The Absolutely Essential Higher Ed Superpower

Gaining visibility into what's going on inside your systems lets IT teams be proactive, and that makes all the difference in how effective they are.

Brandon Shopp
Group Vice President of Product Management
SolarWinds

NEVER HAS HIGHER EDUCATION BEEN MORE reliant on technology and the IT organization. As a result, colleges and universities are much more at risk from cybersecurity vulnerabilities today than ever before. At the same time, as technology dependence has grown, staffing and budget haven't, which means **IT solutions for educational institutions** truly need to do more with the same or, in some cases, less than they've historically had.

The pressure is immense. If a student can't access an application or a resource, if a faculty member can't get onto web conferencing, if a staffer can't send e-mail, the institution will fail in its missions: educating students, making research discoveries, and doing everything in its power to secure the future of the world.

With so much at stake, the one superpower IT teams in the education sector need to develop above all others is X-ray vision. Gaining visibility into what goes on inside your systems lets you become proactive, allowing you to see exactly where to target your time and attention and quickly troubleshoot problems for speedier response.

Unless you were born on Krypton, the best way to achieve this level of visibility is to capitalize on tools that deliver the same capabilities. Those **IT tools for higher education** would be expected to provide oversight in at least four areas:

- Doing status checks on the health and performance of infrastructure, on-premises, hosted, and in the cloud

- Tracking the delivery path along which data traverses, identifying connections, dependencies, and topology

- Diagnosing network performance and endpoint compliance

- Applying machine learning to automate response and augment human capabilities

3 Priorities for Visibility

I can cite three scenarios where visibility proves invaluable in the education environment: jumping on network problems, indicating application snags, and staying on top of security risks.

USE CASE #1:
Helping identify the network problem

If a student is getting choppy video or audio during a class session, does the problem rest with Zoom, the university infrastructure, the home network, the service provider, the hotspot, or something else? Where does the user start? Who does he or she call? The longer it takes to figure that out – to do a root cause analysis of the problem – the longer it will take to resolve it.

SolarWinds school network monitoring software opens up visibility on the path that an end user follows in accessing a resource, all the way from the service provider's network through the university's VPN out to Zoom and into the user's device. Armed with this information, IT can identify where the bottleneck is taking place and provide evidence for the solution phase.

USE CASE #2:
Helping identify the application problem

Universities are hotbeds of homegrown applications. When issues surface for users and they take it to their help desk, how does the IT staffer narrow down the source of the problem? Piecing together the mystery may require jumping from tool to tool, a time-consuming and inefficient troubleshooting process. Plus, the whole rigamarole leads to longer downtime, which results in growing user dissatisfaction.

By allowing for full-stack observability through a single display, SolarWinds can track how data traverses the network, following it through the server, virtual machine, application, and database. The software can identify data

interdependencies and pinpoint where the problem occurred, providing a boost to the help desk, so they don't have to do the mental merging themselves: "Hey, check this server! All of a sudden, the CPU on it spiked up to 100%. Something's going on. You need to investigate."

USE CASE #3:
Helping identify the full attack surface

With every new service a college or end user adopts, the attack surface grows. Whether that's a cloud service from Amazon, Microsoft, Google, or another company, an internal application running on-premises, or a slate of devices getting onto the network at the start of a new semester, all of them are generating traffic and logs and opening up potential security risks into your organization.

When your institution leverages third-party resources, it has placed a certain amount of trust in them – that they have the appropriate security controls in place, they're doing the appropriate testing, and they'll hold up to their end of the shared responsibility deal. On the university end, IT remains responsible for making sure users are authenticating, two-factor is turned on, and operations are being audited.

By keeping an eye on the full stack – traversing on-premises, hosted solutions, and the cloud – SolarWinds analyzes all the data generated, standing by, primed to flag possible anomalies in the crowd before they turn into full-fledged security events.

Troubleshooting for Friction-Free Experiences

What these use cases have in common is the need to troubleshoot problems across products and platforms and thereby ensure a frictionless experience for users.

Whether you face an immediate problem – a security incident, an outage – and need help solving it, want to make your team more effective, or have a compliance need that calls for new levels of visibility and auditability, SolarWinds produces tools to help IT stay on top of potential issues, improve performance, and keep the institutional mission on track. X-ray vision really does have its advantages.

Brandon Shopp is the group vice president of product strategy for security, compliance, and tools at SolarWinds. Previously, he was the vice president of product management at AlienVault and senior director of products at Embarcadero Technologies.