Cisco and Splunk: Under the Hood of Cisco IT

Robert Novak, Cisco Big Data Partner CSE

George Lancaster, Engineer, Cisco IT

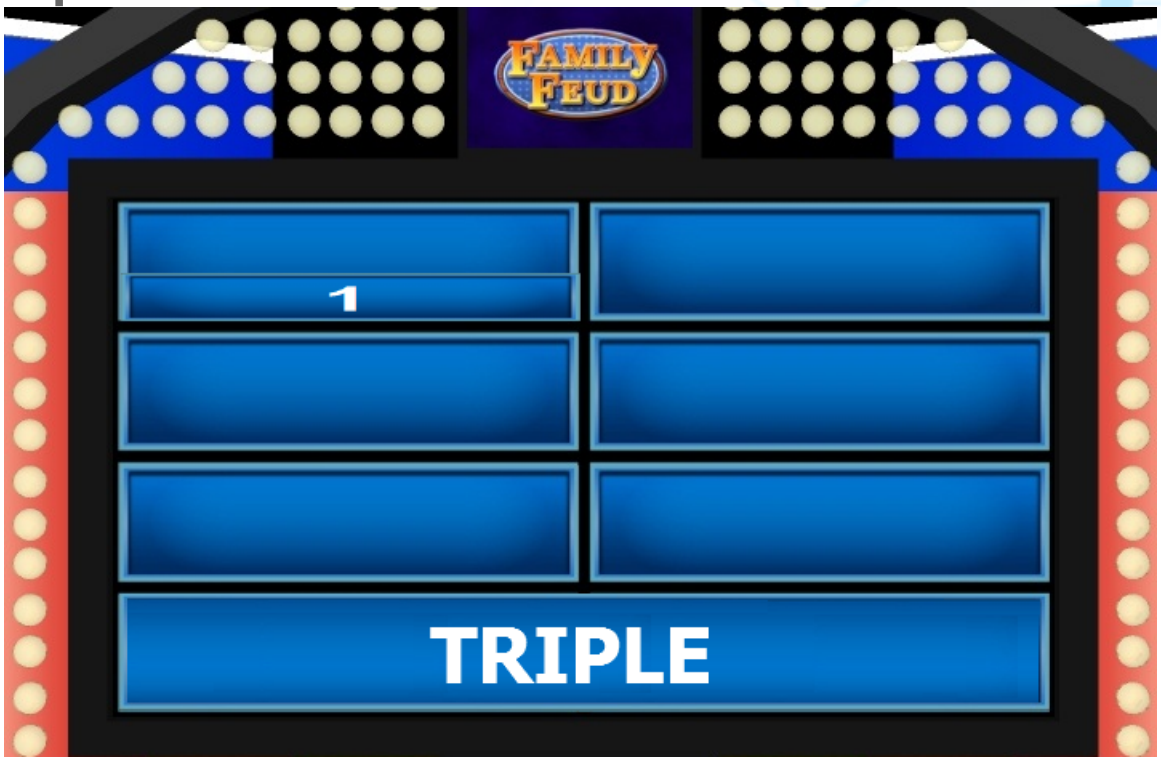
September 2015

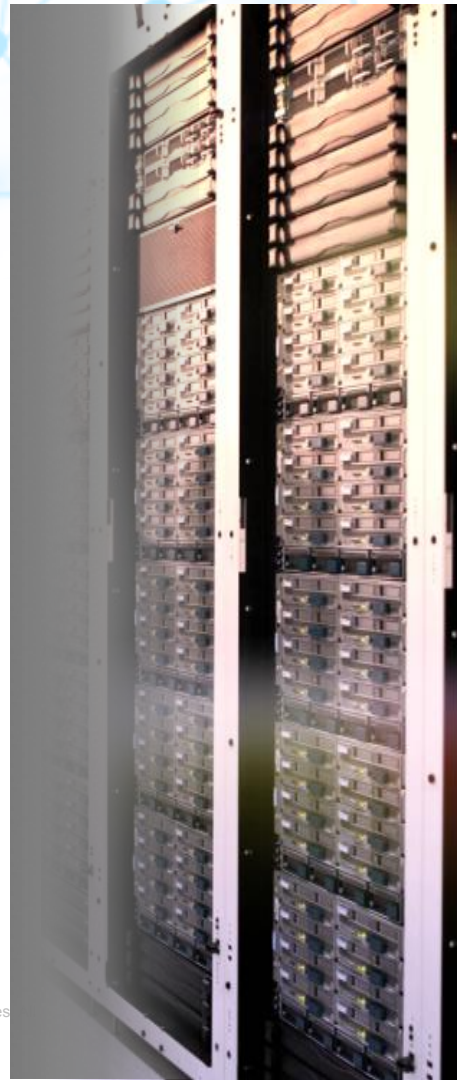
Agenda

- Cisco's History with Splunk
- How Cisco Uses Splunk
  - IT Operations
  - Security Analytics
- There's an App for that!
- Splunk + Cisco UCS = Better Together
- Learn More

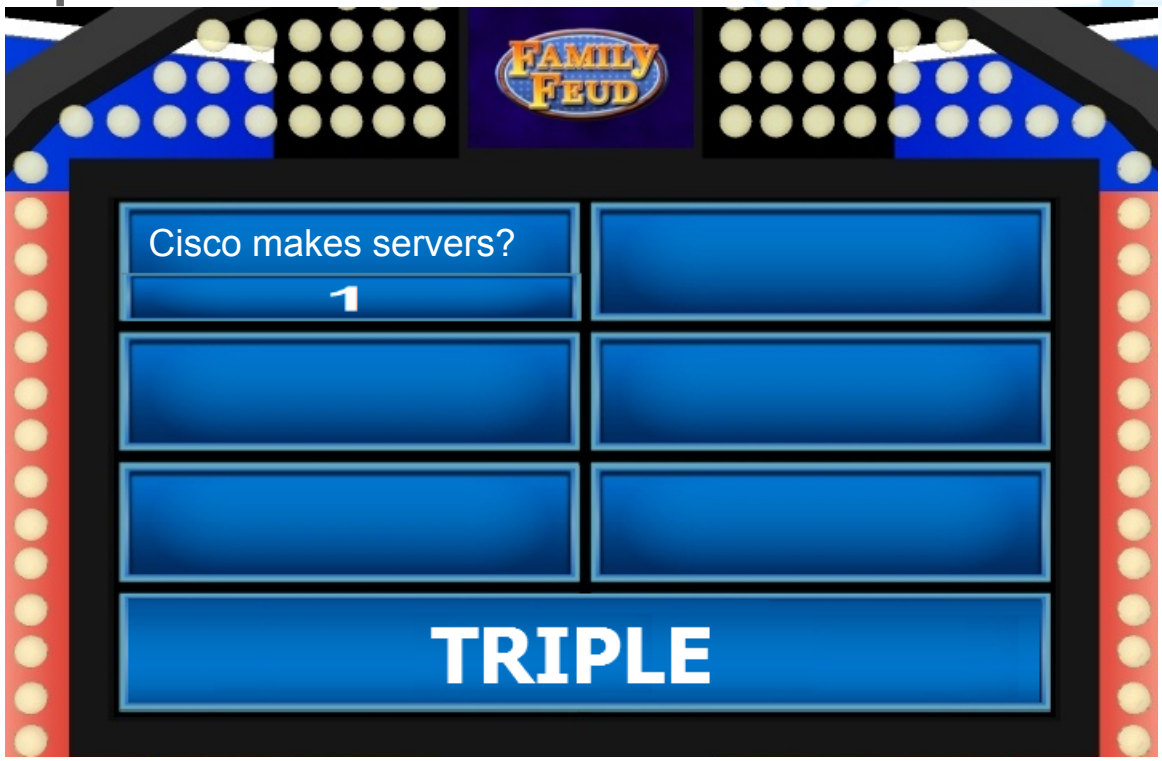
Would you like to play a game?

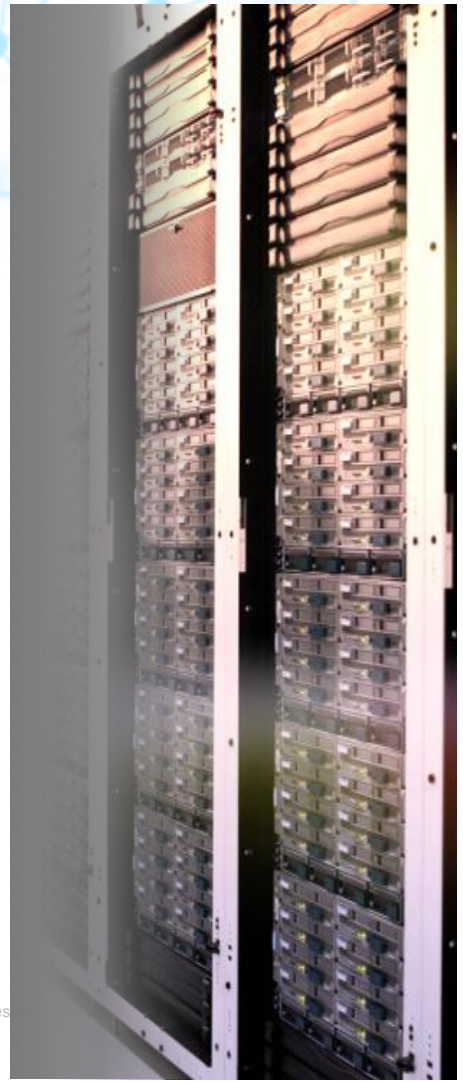
Top 3 Questions



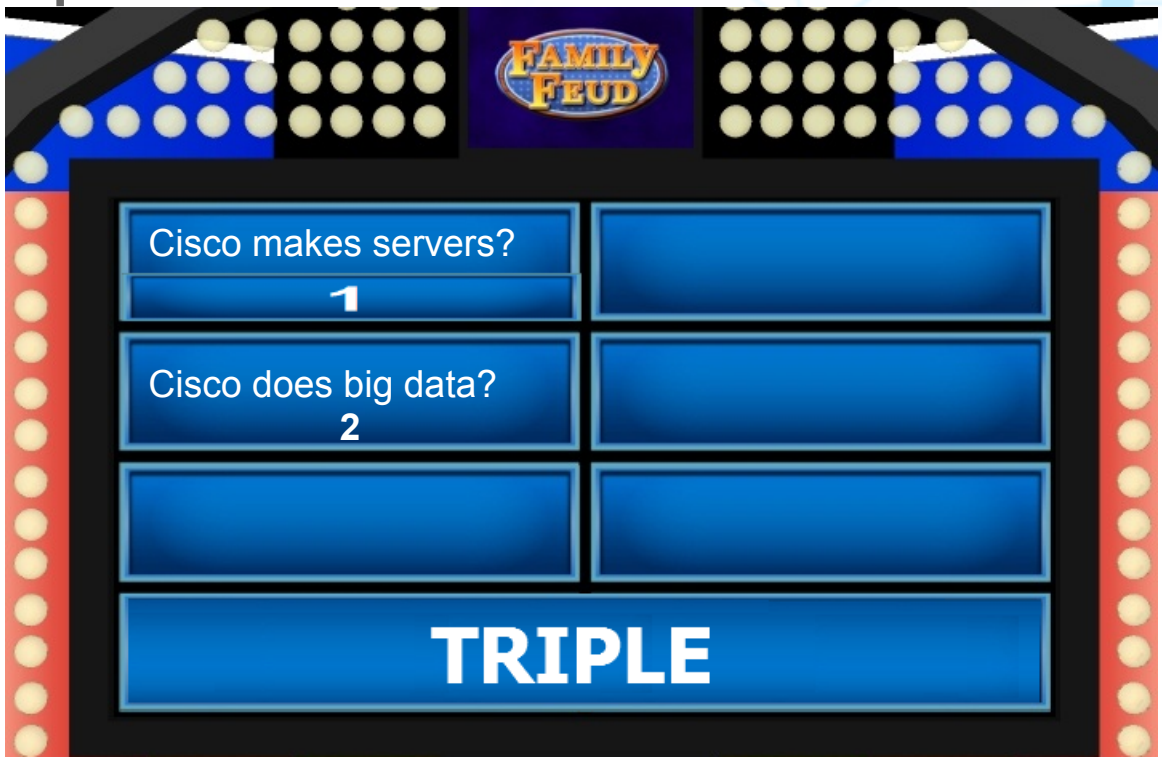


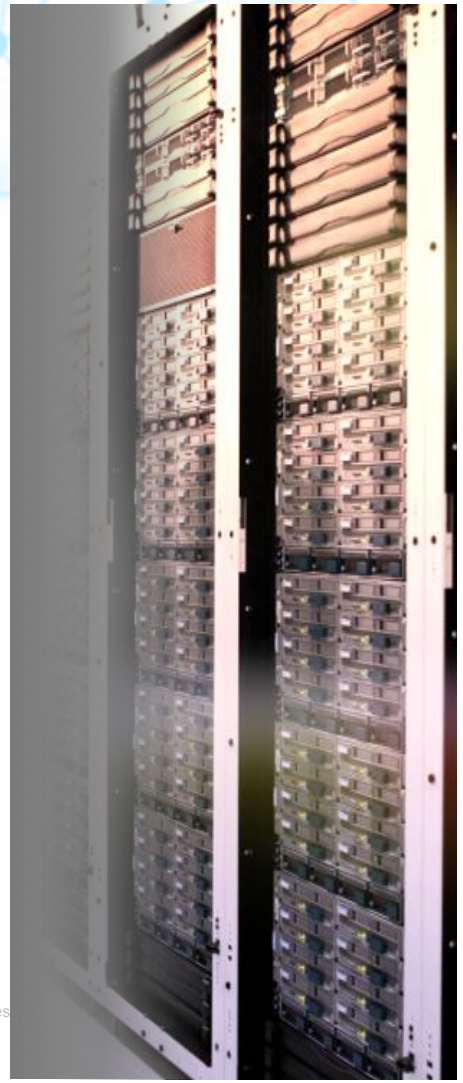
Top 3 Questions



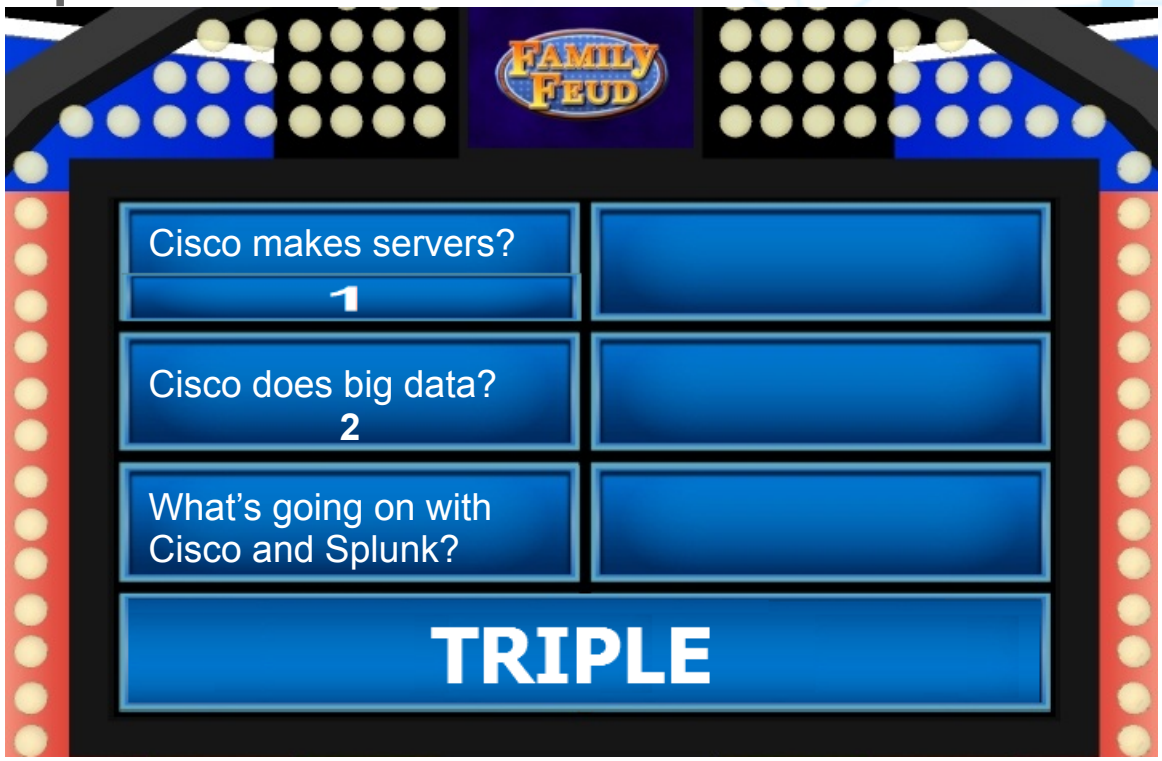


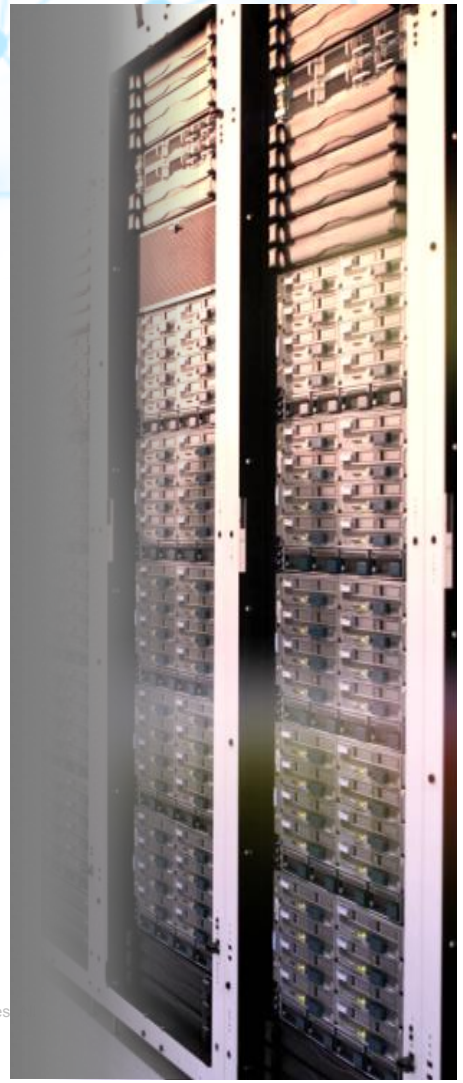
Top 3 Questions





Top 3 Questions





Funny you should ask…

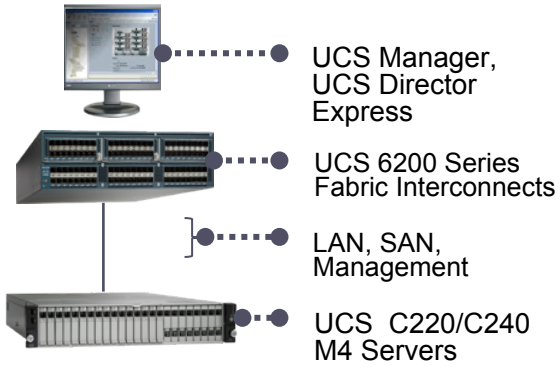
Big Data & Analytics – Gain Insight from your Data

Data is the lifeblood of any applications and business. While the real value is in the analytics and the ability of a company to use that intelligence to gain a desired business outcome

Data Analytics with Splunk on Cisco UCS

Splunk drives operational insights and outcomes for our customers on Cisco UCS Infrastructure

splunk>

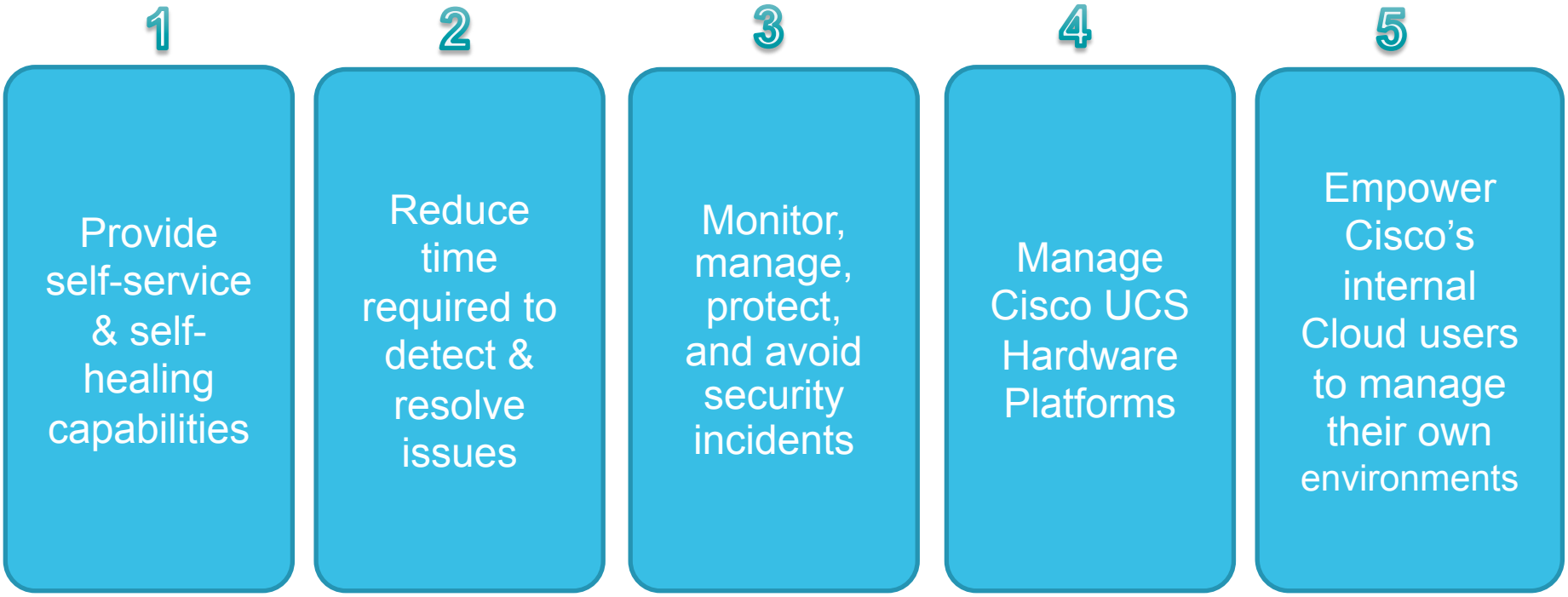


Cisco's Footprint with Splunk

How Cisco Uses Splunk

Data Analytics with Splunk on Cisco UCS for Cisco's IT Operations

Cisco IT Operations Challenges



Cisco's IT Operations Results

"Splunk pulls data from all the logs and gives our operations teams a single place to look and work together to solve problems."

— Piyush Bhargava, Distinguished Engineer, Cisco IT

- ✓ **Proactive monitoring** enables **50% reduction** in high priority issues
- ✓ **80% reduction** in operational costs
- ✓ **90% improvement** in problem resolution and root cause analysis times
- ✓ Improvements in system stability, availability and performance

IT Operations @ Cisco

Cisco IT uses Splunk to index a broad range of system logs and machine data for networking devices, operating systems, unified communications, video events, and applications.

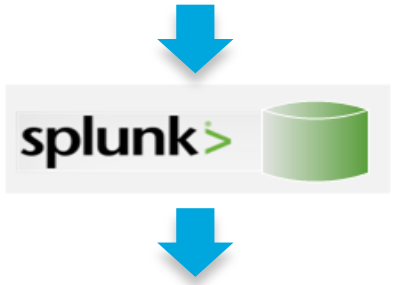
- ✓ Aggregated multiple siloed systems into Splunk
- ✓ Monitoring 70+ Applications
- ✓ 846% increase of search volume per day in one year
- ✓ Operational Intelligence in minutes rather than hours

Don’t take my word for it…

Cisco's Splunk Environment

Insights Across Cisco - Platform

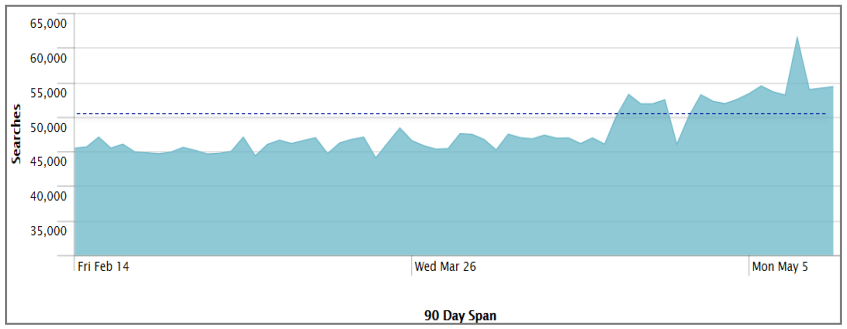
Business Unit	Platform	SPLUNK App	Sources and Logs				
			SYSLOG	Windows	Active Directory	ACS	Storage
• Infra Structure • IT OPS • Security • Commerce • Sales & Marketing • Channels • Engineering • Webex	• CCIX (web + app) • FTP • RAC DB • WSG • PING • OBIEE • ACE	• Splunk on Splunk • Deployment Monitor • UCS App • JMX App • Unix App • NetApp App	• Network • Linux / Unix • UCS • VMWare ESXi • Datacenter battery / temperature logs	• Pre-Prod Event Logs • Production Event Logs	• Event Logs	• Event Logs • AAA Logs • ISE Logs	• Event Logs



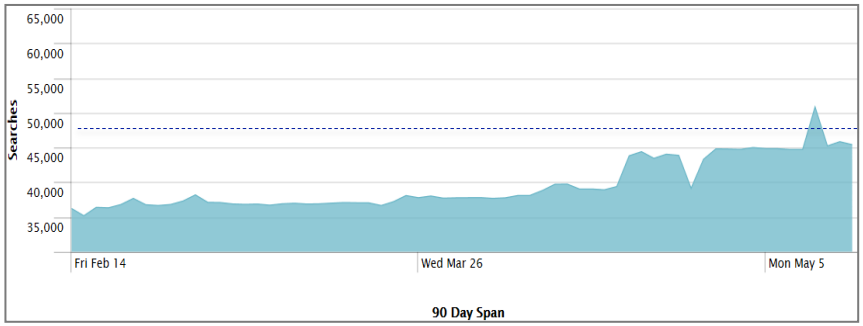
Search Heads	Indexers	Storage	Data Center
• 16 VMs (64 core X 32 GB)	• 20 VMs (16 core X 16 GB) • 70 + Unique Indexes	• 56 TB SAN – Hot & Warm • 28 TB NAS - Cold	• Prod: RCDN – 8 SH & 10 Indexers • Prod: ALLEN – 8 SH & 10 Indexers • Dev: RTP – 4 SH & 2 indexers

Splunk Searches – Daily Average

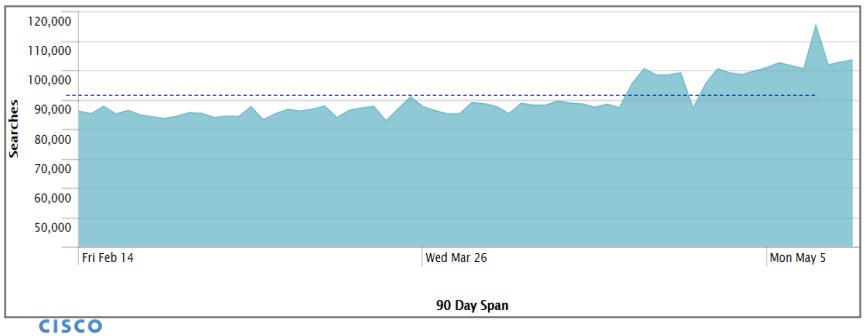
1. Interactive Searches = 55K+



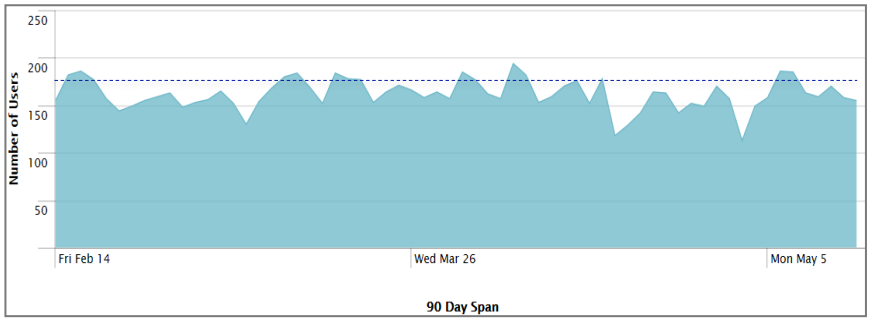
2. Scheduled Searches = 45K+



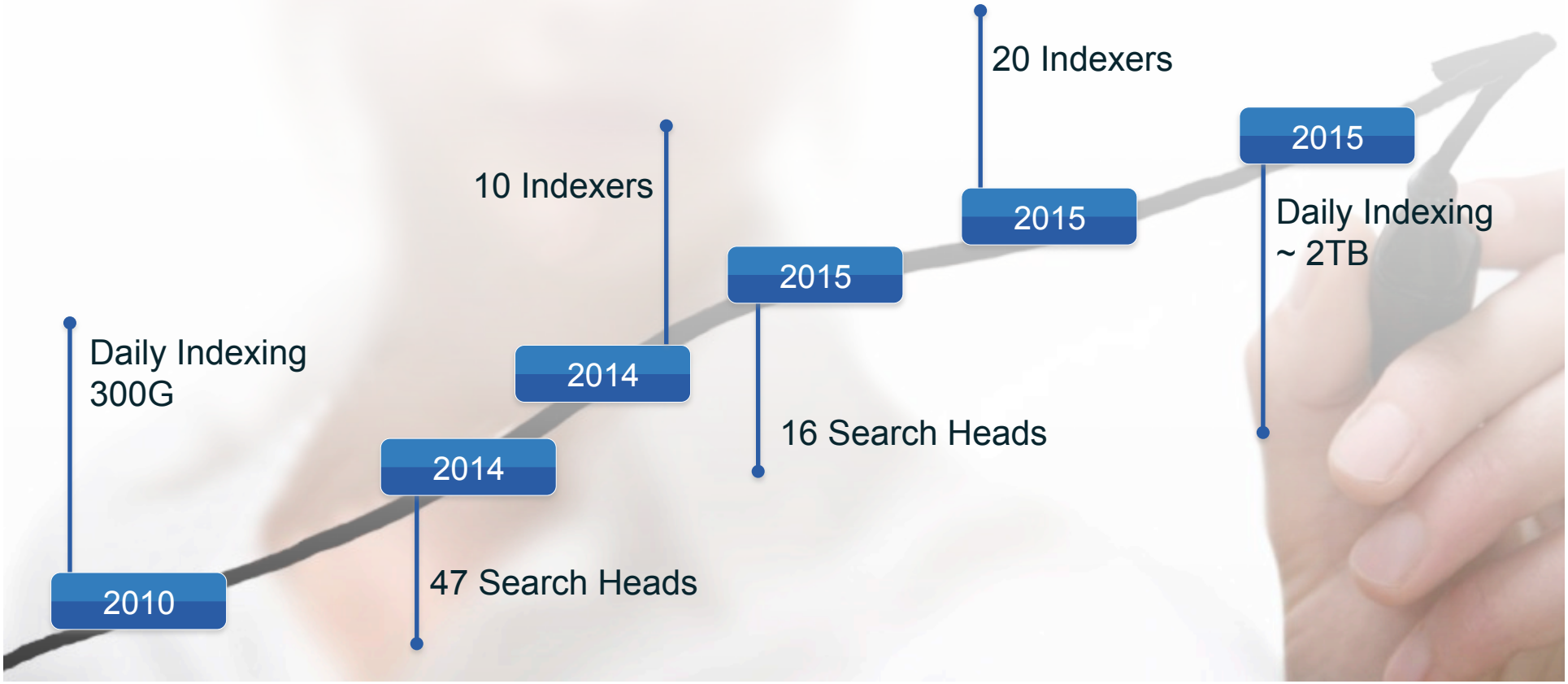
3. Total Searches = 100K+

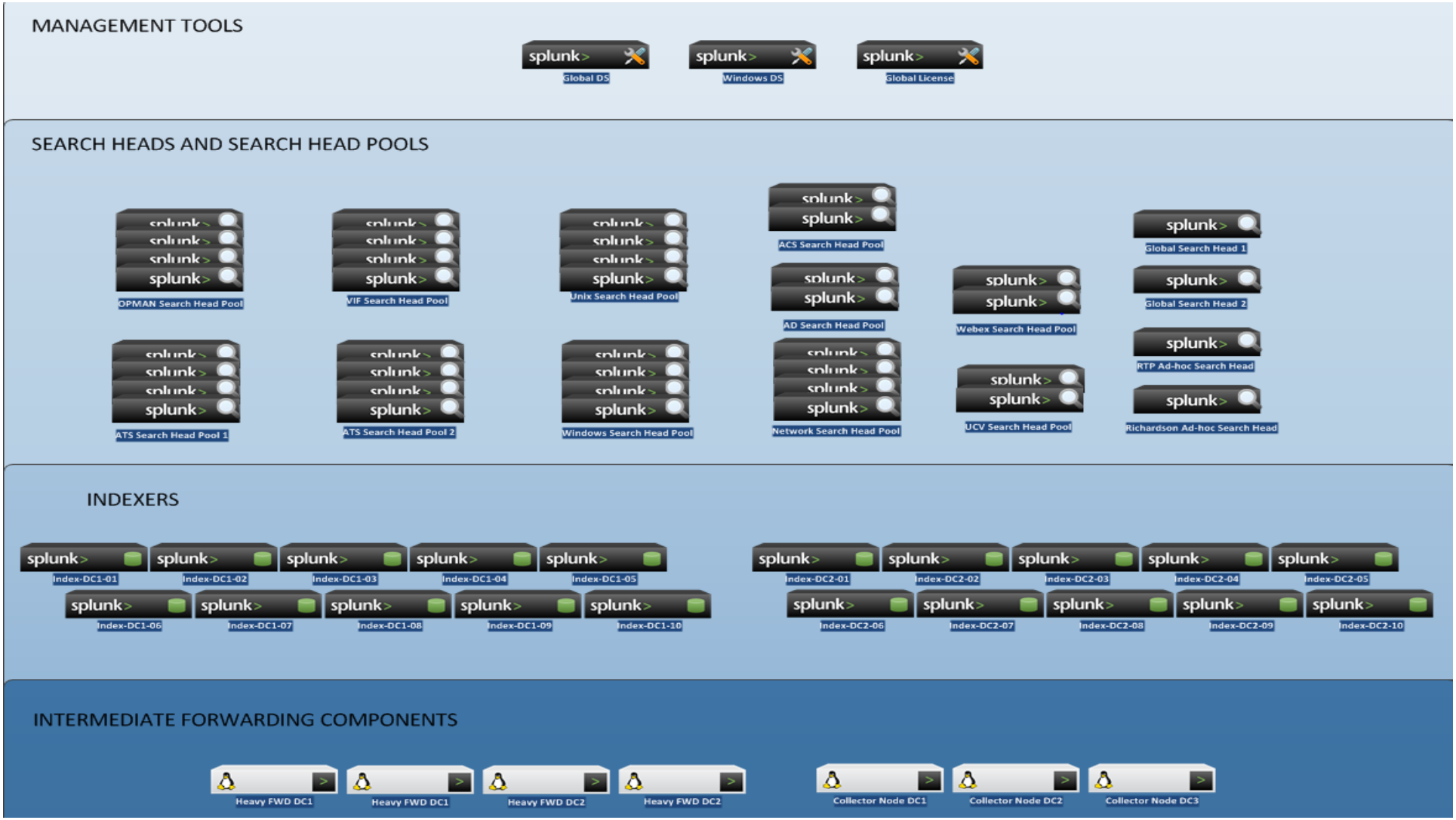


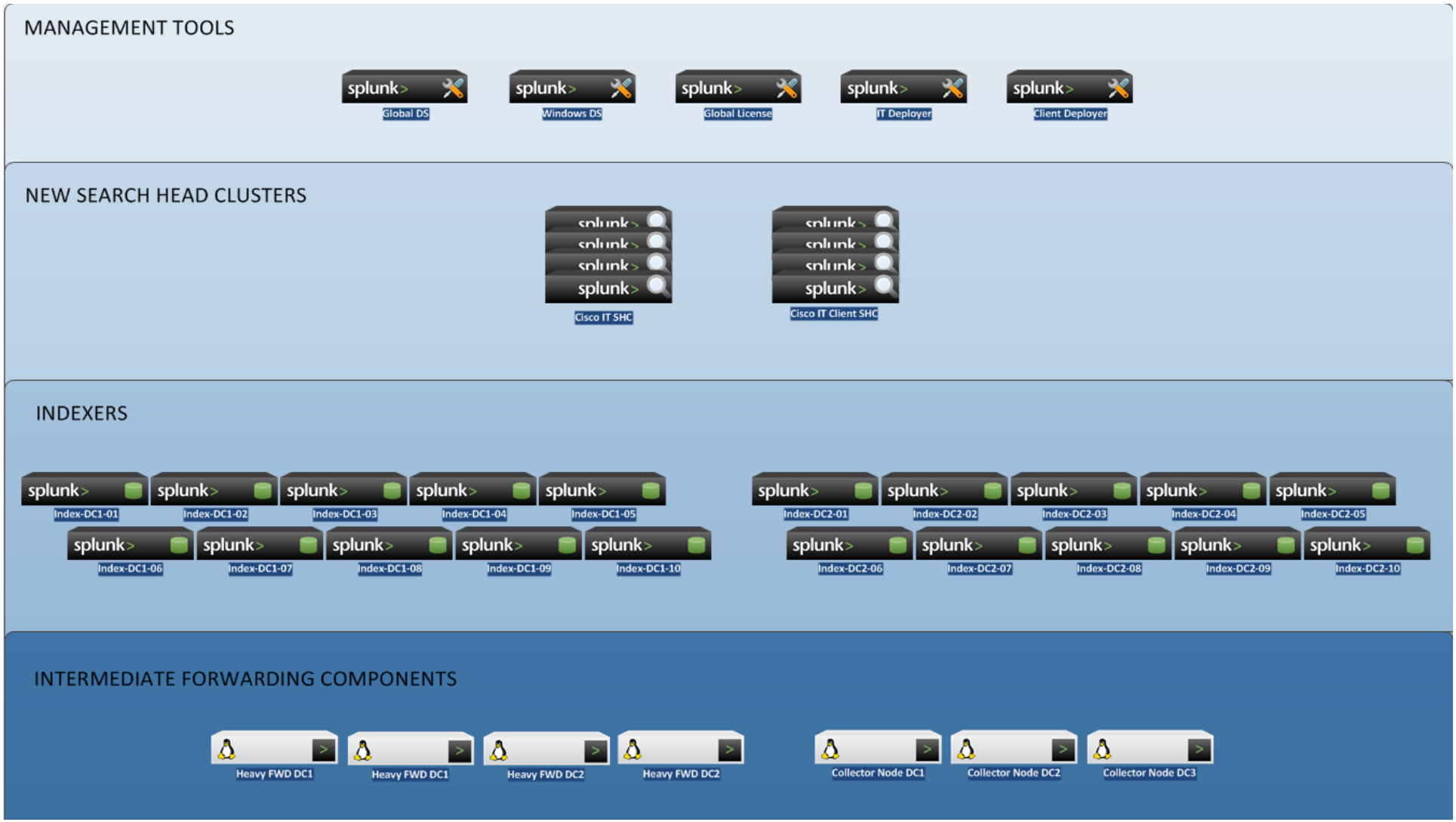
4. Number of Users = 180+



Cisco's IT Operations Evolving with Splunk




MANAGEMENT TOOLS
Global DS
Windows DS
Global License
SEARCH HEADS AND SEARCH HEAD POOLS
OPMAN Search Head Pool
VIF Search Head Pool
Unix Search Head Pool
ACS Search Head Pool
AD Search Head Pool
Webex Search Head Pool
Global Search Head 1
Global Search Head 2
RTP Ad-hoc Search Head
Richardson Ad-hoc Search Head
ATS Search Head Pool 1
ATS Search Head Pool 2
Windows Search Head Pool
Network Search Head Pool
UCV Search Head Pool
INDEXERS
Index-DC1-01
Index-DC1-02
Index-DC1-03
Index-DC1-04
Index-DC1-05
Index-DC1-06
Index-DC1-07
Index-DC1-08
Index-DC1-09
Index-DC1-10
Index-DC2-01
Index-DC2-02
Index-DC2-03
Index-DC2-04
Index-DC2-05
Index-DC2-06
Index-DC2-07
Index-DC2-08
Index-DC2-09
Index-DC2-10
INTERMEDIATE FORWARDING COMPONENTS
Heavy FWD DC1
Heavy FWD DC1
Heavy FWD DC2
Heavy FWD DC2
Collector Node DC1
Collector Node DC2
Collector Node DC3


MANAGEMENT TOOLS
Global DS
Windows DS
Global License
IT Deployer
Client Deployer
NEW SEARCH HEAD CLUSTERS
Cisco IT SHC
Cisco IT Client SHC
INDEXERS
Index-DC1-01
Index-DC1-02
Index-DC1-03
Index-DC1-04
Index-DC1-05
Index-DC1-06
Index-DC1-07
Index-DC1-08
Index-DC1-09
Index-DC1-10
Index-DC2-01
Index-DC2-02
Index-DC2-03
Index-DC2-04
Index-DC2-05
Index-DC2-06
Index-DC2-07
Index-DC2-08
Index-DC2-09
Index-DC2-10
INTERMEDIATE FORWARDING COMPONENTS
Heavy FWD DC1
Heavy FWD DC1
Heavy FWD DC2
Heavy FWD DC2
Collector Node DC1
Collector Node DC2
Collector Node DC3

Data Analytics with Splunk on Cisco UCS for Security Analytics

Using Splunk @ Cisco CSIRT

About CSIRT

- Cisco Computer Security Incident Response Team (CSIRT)
- CSIRT = Security Monitoring and Incident Response
- Architecture, Engineering, Research, and Investigations
- Enterprise global threat and 24x7 incident response

CSIRT Environments Recent Snapshot

- ✓ 300 locations in 90 countries
- ✓ 400 buildings
- ✓ 1500+ labs
- ✓ 100,000+ employees on network
- ✓ 50-300 malware-related cases opened in a typical week
- ✓ 650,000+ ip devices on network
- ✓ 130,000 windows hosts
- ✓ 50,000 Linux hosts
- ✓ 40,000 routers
- ✓ 2-3 million highly tuned ids events per day
- ✓ 10+ billion netflow records per day

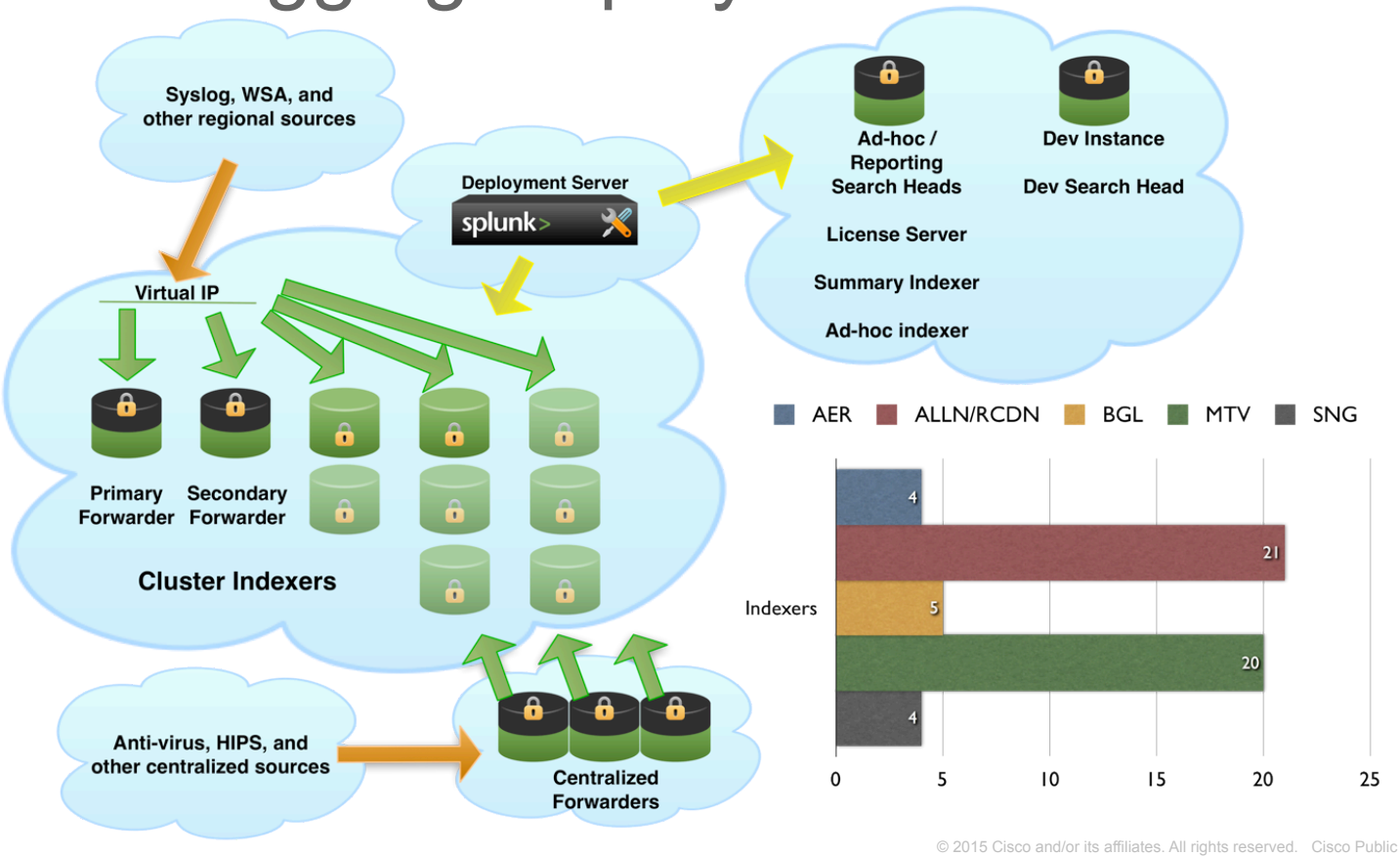
Replacing a SIEM @ Cisco

- Challenges: SIEM could not meet security needs
  - Very difficult to index non-security or custom app log data
  - Serious scale and speed issues. 10GB/day and searches took > 6 minutes
  - Difficult to customize with reliance on pre-built rules which generated false positives

Replacing a SIEM @ Cisco, cont'd

- Enter Splunk: Flexible SIEM and empowered team
  - Easy to index any type of machine data from any source
  - Over **60 users doing investigations**, correlations, reporting, advanced threat detection
  - All the data + flexible searches and reporting = empowered team
  - 2TB/day and searches take less than a minute. 7 global data centers with 350TB stored data
  - Flashback Malware Example
  - Estimate Splunk is 25% the cost of a traditional SIEM

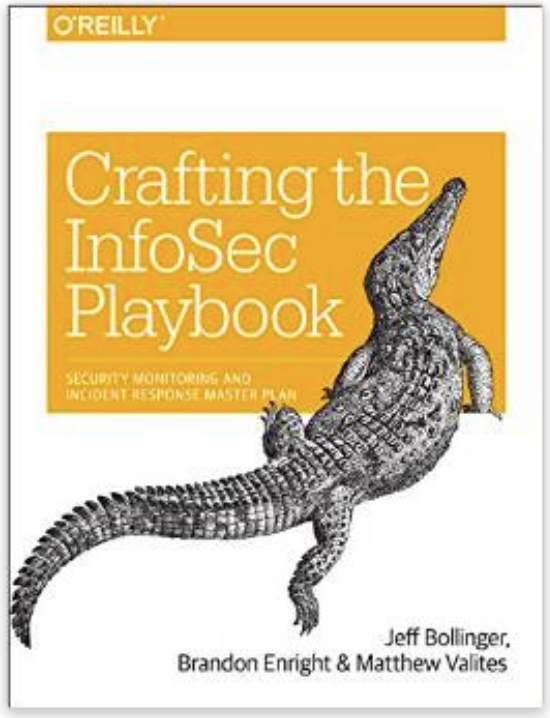
CSIRT Logging Deployment



Cisco Security Analytics Results

- **33 percent reduction** in the time required to conduct security investigations
- All security data is readily available in a single, **centralized portal for faster and simpler access**
- Substantially easier correlation allows for **more thorough investigations**
- Ability to **automate routine tasks** and search log data allows CSIRT analysts to work more effectively

“And they wrote the book …”



Cisco’s CSIRT engineers applied their experiences during the CSIRT deployment to a new O’Reilly book now available at most booksellers

bitly.com/infosecplaybook

29

There’s an app for that…
(or a technology add-on, at least)

Splunk Apps for Cisco Environments

Splunk app for Enterprise Security

120+ security apps & add-ons

- Cisco ASA
- MobileIron
- Cisco ESA
- OSSEC
- Cisco WSA
- NetFlow Logic
- Cisco ISE
- Active Directory
- Sourcefire
- Bit9 ETD
- Cisco Security Suite
- Norse Darklist

500+ apps/add-ons

- Cisco ACI, IOS, Nexus 9000
- Cisco UCS
- VMware
- NetApp
- Servicenow
- UNIX/Linux

splunk>

Splunk App for Cisco UCS

- **NEW AND IMPROVED as of May 28, 2015**
- Aggregates, monitors, trends and analyzes all relevant data from Cisco UCS Manager instances
- Enables proactive capacity and performance monitoring/ management, fault trending, power and cooling, and more
- Works with other Splunk add-ons and data sources (including Enterprise Security and PCI Compliance add-ons) to aggregate and correlate data across your enterprise

Splunk on Cisco UCS

What is Cisco's Unified Computing System (UCS)?

Unified Management: UCS Manager uses policy-based configuration to ensure consistent deployments

Unified Fabric: Integrated 10 Gigabit Ethernet and Storage Networking (FCoE/iSCSI)

Service Profiles: Maintain consistency across batches of servers and multiple applications. Deploy and expand in record time.

Performance: Built with 10GbE at the core, 40GbE available, repeatable configurations and performance, and over 100 benchmark records

Why Splunk on Cisco UCS?

Time to Deployment: Spin up a mutually validated, pre-tested environment in minutes rather than days or weeks

Total Cost of Ownership: Integrated networking and management reduce customer cost and effort to migrate, deploy, and expand

Time to Grow: Expand servers and network capacity quickly and consistently

Cisco UCS + Splunk = Better Together

Seamless Scalability Facilitates Rapid Growth

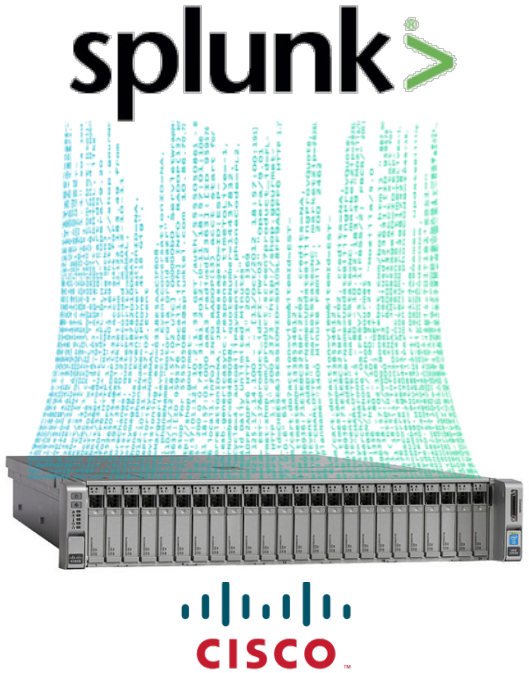
- Scale Splunk from a single server to distributed/clustered deployment
- Grow your clusters efficiently and consistently
- Runs on the same UCS C-Series servers as other big data platforms

Split Second Response Times

- Exceptional performance for “needle-in-a-haystack” searches
- **Consistent performance** as simultaneous users increase

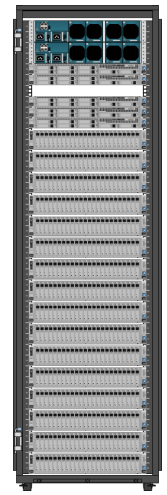
Simplified **Repeatable Deployments**

- Four pre-tested UCS Integrated Infrastructures
- Capacity or performance optimization
- NEW! Cisco Validated Design (CVD) with HA and Archiving



Cisco UCS Reference Architectures

	Single Server	Clustered Deployment
Retention optimized	250 GB indexed per day 4 months retention	Up to 4TB indexed per day 1 year Retention
Performance optimized	250 GB indexed per day 1 month retention	UP to 4TB indexed per day 3 months Retention



Cisco Validated Design (CVD) for Splunk

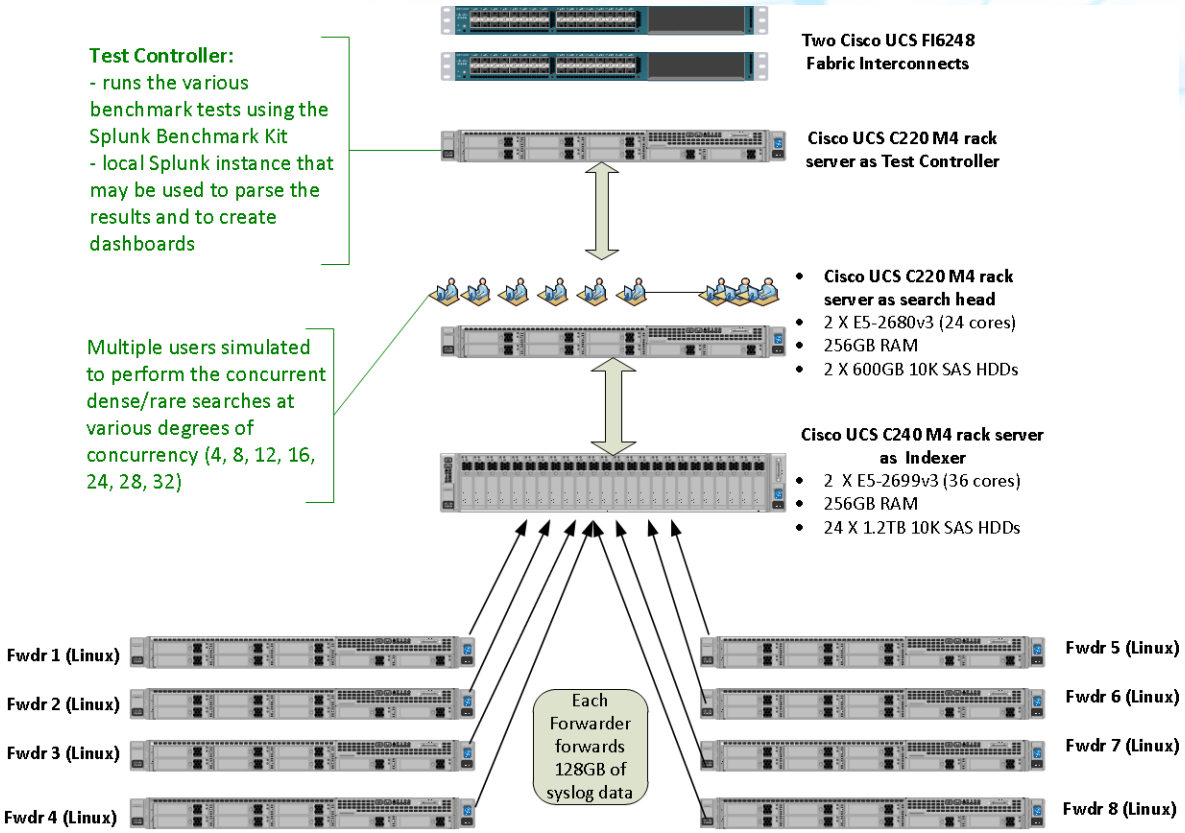
- Developed by Cisco and Splunk engineers in Spring 2015
- 250+ page guide to design and deployment, pallet to production
- Based on UCS C-Series (C220, C240, C3160) servers and Splunk Enterprise software
- Includes high availability & data archiving
- Download for free at cisco.com/go/bigdata_design

Cisco UCS Integrated Infrastructure for Big Data with Splunk Enterprise

With Cluster Mode for High Availability and Optional Data Archival

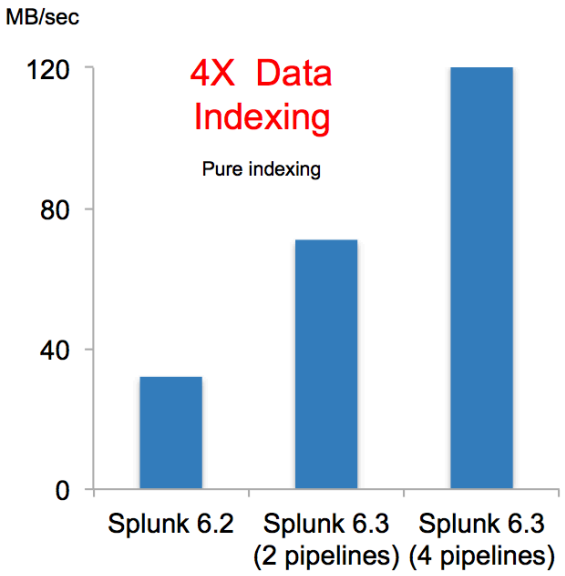
Last Updated: June 8, 2015

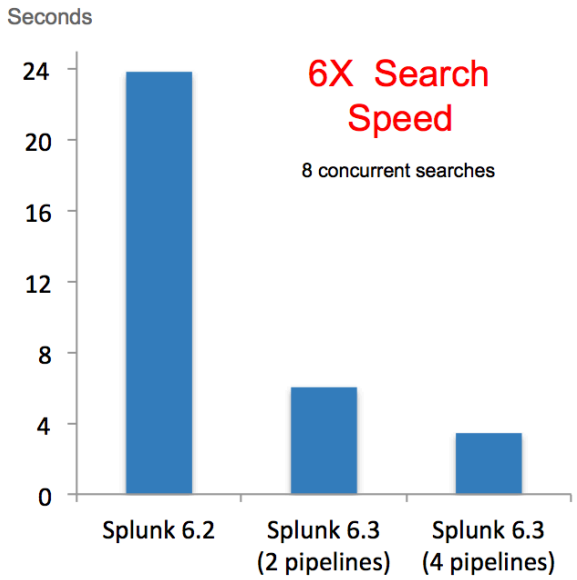
Splunk on UCS : Performance Benchmark Test bed Topology

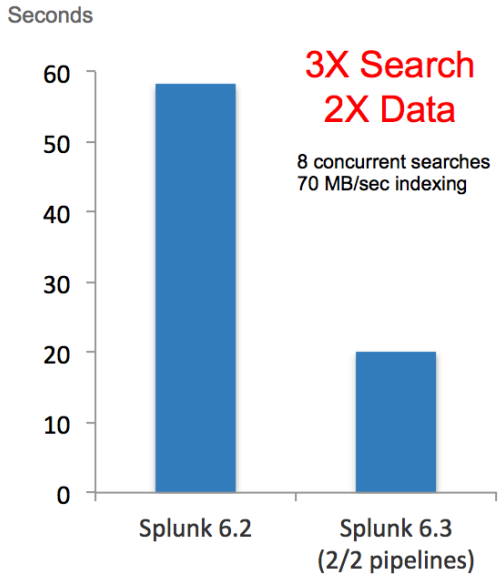


NOTE: Each forwarder forwards about 128GB of raw syslog style event data to the Indexer

Splunk – Cisco UCS Benchmark Results (6.2 v/s 6.3)







Learn more about Splunk and Cisco UCS

Learn More About Splunk on Cisco UCS!

SplunkBase app resources: splunkbase.splunk.com

Cisco's Big Data Design Hub: cisco.com/go/bigdata_design
features Cisco Validated Designs (CVDs) and other architectural docs

Big Data Applications Hub: cisco.com/go/bigdata
features reference architectures, solution briefs, infrastructure, automation, etc.

Thank you.


CISCO
TOMORROW starts here.

Cisco Big Data & Analytics Solutions

Data Management:
Build the Foundation

Cisco and Hadoop partners providing a lower cost & scalable storage platform to capture and analyze new & traditional data

Data Warehouse Optimization:
Save Millions

Offload data and move ETL processing from expensive EDW to low cost Hadoop leveraging Cisco Data Virtualization for easy access

Data Analytics:
Turn Data into Business Outcomes

Cisco and strategic analytics ISV's to gain insight from your data for competitive business advantage