

Indiana University of Pennsylvania removes legacy software, transforms IT operations and security with Tanium

Since replacing their previous patching tool, this public research institution's IT team is finding Tanium to be a game-changer.



ORGANIZATION

Indiana University of Pennsylvania

INDUSTRY

Education

EMPLOYEES

Approximately 1,400

LOCATIONS

- Indiana, Pennsylvania, USA
- Punxsutawney, PA
- Pittsburgh, PA
- Armstrong County, PA

REVENUE

\$216.7 million

ENDPOINTS UNDER MANAGEMENT

4,500 (plus
350 servers)

Indiana University of Pennsylvania (IUP) is a renowned academic institution celebrated for its nationally ranked research excellence, distinguished doctoral programs, and world-class culinary arts program. Nestled in the heart of Pennsylvania, with campuses in Indiana and Punxsutawney and instructional sites in Pittsburgh and Armstrong County, IUP combines a commitment to academic rigor with innovative, hands-on learning opportunities to shape future leaders in education, the arts, sciences, healthcare, and beyond.

IUP has undergone a remarkable transformation of its IT operations and cybersecurity posture by adopting Tanium's Autonomous Endpoint Management (AEM) capabilities. Facing challenges of a decentralized environment, manual processes, and limited visibility, IUP's journey with Tanium highlights the platform's ability to modernize operations, enhance security, and foster a more efficient, collaborative IT environment, creating a recipe for success for the university.

A legacy of decentralization

For decades, IUP's IT operations were decentralized, with each of its eight colleges managing its own systems and security protocols. According to Ben Dadson, IT Coordinator, Enterprise Infrastructure and Systems at IUP, this approach led to inconsistent desktop configurations, varied levels of security, and resource disparities between departments.

"Some colleges had more funding and better resources, while others struggled to maintain basic technology standards," Dadson says. "There was no consistency in security measures, or software management."

In 2007, the IT infrastructure for the colleges were merged into a central organization. In 2010, the endpoint management came under central IT. Following a presidential mandate in 2012 that all systems follow governance and standardization developed in central IT, all college-managed servers were added to IT central management.

To make matters worse, the university's previous patch management solution couldn't provide visibility into remote devices or patch systems that were not on-premises. The patching tool also couldn't provide real-time reports of what had happened after the patches were updated. If a patch created an issue for one of the devices, the team wouldn't know it, and the issue might not get resolved. This lack of visibility and control over remote endpoints created vulnerabilities and forced IT teams to adopt time-consuming manual processes to ensure security compliance.

Enter the 'game-changer'

After hearing about Tanium from IUP's trusted partner, CDW-G, followed by an initial review of Tanium's capabilities, Dadson commissioned a proof-of-concept with Tanium to compare the two products. The results were clear. Not only did the Tanium platform exceed the former patching capabilities, but its solutions went beyond patching. "For us, it was a game-changer," says Dadson. Tanium's cloud-based service gave his team real-time visibility into all machines – regardless of location.

Switching was easy. "Tanium just worked," says Dadson.

KEY RESULTS

80% reduction in patch management time

Tanium automated and streamlined IUP's patching processes, reducing manual effort and overnight work by 80%.

4,500 desktops and 300 servers under management

IUP successfully used Tanium to manage, secure, and monitor its extensive IT infrastructure across 4,500 desktops and 300 servers (including both Windows and Linux machines).

100% visibility into remote and on-premises endpoints

Tanium provided IUP with complete visibility into all devices, including those operating remotely, which was critical for maintaining security and compliance post-pandemic.





Key benefits and outcomes

From real-time visibility to improved security and operational efficiency, IUP has seen measurable campus-wide impact since deploying Tanium.

1. Real-time visibility across endpoints

Tanium provides IUP with unmatched visibility into its 4,500 desktops and 300 servers, including devices operating off campus.

“The first time I saw a machine’s IP address from a home network, it was mind-blowing to see all that information,” Dadson says. “We could see devices at home, check their status, and even identify the last time they were online.”

Even when a device is powered off, Tanium retains cached information, offering a historical view of its status and activity. This visibility is critical for ensuring the security of devices accessing sensitive university resources.

2. Efficient and automated patch management

Tanium transformed IUP’s patching process, reducing manual effort and increasing efficiency, making three-hour manual sessions a thing of the past. Using Tanium, IUP set up staggered reboot schedules based on tags, ensuring minimal disruption to users while maintaining compliance.

“Before Tanium, patching was a labor-intensive process that required staff to work extensive hours, manually monitoring and rebooting servers,” Dadson explains. “Now, we’ve automated the entire process, reducing patch time by 80%.”

3. Enhanced asset and software inventory for cost savings

Tanium’s asset management capabilities enable IUP to identify underutilized software and hardware, leading to significant cost savings and allowing the university to switch to more effective licensing models. Tanium’s reporting capabilities help save money by locating obsolete hardware – such as machines with mechanical drives – and optimize inventory management by identifying devices that haven’t been used in months.

4. Improved security and risk mitigation

Tanium addresses long-standing security concerns by identifying devices with elevated admin privileges and resolving vulnerabilities across endpoints. Tanium helps IUP pinpoint devices and accounts with excessive privileges, mitigating the risk of lateral movement and data breaches.

5. Cultural and operational transformation

Tanium’s automated features free up IUP’s IT staff to focus on strategic initiatives rather than mundane, repetitive tasks. Instead of handling tedious patching processes, the time saved is reinvested into improving other university systems, such as student registration and reporting tools.



Continued success beyond patching

IUP's journey with Tanium didn't stop at patching. IUP's IT team continues to solve real-world challenges that many higher education institutions still struggle to address today.

1. Recovering a lost laptop

When IUP launched a program to loan laptops to students during the pandemic, it introduced logistical challenges, particularly with tracking devices once they left campus. One laptop, assigned to a student who graduated and left the university, was considered lost. However, Tanium's real-time visibility came to the rescue.

When the missing machine was unexpectedly connected to the IUP network, the Tanium system provided the IP address and the last logged-in user – the data needed by the IT team to pinpoint the machine's location on campus. With this information, the team contacted the user, recovered the laptop, and returned it to the university's inventory.

2. Reducing lab devices

Managing IT infrastructure for an academic institution often involves maintaining computer labs equipped with dozens – or even hundreds – of devices. Identifying these underused devices in the past required manual checks and assumptions.

Tanium's asset inventory and usage tracking capabilities transformed this process for IUP. By analyzing device usage data, the IT team discovered many lab machines were rarely used, allowed them to remove unnecessary devices, streamline hardware inventory, and cut costs, all while ensuring that students have access to fully functional and up-to-date technology.

3. Proactive issue resolution

When IUP's security officer flagged concerns about open SQL ports on several servers, it posed a serious security risk. Using Tanium, the IT team quickly identified all servers with open SQL ports, verified the configurations, and determined which versions of SQL were running on those machines. This comprehensive visibility allows them to take immediate action, closing unnecessary ports and ensuring all systems are updated to the latest, secure versions of SQL.

"In less than two minutes, we resolved a security concern that previously could have taken hours or even days," says Dadson. "Tanium's ability to consolidate information across devices and provide actionable insights is unmatched. It's like having a superpower for proactive threat management."

4. Supporting faculty in remote locations

A unique example of Tanium's remote support capabilities occurred when a faculty member traveled overseas on academic business. While abroad, the professor needed to connect a printer to their laptop but lacked the administrative privileges to install the necessary drivers.

The IT team leveraged Tanium to deploy the required software directly to the professor's laptop, resolving the issue in real time. Instead of compromising security by sharing admin credentials, Tanium provided a secure and efficient solution.

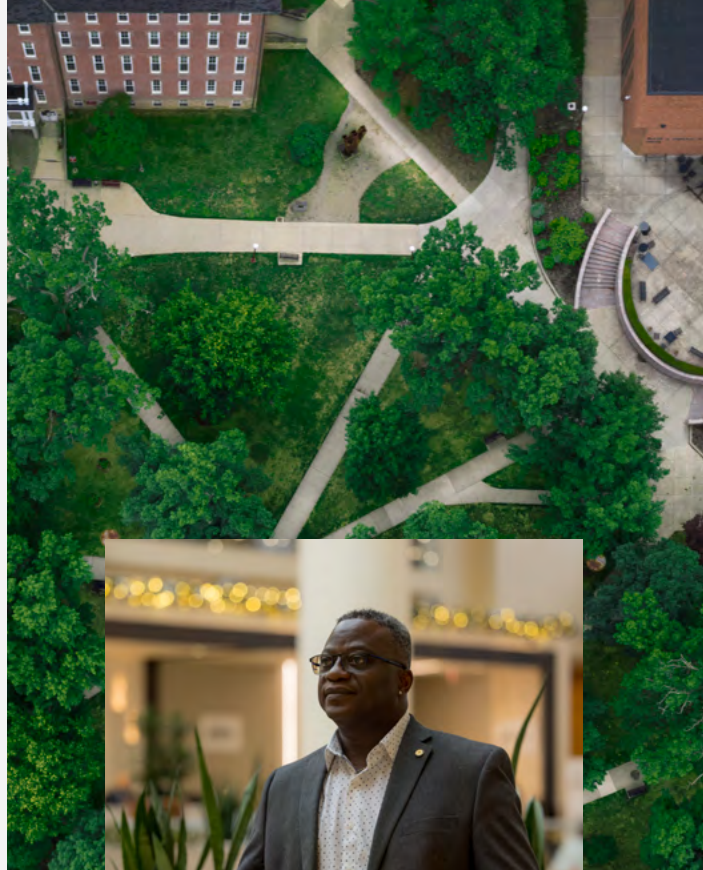
Empowering a new legacy of modernization

IUP's leadership has been impressed with Tanium's capabilities and its impact on university operations. Tanium's comprehensive approach has improved collaboration between IT and security teams that now operate on a unified platform with a shared source of truth, enabling faster decision-making and more effective incident response.

"Our CIO is thrilled with the services Tanium provides," says Dadson. "He even used it himself to review asset numbers and assess how many machines were in use, which helped streamline our inventory and guide decisions."

When asked to summarize the impact of Tanium, Dadson doesn't hesitate, "It's the best I've seen in my 30 years in IT. Tanium gives you visibility, control, and peace of mind. It's not just a tool – it's a platform that transforms how you manage and secure your environment."

As a graduate of the university with over three decades of service at IUP, Dadson is a steadfast technology leader and advocate for innovation at his alma mater. His commitment to enhancing the university's IT operations mirrors the institution's broader dedication to excellence. By partnering with Tanium, IUP has achieved a powerful blend of visionary leadership, cutting-edge technology and a shared commitment to protecting the university's future.



"It's the best I've seen in my 30 years in IT. Tanium gives you visibility, control, and peace of mind. It's not just a tool – it's a platform that transforms how you manage and secure your environment."

Ben Dadson

IT Coordinator, Enterprise Infrastructure and Systems at IUP



The Power of Certainty.™

Visit us at www.tanium.com and follow us on [LinkedIn](#) and [X](#).

© Tanium 2025