

Absolute for Higher Education



We've had success with detecting laptops that have 'walked off' of campus, and using Absolute to detect and remediate the potential security threats.

MATT SEIWERT
INFORMATION SECURITY ANALYST
WICHITA STATE UNIVERSITY



[Read the Case Study](#)

Protect, recover and fix all your devices — 100% remotely.

For all the advantages remote learning offers higher education, it has also created new challenges for information security, as devices may travel with students and faculty across campus or across the world.

Common IT asset management challenges:

- Operational inefficiency due to managing multiple campuses
- No way to see and manage all devices from a central dashboard
- Inability to track, locate, and freeze devices
- Inability to identify and recover missing devices, or delete sensitive data on unrecoverable devices
- Poor accountability when devices are lost or stolen
- No control or visibility into off-network devices used by remote faculty, staff, and students

Common security challenges:

- No way to ensure all remote, off-network devices are up to date and properly configured for security and remote access
- Failing security controls like encryption, outdated anti-malware, and vulnerable OS versions create a risk of a data breach or cyber/ransomware attack
- No way to know if protected, personal data is on a device
- Uncertainty whether all endpoints remain compliant with HIPAA, FERPA, PCI, or GDPR
- Lack of expertise adopting and implementing NIST CSF or other cyber security frameworks

For colleges and universities to be properly equipped to deliver full remote learning experiences, institutions need a centralized way to track, manage, and secure data and devices, on and off the campus network.

Innumerable risks, one solution.

Improve Efficiency with a Single Cloud-Based Console

Dramatically improve your IT operational efficiency by seeing, managing, controlling, and securing your entire device population — Windows, Chromebook, and Macs — from one place. Absolute is firmware-embedded by every major PC manufacturer; you can activate remotely and begin identifying and solving security issues quickly.

Track and Secure your Assets

Activate a persistent connection to all your endpoints, giving you unrivaled visibility and control — including the ability to geolocate, freeze, and wipe remote devices.

Reduce Device Theft and Loss Throughout the Year

Flag a device when it's missing, and you will be notified via email the next time it connects to the internet. If stolen, **Absolute's Investigations** team helps by collaborating with law enforcement to track and recover the location of stolen devices — even off network.

Maintain your Security Controls

Absolute Persistence's self-healing capability can be extended to AV, encryption, VPN, or any other application that you depend on — so they're always installed, up-to-date, and working correctly. **Application Persistence** means data and assets are always protected, compliant with regulations, and prepared for audits—whether you're satisfying CARES Act requirements or other regulations like HIPAA.

Fix Vulnerabilities Remotely

With **Absolute Reach**, your IT team can remotely execute scripts to repair, patch, and remediate devices. Get alerted to suspicious activity, inappropriate use, and early precursors of security issues — so you can take remote action to prevent incidents and ensure compliance.

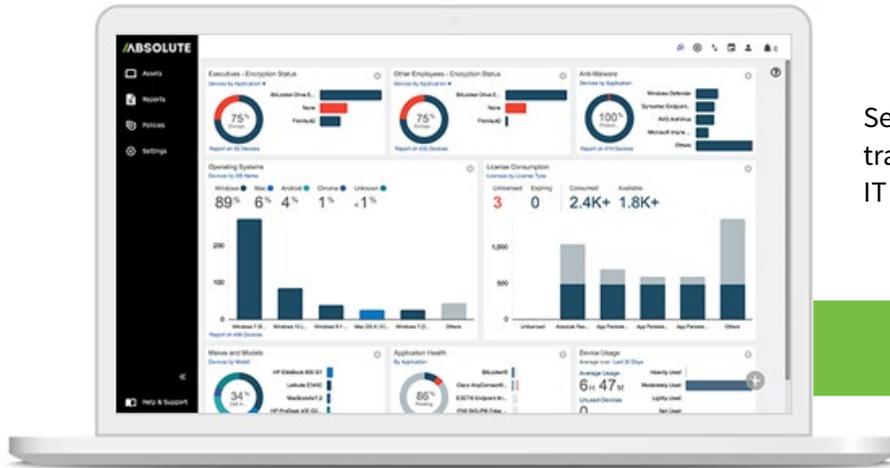
Ensure Continuous Compliance

With Absolute, your IT and security teams can see, understand, and control endpoints from a single cloud-based console across different platforms — including off-network remote machines.

Absolute keeps you audit-ready, helping you achieve and prove compliance with regulations such as HIPAA, FERPA, PCI DSS, GDPR, and CCPA. Create automatic, flexible compliance checks adaptable to any cyber security framework, such as the NIST CSF or other standard. Easily identify noncompliant devices, and automatically update and restore controls that prevent compliance lapses.

Maintain complete endpoint security with Absolute:

- 1 Activate an undeletable tether to all devices.**
Absolute is already embedded in the firmware of your devices, where it can't be removed; once activated, you instantly have a self-healing, digital connection to all your endpoints both on and off your institution's network.
- 2 Automate inventory and audits.**
Your Absolute console is automatically fed information from your endpoints — on and off your network. Your inventory is always up to date and audits become quick and efficient without needing additional infrastructure.
- 3 Reduce attack points.**
Enforce security controls and configurations and upgrade your gold image to a diamond.
- 4 Identify broken or disabled safeguards.**
Encryption and anti-malware monitoring restore faulty safeguards remotely — with zero human touch.
- 5 Keep everyone working and productive.**
Ensure continuity with self-healing critical applications.
- 6 Locate devices with sensitive data.**
Mitigate exposure by automating controls or deleting data remotely on demand.
- 7 Isolate, freeze, or wipe devices — remotely.**
Automated alerts focus attention where it's needed; Deploy powerful remediation capabilities to fix any issues — on or off network.
- 8 Get support from our experts.**
Our team of cyber security experts will help you assess your endpoint risk and the maturity of your security controls, so you can prioritize corrective actions and strategies.



See how Absolute can transform your organization's IT and Security

REQUEST A DEMO

ABOUT 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 corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT to enforce asset management, security hygiene, and data compliance for today's remote digital workforces. Patented Absolute Persistence™ is embedded in the firmware of Dell, HP, Lenovo, and 26 other manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at absolute.com and follow us at [@absolutecorp](https://twitter.com/absolutecorp).



EMAIL:
sales@absolute.com



SALES:
absolute.com/request-a-demo



PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000



WEBSITE:
absolute.com

