Harder for hackers.
Simpler for you.

TREND MICRO™

TACKLING THE CHALLENGE OF HIGHER EDUCATION CYBERSECURITY

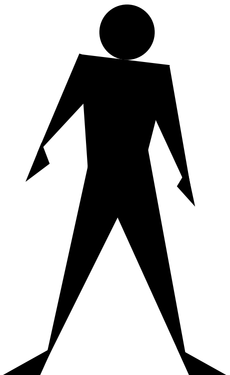
Discover how Trend Vision One™ can enhance security for your institution's complex digital infrastructure.

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information.

Fueled by 35 years of security expertise, global threat research, and continuous innovation, Trend's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 70 countries and the world's most advanced global threat research and intelligence, Trend enables organizations to simplify and secure their connected world. TrendMicro.com

CONTENTS



SECTION 1: INTRODUCTION

Assessing the threat landscape

The higher education sector in the UK has emerged as a prime target for cyber threat actors. This year, 2024, the Cyber Security Breaches Survey conducted by the Department for Science, Innovation and Technology (DSIT) showed that all types of education institutions were more likely to have suffered a cybersecurity breach or attack than the average UK business. Higher education institutions were the most likely to have identified breaches or attacks within the past 12 months, at 97% compared with just 50% of average businesses[1].

In 2024, the Director General of MI5, Ken Mc Callum, addressed leading universities alongside the CEO of the National Cyber Security Centre (NCSC) to discuss the threats facing higher education. He shared that, specifically, UK universities are in the crosshairs of nation state threat actors seeking to gain an economic advantage by hacking highly prized research and intellectual property. Universities hold sensitive, often publicly funded research, making data sovereignty a key concern. Protecting this critical data is not just about safeguarding academic output but also ensuring that the UK's economic and national security interests are preserved.

Universities and colleges handle vast amounts of sensitive research, and personal and financial data, and higher education is an extremely economically valuable sector. The total economic impact of the UK higher education sector on the UK economy is more than £265 billion – and for every £1 of public money invested in higher education, £14 is put back into the economy[2]. It is therefore no surprise that a large-scale economic impact like this would inevitably draw the attention of malicious actors. Cyber-resilience in this sector is vital not only for the continuity of academic work but also for protecting the significant economic value and the national infrastructure connected to the higher education system.

[1] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex

[2] https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2024-09/LE-UUK-Impact-of-university-TL-and-RI-Final-Report.pdf

Harder for hackers.
Simpler for you.

Why do attackers specifically target universities?

According to the NCSC and JISC (Joint Information Systems Committee), the motivations of attackers targeting higher education fall into four categories:

- Seeking to extort payment through ransomware or other methods.
- Theft of valuable research data or knowledge.
- Using digital infrastructure to directly monetise assets, e.g. bitcoin mining.
- Seeking to disrupt and destroy.

Attackers are further attracted by the fact that universities have attempted to remain accessible in support of research and education. Unfortunately, this openness combined with the typical scale of a university's digital estate creates a large and vulnerable attack surface.

Attacks and their implications

According to the National Cyber Security Centre (NCSC), the UK's higher education has been "exponentially" targeted by cyber attackers due to the critical data it manages, this was especially relevant during the period of research into the COVID-19 pandemic.

Oxford University attack

Oxford University houses one of the most advanced biology labs in the world and, while it was studying COVID-19, its system was attacked. This attack was discovered in February 2021, when hackers were found to be selling access to the lab's equipment on the dark web, which could be used for sabotage or data theft.

A breach of this nature could place research data at risk of being stolen, including research into the coronavirus. It also poses the threat of sabotaged research, if hackers were able to compromise the mechanics of the equipment. This attack was referred to the NCSC and ICO for investigation.

Russell Group data breach

In September 2023, 2.2 million breached credentials were discovered as being for sale on the dark web related to the top 100 UK institutions. 57% of these credentials belonged to the Russell Group Universities.

This could pose a major risk to sensitive research if threat actors are able to access user accounts with compromised credentials. 54% of those breached credentials came from UK universities with research facilities, with government-funded programmes in areas like nuclear energy and defence.

The challenge of protecting UK higher education's data is exacerbated by the sector's growing digital footprint. As universities increasingly rely on online learning platforms, cloud-based research databases and remote working solutions, the attack surface will continue to grow.

Higher education institutions must find a cost-effective way to mitigate these specific risks, while ensuring compliance and without hindering digital transformation that is vital to academic progress. For higher education, effective cybersecurity is not just about protecting data, it's about safeguarding academic integrity, ensuring continuity of research and teaching and maintaining the trust of its students and the wider public.

That's why we developed Trend Vision One™: our unified platform for attack surface risk management (ASRM) and extended detection and response (XDR) helps you manage and minimise risk across the attack surface while reducing costs, optimising staff productivity and preserving investment in digital transformation projects. These are designed to manage and mitigate risks across the large, diverse and complex university systems ensuring that cybersecurity measures support, rather than hinder, digital transformation and academic excellence.

The University of Warwick, for example, adopted Trend Micro Cloud App Security, which allowed the Cloud Services team to document exploit detection to help find malware including ransomware in Office formats, reduce the volume of malware arriving in users' inboxes, and provide a single dashboard to enable a clear view of any malicious content being blocked. Des Butcher, Head of Cloud Services at University of Warwick, explained: "We can see a measurable benefit: a reduction in the volume of malware arriving in our users' inboxes. We can look at the dashboard and get a view of potentially thousands of pieces of malicious content getting blocked."

How does Trend Micro meet the needs of higher education?

Discover how Trend's advanced cybersecurity solutions tackle the unique challenges faced by higher education institutions. Learn about the key threats, their impact on your organisation, and how our integrated approach can help you secure your network, protect valuable research, and maintain operational continuity.

- **Enhanced threat intelligence:** Proactive defence and timely threat detection to prevent cyber incidents before they impact operations.
- **Real-time threat monitoring:** Advanced analytics provide deep visibility into network activities, enabling quicker identification and mitigation of potential threats.
- **Flexible, scalable security:** Security that adapts to evolving needs across a vast array of contracts and suppliers, focused on scalability and managing numerous relationships efficiently.
- **Compliance and regulatory support:** Ready to support compliance with regulations such as GDPR, the Cyber Assessment Framework (CAF) and the forthcoming Cyber Security & Resilience Bill 2024.
- **Integration and automation:** Automated threat detection and response streamlines security operations, integrating security tools and vendors to enable a unified strategy for managing supply chain risk.

Section 2: Protecting research and reputation

SECTION 2: PROTECTING RESEARCH AND REPUTATION

Navigating challenges in higher education

As UK universities continue to digitise and expand their research capabilities, they face growing cyber threats that put sensitive data, research and reputations at risk.

Protecting research

UK universities are prime targets for cyber attackers due to the value of the work they produce. Research, especially that which supports government-funded or nationally significant projects, makes them attractive targets for cyber attackers. Safeguarding this research is not only crucial for academic success but also for the protection of critical national assets. Email continues to be the biggest entry point for attackers to infiltrate networks, putting vital research at risk. A single breach can jeopardise the security of valuable projects, causing significant setbacks.

A breach not only results in financial loss but also undermines trust in a university's ability to protect its intellectual property. For leading research institutions, a breach can make it difficult to secure future partnerships or funding. The loss of confidence in a university's ability to protect sensitive national projects can have far-reaching consequences on its role in supporting national infrastructure and innovation.

Preserving reputation

Universities store huge amounts of sensitive data, from personal information to financial details. Attackers are increasingly focusing on locking down IT systems through ransomware, which enable extortion and blackmail. This not only threatens research data but can also disrupt essential university functions such as student enrolment, online learning platforms, exam systems, and administrative operations, creating long-lasting challenges.

The consequences of a breach are serious. This can cause service outages, which lead to high costs and lost revenue, especially during busy periods such as student clearing. Beyond financial damage, these incidents also hurt a university's reputation, making it harder to attract new students and research funding.

Mitigating insider threats

Universities are especially prone to insider threats due to their large and constantly changing staff and student populations. Phishing attacks are common, and ensuring secure access is complicated by various network setups. Many universities still rely on outdated systems for critical research, which leaves them exposed to potential breaches.

Insider risks are heightened by poor security practices, with only 5% of universities mandating security training for students. Plus, research teams managing their own cybersecurity or departments moving to the cloud without oversight can create dangerous blind spots, making it easier for breaches to occur.

Exploring the specific risk factors for higher education

- **Student turnover:** Universities have a large number of younger network users with limited awareness of organisational cyber threats. There is also a large annual turnover, which makes it harder to ensure consistent operational security.

- **Large attack surface:** University networks have grown with increases in student numbers and reliance on technology. A large part of the attack surface consists of web-facing portals. If an attacker can exploit any one of these entry points they can gain access to an internal network putting sensitive data and systems at risk.

- **Cyber professional shortages:** Universities suffer from budgetary constraints, which leads to overburdened cybersecurity teams, alert fatigue and the inability to recruit new security members.

- **Large amounts of high-value data:** Universities gather and store data relating to student and staff Personal Identifiable Information, research, finances, housing, contractors and partners, medical or clinical studies, commercial activities and politically sensitive data. This must all be stored securely, but it is constantly being accessed, making it an attractive target.

- **Open access:** The increased need for remote access to teaching and learning, plus local and international collaboration, increases the attack surface with more open applications, services and infrastructure.

The importance of Zero Trust

Universities need to adopt a Zero Trust approach to secure access to critical resources, including on-premises infrastructure, infrastructure as a service (IaaS), containers, Big Data, and other modern IT services. Privileged access abuse remains one of the leading cause of breaches, as gaining access to higher-privilege accounts enables attackers to cause significant damage across the institution's systems.

Zero Trust enables granular micro-segmentation of IT infrastructure, allowing the enforcement of policies based on asset sensitivity alongside visibility and control over users and applications. This dramatically reduces the size of the threat surface long before any advanced anti-malware solutions come into play. When augmented with continuous automated scanning for known and unknown threats, the risks of network penetration are significantly reduced.

Some of the benefits of delivering Zero Trust include:

- Reduction of the attack surface and the risk of accidental cyber incidents.
- Accurate identification of network traffic.
- Effective detection and mitigation of known and unknown threats trying to piggyback on allowed traffic.
- Protection for known vulnerabilities.
- Reduced risk of successful data exfiltration.

Trend Vision One helps to protect vast and complex networks, simply and reliably:

- Attack Surface Risk Management (ASRM) provides holistic security management that continuously assesses risk, suggests recommendations and automates remediation building your resilience to maintain institutional reputation.
- Extended Detection and Response (XDR) with AI provides the ability to detect, hunt, investigate, analyse and respond to threats so that they can be rapidly contained and help preserve trust with students, faculty and research partners. The University of Warwick, for example implemented Trend Micro Cloud App Security to strengthen their defences. Des Butcher, Head of Cloud Services at the University of Warwick, stated, '*We can see a measurable benefit: a reduction in the volume of malware arriving in our users' inboxes. We can look at the dashboard and get a view of potentially thousands of pieces of malicious content getting blocked.*'
- Generative AI helps to contextualise risk, reduce noise and upskill analysts and cybersecurity teams as they prioritise alerts and tackle fast-moving threats.
- Network detection and response (NDR) analyses contextual telemetry from high-risk, otherwise invisible parts of networks such as unmanaged assets and shadow IT deployments.
- Our Zero Day Initiative (ZDI) generates vulnerability insights and provides protection up to 79 days ahead of the industry average, before a breach occurs. Its granular controls provide critical safeguards against privileged access abuse, reducing the risks of internal and external threat actors compromising sensitive research or academic operations.

SECTION 3: OVERCOMING BUDGETARY CHALLENGES AND SKILLS SHORTAGES

Seeking cost-efficient cybersecurity

Universities are under growing financial pressure, with concerns around sustainability and viability highlighted by the Public Accounts Committee. Rising energy costs, tuition fee caps, and inflation have placed significant strain on university budgets, forcing institutions to prioritise finding cost-effective solutions in all areas, including cybersecurity. Balancing these competing financial pressures while maintaining adequate security is an increasing challenge for many universities, as they are also dealing with the growing threat of cyber attack.

In response to these budget constraints, for some, it is tempting to turn to pre-bundled, generic solutions like Microsoft's, which are perceived as providing security that is 'good enough'. However, these 'good enough' packages tend to come with trade-offs. They often face integration issues with non-Microsoft devices, generate a large number of false positives, and require extensive configuration.

Also, limited support for older Windows environments, which are common in academic institutions, can create further vulnerabilities. As Jon O'Grady, United Communications Manager of De Montfort University pointed out, "We used basic Office 365 protection for years but had been affected by multiple phishing attacks on our students, so we made the decision to enhance our security in this area."

The financial pressure doesn't end there. Universities must then dedicate extra time, training, and resources to manage these cybersecurity solutions, further straining their budgets. The lack of proper integration and limited support for legacy systems exacerbate the risk of security breaches, leading to potentially higher costs in the long run. Instead of streamlining operations, inefficient solutions can actually increase financial burdens, forcing universities to divert resources away from core academic missions to manage cybersecurity risks.

Harder for hackers.
Simpler for you.

Mitigating the skills gap

The skills gap in cybersecurity further complicates compliance efforts. The UK, like most countries around the world, is suffering from a major shortage in skilled cybersecurity professionals.

According to the UK Government's Cyber Security Skills in the UK Labour Market 2023 report, 50% of all UK businesses have a basic cybersecurity skills gap, with little improvement from the previous year. In the public sector, this skills shortage is often more acute due to competition from the private sector for talent.

The report also found that 33% of organisations have an advanced cybersecurity skills gap, and there's an estimated shortfall of 11,200 people to meet the demand of the cyber workforce. This shortage of skilled professionals makes it difficult for higher education institutions to implement and maintain robust cybersecurity measures.

For higher education, these challenges have several implications –

- **Increased vulnerability:** The skills gap can lead to security vulnerabilities if universities lack the expertise to implement and manage complex security systems.
- **Compliance risks:** Without adequate skills and resources, universities may struggle to meet regulatory requirements, potentially leading to non-compliance and associated risks.
- **Inefficient resource allocation:** The complexity of compliance and the skills shortage can lead to inefficient use of limited resources, as universities struggle to balance security needs with other priorities.

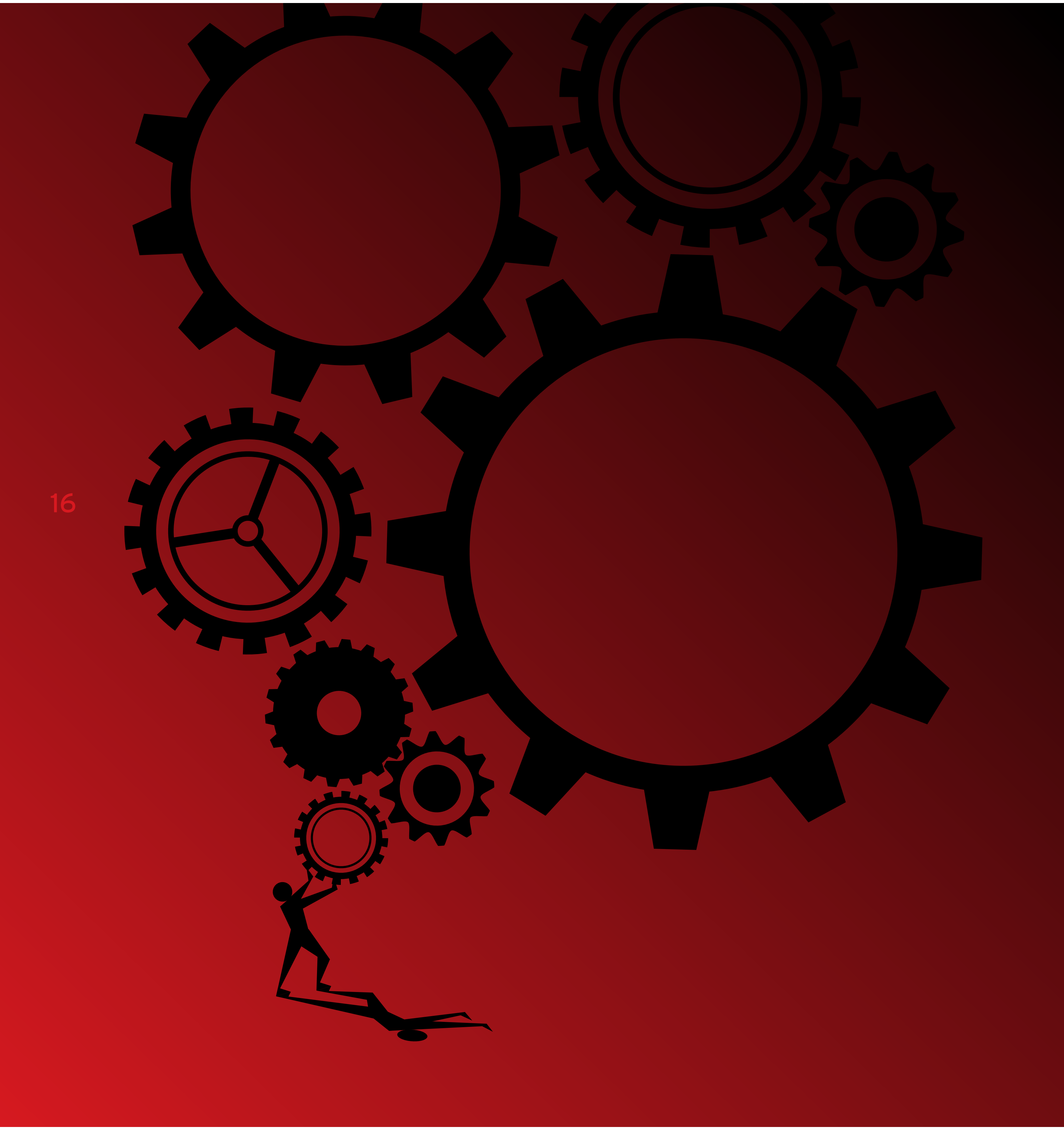
Looking ahead, finding cost-effective security measures and addressing the skills gap will be crucial for improving your overall cybersecurity posture. This may involve leveraging technologies like automation and AI to enhance compliance processes, as well as developing innovative approaches to attract and retain cybersecurity talent.

Unlocking the economic value of Trend Vision One:

- The Enterprise Strategy Group's economic validation of Vision One demonstrated a 70% reduction in cybersecurity cost, combined with a 17% reduction in data breach risk and 20% reduction in employee turnover.
- It further demonstrated a reduction of alerts per day from 1,000 to 4 and reduced the average cost of a data breach by £1.3m while resulting in $2.43m average cost savings from improvement in customer churn.

Trend Vision One provides comprehensive security that relives the pressure on cybersecurity teams:

- Attack Surface Risk Management (ASRM) provides a library of ready-made workflows to improve security teams' productivity and speed when completing critical tasks related to security and compliance. This is especially useful considering the cybersecurity skills shortage.
- Vision One's Generative AI cybersecurity assistant (Vision One Companion) provides enhanced capabilities, accessibility and efficiency. It helps cybersecurity professionals respond to complex scenarios more swiftly, mitigating the skills shortage and improving outcomes, whilst allowing existing teams to be more effective without universities needing to constantly recruit new talent.
- Seamless integration across diverse devices, networks, and legacy systems, reducing management complexity and maximising the value of existing infrastructure.
- Flexible, scalable solutions that provide cost-effective security ensuring compliance and operational efficiency. This approach helps counter the limitations of 'good enough' solutions, offering robust protection without overextending budgets.



SECTION 4: SECURING COMPLEX AND POROUS NETWORKS

Protecting sprawling network endpoints

Universities face significant challenges in managing cyber risks due to the complex, sprawling nature of their IT networks. These networks often comprise smaller, private networks serving specific faculties, labs and departments, which makes consistent security enforcement hard to achieve. According to the NCSC, each of these smaller networks requires unique security considerations, which further complicates the task of protecting the institution as a whole. The open-access nature of universities, necessary to foster academic collaboration, presents an inherent vulnerability, as vast digital estates can be easily exploited by malicious actors.

The growing number of remote students, home workers, and external researchers accessing university networks adds to the complexity. These distributed access points, particularly at the network edge, significantly increase the risk of security breaches. The primary attack vector is often email, which is widely used across all academic functions, and it makes universities vulnerable to phishing and other email-based cyber threats. With large digital estates and porous access points, the ability to monitor and secure all entry points is critical to preventing widespread breaches. Ensuring strong and consistent security across these distributed networks is crucial, but with such a broad and varied user base, it can be a challenge for under-provisioned IT teams.

Defending against third-party and supply chain risks

Third-party vendor relationships also add a significant complication to the effort of preventing data breaches. When a third-party relationship is established, the university's attack surface combines with that of the new third-party vendor. This makes the vendor's security risks the university's concern. Third-party vendors often process sensitive information, so if their security risks lead to a data breach, any internal data they have access to is also compromised.

For example, a university outsourcing document processing to a third-party legal entity also suffers a data breach when that vendor is compromised, and any shared student information is accessed. Many universities are unknowingly increasing their risk of suffering third-party breaches through the poor cybersecurity standards of their vendors.

Although supply chain attacks account for a very small proportion of overall global attacks, they are often the most destructive. For example, weaponised 'updates' delivered to endpoints via a compromised accounting software update service, could infect devices in universities across the UK. Compromising a legitimate software update and using it as a delivery mechanism is a clever way of exploiting a chain of trust that leads back to the primary target, and it indicates careful operational planning and positioning by an advanced attacker.

It may not surprise those familiar with the history of supply chain security to learn that higher education institutions usually consider information risk only for a limited number of suppliers, often based on contract size.

This approach presents three problems:

1. **Other contractors that pose risks, such as legal firms, are often overlooked.**
2. **It is not scalable for universities that have too many contracts to consider them individually.**
3. **Suppliers often share information with their own suppliers, who in turn share it with theirs and so on, increasing risk as visibility and control decrease.**

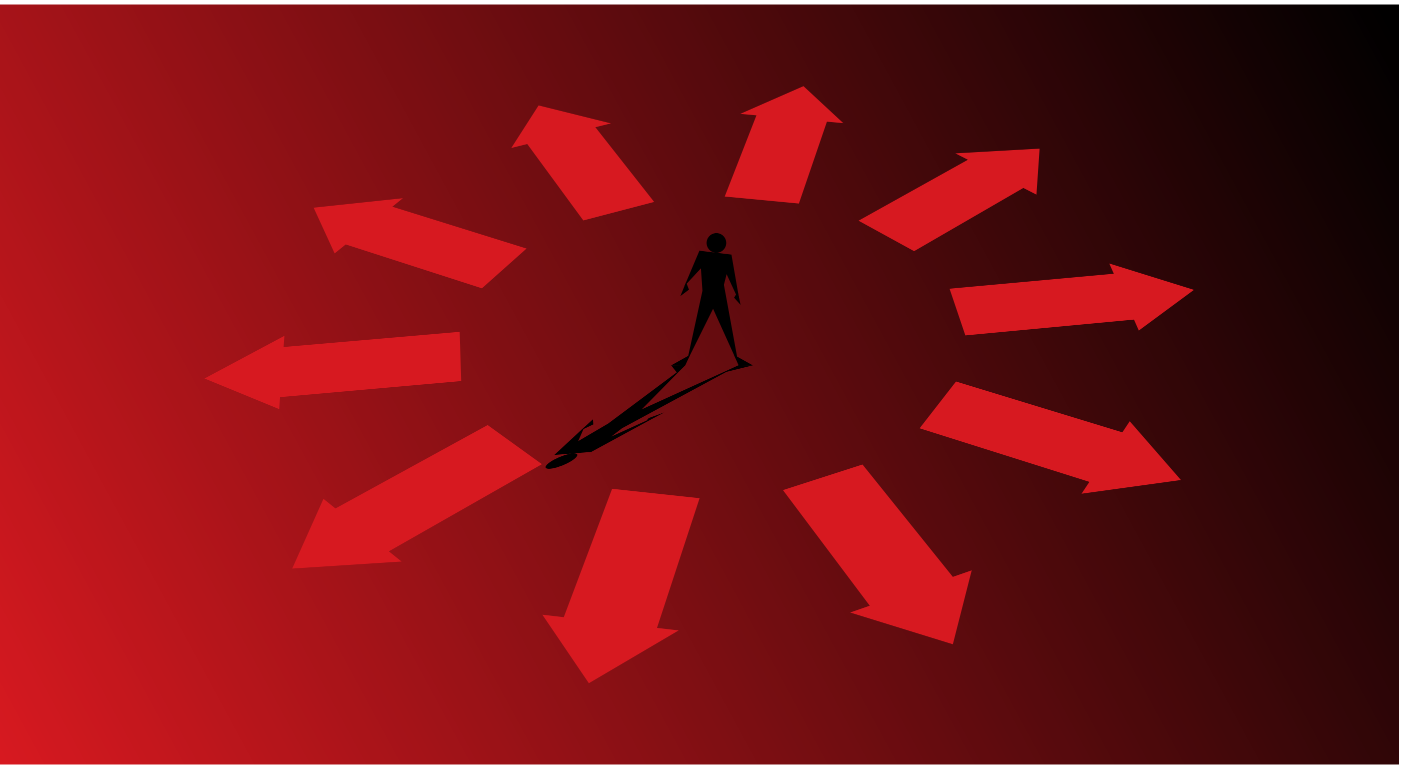
Universities need solutions that scale with their ever-expanding digital ecosystems and supplier networks. The sector must work harder to get safety assurances in the event that risks to the confidentiality, integrity and availability of overarching systems are identified. Security challenges like these must be resolved for universities to safely operate – both individually and co-operatively with other institutions – in networked, multi-vendor, and cloud-based environments.

Trend Vision One can help universities manage risk across their attack surface:

- Attack Surface Risk Management (ASRM) and Network Detection and Response (NDR) are designed to handle the complexities of sprawling university environments. ASRM identifies and monitors the university's risk exposure across multiple attack surfaces, while NDR provides comprehensive threat detection across the entire digital ecosystem.
- Designed for flexibility and scalability, adapting to the varied needs of university environments – from remote learning platforms to extensive research networks.
- Supporting zero-trust initiatives to minimise supply chain and identity-based risk such as credential phishing.
- Understanding user behaviour and enforcing authentication policies to reduce third-party risk.
- Correlating security events across identities, email, endpoints, files, commands, processes and other assets to stop identity and supply chain attacks in their tracks.

Trend Micro Zero Trust Secure Access (ZTSA) follows the principles of zero-trust networking. It can strengthen the overall security posture by enforcing strong access control permissions from multiple identity services across the organisation.

Rather than granting access to the entire network, as a VPN does, ZTSA provides a gateway to specific applications and resources, restricting access to everything within the network that is not being employed. If valid user credentials are stolen, the level of access they will grant to the organisation can be contained, effectively reducing the blast area of any attack.



SECTION 5: SECURING THE FUTURE OF HIGHER EDUCATION

Challenges facing higher education

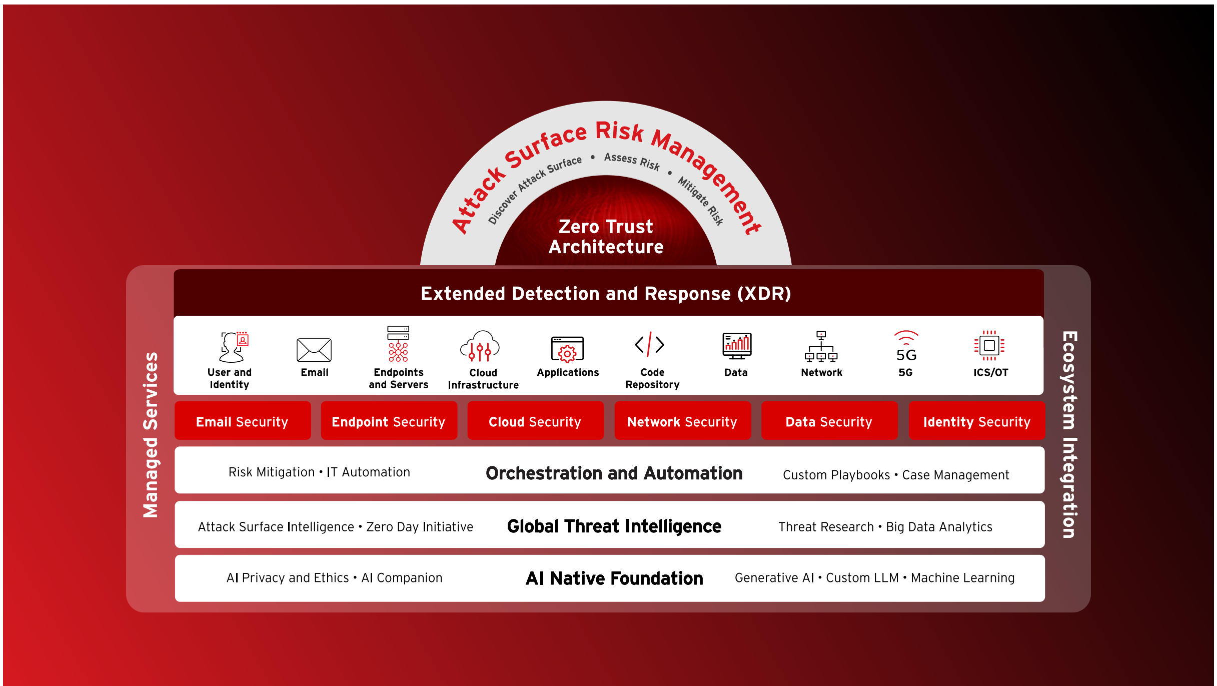
- A constantly evolving threat landscape, with government organisations being routinely and relentlessly targeted by a range of malicious actors.
- The complexities of cloud migration and management, balancing the benefits of cloud adoption with the need for robust security measures.
- The ongoing cybersecurity skills gap, with 50% of UK businesses facing a basic cybersecurity skills shortage[3].
- Budgetary constraints that require difficult decisions about resource allocation for cybersecurity initiatives.

Invest in the most complete attack surface coverage

Trend Vision One provides comprehensive visibility and proactive risk management, reducing the need for multiple tools. This consolidation not only cuts costs but also streamlines workflows, allowing for faster threat detection and response.

This platform's virtual patching capability ensures protection of critical assets from both known and unknown threats, supporting business continuity and safeguarding data from students and staff. It can help you transform cybersecurity from a cost centre into a strategic enabler, ensuring robust protection while enhancing operational efficiency.

[3] https://www.infosecurity-magazine.com/news/cybersecurity-skills-gap-stagnant/


Attack Surface Risk Management
Discover Attack Surface • Assess Risk • Mitigate Risk
Zero Trust Architecture
Extended Detection and Response (XDR)
User and Identity
Email
Endpoints and Servers
Cloud Infrastructure
Applications
Code Repository
Data
Network
5G
ICS/OT
Email Security
Endpoint Security
Cloud Security
Network Security
Data Security
Identity Security
Risk Mitigation • IT Automation
Orchestration and Automation
Custom Playbooks • Case Management
Attack Surface Intelligence • Zero Day Initiative
Global Threat Intelligence
Threat Research • Big Data Analytics
AI Privacy and Ethics • AI Companion
AI Native Foundation
Generative AI • Custom LLM • Machine Learning
Managed Services
Ecosystem Integration

Harder for hackers.
Simpler for you.

Evolving threats require an evolving cybersecurity solution

Strong cybersecurity isn't just about protecting networks—it's about supporting the long-term success of universities' missions. No matter where a university is on its journey toward smarter learning, the landscape is changing. IT networks can no longer be separate, siloed entities. This shift requires a much more holistic view of security than most other sectors. It is vital that those responsible for security and operational uptime across IT and network-enabled applications are working together.

Integrating people, processes and technology for comprehensive security

This is easier in theory than in practice, but it must become a key point of focus to ensure that risks to the university are fully understood and that the people, processes and technologies needed to mitigate and manage those risks are effective.

Cybersecurity must be viewed as a key enabler, not an obstacle, to digital transformation. The right technology can be used to dramatically streamline and optimise the use of people and process, while also securing your network. The best examples of this kind of technology are heavily automated, able to dynamically adapt to the threat landscape without human interaction while delivering always-on protection.

Leveraging automation to reduce analyst workload

Analysts can no longer be expected to sift through logs and attempt to follow up on every alert in an intrusion detection system. Automated protection that a university can trust is vitally important, but removing the workload associated with 'everyday' threats from the security team is only part of the puzzle.

Universities are facing a wide range of threat vectors and so their technology must work harmoniously with staff and students to augment their capabilities, allowing faster determination and investigation of security incidents.

In cases where technology alone cannot reach a decision of whether certain activity is malicious or benign, it must then be able to deliver actionable intelligence to analysts. It should give them the context of what has happened, who or what was involved, and any indicators of compromise that could be useful.

Future-proofing your university's cybersecurity infrastructure

Security must be unified across the entire environment. For higher education, this calls for an integrated ecosystem, covering the campus to the virtual classroom and the student. Keeping an eye on the long-term potential of any new security solution is good practice to ensure that the security in one part of your infrastructure will not have to be built from the ground up when new opportunities or needs arise elsewhere.

In short, when securing your university, making the right technology choices now can avoid putting your students, staff and research projects at risk, and it can cost far less than a future rip-and-replace effort that might be required to overcome developing threats. Investing in cybersecurity today is an investment in the future of higher education.

Why Trend as Partner for higher education

“Trend Micro is a good fit for customers who want a consistently strong endpoint protection platform that can support evolving to XDR”[4]

- Trend Micro a Leader The Forrester Wave™

FORRESTER®

“Ranked #1 in IDC’s Worldwide Hybrid Cloud Workload Security Market Shares report”[5]

- IDC Worldwide Security Market Shares

IDC

“Trend Micro ranked #1 in the production category for ensuring early attack prevention”[6]

- MITRE Engenuity Att&CK Evaluations: Quick Guide

MITRE

“Trend has been named and recognized by Gartner in both Endpoint (EPP/EDR) and Network (NDR) security”[7]

- Gartner: Trend Micro a Leader in the Endpoint Protection Platform Magic Quadrant

Gartner

[4] https://www.trendmicro.com/explore/forrester-wave-asm

[5] https://statics.teams.cdn.office.net/evergreen-assets/safelinks/1/atp-safelinks.html

[6] https://www.trendmicro.com/explore/industry-recognition-eu/01436-v1-en-rpt?xs=391652

[7] https://resources.trendmicro.com/Gartner-MQ-EPP-2024.html

Harder for hackers.
Simpler for you.

TREND MICRO™

WANT TO LEARN MORE?

Book a 15-minute discovery call with one of our higher education cybersecurity advisors

Speak with us >

Start your complimentary 30-day trial

Activate here >