SECURING THE NEW CAMPUS PERIMETER

SUPERCHARGING USER IDENTITY SECURITY

Lenovo

About This Whitepaper

This paper looks at the importance of identity management to today's higher education leaders, exploring current challenges and how layered authentication and security can drive better cybersecurity and ultimately enable trust.

When it comes to information security at today's colleges and universities, no news is good news. That means another week without student records or financial data being exposed. For private sector organizations, the risk is often profit, and the costs keep rising.

Whether its institutional data being held for ransom or accidental misdelivery, the damage to institutions of higher education is far greater. Trust is absolutely critical to the success of any college or university, and student and community expectations around data security and privacy are continuing to grow.

An inability to protect the institution's applications, information, and investments ensures these expectations can't be met. This failure can be corrosive to both the mission and the business model, stalling or stopping hard fought transformation efforts.

intel® vPro® Platform

Powered by the Intel® vPro® Platform

To learn more about ThinkShield, visit http://solutions.lenovo.com/thinkshield.

Risk impacts trust, and its impacts can multiply exponentially.

- Legislators and communities are less willing to invest in technology innovation – even when technology isn't the root cause of a particular incident
- Funding for special priorities and programs could be put at risk
- Institutional decision-makers are reticent to move forward with new ideas
- Students and faculty are less willing to embrace emerging data-dependent opportunities including AI and deep analytics
- The cost of modernization and managing risk in particular, will rise

It all adds up to costs that far exceed Ponemon's estimate of $76 per single record breached in the public sector.[1] To the point where dollar numbers, as high as they climb, become practically irrelevant. The cut is much deeper than money.

So how do you stay out of the news? Or, more realistically, how do you empower modern borderless campuses that extend reach without sacrificing trust? And, when failures do occur, how do institutions and the communities they serve turn the page?

Zero trust has become the new gold standard in security. Never assume, always validate, never trust. While it's easy to do with machines, what about student and faculty users?

Information security: an old game with new rules

Prior to digitalization, information security was an issue of governance, risk, and compliance. It mostly revolved around physical facility security and careful control of who had access to a particular file. By controlling sites and carefully managing users, institutions mostly stayed ahead of bad actors. It was a game of traditional espionage.

The LAN (and eventual internet gateways) changed everything. Connectivity became risk, and potential threats multiplied. Researchers began to build code that could explore networks, scan for information, and more importantly, self-replicate.

These early efforts were mostly harmless (the famous Morris Worm excepted), but the technologies were soon used by nation states and their agents to access and steal information and, in some cases, damage host networks.

A New Age: Spies and Arsonists

As digitalization becomes more complex and complete, the cost of risk continues to race ahead. That brings us to today. Colleges and university networks are now directly connected into more than themselves, now inextricably linked with other institutions and organizations. They also operate under a variety of compliance frameworks, governing the security of data in its many forms. Medical records, student information, payment systems, physical infrastructure – it's all accessible and thus at risk.

[1] 2018 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach

intel® vPro® Platform

Powered by the Intel® vPro® Platform

To learn more about ThinkShield, visit http://solutions.lenovo.com/thinkshield.

This hyper connectivity unfortunately gives the black hats, be they spy, thief, anarchist or arsonist, direct access to the information supply chain that powers higher education. And, as with any supply chain intrusion, it puts the product at risk. In this case, it's the trust and confidence required to transform teaching, learning, and discovery. It's turned into a technology arms race, and as the headlines demonstrate, the good side is falling behind.

The (limited) promise of technology

As threats evolve, so do security solutions and strategies. The virtualization of workloads and workplaces makes site security is less and less important, and the connected user now represents the campus network perimeter, whether they're:

- Logging in from a department office or lab
- Connecting from the road en route to a conference
- Studying and collaborating across campus
- Accessing systems and applications from on- and off-campus housing
- Collaborating with partner institutions and organizations around the world

Securing this user is now more important than the site itself.

With each wave of innovation, new tools are brought into the fight for security and privacy. On the other side of the threat, bad guys are working equally hard – and sometimes even harder. They have the same tools, the same talents, and something even more liberating – no compliance or budget concerns.

Security technology is evolving along familiar patterns. The first phase was network focused, with content blockers, VPN appliances, and strict perimeter controls. Hardware was abstracted into software, and fixed and tangible security assets became virtualized and distributed. Today's clouds and data centers are increasingly micro segmented. AI is helping turn activity information into actionable threat intelligence.

But the user?

Mostly unredeemed. Despite user-focused content and training and follow-up trainings, they continue to be a risk. No amount of usability testing or solutions design can overcome a user intent on harm or more likely distracted into mistake. In the days of physical facility protection, this could be easily mitigated. But now that the user is the perimeter, the challenge gets infinitely more complex.

When solving for cybersecurity, the user is always an unknown X. Even the most predictable person does unexpected things. And even the most diligent, security-minded student or staff member will make choices that circumvent carefully constructed controls. But as threats evolve and the bad guys flex, user and identity management are the front line in protecting information and empowering community confidence.

What makes it hard

Traditional user security was straightforward. A single user on a single device, typically from a single location, often using a single tool. Student mobility and BYOD made it slightly more complicated, but VPNs and device-side management mitigated the risk. Today is quite different, with users:

- Connecting across more devices, from more locations, inside more applications – some IT-managed, some not
- Sharing a wide range of sensitive, protected information
- Collaborating with other institutions and partners in the communities, accessing sharing information
- Doing it all inside an increasingly fast-paced, digital-first culture

If it seems complex now, just wait. Experience teaches us that each of the variables above will multiply over time. And, of course, the same time period will see new threats emerge. With each innovation, traditional defenses become more and more obsolete. It's not just new tools that are needed, but a whole new mindset.

From prevent to detect: a move towards adaptivity

We can see the new mindset in the shift of risk frameworks, from when to if. The process used to focus on prevention – the new mantra is detection. This shift from prevent to detect means security decision-makers must value speed and intelligence over brute strength.

Zero trust works better with layered defenses, authentication included. This enables adaptive security that can evolve to as threats do. The combination of a proactive multifactor baseline with the ability to add on extra protocols gives IT granular security that doesn't have to slow down the majority of security profiles: known, trusted users logging in from known locations to accomplish expected tasks.

Enter behavioral analytics and AI

The trick is detecting when these profiles change. Continuous monitoring used to do a lot of the work, but even that can't watch, think, and react unassisted. That's where AI comes in, ingesting and analyzing millions of user and network records in behavioral analytics. They monitor user activity at scale, looking for patterns and benchmarks. This is where AI excels, sifting and sorting log information in real time.

In the event a pattern is broken, or a disparity otherwise detected, IT can put new layers in place that go well past standard two-factor authentication. The challenge in doing this is to not discourage a user from complying. Students and staff are used to modern application authentication, but what about new tools and strategies?

The future doesn't lie in a single control, but rather the ability to deploy them where and when needed. The future of layered user identity management is stronger on-device authentication support. This gives IT and users a robust set of control that maximize choice while balancing convenience and compliance.

- Makes for more powerful identity proofing and faster onboarding
- Enables users to work inside overlapping and competing frameworks
- Allows IT to deploy a single device across multiple networks and security profiles

It's one of the reasons Lenovo made authentication such a big part of our ThinkShield security portfolio. It enables IT to stack authentication methodologies up, as required, without a lot of extra work. Combined with the other three layers of the ThinkShield platform – online, data, and device, ThinkShield authentication gives institutions the right starting point for adaptive, behavior-driven authentication.

Built for ideas like this: ThinkShield

It's one of the things that makes ThinkShield more than a well-integrated set of best in class protection tools. It's the ability to lean into trusted hardware to ensure that you have protection that's the most tamper- and spoof-proof in the market, including the on-chip fingerprint reader.

Geofencing via GPS	Intel® Authenticate Multifactor
Broad smart card	Bluetooth (proximity verification)
Intel password and PIN	Secure NFC (tap to logon)
Biometric support via camera	Match on chip fingerprint reader (w/ antispoof tech)

Solving the back end: Passwords aren't going anywhere

A quick Google search shows us that, about every two years, somebody announces that the era of passwords is drawing to a close. It's been going on forever. But passwords are probably here to stay for the time being.

- Users are familiar with them and know how they work
- They're universal, working even without integrated hardware
- They're ideal for web applications that typically don't access device-side authentication

By now, everybody understands the value of password strength and complexity, but they don't help if the credentials are stolen. That's where application-side password security becomes important.

Encrypting password has technical costs, so developers often look for easier ways to manage and store credentials. This includes password databases that aggregate credentials, creating an enormous target for cyberintruders and thieves.

intel® vPro® Platform

Powered by the Intel® vPro® Platform

To learn more about ThinkShield, visit http://solutions.lenovo.com/thinkshield.

Once breached, application and system user accounts can easily be compromised. And, without solid authentication in place, hijacking credentials enables bad guys to move without detection, especially lateral (east-west) breaches. That's one reason they take so long to be detected.

FIDO FOR THE FUTURE

Lenovo understands the utility of passwords – but we know they're not ideal for the web-based, mobile-first way we compute today, especially digital natives. That's why our work at FIDO, along with other industry leaders including Intel, is so groundbreaking.

The vision of FIDO is to enable a new standard of hardware-driven authentication. Using a personal device or hardware token, the user authenticates locally via a selected authentication measure and a private key. The device then connects to a FIDO-enabled server online, authenticating with a public key. While it doesn't eliminate passwords completely, it eliminates password databases as a threat and a target

Together, a cohesive whole

We are committed to being a security-first organization and building our products the same way. It's why leading institutions of higher learning around the world make us a trusted partner in their technology transformation.

- A secure global hybrid supply chain built with trusted partners
- Industry standard certified parts and components
- Unique device-level security features as a part of ThinkShield security solutions

Building Trust in a World of Traps: a Quick Checklist

As institutions work to transform how they empower students and faculty, security will always be a constraint – but it doesn't have to be an obstacle. Creating layered, user-centered security controls is critical to accelerating and elevating the mission. And, on an increasingly mobile, multiload, always-on campus, this starts and ends with securing the user and their identity. Without that, real confidence can never be achieved. But where do you start?

1. Map the challenge

Getting a big-picture view is the start. This means understanding all related applications and systems. For most institutions, this means:

- Identifying all SaaS applications used by departments and partners, formally and informally
- Working across functions to ensure all tools and services are captured

2. Identify gaps

Rather than working on what's going well, focus on constraints. For most organizations looking at authentication, these starts with fixing inconsistent, poorly managed user provisioning / deprovisioning and answering critical questions:

- How long does it take to add a user?
- How long does it take to remove a user from trust?
- What about institution partners?

intel® vPro® Platform

Powered by the Intel® vPro® Platform

To learn more about ThinkShield, visit http://solutions.lenovo.com/thinkshield.

3. Prioritize high risk users and systems

Not all logins are created equal. Working with IT and service partners, identify systems that are high risk due to the nature of information accessed and other compliance frameworks. Educause recently posted an article that gives higher ed decision-makers a great start.

- Develop risk scoring for both users and applications
- Overlay scores on top of existing compliance frameworks
- Pay special attention to seasonal / contractor users

Empowering learners and their champions

Lenovo delivers thoughtfully crafted solutions that empower a new generation of explorers and leaders. Our broad technology portfolio ensures a solution for every need, all backed by legendary Lenovo quality, a security-first approach to products and services, and a commitment to long-term transformation partnerships.

Powered by the Intel® vPro® Platform

For more information about Lenovo solutions for education, please visit www.lenovo.com/highered.

To learn more about ThinkShield, visit http://solutions.lenovo.com/thinkshield.