How higher education can address its biggest IT and cybersecurity challenges with better client management

Practical advice on how higher education IT teams can defend against new threats, resolve network management problems and meet budget pressures.

How higher education can address its biggest IT and cybersecurity challenges with better client management

Practical advice on how higher education IT teams can defend against new threats, resolve network management problems and meet budget pressures.

Contents

Help for higher education IT: How to overcome three big challenges

In higher education, IT groups have a single mission — they must provide a safe, secure and stable environment for students, faculty and staff. But since the COVID-19 pandemic, that mission has become increasingly difficult to perform.

Institutions have sent their students and staff home, they have created online learning models from scratch, and they have become more and more reliant on new and potentially vulnerable technologies.

These changes have created three primary challenges that higher education institutions are struggling with — new cybersecurity threats, fragmented and changing networks, and increased IT budget pressures.

We wrote this eBook to help higher education institutions overcome these challenges. To do so, we'll explore:

- Each of the three challenges in depth, including why institutions now struggle with them and how institutions can overcome them.
- The common root causes beneath all three challenges, and the four steps that higher education IT groups can follow to resolve them.
- How Tanium can help higher education IT groups overcome these challenges, including the results that one university gained from deploying our platform.

Cybersecurity

The two main cybersecurity threats institutions now face

Higher education's threat landscape has changed, and institutions must adapt their defenses to address it. From the beginning of the COVID-19 pandemic, the education sector has been a major target for cybersecurity attacks. At times, attacks against education grew faster than attacks against any other sector (30% vs. 6.5%), while 62.8% of malware encounters in October 2020 were reported within the education sector alone.[1]

During this time, higher education institutions have been targeted with two primary threats.

- **Advanced ransomware.** Institutions have experienced an increase in attacks from profit-driven Advanced Persistent Threat (APT) groups, and many of these attacks have been ransomware campaigns. The higher education sector experienced 100% more ransomware attacks in 2020 compared with 2019, and the average ransom demand reached $447,000.[2]
- **Nation-state sponsored attacks.** Institutions have also experienced an increase in attacks from nation-state sponsored threat groups that seek research data. Historically, these cyber-espionage attacks often sought information about military research conducted at universities[3], but over the past year, threat groups have also sought COVID-19 vaccine research data.[4]

Both threats use complex, multistage attack patterns, and take advantage of the increased endpoint (desktop, laptop, and other devices) vulnerabilities that higher education institutions opened in their overnight move to remote operations.

A typical attack pattern for both threats will follow these steps.

1. The attacker scans the organization's network for vulnerabilities.
2. They launch standard attacks like phishing or exploit any known vulnerabilities they find such as unpatched or out-of-compliance assets.
3. They penetrate the institution's network and move laterally through vulnerable systems.
4. They develop a foothold in the environment, gather intelligence on critical systems, and exfiltrate as much sensitive data as they can.
5. If the attack includes ransomware, they will eventually lock up systems and demand a ransom.

To defend against these threats, institutions must develop an approach to cybersecurity that is just as complex and multistage as the attack patterns themselves, and which emphasizes rapidly closing known vulnerabilities.

How to defend against ransomware and nation-state sponsored attacks

To defend against these threats, higher education institutions must be able to:

1. Develop an accurate picture of the assets in the network, the known vulnerabilities on those assets, and the measurable risk each carries.
2. Remove the known vulnerabilities on the assets by constantly patching, updating and properly configuring them.
3. Ensure assets are in compliance by enforcing compliance rules on an ongoing basis – and ideally in an automated way.
4. Proactively hunt for indicators of compromise to in-progress attacks before they develop too far.
5. Investigate discovered attacks to identify their root cause, their lateral spread, and assets and pieces of data the attacker touched.
6. Remediate attacks, evict attackers, and regain control of systems without significant data loss.

To perform these steps and defend against these attacks, institutions must focus on developing a few core capabilities.

- **Endpoint visibility.** Institutions must be able to collect real-time data on the status and behavior of their endpoints, the applications on those endpoints, and the users deploying those endpoints. They must be able to detect malicious actors before they exfiltrate data or lock systems and maintain visibility throughout an attack to drive investigation and remediation.
- **Endpoint control.** Institutions must be able to perform fundamental security controls such as patching, updating and enforcing compliance on endpoints. With these capabilities, institutions can continuously raise the barrier to entry for malicious actors. IT can confidently block or evict attackers with improved rapid response to zero-day threats and in-progress security incidents.

Institutions must be able to apply this visibility and control in near real-time across their diverse, distributed and dynamic endpoints. To do so, they often need to reconsider their legacy endpoint management and security tools. Most legacy tools were developed to apply visibility and control to on-premises endpoints, and often fail to manage and defend assets accessing today's remote networks.

If an institution is unable to maintain visibility, control, and effective defenses with these new challenges, it should consider replacing its legacy tools with cutting edge endpoint management and security solutions designed specifically for modern networks.

CHALLENGE TWO

Fragmented, changing networks

The three reasons higher education networks are uniquely difficult to manage

Higher education institutions deploy unique networks that make them particularly difficult to manage. Their networks are:

- **Open.** As one academic security researcher noted, institutions often structure open networks that students, faculties, donors and members of the public can "connect pretty easily to"[5]. This makes them highly dynamic with assets coming on and off network, and more challenging to secure against intrusions. Another researcher notes that institutions have been a well-known and well-explored target simply because they "were one of the first places that had internet access" and thus they have been accessible to cybercriminals for longer than most other verticals.
- **Fragmented.** Many institutions operate multiple individual schools under their umbrella, each with some degree of independent IT infrastructure. Many institutions also have their own research centers, each running multiple projects, and often in close connection with different public or private organizations. And each of those schools and research centers has its own students, teachers, researchers and admins, each of whom might connect their own assets to the network and may or may not be known to the institution's central IT.
- **Transforming.** By January 2020, 83% of institutions were already moving through some stage of digital transformation: 13% were actively transforming, 32% were developing a transformation strategy, and 38% were beginning to explore what their upcoming transformation might look like. During these transformations, institutions must simultaneously operate a full spectrum of modern and legacy infrastructure components , each conceivably requiring its own management tools.[6]

Since the COVID-19 pandemic, the move to learn-from-home models increased each of these challenges. Institutions accelerated their digital transformations, further fragmenting their technology infrastructure, and creating even more access to their networks. By July 2020, most institutions had already moved 500 – 2,000 courses online each and adopted a wealth of new cloud assets.[7]

The result: Higher education institutions now operate networks that are increasingly porous and distributed, that are filled with Shadow IT assets, and that host a wide range of hardware, software and operating systems — and their IT departments must find a way to effectively manage them all.

How higher education IT can effectively and efficiently manage its networks

To effectively manage their networks, higher education IT groups must be able to:

1. Identify assets that connect to the network and maintain some degree of visibility and control over them, even if they repeatedly move on and off network.
2. Maintain pristine IT hygiene over all manageable assets in the network to raise the barrier of entry and lower the chances of a breach within an "open" network.
3. Search for a wide range of different assets in the environment — beyond the known catalog of IT-provisioned assets — to find Shadow IT endpoints and applications.
4. Establish visibility and control over a broad continuum of both legacy and modern endpoints and applications that might be operating side by side.
5. Define and enforce compliance rules to ensure passwords are changed frequently, and to better prepare for audits.
6. Extend endpoint management and security capabilities to remote devices, home networks and cloud-based assets.

To perform these actions, institutions must focus on following a couple of core principles.

- **Think beyond the perimeter.** Institutions operate a porous perimeter under normal circumstances. For the past year — and for the foreseeable future — that perimeter is effectively gone. In response, institutions must move their core endpoint management and security actions to the endpoints themselves through edge computing.
- **Centralize and consolidate capabilities.** Institutions must overlay visibility and control over the wide range of assets within their networks without obstructing the autonomy of their individual schools, research centers, students, faculty and administrative staff. All of this must be accomplished without increasing the complexity, effort and costs demanded of internal IT groups.

To do so, institutions must rethink their legacy endpoint management and security tools. Most legacy tools were developed to manage and secure endpoints that live on-premises, that continuously connect to a central network and sit inside of a hardened perimeter. In addition, they are typically isolated point solutions that require an additional tool to manage and secure different categories of assets — leading to increased costs, complexity and effort, while often failing to apply unified visibility and control over fragmented, diverse networks.

If institutions struggle to maintain visibility, control and effective management within their networks, they should consider replacing their legacy tools with modern endpoint solutions.

CHALLENGE THREE

IT budget pressures

Why higher education IT groups face significant budget pressures

Higher education institutions have faced budget issues for years, and these pressures have only increased in the months since the beginning of the pandemic. While their flat-fee model has kept their revenue steady or in decline alongside student volume, institutions' costs have increased dramatically. The COVID-19 pandemic has only accelerated these trends and placed additional financial pressures on institutions.

- **Enrollment is further down.** Overall, higher education enrollment is down 2.9% year-over-year. New student enrollment appears hardest hit, with undergraduate enrollment down 4.5% and freshman enrollment down 13%.[8]
- **Recovery costs could be 4–5x higher than expected.** In 2020, U.S. institutions requested $46.6 billion to cover their costs from lost revenue and reopening their campuses.[9] Those estimates have now reached $183 billion.[10]
- **Budgets are being slashed.** Over the past year U.S. institutions have closed entire majors, released tenured faculty, and eliminated 300,000+ nonfaculty jobs, leading to a situation where "nothing is off limits" to meet budget reductions.[11]

All of these financial challenges trickle down to budget pressures within the IT department, where security and operations teams must find a way to more efficiently manage their challenging infrastructure and secure it against the new wave of attacks.

Unfortunately, higher education IT groups often operate inefficiently for a few common reasons. They often:

1. Use a significant number of manual processes.
2. Perform a high level of support for end-user performance issues.
3. Operate multiple-point tools, each with its own licenses and teams.
4. Maintain on-premises infrastructure to drive their management and security tools.
5. Pay for end-user applications that are not being used enough to justify their expense.
6. Are woefully understaffed to meet rising workload demands of the new technology and cybersecurity landscape.

To meet their budget pressures, higher education IT groups must find a way to overcome these challenges, eliminate these efficiencies, and reduce their costs without sacrificing their performance.

How institutions can reduce costs and increase efficiency without sacrificing performance

To reduce their costs without harming performance, higher education IT groups must be able to:

1. Streamline and automate as many of their processes as possible, in particular routine, time-consuming tasks like patching, updating and enforcing compliance rules on assets.
2. Continuously monitor end-user performance data to identify issues and proactively resolve them across the network before they turn into reactive support tickets.
3. Reduce the number of tools under IT management by replacing point tools with multi-purpose platform solutions.
4. Replace legacy tools that require on-premises infrastructure with modern, distributed tools that leverage distributed, cloud-based, serverless architecture.
5. Catalog all end-user applications in the network, monitor the usage levels of each application license, and reclaim licenses that are not being used often (or at all).

To perform these actions, institutions must focus on a few core actions.

- **Improve endpoint visibility.** Many of these inefficiencies occur because higher education IT groups do not have a clear picture of what's happening in their environment and what those inefficiencies cost. They often lack visibility into their hardware, software, usage levels and performance issues — and gathering meaningful data on any of these points often requires its own time-consuming and expensive exercise.
- **Modernize and consolidate tools.** In addition, institutions often have far more tools and end-user applications in their environment than they need. Each of these tools and applications has its own license fee, has its own compliance rules, requires its own infrastructure, and demands a high degree of manpower to operate or support.

Most of these challenges have the same root cause — many higher education IT groups continue to use legacy tools to manage and secure their endpoints. These legacy tools were developed to provide visibility and control over a small, static, and simple collection of on-premises endpoints. They typically fail to deliver efficient or effective outcomes within today's large, dynamic, diverse, and distributed endpoints.

If an IT group cannot operate an efficient network and meet its budget pressures, it should consider replacing its legacy tools with modern endpoint management and security solutions that were designed specifically for modern networks and endpoints.

How IT can overcome all three challenges in four steps

At first, these three challenges look quite different. But once you review them one after another in detail, you quickly see that they all emerge from the same root causes. Higher education institutions:

- **Lack meaningful visibility into their networks.** They can't see the asset in their networks or their known assets' critical security and performance details.
- **Lack meaningful control over their networks.** They can't take simple steps to prevent threats, respond to incidents and maintain efficient performance.
- **Lack modern tools.** They still use legacy tools built to work on-premises and now fail to manage and secure today's distributed networks.

To remediate these root-cause problems — and to help solve their security, network management and budget challenges — higher education IT groups must follow a simple four-step process.

- Step one: Assess their gaps
- Step two: Develop comprehensive endpoint visibility
- Step three: Establish real-time endpoint control
- Step four: Reevaluate their existing endpoint tools

Let's look at each step in greater depth.

Step one: Assess their gaps

IT groups must ask themselves a few questions to determine where they experience gaps in their core endpoint management and security capabilities.

- Do we have an accurate, comprehensive, and real-time inventory of the assets in our environment?
- Can we perform continuous monitoring and/or spot scans for new assets, specific indicators of compromise, performance inefficiencies or compliance requirements?
- How long does it take to perform critical controls — like applying patches, updates, or new configurations — to all relevant assets?
- How long does it take to detect and respond to security and performance issues, or to bring new assets in the environment under control?
- How many endpoint management and security tools do we currently use?
- How many of those tools have maintained functionality over the past year's move to distributed operating models?

Step two: Develop comprehensive endpoint visibility

To resolve the three biggest challenges outlined in this eBook, higher education IT groups must develop enough endpoint visibility to:

- Create a comprehensive, real-time inventory of their endpoints that includes their software, their vulnerabilities and their user behavior.
- Identify assets that connect to the network and maintain some degree of visibility over them, even if they repeatedly move on and off network.
- Search for a wide range of different assets in the environment — beyond the known catalog of IT-provisioned assets — to find Shadow IT endpoints and applications.
- Validate the application of patches, updates, configurations, and other controls across the endpoints in their environment.
- Continuously monitor end-user performance data to identify issues and proactively resolve them across the network before they turn into reactive support tickets.
- Create and automatically enforce compliance rules across their IT estate – to reduce the manual steps associated with continuous compliance and the mad rush to prepare for audits
- Perform either continuous scans or real-time spot searches for specific indicators of compromise across their endpoints.
- Define the source of any discovered attack, map its attack chain, and identify the assets and data the attack compromised.
- Catalog the end-user applications in the network, monitor the usage levels of each application license, and reclaim licenses that are not being used often or at all.

Step three: Establish real-time endpoint control

Higher education IT groups must also develop enough endpoint control to:

- Patch, update, configure, or otherwise apply controls to hundreds of thousands of endpoints in hours or days, not weeks or months.
- Streamline and automate as many of their processes as possible, in particular routine, time-consuming tasks like patching, updating and enforcing compliance on assets.
- Maintain pristine IT hygiene over all manageable assets in the network to raise the barrier of entry and lower the chances of a breach within an "open" network.
- Harden assets in real-time against any discovered attack pattern to stop its spread, to evict the attacker, and to prevent additional incidents.

Step four: Reevaluate their existing endpoint tools

Finally, higher education IT groups must review their existing endpoint tools to determine if their existing stack can extend endpoint management capabilities to remote devices, home networks, and cloud-based assets.

During this evaluation, they must consider replacing legacy tools that require on-premises infrastructure with modern tools that leverage distributed serverless architecture and edge computing.

In addition, they must search for ways to reduce the number of tools in their stack by replacing point tools that perform a limited number of capabilities with modern, comprehensive platforms that consolidate capabilities.

Modern, comprehensive platforms like Tanium.

Meet Tanium: How our platform helps solve your biggest challenges

How Tanium quickly and easily brings these solutions to life

Tanium is a modern, unified endpoint management and security platform.

With Tanium, higher education institutions can improve their fundamental cybersecurity posture against modern threats, bring their fragmented networks under central management, and increase their IT group's efficiency and cost-effectiveness.

Tanium can drive each of the core capabilities outlined in this eBook and resolve the root-cause problems underlying the three big challenges that institutions struggle with.

- **Comprehensive endpoint visibility with Tanium.** When organizations first launch Tanium in their environment, they typically find 10–20% more assets than they knew they had. Tanium then builds a comprehensive, real-time catalog of the hardware and software assets in the environment, and provides critical security and performance metrics for each of those assets.
- **Real-time endpoint control with Tanium.** Tanium can patch, update, configure, or otherwise apply controls to hundreds of thousands of endpoints in hours or days.
- **IT modernization with Tanium.** Tanium consolidates most endpoint management and security capabilities into a single platform with a single instance, agent and pane of glass. Tanium leverages distributed edge computing that does most work on the endpoints automatically. This helps create scalable visibility and control across modern networks with minimal strain.

Tanium has helped many organizations in multiple industries — including higher education — solve their biggest IT and cybersecurity challenges.

Here's just one example.

How one university used Tanium to solve its IT and cybersecurity challenges

Recently, a prominent university in the U.K. used Tanium to:

- Discover hundreds of unknown assets in its network, and hundreds of thousands of open vulnerabilities.
- Reduce its missing critical patches from 38,000 to fewer than 300, and reduce its missing updates from hundreds of thousands to fewer than 1,000.
- Remediate multiple zero-day threats across its asset networks within minutes of discovering them.
- Bring a fragmented network consisting of endpoints from

four different schools and multiple research groups under centralized visibility and control.

- Replace 4–5 endpoint tools with a single unified platform.
- Save tens of thousands of dollars annually from license fees alone.
- Substantially reduce the manpower required to perform critical tasks like patching, further reducing its overhead to manage and secure its assets.

The university's CIO sums up his experience with Tanium in a single simple statement:

"If we hadn't invested in Tanium, we would still lack full visibility into our assets, we would still have hundreds of thousands of missing critical patches, and it would only be a matter of time before we were targeted by threat actors and potentially put in a really difficult position."

NEXT STEPS

Solve today's challenges while still preparing for tomorrow's

In this eBook we've provided practical advice on how to solve the biggest challenges you face today. If you follow the advice we outlined above, then you will dramatically improve your security, your network management and your efficiency.

In addition, you will be far more prepared for whatever challenges tomorrow brings. While we cannot say for certain what those challenges will be, we believe they will be solved with a similar approach: a thorough and solid foundation of comprehensive endpoint visibility and real-time endpoint control delivered through a modern, distributed solution.

To learn how Tanium can help you overcome today's challenges and better prepare for tomorrow's, visit **Tanium.com** or **request a demo today.**

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

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

References

1 https://securityboulevard.com/2020/12/why-higher-education-is-a-prime-target-for-cybercriminals/

2 https://www.zdnet.com/article/ransomware-sharp-rise-in-attacks-against-universities-as-learning-goes-online/

3 https://www.onelogin.com/blog/3-reasons-higher-ed-hacked

4 https://www.ajg.com/us/news-and-insights/2020/may/cyberattacks-on-life-science-companies-and-research-universities-for-covid-19-vaccine-data/

5 https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

6 https://er.educause.edu/articles/2020/1/how-colleges-and-universities-are-driving-to-digital-transformation-today

7 https://evolllution.com/managing-institution/operations_efficiency/the-digital-transformation-in-higher-education-and-its-aftereffects/

8 https://www.insidehighered.com/news/2020/11/12/enrollment-declines-continue-national-student-clearinghouse-finds

9 https://www.insidehighered.com/quicktakes/2020/09/29/colleges-financial-toll-coronavirus-worse-anticipated

10 https://www.chronicle.com/article/how-to-fight-covids-financial-crush

11 https://www.chronicle.com/article/how-the-pandemic-has-shrunk-higher-educations-work-force