Nexpose Identifies Vulnerabilities, Assists Remediation at LoneStar College System

About LoneStar College System

The LoneStar College System is a thriving community college system serving over 90,000 credit and continuing education students per semester. It offers a broad variety of academic and vocational programs on five campuses and 10 instructional outreach centers located in the North Houston, Texas metropolitan area.

Like most educational institutions, the IT infrastructure at LSCS supports a wide variety of end-user devices, operating systems, and applications. The college system's Office of Technology Services (OTS) support two main datacenters and fourteen campus datacenters with over 900 physical and virtual servers supported. The college system has an extensive Wintel and Linux server environment and a robust voice/video/data network environment. Students, faculty, and staff can access IT services from anywhere through the wireless network. Such an open computing environment is inherently difficult to protect from breaches, disruptions, and intrusions.

Client
LoneStar College System

Industry
Higher Education

Website
www.lonestar.edu

Challenge: No Visibility into Security Posture

Before 2008, LSCS supported separate campus IT operations at each of its five campuses with distributed IT support services. Then a new CIO joined the college, and within a month, the Lone Star College System had completely centralized its IT services to support a new vision. Associate Vice Chancellor of Technology Services Link Alander explains, "Through that process we had a series of changes and challenges that had to be achieved to improve reliability and security."

While the college had so far avoided any significant security incident or data breach, it understood the need for a proactive security posture that would maintain user trust. It also needed tools to help prove compliance with regulations such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and other regulations.

The LSCS security initiatives are part of 11 strategic technology initiatives, incorporated into the overall LSCS strategic plan for 2009 through 2011. One of its primary security goals is to use ISO 27000 standards as a framework.

In 2008 and 2009, the LSCS IT team hired external security firms to conduct assessments of data center servers, applications, and the network core. "During that process it became clear that the majority of the risks that we had could easily be prevented," says Alander. "So, we began the process of looking for something that would take care of all of the little risks that could have a major impact on us."

Case Study Highlights

Challenge

With over 900 physical and virtual servers and 14 campus datacenters, the LoneStar College System needed to be able to scan its distributed IT support services for vulnerabilities to keep its systems and data secure.

Solution

Nexpose began delivering value immediately, delivering measurable results in employee productivity and security within just a month. Nexpose automatically scans all fourteen datacenters and the network core weekly to keep the security teams up to date.

Intended to identify and mitigate vulnerabilities, the assessments instead became a source of frustration for the LSCS team, because remediating the identified issues proved elusive. "Everything we got in the first report was filtering through a pile of 'stuff,'" says Alander. "They would turn out problems, but not really offer us solutions at the same time. We found a lot of information that we couldn't make heads or tails of to take immediate corrective action."

The team persisted through four assessments from several providers. Says Alander, "We finished one security assessment, and we were appalled. We thought that we'd improved significantly since our last one, and we really hadn't."

"Nexpose silently accomplished everything it needed to accomplish, and it's made us more secure."

Link Alander
Associate Vice Chancellor of Technology Services
LoneStar College System

Solution: Better Security, Higher Productivity in One Month

After the fourth assessment, an account manager from Rapid7 contacted the LSCS team, who agreed to evaluate Rapid7 Nexpose Enterprise Edition, a vulnerability assessment, policy compliance, and remediation management solution. Deployable as software or as an appliance, Rapid7 Nexpose scans for vulnerabilities and performs checks across Web applications, databases, networks, operating systems, and other software products. It locates and identifies threats, assesses their risk to the environment, and offers step-by-step remediation plans.

Nexpose ended the team's frustrations. "Our initial review of Nexpose matured very quickly," says Alander. "We put in the demo set and saw immediate results with it. From there, we integrated Nexpose as part of our security strategy. It's shown us things that we've never seen before. Out of all the reports we saw before Nexpose, the tool showed us so many more vulnerabilities that were easy to close and fix."

During deployment, the LSCS team hired three temporary technicians to help remediate the long list of vulnerabilities discovered by Rapid7 Nexpose Enterprise Edition. Two weeks after deployment, the systems administrators met to discuss procedures for getting the most value from the tool. The team had had no formal training for the tool, yet Alander says, "It didn't take any time at all to find out exactly how it fit into the organization, how we would utilize it, and how we would manage it going forward."

Nexpose began delivering value to LSCS immediately, delivering measurable results in employee productivity and security within just a month. Nexpose automatically scans all fourteen datacenters and the network core every weekend, generating reports that Alander, the systems administrators, and the executive OTS management team review every Monday. Remediation tasks are prioritized and delegated. The software provides easy-to-follow remediation instructions, and Nexpose reports inform Alander that his staff has followed up on each task. The reports also assist LSCS with proving regulatory compliance.

In complex IT environments, explains Alander, "Typically, major security fixes require senior-level network and systems administrators. What we've found with Nexpose is that the information provided on the risk, and how to fix it, is so clear that any systems administrator can take action without causing other damage to the system." And, "the tool provides clear remediation tasks and is easy to use to secure our environment," states Allen Sweeney, Senior Systems Administrator at LSCS.

Alander says his team is evaluating integration of Nexpose through its extensible, XML-based API into the emerging security infrastructure at LSCS, including helpdesk, software patch management, and other datacenter management systems. The team may also use Nexpose to scan (and remediate) workstations and other user devices. Alander views the capabilities of Nexpose as foundational to the college's efforts to attain ISO 27000 compliance.

"Nexpose silently accomplished everything it needed to accomplish, and it's made us more secure," says Alander. "We've locked down our environment to threats and risks that people didn't even know they had."

"This is one of the few products that out of the box provided immediate results and value to the organization" states Shah Ardalan, Vice Chancellor/CIO, Lone Star College System.