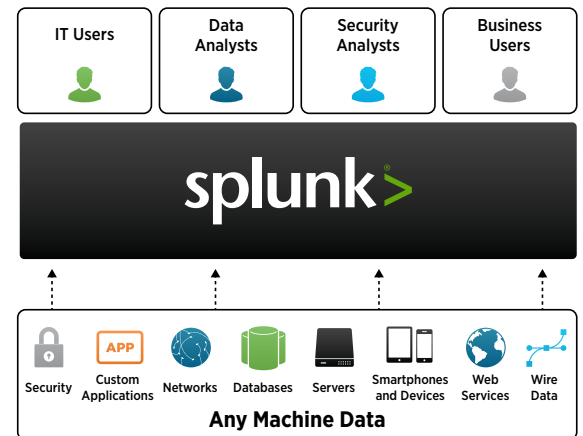


SPLUNK® FOR HIGHER EDUCATION

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

- Identify problems, risks and opportunities to drive lower costs and provide more effective operations
- Detect security risks and network abuse
- Improve student and faculty experience across all systems used
- Manage and monitor machine data from multiple sources
- Collect and audit data to meet regulatory requirements



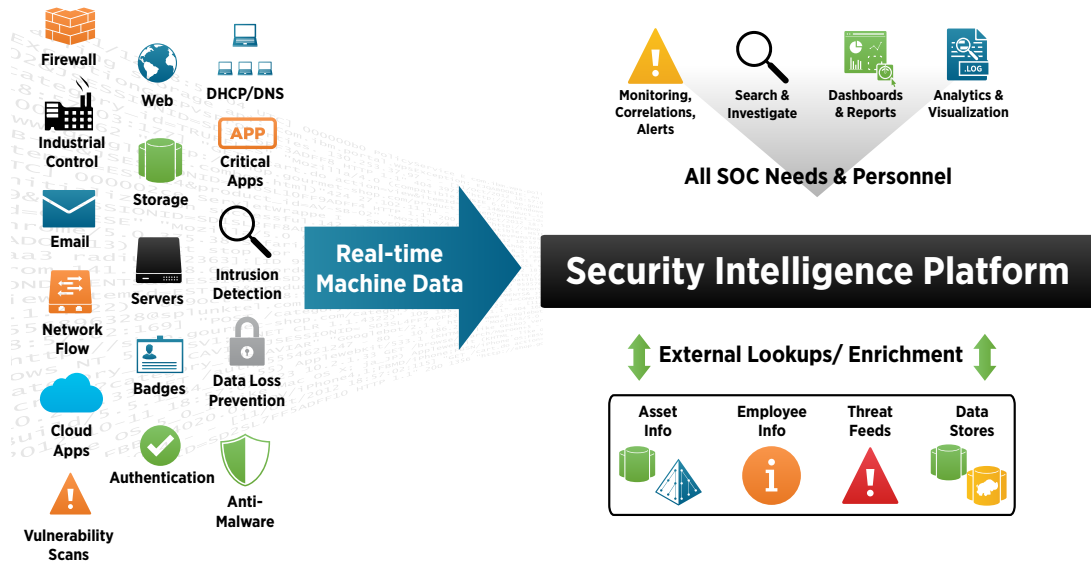
Today's educational institutions face challenges that place ever-increasing demands on their technology infrastructure. Enrollment at many institutions continues to fluctuate, while budgets at many schools are flat or declining, which makes getting the most out of technology investments essential. And since most campuses adopt open network infrastructures, network abuse and security threats can start anywhere, driving the need for security teams to be proactive instead of reactive.

Machine Data & Higher Education

Machine data is an untapped opportunity for institutions of higher education. Campus networks, infrastructure, applications, servers, learning management systems and end-user devices generate huge volumes of data that—when leveraged—can provide unparalleled insight into problems, usage patterns and trends across an entire campus IT infrastructure.

The Splunk platform can read data from just about any source imaginable, including student registration systems, learning management systems, networks, web servers, log files, firewall data, remote sensors, mobile and online learning applications, legacy applications, application servers and structured databases. The Splunk Platform uses untapped machine data to identify problems, risks and opportunities to drive lower costs and provide more effective operations, as well as make educational institutions more secure.





Security & Compliance

Campuses are particularly vulnerable to security threats given the number of users they serve. 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 products can handle this challenge by collecting and indexing 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.

Detecting Network Abuse

Building an open network infrastructure means the potential for users to abuse these privileges is high, which can strain network resources and consume large and unexpected blocks of IT staff’s time. Splunk can detect abusive activity as it occurs by correlating machine data across a wide variety of sources.

Enhancing Campus Services

Campuses can gain insight into key issues and metrics across their applications and IT infrastructure by using Splunk software 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.

[Download Splunk Free](#) or explore the online sandbox. Splunk provides a range of solutions for higher education. Splunk Professional Services will work with each customer to identify the appropriate data sources required to meet your needs. Contact [Sales](#) to get started today!



Learn more: www.splunk.com/asksales

www.splunk.com