# Operational Intelligence for Educational Institutions

*Robert H Reed*
*Worldwide Education Evangelist*
*12 July 2012*

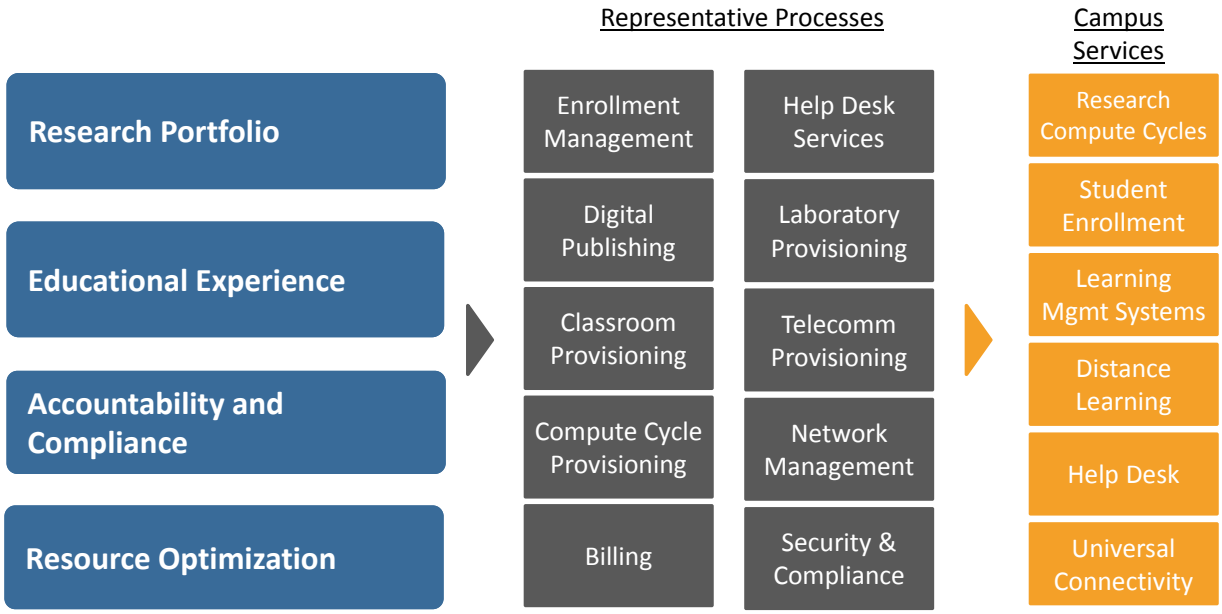
# 300+ Educational Institutions Use Splunk




splunk> Listen to your data.

# Areas of Strategic Focus Areas for Education

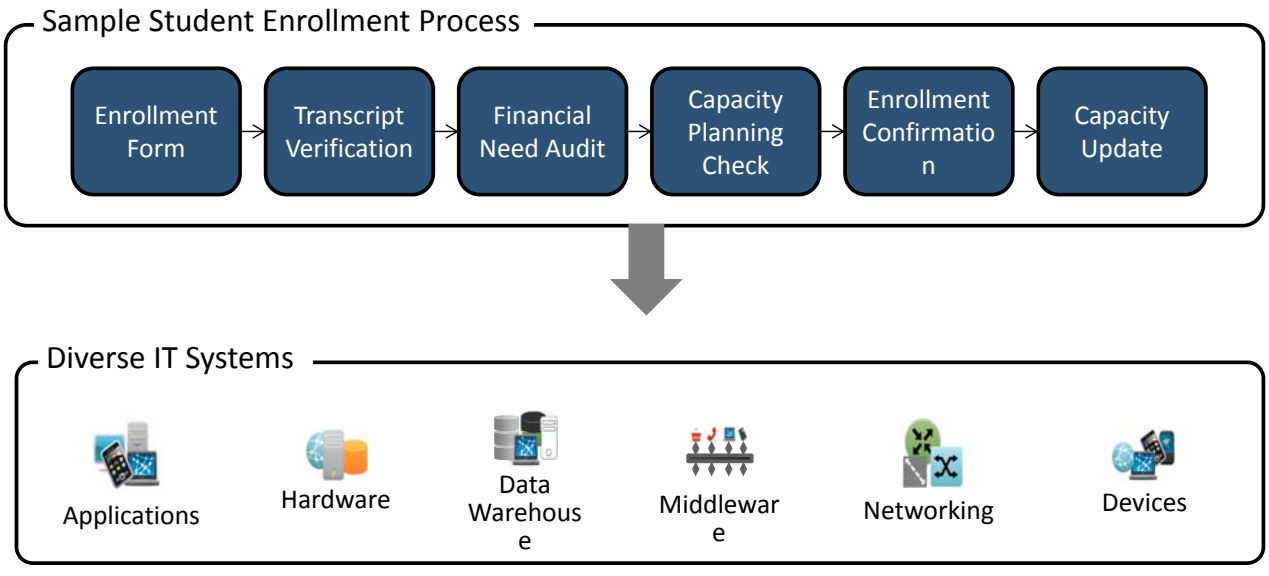
## Diverse Processes Support Diverse Campus Services



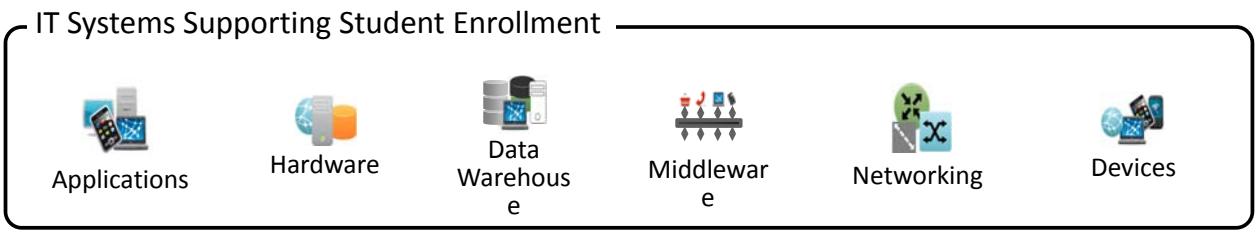





# Processes and Services Supported by Diverse IT Systems



# Getting Visibility Across Systems is Challenging

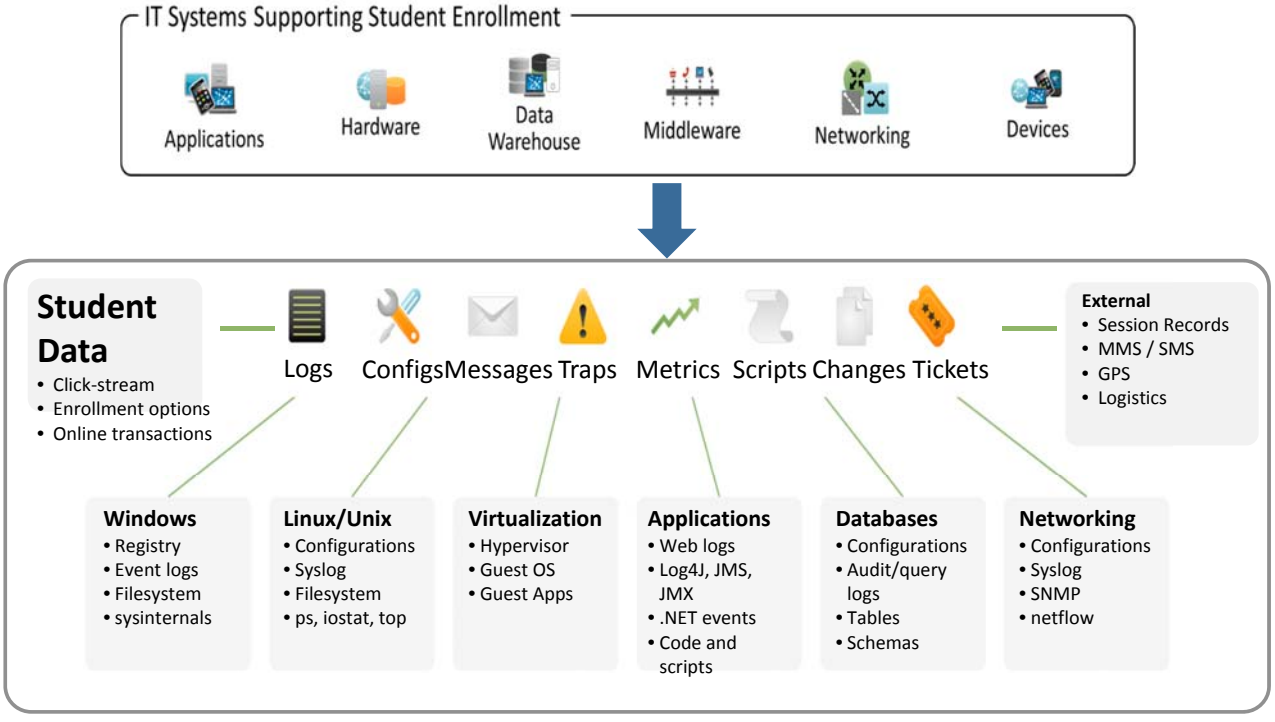



- Search & Identify
- Monitor Systems
- Operational Visibility
- Business Insights

- What caused the delay in enrollment completion?
- How long did it take to complete the transaction?
- How many forms are abandoned and at what point?
- What types of devices are accessing enrollment pages?
- When are the peak student enrollment times?
- What is the *real* peak processing capacity of the system?




# IT Systems Generate Large Amount of Data



# What is Splunk?

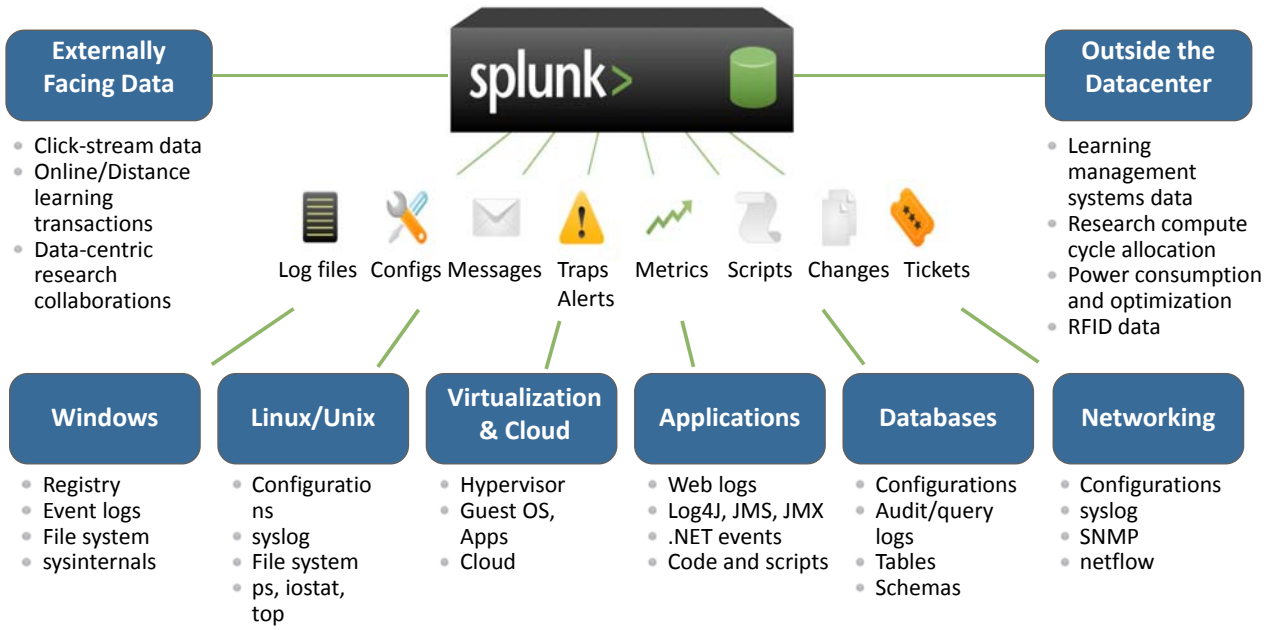
Collects, indexes and harnesses your machine-generated IT data to identify problems, risks and opportunities
and drive better decisions for IT and the institution



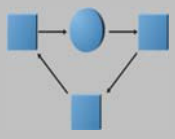


# Splunk: The Engine for Machine Data

Turns Machine Data into Insights to Support Institutional Objectives

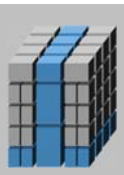


# What's Different About Machine Data



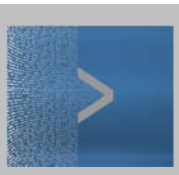
Relational Databases

- Financial records, manufacturing and logistical information, personnel data
- Data highly structured — database highly structured
- Inflexible schema, long deployment cycle



Multidimensional Databases

- Multidimensional data for business management and statistics
- Math computation strength – dense data
- Pivots data for flexible analysis
- Monthly reporting or research summarization, not for real-time events



Engine for Machine Data

- Time series unstructured data, with no predefined schema
- Generated by all IT systems, non-standard data, unpredictable formats
- Massive volume; fast navigation and correlation paramount





# Delivering Operational Intelligence

Single Data Store | Single UI | Across Use Cases

## Three Primary Capabilities

### Search/Navigate

- Data drilldown
- "Needle in a haystack"
- Root cause analysis/troubleshooting
- Incident investigations

### Real-time Visibility

- Live dashboards
- Event correlation
- Monitoring and alerting
- Performance issues
- Transaction levels
- SLA tracking

### Historical Analytics

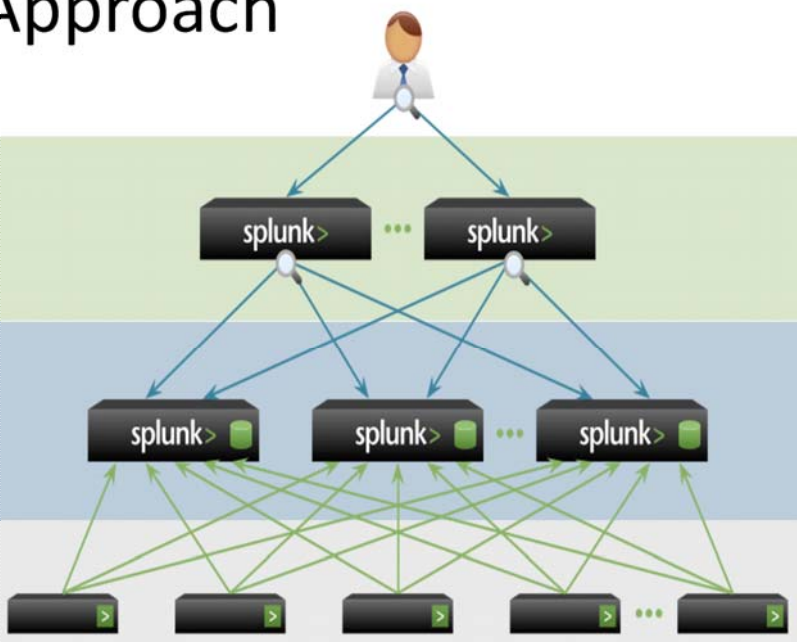
- Baseline and thresholds
- Trending
- Operational insights
- Historical patterns
- Compliance reports

# The Splunk Approach

**Flexible Reporting and Analysis**

**Real-time Indexing**

**Universal Collection**




Rapid time-to-deploy: hours or days

splunk>





splunk®

Make machine data accessible, usable and valuable to everyone.

# Leading Global Universities Drive Results with Splunk

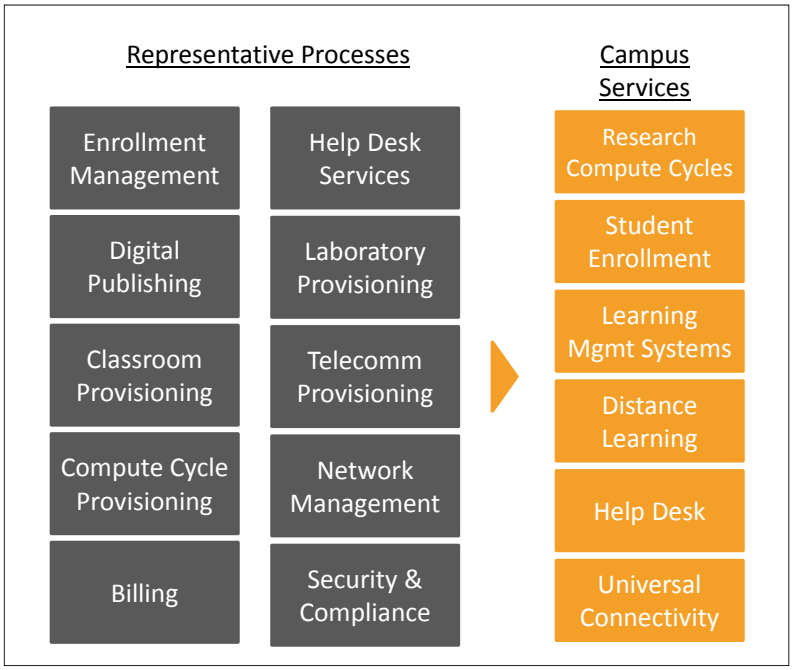
| | |
|---|---|
| Berkeley | Splunk for visibility into configuration, change, and security events across its infrastructure |
| Nanyang Technological University | Splunk for single search across logs and devices for better security tracking and response |
| The University of Texas at Austin | Splunk for analysis of IT security events, exposures and attacks across the University of Texas System |
| The Open University | Splunk for PCI compliance needs |
| Georgetown University | Splunk for continuous monitoring and pro-active alerting of IT infrastructure |
| LSU | Splunk for log centralization across Windows and Unix servers to replace their homegrown solution |




# Splunk Delivers Operational Intelligence to Education

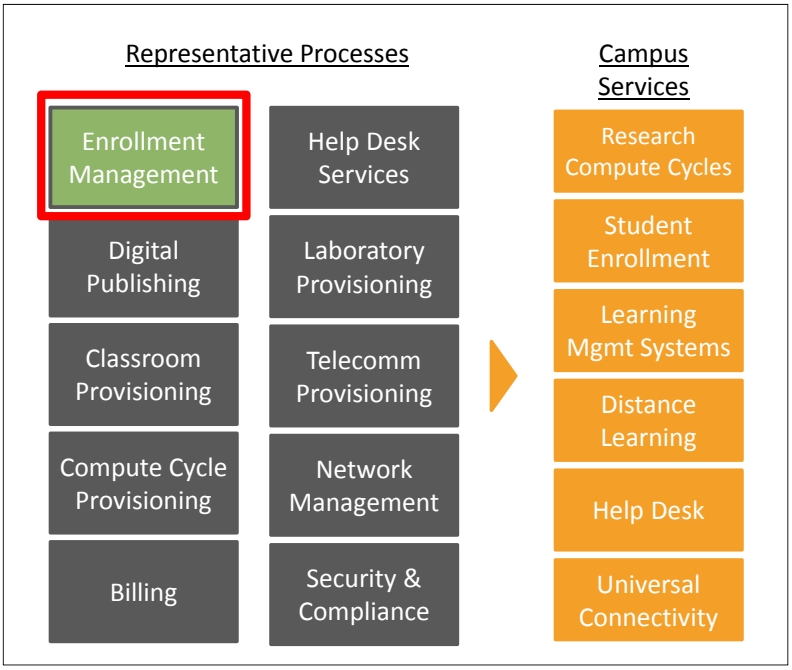
## Across Diverse Processes and Services

splunk>



# Splunk Delivers Operational Intelligence to Education

## Across Diverse Processes and Services





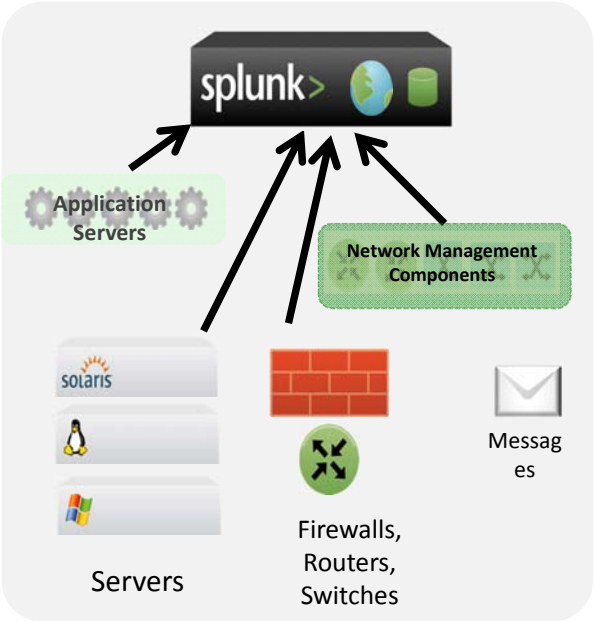



# Large State School on East Coast of US

## Using Splunk to manage loads from course registration

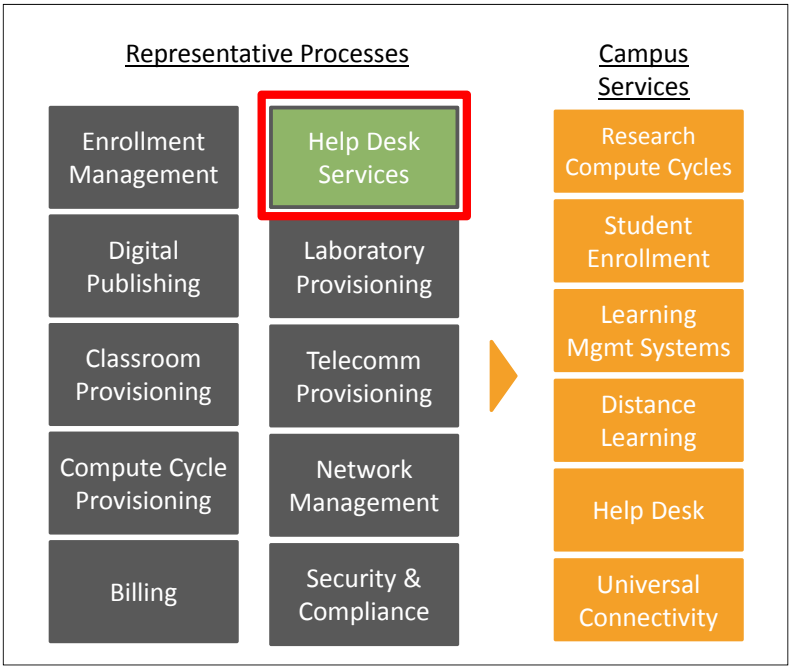
- Class registration stresses infrastructure (1000 hits per second peak loads)
- Splunk dashboards indicate spikes, anomalies, and errors
- Allows IT staff to dig into applications and components to understand where problems lie
- Splunk grabs performance data for graphing and correlation with load and error data

**"We get paid by course credit—downtime could mean loss of revenue."**



# Splunk Delivers Operational Intelligence to Education

## Across Diverse Processes and Services

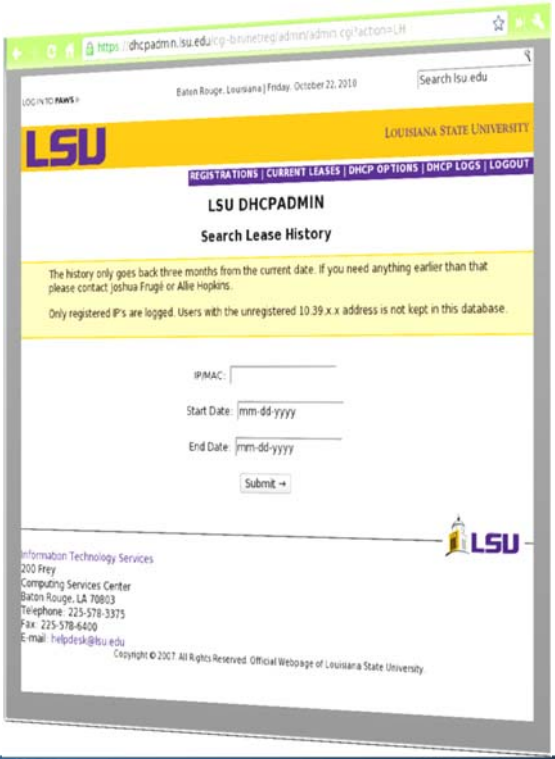







# Empowering the Help Desk at Louisiana State University

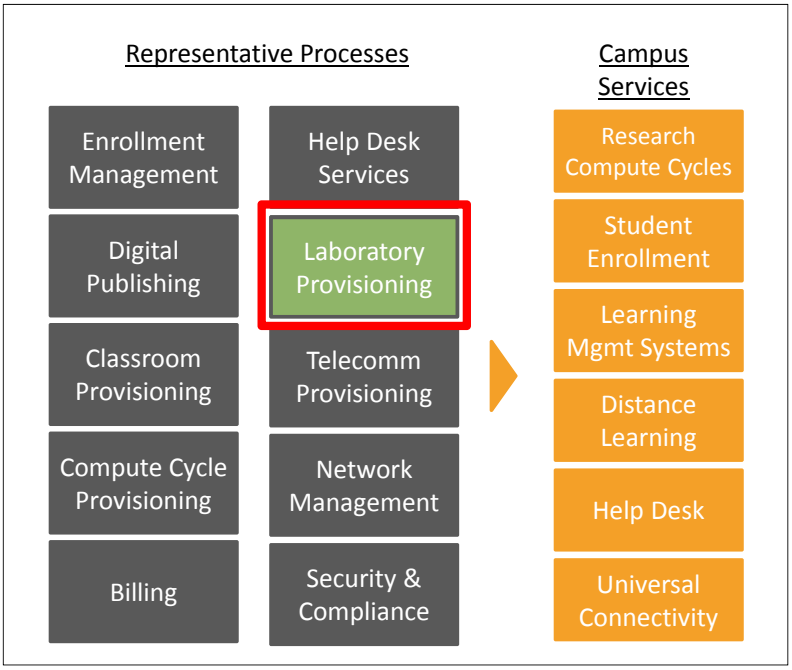
- Splunk makes Help Desk staff self-sufficient by providing direct, secure access to the data they need
- Splunk search functionality helps them find the data they need with little training or expertise
- Saved valuable IT time and resources for the campus




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

# Splunk Delivers Operational Intelligence to Education

## Across Diverse Processes and Services

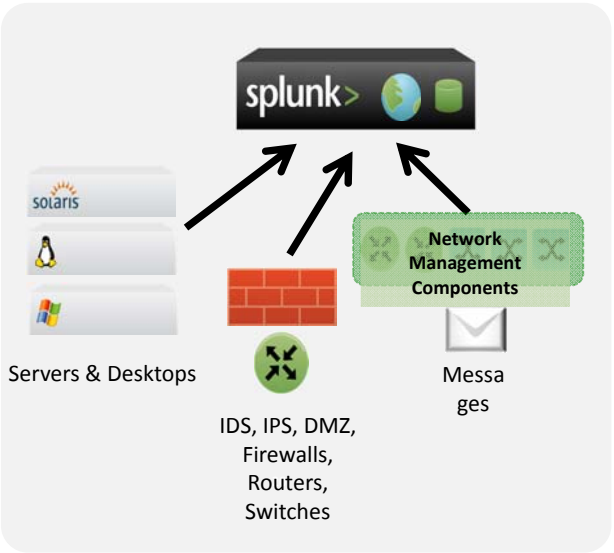





# Large University in the Southeast US

## Splunk to address challenges with labs and logging infrastructure

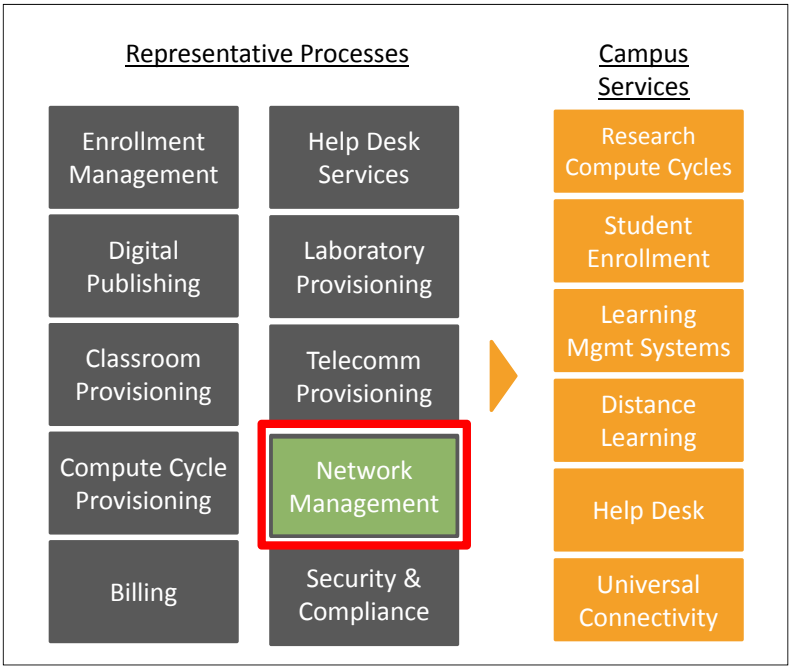
- Classroom Support uses a Splunk-generated report to track student lab usage
- Splunk search empowers end users; database expertise not required to get results
- Point and click drill down reinforces intuitive approach
- Free-text search often produces serendipitous results ("look what I found!" moments)




**"Splunk's quicker and easier to use than other tools and you get more contextual info from it."**

# Splunk Delivers Operational Intelligence to Education

## Across Diverse Processes and Services

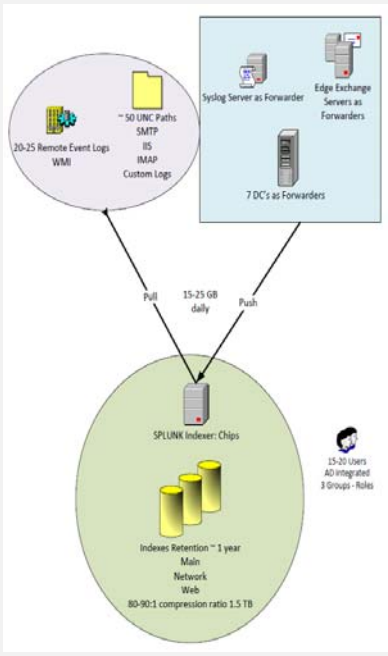







# Cost savings throughout the institution at Winona State

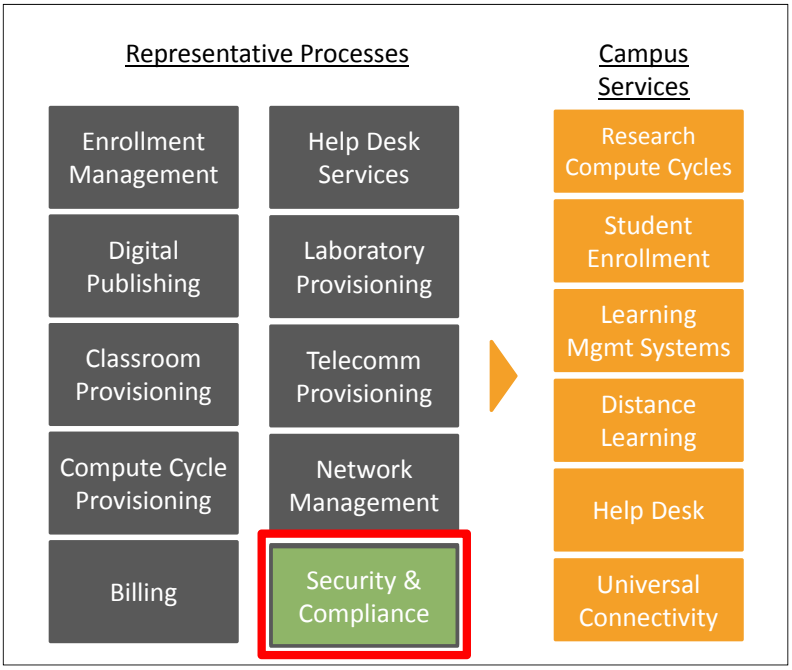
- Began using Splunk for easier searching/archiving of schemaless log files for compliance purposes
- Helps with allocation of under-utilized network assets
- Graphs and tracks printer usage
- Identifies top internal network attacks
- RIAA takedowns take 15-30 minutes, saving hundreds of labor hours per year




Basic network architecture

# Splunk Delivers Operational Intelligence to Education

## Across Diverse Processes and Services







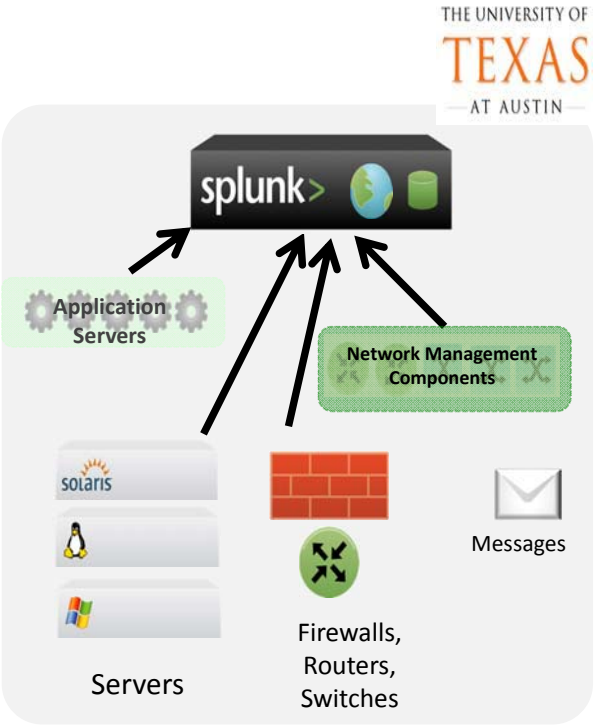

# Splunk at The University of Texas

**Splunk used for**

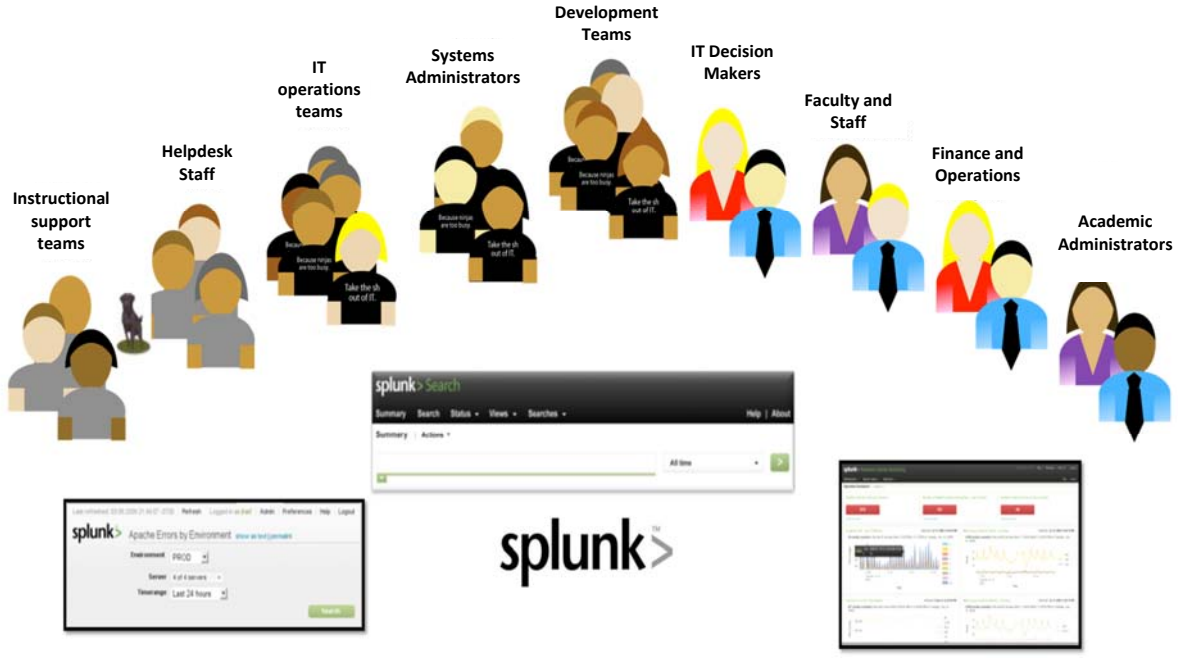
- Threat identification and control
- Outbreak management
- Campus-wide innovation
- Value-add Splunkbase apps

**Business Impact**

- **Saves hundreds of hours per year** in security analyst time by automating workflows and providing faster insight into events and anomalies
- **Reduces organizational risk** by preventing costly network breaches and negative publicity
- **Reduces incident investigation time** by providing fast access and analysis of log data from any source
- **Improves security posture** by filtering out false positives and providing data visualization
- **Avoids loss of intellectual property**
- **Ensures uptime and service continuity** by catching unknown threats and new zero-day attacks



# New levels of visibility for IT and the institution








# What Makes Splunk Different?

## Any Data

- Any format of data, from any source
- Full access to 100% of data for months/years
- Cradle-to-grave data management

## Completely Flexible

- Supports any analysis, reporting or monitoring across IT silos
- Highly flexible dashboards present any view for any user
- Adapts to change—schema-on-the-fly design supports new or unexpected data

## Rapid Results

- Installs in minutes
- Can get started small and grow over time—from laptop to datacenters
- Realize value in weeks not months or years

**Splunk: The Engine for Machine Data**

splunk>

# Machine Data Insight Delivers IT Efficiencies

## Benefits Gained by Splunk Customers in Education

splunk>


- Improve Security
- Increase Research Productivity
- Ensure Compliance
- Deliver Effective Learning Technologies
- Detect Network Abuse
- Enable Robust Content Delivery
- Enhance Campus Services
- Positive Bottom-Line Impact for Institution





# Splunk Community

- Get answers from the Splunk community: (http://splunk-base.splunk.com/answers/)
- Find and share Splunk apps (http://splunk-base.splunk.com/apps/)
- Splunk blogs: (http://blogs.splunk.com/)
- Splunk ninja dojo (http://splunkninja.ning.com/)
- Local events and user groups (http://www.splunk.com/page/events)

# Splunk Classes & Certifications

Overview of classes

http://www.splunk.com/view/education/SP-CAAAAH9

USING SPLUNK
SEARCH & REPORT
ADMINISTRATING SPLUNK
DEPLOYING SPLUNK
DEPLOYING APPS with SPLUNK

Videos

**http://www.splunk.com/view/education-videos/SP-CAAAGB6**

Search and schedule classes

**http://inter.viewcentral.com/events/cust/default.aspx?cid=splunk&pid=1**





# Teach Splunk?


140,000–190,000 more deep analytical talent positions needed

and

1.5 million more data-savvy managers needed to take full advantage of big data *in the United States*

Contact *rreed@splunk.com*

*Source: McKinsey Global Institute, May 2011: Big data: The next frontier for innovation, competition, and productivity*
*http://www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf*

# 4,000+ Licensed Customers in 75+ Countries