CASE STUDY

University of Salford unifies threat coverage with Tanium, ServiceNow, and Microsoft Sentinel

University of Salford MANCHESTER

Industry
Education

Size
25,000 students

Headquarters
England

Managed endpoints
8,000

Results

- Tighter integration between IT operations and security
- Improved visibility and risk assessment
- Faster response times

The UK-based university is now using Tanium XEM, ServiceNow CMDB, and Microsoft Azure Sentinel to achieve real-time endpoint visibility and drive lightning fast security response.

The University of Salford is a leading university located in Salford, Greater Manchester, England. Within the university, there are four schools and roughly 25,000 students who attend virtually and in person.

Like most higher education providers today, the University of Salford is optimizing its network to ensure a safe and reliable hybrid community environment. However, this is no easy task. Following the pandemic, university members now teach, learn, and research using a mix of personal devices and networks — making the university's attack surface much larger and more distributed than it was in the past.

As a result, the universities IT department is actively working to modernize endpoint management and shrink its attack surface.

"The pandemic drastically altered the way we approach endpoint management," says CIO Mark Wantling. "We needed a way to increase visibility, and track threats in real-time across thousands of different devices and locations."

The university is now using **Tanium Converged Endpoint Management** (XEM) along with ServiceNow and Microsoft Azure Sentinel for security information and event management. By integrating Tanium with these platforms, the security team can respond to incidents with maximum speed and precision — discovering and mitigating threats before they lead to harm.

> "Being able to identify something consistently and quickly across platforms, and then respond potentially with automation or Playbooks through Azure Sentinel and Tanium improves our response speeds and mitigates the potential impact of a breach."

Mark Wantling
Chief Information Officer,
University of Salford

Triple coverage with Tanium XEM, Azure Sentinel and ServiceNow

The University of Salford first **implemented Tanium** back in 2021, in order to gain real-time visibility across its network and centralize vulnerability management. The platform was an immediate success, with Tanium quickly discovering hundreds of shadow IT endpoints and thousands of missing critical patches and vulnerabilities.

In the second phase of the project, the security team integrated Tanium with ServiceNow CMDB to establish a single source of truth across both platforms. Tanium now feeds security data directly into ServiceNow.

For Wantling, the integration between Tanium and ServiceNow is a natural fit.

> "By plugging Tanium into ServiceNow and Sentinel, our operations team can achieve total visibility across all three core platforms without any data silos."

Mark Wantling
Chief Information Officer,
University of Salford

"Having a consistent CMDB is a foundational security requirement," Wantling explains. "My view is there's no point in having a single source of the truth in Tanium if we're not going to use it in ServiceNow as well. The two platforms go hand in hand."

The university is also in the process of linking Tanium to Microsoft Azure Sentinel, which is a highly scalable, cloud-native platform for security event monitoring and orchestration.

"We have quite a small security team," says Wantling. "To correlate information and create a quick and effective response, we need Tanium to integrate fully with Azure Sentinel. This latest integration is a game-changer for the university."

Breaking down silos

The university also has full visibility across all its distributed endpoints over a single pane of glass. And, thanks to Tanium's flexible integrations, the university's security and operations teams can also share data effortlessly and work more closely together.

"This has completely changed the way our team works and operates," Wantling says. "Our operations and security teams now work on the same dashboard with the same metrics and the same objectives. They now share a single source of truth, which makes reporting infinitely easier and more impactful."

Faster response times

The solution is lowering security response times and making it easier for team members to discover and remediate threats.

"We have thousands and thousands of endpoints, and what we're seeing is that time to respond to any potential threat is reducing," Wantling says. "Being able to identify something consistently and quickly across platforms, and then respond potentially with automation or Playbooks through Azure Sentinel and Tanium improves our response speeds and mitigates the potential impact of a breach."

Improved risk assessment

The team also uses Tanium Impact to identify, prioritize, and remediate access rights and dependencies. This makes it possible to instantly detect and shut down lateral movement. With the help of Impact, the team can quickly discover high-risk areas, users and devices, and spring to action. A process that used to take weeks can now be performed with a simple query.

"With Impact, we can focus our efforts on the users and devices that need the most attention," Wantling says. "The correlation of risk between user and device is massively important for us."

Driving cultural change

According to Wantling, the team is deliberately setting the pace of change as they implement Tanium and using it to drive culture change within the university. The university views Tanium as a key part of its security framework and will continue integrating the platform throughout the organization where it makes sense.

"I think changing a university is difficult," Wantling says. "It's painful, particularly across an IT team, which is very well-established. We are stepping through our implementation of Tanium and increasing our usage of it all the time, but it comes with culture change as well."

Looking forward, the university also intends to move towards Zero Trust, or a framework that assumes an organization's security is constantly at risk from internal and external threats. Tanium will serve as a foundational element and allow the team to build an effective Zero Trust model.