Tenable for Higher Education

Defend Your Educational Institution's IT Environment with Continuous Network Monitoring

Key Challenges

Higher education institutions support an open and shared environment, which is critically dependent on IT infrastructure to support the daily operations of students, faculty, and administrators. At the same time, they must defend their users by continuously monitoring for attacks and breaches while demonstrating adherence to multiple compliance standards.

Higher education institutions face certain unique attributes:

- Open/Free Networks: Open, free networks that must accommodate a variety of users with different access levels – enrolled students, faculty, and prospective students, as well as administrative staff.
- BYOD: Students and faculty bring their own devices (BYOD) to connect to university networks and access university servers and personal applications. IT often does not have control of these devices.
- Shared Resources: Faculty and staff members connect to internal resources as well as the Internet from shared systems or personal devices.

Security solutions must address the diverse deployment requirements, technical breadth, maturity level, and work with existing workflows and investments of higher education institutions to be effective.

Next-generation security solutions must also include continuous monitoring of the IT environment of higher education institutions to not only identify vulnerabilities, advanced threats, and compliance issues, but also provide advanced analytics to prioritize responses and measure the effectiveness of deployed security investments and programs.

Solution Overview

Tenable's Continuous Network Monitoring™ solution provides complete visibility and insight to meet these needs and answer challenging questions that higher education IT executives and administrators face such as:

Tenable Helps Answer Key Questions that IT Technical and Executives Teams Face	
Technical Teams	**IT Executives**
• What unknown devices are connected to my student, faculty, and administration networks? • Which are vulnerable or out of compliance? • How many systems are already compromised and spreading malware inside my campus network? • What risk do they pose to other student, faculty, and administration systems? • Within my internal faculty network, what requires immediate action? • Is personal student information being openly sent to malicious sites?	• Across my entire institution, where is the most critical risk? • How much risk do mobile devices pose? • What responses should be taken by network and security teams to minimize impact to critical education IT infrastructure? • How do we identify systems that go out of compliance to expedite compliance audits? • Are security deployments effectively configured to stop threats? • Are IT teams responding in a timely manner to exposed and vulnerable administrative systems that process student records?

Solutions:

- SecurityCenter Continuous View™
- SecurityCenter™
- Tenable.io™
- Nessus® Manager
- Nessus® Professional

Key Benefits

- Detects unknown student and faculty-owned devices
- Spotlights which systems are out of compliance for proactive remediation
- Isolates security weaknesses and attack paths in university networks
- Delivers advanced analytics to zero-in on the most critical issues and actions to reduce the most risk
- Measures effectiveness of deployed security investments and policies
- Identifies accuracy and timeliness of patch management processes

Vulnerability Assessment	Vulnerability Management	Vulnerability Analytics	Continuous Network Monitoring
Nessus Professional	Tenable.io/ Nessus Manager	SecurityCenter	SecurityCenter Continuous View (CV)
• Ad-hoc scanning • Vulnerability & configuration auditing • Malware detection • Basic reporting	• Cloud-based or on-premises • Configuration/patch validation • Malware detection • Agentless & agent-based scanning	• Advanced visualization • Advanced reporting • Trending analysis • Compliance & customization • Tiered management	• Continuous asset discovery & profiling • Event & activity monitoring • Advanced analytics • Integrated forensics • Security assurance metrics

Tenable solutions also allow higher education organizations to grow with their network and adopt additional capabilities to improve risk posture and security effectiveness. Whether your needs are for periodic assessment with vulnerability management or continuous network monitoring for technologies such as mobile devices and cloud applications, Tenable offers the right solutions to meet your needs.

Benefits

Tenable solutions offer the following key capabilities and benefits to higher education institutions:

- **Improves Visibility:** Which student and faculty-owned devices are connecting to the university network, and are the devices vulnerable or infected?
- **Spotlights Compliance Issues:** Which systems are out of compliance against industry standards (such as FERPA, GLBA, HIPAA, PCI DSS) so they can be proactively remediated before the next audit?
- **Isolates Security Weaknesses:** What security weaknesses and attack paths exist in the university network that should be corrected? What actions can eliminate the most risk?
- **Delivers Advanced Analytics:** What are the most critical issues in your environment? What actions will reduce the most risk?
- **Improves ROI:** How do you measure security effectiveness including whether the current security and patch management programs need to be improved? Are responses to vulnerabilities, threats, and compliance issues timely in resolving issues?

About Tenable

Tenable™ is the Cyber Exposure company. Over 23,000 organizations of all sizes around the globe rely on Tenable to manage and measure their modern attack surface to accurately understand and reduce cyber risk. As the creator of Nessus®, Tenable built its platform from the ground up to deeply understand assets, networks and vulnerabilities, extending this knowledge and expertise into Tenable.io™ to deliver the world's first platform to provide live visibility into any asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, large government agencies and mid-sized organizations across the private and public sectors. Learn more at tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact