CASE STUDY

The University of Salford Finds and Closes Hundreds of Thousands of Endpoint Vulnerabilities

With Tanium, British educational institution updates and secures 5,000 devices while eliminating the costs and complexities of five endpoint management tools

When COVID-19 struck, the University of Salford knew it was facing a serious challenge in managing its risk against cybercrime. After decades of running a classically centralized, campus IT infrastructure, Salford was not fully prepared for the study-from-anywhere era.

Like most universities around the world, the University of Salford quickly transitioned to remote learning. Overnight, that created new IT management and security challenges as students and teachers connected to the university through home wi-fi networks and personal computers.

Soon, a wave of cybercrime began against British educational institutions. Profit-driven groups launched an array of sophisticated digital attacks while state-backed entities probed research networks for vaccine-development data.

Salford knew the university was at risk, but it didn't know what would happen if the organization's

network was hit, says Mark Wantling, Chief Information Officer for the university.

Wantling initiated a security assessment to find out. The results were concerning.

Salford realised the university was vulnerable to a digital breach and immediately moved cybersecurity to the top of its risk priorities. Overnight, closing cybersecurity gaps became a board-level problem for the university, Wantling says.

Technology Challenges

Despite recognizing its exposure to cyber risk, Salford lacked the necessary capabilities to effectively protect its network of devices, Wantling says.

The university had five endpoint management tools, but they didn't work well together, required their own teams, and created their own data.

University of Salford MANCHESTER

Industry
Education

Headquarters
Salford, England

Employees
2,700+

Students
20,000+

Endpoints
5,000+

Tanium Products
Discover, Asset, Patch, Deploy, Comply

Key Benefits

- Discovered hundreds of "hidden" endpoints and hundreds of thousands of open vulnerabilities.
- Quickly fixed 38,000 missing patches and updated software on hundreds of thousands of endpoints
- Remediated multiple zero-day threats in minutes across the entire network
- Saved tens of thousands of dollars in licensing fees by replacing five endpoint management tools with Tanium

Also, each tool only addressed a subset of all the university's endpoint management issues, Wantling explains. They simply didn't provide the breadth and depth to support the comprehensive and rapid security response capabilities the university needed.

Adding to the university's challenges, the institution's IT infrastructure was large and siloed. The university operated four different schools supported by a complex blend of on-premises and cloud systems.

> If we hadn't invested in Tanium, we would lack complete visibility into our assets and still have hundreds of thousands of missing critical patches. It would only be a matter of time before we were targeted by cyber criminals and potentially put in a really difficult position.

Mark Wantling
CIO, University of Salford

Because of these challenges:

- Salford did not have comprehensive visibility of its assets or what vulnerabilities those devices carried.
- The university struggled to apply software patches and updates to reduce its risk.
- There was concern if the university were attacked, it couldn't respond fast enough to prevent harm.

Salford knew it needed to find a significantly better way to manage and protect the endpoints connecting remotely into its institutional network. That's when Wantling turned to Tanium.

How Tanium Helped

Wantling initially used Tanium to create comprehensive real-time visibility into the university's network of connected computers and other devices.

With Tanium, Salford:

- Discovered hundreds of shadow IT endpoints
- Identified hundreds of thousands of missing critical patches and software updates
- Established real-time visibility into its 5,000 on-premises, remote, and cloud-based assets
- Created a common system of record for its IT, security, risk and executive teams

As a next step, Salford used the Tanium Platform to close any vulnerabilities across its distributed network of remote devices connecting students, teachers and administrators.

With Tanium, Salford:

- Reduced its missing critical patches by more than 99%, from more than 38,000 to 238
- Reduced its missing updates from several hundred thousand to under 1,000
- Reduced its patch window from several weeks to under 24 hours
- Reduced the time and effort to carry out software patches by 66%, with near-perfect coverage

By using Tanium for endpoint visibility and control, Salford transformed its risk posture and its incident response capabilities, Wantling says. Within a two-month period, the university experienced two zero-day threats. Each time the institution used Tanium to quickly identify vulnerable assets across its distributed network, patch them, and report to the board on the incident in less than a few minutes.

Thanks to Tanium's comprehensive capabilities, Salford was able to consolidate all of its endpoint management and security tasks onto the Tanium Platform, replacing its five previous tools and saving tens of thousands of dollars in annual licenses while bringing far greater efficiencies to its operations.

TANIUM

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.