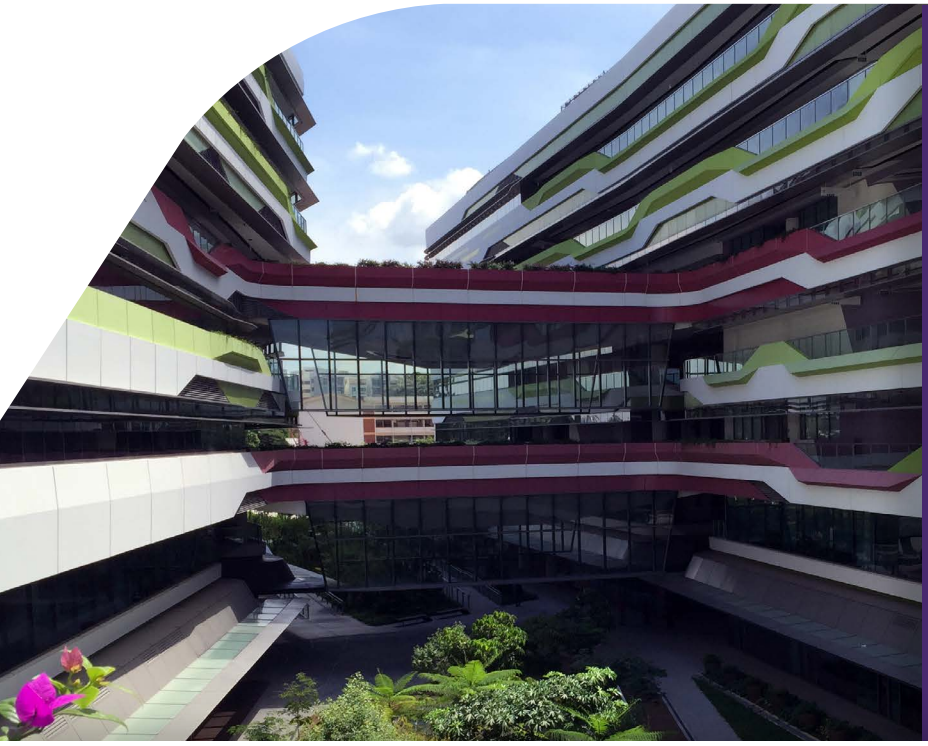

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Industry

Higher education

IT environment

Approximately 900 faculty and staff and 2,000 students studying and working in an environment consisting of managed and unmanaged devices.

ARMIS HELPS SINGAPORE UNIVERSITY IMPROVE VISIBILITY, BOOST ITS SECURITY POSTURE, AND BUILD A SECURITY CULTURE

By gaining a better handle on unmanaged Bring Your Own Devices (BYOD) and research equipment, IT intends to instill users with a greater sense of security accountability

Understanding the stark realities of today's increasingly complex threat landscape, the Singapore University of Technology and Design (SUTD) is on a mission to up-level its cybersecurity. Like most institutions of higher learning, the university was well aware of the risks posed by unmanaged network-connected assets used by students or under the ownership of research groups. The first order of business was to find a way to gain visibility into these unmanaged devices. The IT team chose Armis to identify these devices and provide a complete IT asset inventory with comprehensive, granular data for each device. The team is sharing their newly acquired knowledge with stakeholders to pave the way for a stronger security posture supported by heightened security awareness among users.

CONNECT WITH US

Singapore University of Technology and Design (SUTD) is a boutique university, with approximately 2,000 students and 900 faculty and staff. Founded in 2009, the research-intensive university offers four-year undergraduate programs in computer science, engineering, artificial intelligence, architecture, and related fields. Besides undergraduate, master's and post-graduate degree programs, skill-based professional education and training courses are also available at the SUTD Academy.

SUTD is heavily involved in ground-breaking research and design innovations that span many different disciplines. The university's key focus areas are in Healthcare, Cities, Aviation and Sustainability, with Artificial Intelligence/Data Science and Digital Manufacturing capabilities across all of them.

Challenges

- Gain visibility into Bring Your Own Devices and IT assets controlled and operated by research groups.
- Define and enforce security policies.
- Create a culture of security awareness and accountability.

Solving the problem of near-zero visibility to unmanaged assets in a university setting

The increasing complexity of today's threat landscape compelled IT Director Lek Han Ang and other top-level decision-makers to rethink the university's approach to security and risk. Ang, who has served in this role for 11 years shared that, at the outset, the university relied on a traditional set of security controls, including antivirus and on-premises firewalls, to protect managed devices. But in an environment that Ang describes as "vibrant and always changing," he and his team had no visibility to unmanaged personal devices and computing assets used for research purposes that connect to the network. Ang knew they existed, but he needed to know more about them in order to better secure the overall campus environment.

He and his team embarked on this mission by first engaging global consulting firm KPMG to perform a thorough assessment of the university's security maturity level and to identify protection gaps. KPMG provided a status report and a security roadmap, which featured 15 projects focused on three key areas: refining processes, managing security and compliance based on the International Information Security Standard, ISO 27001, and solving the problem of the weakest link—people who may lack security awareness and often inadvertently engage in risky behaviors.

Apart from managed devices and the personal mobile devices routinely used by staff and students, departments or research groups often purchase their own equipment, funded by grants, and set up their own servers and desktops. These are outside the purview of IT. Most of these equipment are installed in research labs or offices and do not follow the IT department's strict hardening guidelines and security policies, or even simple password recommendations.

On a quest to strengthen the university's security, Ang and his team asked a fundamental question: "How do you create and enforce policies if you don't know what you have?" In the early days, Ang and his team asked departments to declare their assets on an Excel spreadsheet, but few complied, making it difficult to create and enforce security policies. It quickly became obvious that the honor system approach wasn't working.

Armis quickly solves the visibility dilemma

After evaluating multiple tools, Ang decided that the Armis security platform, with its agentless, passive monitoring capability, was the best way to gain visibility to unmanaged devices connecting to the network. He moved forward with a proof of concept in mid-2022.

In a short period of time, Armis discovered devices that were previously unknown to IT. These included computers, tablets, mobile devices, and internet of things (IoT) devices, such as cameras, building control systems and gaming consoles used by students at on-campus housing. Armis provided Ang and his team with insights on both existing devices and new ones: where they are installed, who owns them, their risk profile and application traffics generated.

"In the past, we had no way of knowing when a faculty member sets up a new server or laptop. With Armis, we can see almost everything. Now with this level of visibility, we can stand back and look at the data and implement a triage approach, where we respond to the most critical issues first, such as potentially compromised assets that store the most sensitive information. For example, we would prioritize servers that contain critical research data," said Ang.

In the near future, Ang foresees that Armis will help his team identify equipment that is "abandoned" and no longer in use when a faculty member leaves the university. He pointed out that this can become a security issue if the equipment's patching is not up to date.

Armis results

- Identifying all managed and unmanaged devices, from research servers to personal mobile devices, and IoT.
- Collecting granular data on all network-connected devices.
- Providing drill-down dashboards and reports to help drive behavioral change among users and ease compliance.

Sharing data from Armis to inform and inspire

Once Armis helped establish an accurate asset inventory, Ang and his team fine-tuned their dashboards to organize the rich data collected by Armis sensors.

"We customized our dashboard so that we have a view of the IT-managed estate, as well as the non-IT environment. Each of these views are further broken down by device types—servers, workstations, laptops, tablets, and others. By clicking on each device, we can do a deep dive and derive important details, such as the operating system version, the security protections in place, patching status, browsers installed, and so much more. This has really helped my small team get a handle on our network assets," said Ang.

As a next step, Ang plans to present the findings in the dashboard to the university's provost, who is also the chairman of the university's data protection and security governance committee, and the deans of all schools. Ang believes that this will help his team solve the people problem in security. As he pointed out, people are often the weakest link, especially in a university setting, as they use unmanaged devices that may not be properly updated with the latest operating system versions or security controls to protect against vulnerabilities.

"With all the information Armis has helped us collect, we will be able to demonstrate to stakeholders how we are able to identify risks and vulnerabilities. Our goal is to drive behavioral change among our faculty and researchers so they can take ownership of security," explained Ang. "The easy way out would be to hire more engineers to ensure that servers and laptops are patched and new equipment follows hardening guidelines, but if we do that, the faculty will continue to say 'security is not my responsibility.' Armis is enabling us to demand greater accountability," remarked Ang.

Simplifying compliance and passing audits

Another important use case for Armis is security audits. Governance is very tight, and the university is subject to seven or eight IT and security audits annually. This is a top priority for Ang, who answers to the risk & audit committee and data governance committee. With granular, real-time reporting, Armis makes it easy for Ang and his team to gain insights into the university's security posture, continually make improvements, and demonstrate compliance.

Beyond asset inventory: security response and vulnerability management

Amid the early stages of its Armis deployment at SUTD, Ang and his team intend to broaden their utilization of the tool.

They are currently seeking out a partner who could use Armis to do daily or weekly asset reconciliations and respond and remediate any security issues that may arise.

"The next phase is to maximize Armis beyond asset inventory. Now that we have a good handle on what devices are connecting to the network, we plan to look into how we can use the Armis-Qualys integration for vulnerability management in the near future. We are especially interested in learning more about how Armis generates device risk scores so that we can focus our attention to the most urgent vulnerabilities," said Ang.

"With all the information Armis has helped us collect, we will be able to demonstrate to stakeholders how we are able to identify risks and vulnerabilities. Our goal is to drive behavioral change among our faculty and researchers so they can take ownership of security"

Lek Han Ang

IT Director

Singapore University of Technology & Design

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

888.452.4011 | **armis.com**

20220711-1