What Is Splunk and How Does it Work?
Splunk is a log management, search, correlation, and data visualization tool. More institutions are starting to use this type of predictive analytics tool to better understand the large amounts of machine (i.e., log) data being generated across the institution. Better analyzing this data means that more informed business decisions can be made across the institution.

Splunk works by collecting large amounts of data and then analyzing that data to find patterns within the data. Various Splunk tools can then display that data in charts, graphs, and dashboard visualizations based on parameters entered by staff members (e.g., time period, source, or other data elements). Splunk is a highly customizable tool, and there are a number of different apps and add-on tools to help users make sense of the data analyzed by Splunk.

Who Might Use Splunk, and Why?
Higher education institutions use Splunk because they want to analyze and make sense of their operational environment and data in order to solve problems, troubleshoot potential problems, and define metrics or key performance indicators.

Like any operational intelligence tool, Splunk has a number of practical uses for IT departments. For instance, operational staff can identify and investigate potential information security incidents more quickly in order to implement alerts and mitigation solutions across campus. In another example, development teams can have access to Splunk data (instead of raw log data) to troubleshoot production system issues. This protects the integrity of log data, but gives development teams the information that they need to solve problems. A well-thought-out Splunk implementation allows security departments to quickly and easily answer their chief information officer’s questions about security threats in the institution’s IT environment.

The Benefits and Risks of Using Splunk
The main benefit of using Splunk is that it is efficient and saves staff time. The closest analogy is that it is “like Google, but for log data.” It allows for powerful searches and correlations to be quickly accessible to all users with simple commands. For advanced users, Splunk offers the ability to correlate diverse data sources and build dashboards for insight that was not possible prior to Splunk.

The biggest risk in using Splunk is an improper installation that does not make good use of system resources and leads to poor performance. A Splunk environment needs to be highly redundant as it will become a critical infrastructure tool, and it may be necessary to rearchitect a Splunk cluster to meet user expectations as use of the tool grows. It is also important to ensure that an institution has enough storage space available to retain log data for as long as necessary to meet institutional policies or other regulatory requirements. Finally, some Splunk plug-ins for visualizations are created by the user community, which means that sometimes they are not updated or maintained appropriately.

What Resources Are Needed to Deploy Splunk?
Splunk has two deployment options: on-premises deployment and a dedicated cloud option that is run in Amazon Web Services. Within the two main deployment options, there are many configurations
available. Splunk has a great documentation site to help users understand deployment options for their institution (e.g., how to scale a Splunk deployment).

Splunk is not a free tool. It offers a number of different licensing and subscription models. An institution will need to review the options, and understand its deployment strategy, in order to select the best licensing or subscription model.

A Splunk discussion list is available for the higher education community as an additional resource.

**Splunk Applications**

Below is a list of popular Splunk tools that an institution might consider implementing. Institutions should evaluate which tool works best for their own unique purposes. Neither EDUCAUSE nor HEISC recommends the use of a particular tool; institutions should use these tools at their own risk.

- Azure Technology Add-on (TA)
- Cisco Security Suite
- Crashplan TA
- Microsoft TA
- Palo Alto TA
- S.o.S–Splunk on Splunk
- Splunk App for Active Directory

**List of Institutions That Use Splunk**

- Arizona State University
- Baylor University
- Ohio State University
- University of Texas
- University of Nevada, Las Vegas
- Washington State University
- University of Alabama at Birmingham
- University of Arkansas
- University of Michigan

---

**Sustain and Improve Your Privacy and Information Security Programs**

The **Higher Education Information Security Council** (HEISC) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs.