/ABSOLUTE®

TOTAL CLARITY, COMPLETE SECURITY OVERVIEW

- As universities innovate the design and delivery of learning and student services, they need secure digital foundations that extend their reach and readiness.

- IDC predicts that worldwide spending on security-related hardware, software, and services will reach $151.2 billion in 2023[1]. Just over 12.5% of that spend will be related to endpoint security software.

- Endpoints constitute over 70% of breaches[2]; ensuring they are well-managed is critical.

- With an average of 10 security agents on each device, and over 5,000 common vulnerabilities and exposures (CVEs) found in the top 20 client applications in 2018 alone,[3] the endpoint has never been more fragile.

LENOVO SOLUTION

The ThinkShield Security by Design approach makes a difference in end-to-end protection for our customers. With our secure supply chain, built-in hardware platform security, and strategic partner ecosystem, we deliver solutions for threat and data protection, mobility, infrastructure, and edge computing.

As the threat landscape is continually evolving, so are the needs of our customers. We take a holistic approach to the digital needs of institutions by:

- Supporting user productivity and experience

- Addressing security operational-efficiency challenges

- Reducing risk and response time

Over

70%

of breaches originate
at the endpoint
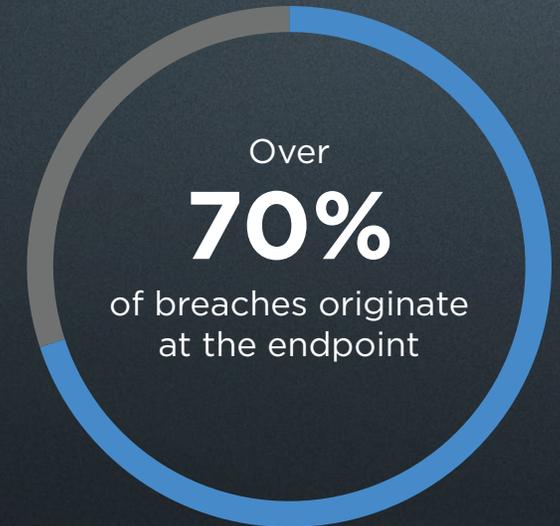
[1] IDC, Worldwide Semiannual Security Spending Guide, October 2019.
[2] Absolute Software, 2019 Endpoint Security Trends Report.
[3] MITRE.ORG

(intel®)

Powered by Intel®.

/ABSOLUTE®

WHO IS ABSOLUTE?

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications, and users against theft or attack—both on and off the university network.

- Absolute's patented Persistence® technology is embedded in the firmware of Lenovo® Think-branded devices featuring Intel® processors for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment
- Allows IT organizations to enforce asset management, endpoint security, and data compliance

HOW DOES ABSOLUTE FIT WITH THINKSHIELD?

As part of our data protection strategy, we have partnered with Absolute to provide higher ed IT admins and security teams with a reliable two-way connection for all of their devices so they can secure endpoints, assess risk, and respond appropriately to security incidents. Most importantly, they can apply remote security measures to protect each device and the data it contains.

WHY THINKSHIELD WITH ABSOLUTE?

- Industry's only tamper-proof endpoint visibility and control

- Lenovo-exclusive capabilities with Remote Supervisor Password (RSVP)
  - Administrators can remotely reach Lenovo devices to create, update, or remove supervisor passwords, thereby reducing the risk of firmware compromise

- Identifies disabled security controls, sensitive data at risk, and user activity or negligence
  - Validates data protection continuously and eliminates compliance failures
  - Reaches deep into every device, discovering sensitive data at risk, and flags endpoints lurching toward compliance failure

- Enables hardened resilience to avoid devastating data breaches and maintain continuity

- Works in conjunction with Lenovo Patch that simplifies Lenovo BIOS, driver, and third-party application updates via SCCM

WHO ARE IDEAL LENOVO AND ABSOLUTE CUSTOMERS?

Every Lenovo higher education customer who has a security mindset and want the confidence that their environment is secure is an ideal target for Absolute Persistence technology.

- IT operations and security teams that need to see, understand, and resolve hidden risks within their device population

- Those who require asset intelligence across every endpoint, device and data analytics to unmask compliance failures, and automated endpoint hygiene to improve their security posture in the face of growing threats

(intel®)

Powered by Intel®.

Lenovo

/ABSOLUTE®

KEY CUSTOMER OBJECTIONS AND ANSWERS

- It's not worth the cost.
  - The math is compelling. A single compliance event can cost hundreds of thousands of dollars—not to mention the university's reputational hit.

- We can already see all our devices.
  - Are you sure? Absolute can give you complete confidence, thanks to a self-healing persistent agent that illuminates device presence and performance.

- We are doing most of this ourselves.
  - But at what depth? And at what cost? There is no match for Absolute visibility and control. And you'll need multiple tools to get anything that's close.

- We don't need another tool.
  - We agree. By leveraging Absolute, you're taking advantage of what Lenovo has already built into our hardware. You get confidence, not complexity.

- Our unified workspace software does this.
  - While tools like Workspace ONE provide device provisioning and management capabilities, Absolute ensures visibility across your fleet, monitors security vitals, and automates device resilience.

PROBING QUESTIONS

- Are you able to identify the encryption status on every university device?

- Are you able to detect changes to hardware, software, firmware, or operating systems on your devices?

- Can you identify personally identifiable information on your endpoints? Can you certify that the information was not targeted in an attack?

- Can you initiate incident investigations, digital forensics, and document the status of every device in the event of a security incident?

- Can you freeze or wipe a device remotely, anywhere on or off your network?

WHERE TO GET HELP

The sales team is more than happy to handle any sort of sales presentation or technical conversation; please contact your sales representative today.

(intel)

Powered by Intel®.

Smarter technology for all

Lenovo