

Splunk for Higher Education and Universities

Using Operational Intelligence to Improve IT Efficiency, Security and Reduce Cost

Challenges for IT in today's Educational Institutions

Today's educational institutions face challenges that place ever-increasing demands on their technology infrastructure. Enrollment at many institutions is at record levels. At the same time, educational institutions face increasing expectations for accountability and compliance. While enrollments and expectations are increasing, budgets tend to be flat or declining, forcing institutions to make difficult choices on how to use existing resources.

The network, infrastructure and applications that form the backbone of educational enterprises have become mission-critical in delivering more robust services under severe resource constraints—getting the most out of technology investments is an institutional imperative, not a nice-to-have. IT must also know how to map its services and solutions to key strategies of the institution so that leadership views them as drivers of success instead of budgets to be managed or reduced. Technologies that can deliver critical institutional insights in a timely and cost-effective fashion can lead the way.

Today, machine data represents a largely untapped opportunity for delivering just these types of results. Campus networks, infrastructure, applications, servers, learning management systems and end-user devices generate a huge volume of logs, messages, traps and metrics—machine data that can provide tremendous value for IT by mitigating risk, detecting system abuses and improving operations. Currently, few IT organizations—whether in commercial, government or educational settings—effectively harness the value of their machine data because technology tends to develop as “silos” of systems focused on specific functions, departments, or groups of systems and people. As a result, IT personnel end up with narrow, focused tools that provide a limited view of interactions which may cross numerous infrastructure and process boundaries.

Splunk helps break down IT silos and provides visibility into machine data across the entire infrastructure to drive results that impact the mission and bottom line of educational institutions.

Splunk Delivers Insight Into Machine Data

Splunk is the engine for machine data. Splunk can read data from just about any source imaginable, including student registration systems, learning management systems, networks, web servers, remote sensors, mobile and online learning applications, legacy applications, application servers and structured databases. By centralizing all this data into a single console, Splunk provides unparalleled insight into problems,

usage patterns and trends across an entire campus IT infrastructure. In addition, institutional usage is not limited by the number of machines, data sources, or users—it is only limited by the total data volume that is indexed. This gives IT the ability to control utilization without being locked into a per-user or per-machine fee.

Splunk delivers real-time analysis and understanding of what is happening across IT systems and infrastructure. It uses untapped machine data to identify problems, risks and opportunities to drive lower costs, more effective operations and better decisions for IT and the educational institution as a whole.

Typical use cases for Splunk in educational institutions include ensuring security and compliance, detecting network abuse and enhancing campus services. The examples below illustrate different ways Splunk can provide new levels of compliance, visibility and service for today's institutions of higher education. Moreover, because Splunk can index any form of time-series data, not just machine data, getting extra value out of Splunk is limited only by the imagination of its users.



“Now multiple people can jump on issues. We're no longer stovepipes but a much more effective team.”

Washington State University

Ensuring Security and Compliance

Campuses are particularly vulnerable to security threats given the sheer number of users they serve across different delivery channels on and off campus. Historically, universities' commitment to academic freedom has also entailed open network architectures. Consequently, security threats can happen quickly and start anywhere within the IT infrastructure. Splunk is particularly well suited to handle the security challenges within a university IT infrastructure. Splunk can collect and index all machine data to enable end-to-end situational awareness. It supports ad-hoc reporting and real-time monitoring of incidents and attacks, which help security teams become proactive instead of reactive.

Many higher education institutions must also meet multiple regulatory requirements and standards including PCI, Sarbanes-Oxley, FERPA and HIPAA, among others. Splunk effectively supports the data collection, auditing, data storage and visibility requirements of these regulations. With Splunk, IT organizations can ensure cost-effective security and compliance to best mitigate risk.

For Weill Cornell Medical College, Splunk has had a transformative effect on their IT security and network operations. The university's incident investigations now take place in minutes vs. hours, and proactive searches head off issues on a routine basis, which also reduces downtime. This has had a direct impact on the bottom line, making incident response an order of magnitude faster and more effective.



"Splunk proved its value the first time we used it for a security incident."

Josh Gluck

Assistant Director, Network and Communication Services Group, Weill Cornell Medical College

Detecting Network Abuse

College campuses strive to be places where information can be shared in an open and widespread fashion, and the IT infrastructure bears much of the responsibility for helping this to happen. Building such an infrastructure also means that the potential for users to abuse these resources is very high, straining network resources and consuming large and unexpected blocks of time for IT staff. Splunk can help detect patterns of abusive activity as it occurs by correlating machine data across a wide variety of sources.

For one college campus in the Midwest, dealing with RIAA takedown notices used to take an IT administrator a solid day to resolve. Hundreds of labor hours per year were spent addressing this particular form of network abuse. Using Splunk, RIAA takedown notices now take 30 minutes or less to handle.

Another campus in the northeast uses Splunk to help with Windows computer lab management, analyzing machine-generated data to track logon/logoff duration, measure printer usage and identify users engaged in illicit or illegal printing.

Enhancing Campus Services

Campuses can gain insight into key issues and metrics across their applications and IT infrastructure by using Splunk to index, search and analyze data. With Splunk, they can easily perform end-to-end transaction tracking across all systems that students, faculty, or staff touch.

One campus on the east coast uses Splunk to manage course registration loads - their Splunk dashboard indicates spikes, anomalies and errors. The dashboard also helps them search for automated behavior by allowing them to dig into the applications and components to understand the root causes of problems.

Another campus in the southeast uses Splunk to empower the help desk. With Splunk, help desk resources get direct and secure access to the data they need to solve user problems without needing extensive training or expertise—or having to escalate the problem to higher support level personnel.



"You had me at hello! Splunk has liberated me."

Louisiana State University

Splunk Delivers Rapid Time to Value

Splunk has been built to deliver rapid time to value. Unlike traditional enterprise software solutions, Splunk can be installed in minutes, is available as a free download and can run a variety of apps and add-ons that extend the capabilities of Splunk and make it easier to use. These applications are available on Splunkbase and include pre-built metrics, reports and dashboards, all of which can be deployed rapidly to augment core Splunk capabilities. In addition, educational institutions can build applications for everything from learning analytics to research compute scheduling on HPC clusters, then share them via Splunkbase.

Machine Data Insight = IT Driving Institution Success

The use cases described here highlight just a few areas where IT departments from campuses across the globe are realizing significant value from Splunk. IT organizations that effectively harness the end-to-end knowledge embodied in machine data can ensure security and compliance, detect and manage network abuse and enhance campus services, all with a positive impact on the bottom line and the mission of the institution.

Download Splunk for free today. Contact us and let us know how we can help you.

Key Splunk Features:

- Index data from any format or source
- Conduct root cause analysis, monitoring or reporting across IT silos
- Create highly flexible dashboards for IT and administrative users alike
- Adapt to change with a schema-less approach; doesn't drop or ignore new or unexpected data
- Scale as needed—index terabytes of data per day

Getting Started with Splunk:

- Free download, installs in minutes
- Start small and grow over time—reduce risk while proving value
- Realize value in days, not months or years

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.