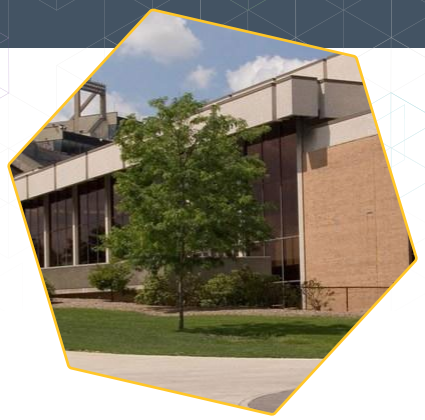
tenable network security

Youngstown State University



Overview

Youngstown State University (YSU), an urban research university in Youngstown, Ohio, is home to more than 15,000 full-time students and 2,000 staff members, with more than 85,000 alumni. The university had a general budget fund for the fiscal year 2011 of $158.8 million, and is made up of seven separate colleges spread over a 145-acre campus. The school offers more than 100 undergraduate majors, 35 masters programs, and doctorates in educational leadership and physical education. With thousands of records containing sensitive, personal data of students and staff, as well as a mass of intellectual property, protecting its networks is of critical importance to the university.

Business Needs

Youngstown State University needed a more efficient and effective security process that would provide a comprehensive, single view of all security activity, while reducing time investment on cumbersome and redundant tasks.

Searching for Consistency

Protecting the records of thousands of students and faculty — which often include financial, health, and personal data — is vitally important for every university. And with thousands of people accessing its network — with both campus computers and personal devices — maintaining visibility into all network activity is a daunting task. YSU, with more than 2,300 machines on its network, is no exception.

YSU's challenging and time-consuming security process included searching for log data and vulnerabilities in several different repositories and manually connecting the dots between security events and network activity. In several instances, the entire staff would be on hand, digging through various systems for data from the IPS and AV logs and manually matching events together. The university needed to reduce overhead investment in its security process by consolidating its view of all network activity and ensuring key events did not go unnoticed.

Time is Money

For YSU's IT group, time is incredibly valuable, and managing the complex network is often more than a nine-to-five job. The team needed to optimize its security process so it could cut costs by reducing the time investment needed to manually search for and match log data, and improve security by introducing automation — especially for compliance reporting. The team focused on making the following improvements:

- **Automated data consolidation:** YSU's manual approach was time consuming, and Welton felt the process wasn't effective enough to ensure the IT staff would catch all important events.
- **Streamlined compliance reporting:** As a large university, YSU is subject to several regulations, including FERPA, GLBA, and PCI. At the time, YSU would write one-off scripts and manually pull together log data to create a report. The organization wanted a simpler way to generate reports, making audits a pain-free, efficient, and repeatable process.

The Tenable Solution

Greater Coverage, One Viewpoint

To address its security and cost concerns, YSU implemented several new practices which restructured the organization's overall security process. This included adding new technology that would automatically collect and correlate data from existing systems, such as anti-virus management, IPS, system logs, and NetFlow data, into a single view. This single viewpoint allowed YSU to quickly and easily understand the true impact of an issue and the level of response needed.

Youngstown STATE UNIVERSITY

Business Needs

- More efficient and effective security process
- Comprehensive, university-wide single view of all security activity
- Reduce time investment on cumbersome and redundant tasks

"Since implementing our new security procedures, we've been able to recoup at least 15 hours per week, or about $50,000 per year, that were dedicated to manual security processes like running vulnerability scans or consolidating log data. That's a significant time savings for a security team of three people, and we've been able to reallocate that saved time to other high-priority projects — giving us an opportunity to be more proactive with security and other IT initiatives."

Mark Welton
Network Security Supervisor,
Youngstown State University

With access to timelier and easier-to-understand security data, YSU was able to:

- **Significantly streamline the audit process,** including enabling staff to save and reuse compliance workflows — eliminating the need to reinvent a query for every audit and saving the organization roughly five hours per audit.
- **Save hundreds of hours annually,** enabling YSU to reinvest that time into other top IT and security projects and proactively manage network updates, modifications, and security.
- **Achieve a complete, university-wide view of all network and security activity,** enabling the organization to quickly and easily identify misconfigured machines, unpatched vulnerabilities, and other security risks.

Beyond Vulnerabilities

Since optimizing its security process, YSU has gained a new perspective on its network. The university has been able to uncover new abnormal activity beyond what Welton had originally expected, including:

- The discovery of botnet activity by analyzing abnormal bandwidth usage.
- Investigating a virus outbreak and discovering the problem stemmed from an unpatched system, which was quickly repaired.

Next Steps and Bottom Line

Youngstown State University plans to further expand its use of Tenable's Unified Security Monitoring™ Platform based on SecurityCenter™, as a part of its overarching security initiative by integrating its patch management system with Tenable's Nessus® vulnerability scanner. This will provide more comprehensive vulnerability assessments, help eliminate the possibility of false positive reports of missing patches, and save time and reduce costs through streamlined reporting, stronger security, and improved compliance.

"I wanted to make sure we weren't constantly on our heels, trying to prevent activities from slipping past us. Instead of spending valuable time manually sifting through data from five different places, we needed a single, consolidated viewpoint into our network activity to help us pin down the real problems and threats."

"Today, we get more than a point-in-time snapshot of our network — we get the full picture, and we get it quickly and easily. Instead of having to grab pieces of information from all over our network, we now get all that information delivered to us, consolidated, whenever we want it."

"We're taking our security to the next level. We're uncovering events that we've never been able to see in the past, and we're now able to quickly report back to senior management on the status of the network."

Mark Welton
Network Security Supervisor,
Youngstown State University

For More Information

Questions, purchasing, or evaluation:
sales@tenable.com or 410.872.0555, x500
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™ network security