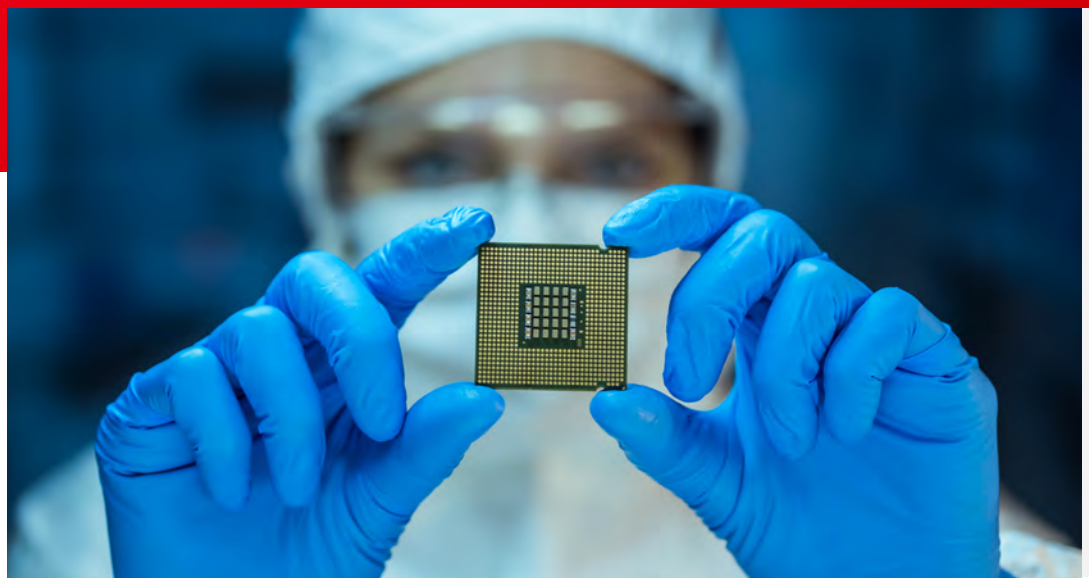
CASE STUDY

TANIUM

Integer supercharges response times with Tanium and Microsoft

How Integer uses Tanium and Microsoft to defend against sophisticated attacks and automate critical security workflows.



Integer®

Industry
Medical device manufacturing

Size
2,800 employees

Headquarters
Plano, Texas

Managed endpoints
300,000

> "With Tanium and Microsoft, we always get fresh insights. You can look at a report with the confidence that you're always going to see either live or last-reported data."

Chris Windham
Security Monitoring and Response Manager, Integer

Integer is a leading global medical device outsource (MDO) manufacturer serving the cardiac, vascular, neuromodulation, and portable medical markets. The company provides innovative technologies and manufacturing for medical device OEMs and develops batteries for niche military, energy, and environmental use cases. Integer has a global presence, with locations throughout North America, South America, Europe, and Asia Pacific.

Like all companies today, Integer is facing an evolving threat landscape that's becoming increasingly dangerous. This forces Integer to act with greater speed and precision when responding to threats.

"Leadership measures our success by how we respond to incidents — how we dive in and find out what is really going on," says Integer Security Monitoring and Response Manager Chris Windham. "We ask questions like — What was the initial cause? Is it blocked? How do we block it? How do we remediate? That response time is basically how they measure us, along with growing the program and thinking of new creative ways to automate."

Modernizing endpoint security and reducing complexity through automation is now a top priority for Integer's security operations center (SOC) team. Using Tanium's XEM platform in close collaboration with Microsoft services like Defender for Endpoint (MDE) and Endpoint Configuration Manager helps Integer respond quickly and efficiently to emerging threats. Integer also uses Tanium to automate security tasks and workflows.

Microsoft and Tanium: Better Together

Integer relies heavily on Microsoft's powerful suite of security services to manage and defend its endpoints from cyber threats. It also uses Tanium to verify that all group security policies remain up and running across multiple endpoints. This prevents team members from having to manually check endpoints for status updates and remediate issues.

Tanium helps Integer derive even more from its suite of Microsoft security services by providing real-time performance and activity monitoring from a central location. By adding Tanium to the mix, Integer can now view all Microsoft policies from a single pane of glass and confirm that they are in the correct state for continuous monitoring and verification.

"When troubleshooting services like Group Policy Orchestrator for Windows (GPO), Tanium continuously runs in the background and fixes our machines, which frees our team to tackle other important tasks."

Integer is also using Tanium's software bill of materials (SBOM) tool to complement Microsoft Defender. With Tanium SBOM, Integer gains instant visibility across its entire software supply chain. In the event of a serious vulnerability like Log4j, Integer can use Tanium in conjunction with Microsoft to hunt for exposure in real-time across its entire digital real estate — including hidden items buried deep within an application's SBOM.

"We have developers building various automation and combining different pieces — but they often have difficulty telling us where specific items are located," Windham says. "Tanium SBOM streamlines software asset discovery, which greatly reduces risk. It goes far beyond what most vulnerability scanners are capable of."

In addition, Integer uses Tanium to extend the Microsoft BitLocker Administration and Monitoring (MBAM) interface. With the addition of Tanium, Integer can select specific locations for custom BitLocker compliance monitoring and reporting.

Accessing on-demand data

Tanium now acts as the system of record for Microsoft information and helps Integer monitor and track policies and activity across all Microsoft endpoints.

"With Tanium and Microsoft, we always get fresh insights," Windham says. "You can look at a report with the confidence that you're always going to going to see either live or last-reported data."

As a bonus, Tanium also integrates with Microsoft Intune, providing yet another source that Integer can use to target specific machines.

Preventing security misconfigurations

Integer can now instantly locate devices and address misconfigurations from a single location. For example, Integer recently used Tanium to detect and resolve a problem with Microsoft Local Administrator Password Solution (LAPS).

"Tanium discovered that LAPS wasn't running in one of our facilities," Windham says. "All these new machines kept being installed and re-imaged, but they didn't have the software. That led our team to look at the SCCM console and determine that the server didn't receive it."

Automating security and access control

Integer uses Tanium to create and manage conditional access scenarios. To illustrate, the company now has VPN posture checks in place so that when users attempt to connect, the host must be compliant with the entire security stack installed.

"Thanks to Tanium, we can automatically remediate that issue before a user even sees it," Windham says. "Plus, if they do have a problem and they call for help, our service desk can look and see if they're missing something like WSS or SCCM and send the necessary package over."

Normalizing and sharing data

Tanium also serves as a single pane of glass for Microsoft information, which in turn normalizes data, and improves integrity.

"Consider something like a computer name," Windham explains. "A computer might have different names across five different sources — like a short name, full name, and something totally different. But that single plane of glass gives me a way to normalize data and report on everything."

Having a single pane of glass also democratizes data access, which benefits everyone in the organization.

"Everybody in the company should be able to access metadata," says Windham. "With Tanium, everyone can see the same data that you're looking at."

> "Leadership measures our success by how we respond to incidents — how we dive in and find out what was really going on. We ask questions like — What was the initial cause? Is it blocked? How do we block it? How do we remediate? That response time is basically how they measure us, along with growing the program and thinking of new creative ways to automate."

Chris Windham
Security Monitoring and Response Manager, Integer

Looking ahead: Integer to keep using Tanium and Microsoft

Based on Integer's initial success with Tanium and Microsoft, the company plans to continue using the two services together to discover threats, reduce manual workloads, and keep security operations running smoothly.

"The seamless automation between the two companies helps the products fix and enhance each other," says Windham.

Integer is presently looking for additional ways to use Tanium and Microsoft together. For example, Integer is exploring Tanium's new integration with the Microsoft Sentinel console. The company also plans to lean more heavily on Tanium as it migrates more workloads into Azure.

For Windham and the rest of the team at Integer's SOC, Tanium is now a must-have tool for security enhancements, data reporting, and threat analysis. Together with Microsoft, the company has a complete solution for endpoint management and security automation.

"Tanium has made my life very easy," Windham says. "With Tanium up and running, I can turn my attention to things where we lack good visibility. I want it to be at the core of our security operations because I know what we can accomplish with it — and how much it enhances our productivity and abilities."