT staff to potential risks immediately and allow an automated response that halts suspicious access. It was essential to make any solution frictionless and transparent to users.

Technology Outcome

The University IT team replaced their existing technology with Cisco Firepower NGFW Internet firewalls to unleash the full advantages of FirePOWER Threat Defence.

"We went through a proof of concept, and shortlisted two possible partner solutions to pilot", said Finnis.

"In the end, Data#3 had more experience, and access to skilled engineers close to campus, so they were the obvious choice."

The Data#3 solution architect utilised a proven methodology, ensuring the complex project could be delivered to the desired specifications.

"Having a highly experienced Cisco specialist from Data#3, who understood the product roadmap and what it is capable of doing, made all the difference," said Finnis.

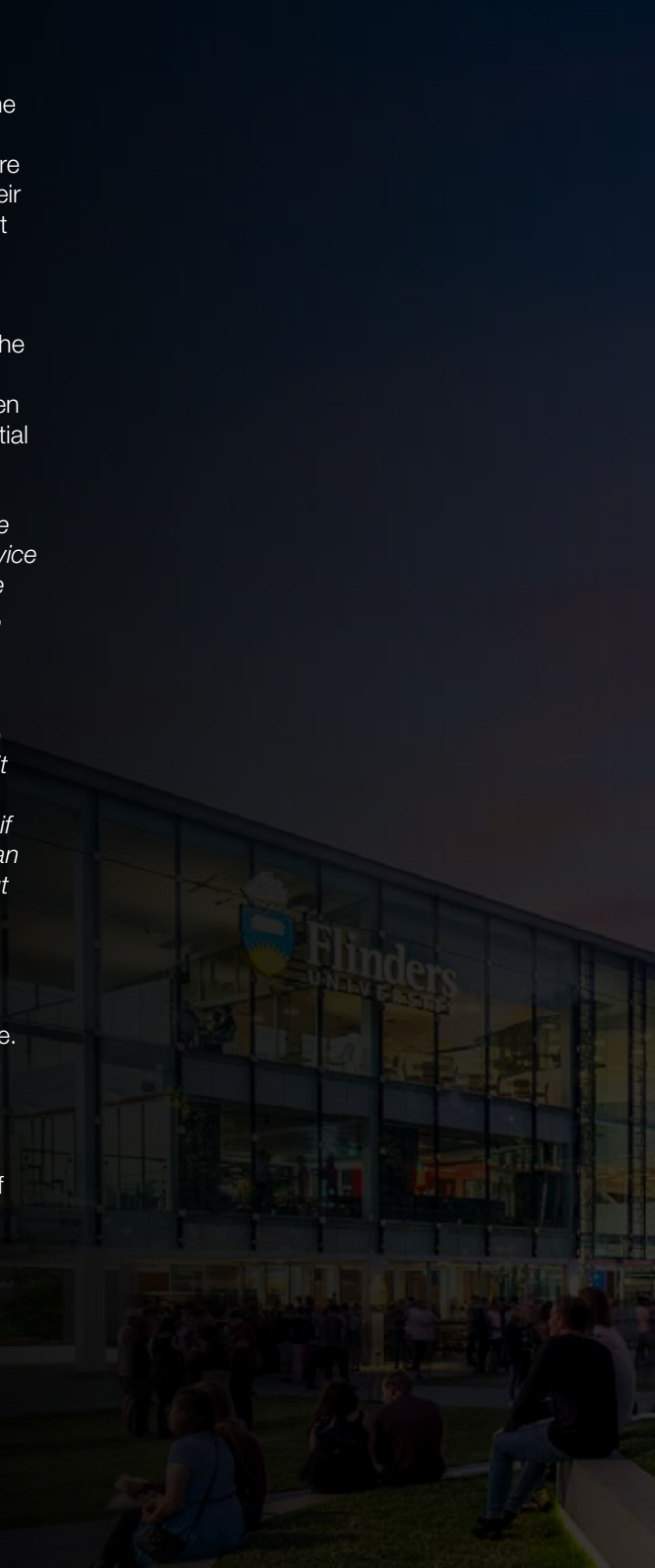
Integration of the Cisco solution with The University's existing network, as well as Active Directory, supports existing secure network segmentation, while links to their Security Information Event Management solution gives easier management and greater visibility and context.

The implementation went to plan, and the switchover on a Sunday afternoon was smooth and uneventful. The IT team then quickly set to work and identified potential threats on the network.

"We see ourselves as a customer service wing, when we detect that a student device is potentially compromised, we know we can help them to improve their security", said Finnis.

"We also use Splunk to aggregate data, from multiple points, including the FirePOWER Threat Defence, analysing it for certain events. The intelligence now available means we get real-time alerts if the student's account is being used in an unusual way, or if there is something out of character."

The University's IT team contacts the student immediately and assists addressing potential risks on their device. This may mean guidance on better anti-virus programs, password protection, and software updates. The team is also working on an automated enforcement system that may limit network access of potentially compromised machines and direct them to a website with remediation information.



Business Outcomes

Threats are now identified much faster. With greater visibility, the team can actively reach out to users with potentially compromised machines. Safeguarding individuals benefits the broader university community, and the team will promote cybersecurity awareness to users during orientation week and in ongoing campaigns.

"The solution from Data#3 allows the university to look back at what occurred before an incident, which makes it possible to prevent a repeat", said Finnis.

"We can do forensic investigation, and look for patterns in what happened in the lead-up to an attack."

Detailed Internet usage information also helps The University to identify user trends, so it can better plan service provisioning. If, for example, many users access a certain application, the team will make a case for using its greater buying power to acquire a licence, making considerable savings over the Shadow IT alternative.

"The solution gives us a very good balance between price and functions that benefit both our staff and student users."

Conclusion

While the environment was already secure, the additional security provided by the new solution positions The University to protect against evolving and future threats. From the top down, The University sees the online safety of students and staff as a key priority and strives to continually increase protection.

"The solution from Data#3 helps us manage the security of our network," said Finnis. "Attacks happen fast, but we now have real-time visibility."

Having a clearly defined objective, and the University's up-front engagement in a proof of concept, helped ensure a successful project with minimal user impact.

"The experience of the Data#3 team, and the local skillset, meant that we could be confident in the best outcome for the university community," said Finnis.

"Our students are safer as a result."

Data#3

1300 23 28 23
facebook.com/data3limited
twitter.com/data3limited
linkedin.com/company/data3
youtube.com/user/data3limited