CASE STUDY

TANIUM

Regis Aged Care secures endpoints, protects residents with Tanium

With healthcare an attractive target for cybercriminals, this Australian provider of services for older adults needed to strengthen its endpoint security.

ORGANIZATION

Regis Aged Care

LOCATION

Australia

EMPLOYEES

8,650

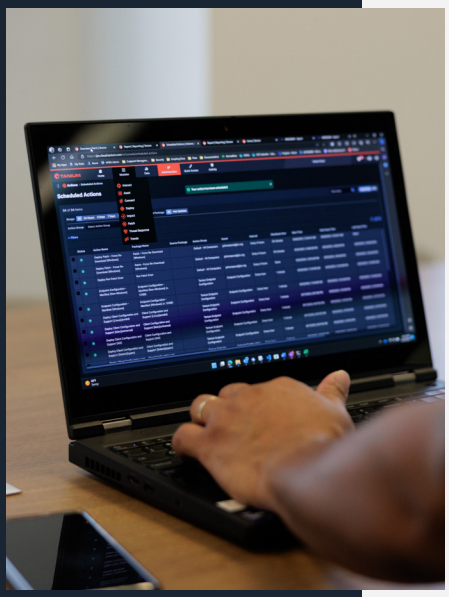
Regis Aged Care has for nearly 30 years enjoyed good business offering residential care, home care and retirement living to more than 7,000 older adults across Australia. More recently, the healthcare industry it's part of has become an attractive target for ransomware, and its supply chain, a hot target for cyber breaches. These cybercrimes threaten not only Regis Aged Care's IT systems but also the privacy and security of its clients.

The core of Regis Aged Care's business is providing care for its residents. As part of that care, it must keep its residents' data safe, secure and private. "Security is embedded in everything we do," says Mazino Onibere, head of cybersecurity risk and compliance at Regis. Mazino faced another challenge, too: His staff didn't always know where their endpoints were, didn't always know what was running on those endpoints, and generally lacked sufficient endpoint control.

After observing the 2017 WannaCry ransomware attack, which affected more than 300,000 computers worldwide, Mazino realized that, while patching is important, it isn't enough.

To strengthen Regis Aged Care's cybersecurity, Mazino searched for a tool that offered what he considered seven essential capabilities:

1. Real-time visibility
2. Fast, scalable patching
3. Ease of use and deployment, with seamless integration
4. Completeness, requiring no other tools
5. Ability to manage endpoints both on- and off-premises
6. Patching automation
7. Alignment with the organization's strategic vision



Checking all the boxes

However, Mazino discovered that very few endpoint management tools could provide all seven capabilities. Some of the tools he explored had grown via acquisition. As a result, they contained multiple parts that were not seamlessly integrated. Others were primarily point solutions, making them too limited for Regis' needs. Still others lacked the ability to automate patching, meaning they would have been laborious, even tedious to use.

In addition, Mazino sought a solution that would empower Regis Aged Care's IT operations and security teams to work together more closely. "We had a dichotomy," he explains. "Security could only look in from the outside. And IT ops were doing what they could from the inside."

The reality was even more complicated. IT operations at Regis are divided among two groups: end-user computing and server engineering. Mazino needed a solution that let all three teams work hand in hand.

"That way," he says, "we'd have complete visibility—and the ability to do something about what we saw." Fortunately, Mazino's explorations led him to Tanium. It was, he says, "the only one that ticked all the boxes."

> **"Just by implementing a single [Tanium] workflow for workstation patching, we climbed from 1% compliant to 98%—and in only two months."**
>
> **Mazino Onibere**
> Head of Cybersecurity Risk and Compliance, Regis Aged Care

Patching compliance, transformed

By using Tanium, Regis Aged Care has gained several valuable benefits. For one, Regis now has complete and real-time visibility into its endpoints, no matter where they're located. That empowers Mazino and his staff to protect the privacy and security of the company's residents more effectively.

This has resulted in a massive improvement in patching compliance. "Just by implementing a single [Tanium] workflow for workstation patching, we climbed from 1% compliant to 98%—and in just two months," Mazino says.

Tanium has also fostered greater collaboration among the security and IT operations groups. "With Tanium," Mazino says, "we have the same data, we're seeing the same things, and we have a complete inventory of our assets, whether they're endpoints, workstations or servers."

Further, Regis Aged Care benefits from Tanium's partnership with Microsoft. Thanks to these strategic integrations, Regis' IT environment is now more secure, higher-performing, and automated.

Although the Regis IT environment is predominantly based on Windows, Mazino now uses Tanium to augment their Microsoft endpoint management tools as his single source of truth for patching. "I wanted a solution that was independent," he says. "Everything we require can be implemented with Tanium."

Regis also plans to use Tanium SBOM, a newer offering designed to quickly identify software supply-chain vulnerabilities. With Tanium SBOM, if an open-source software package in the supply chain is vulnerable, users can protect their IT environments by identifying every application where the package exists.

For Regis, that package is OpenSSL, a widely used software library for secure network communications. "With Tanium SBOM, we will be able to see exactly where OpenSSL is in our environment," Mazino says. "I'm excited about that."

Results

Endpoint visibility

Before using Tanium, Regis Aged Care lacked visibility into all endpoints, especially those being used by remote workers. Now, with Tanium, visibility is complete and in real time.

Patching compliance

Regis used Tanium to transform its workstation patching compliance rate from a scary 1% to a confidence-building 98%—and all in two months.

IT operations + security

By providing a single source of truth, Tanium empowers Regis' IT operations and security groups to work together closely. They both have the same information at the same time and in the same format.

Better with Microsoft

Thanks to Tanium's partnership with Microsoft, Mazino of Regis can use Tanium as his sole information.

> "With Tanium, we have the same data, we're seeing the same things, and we have a complete inventory of our assets, whether they're endpoints, workstations or servers."

Mazino Onibere
Head of Cybersecurity Risk and Compliance, Regis Aged Care

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.