splunk> .conf2017

Drive more value through data source and use case optimization

BEST PRACTICES FOR SHARING DATA ACROSS THE ENTEPRRISE

David Caradonna | Director, Global Business Value Consulting

Date | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf2017

Personal introduction

David Caradonna

Director of Global Business Value Consulting

Splunk> since Nov 2013

Overview

David delivers Enterprise Value Plans to C-Level executives who require assistance with business cases and data source strategies that align with strategic initiatives.

David previously ran the Value Management Office at HP Software for 6 years, and as a seasoned IT executive, David holds 25 years of IT experience in various leadership and IT life cycle functions.

25 years IT Experience; **9 years** Value Consulting; **200+** Splunk Engagements;

Today's Presentation

1. Business Value Consulting at Splunk
2. Top Value Drivers
3. Data Source Strategy
4. Summary / Q&A

Business Value Consulting at Splunk

Help customers document the **projected** and **already realized business value** of making machine data accessible, usable, and valuable for everyone

Common Deliverables:

- CFO-Ready Business Case
- Value Realization Workshops
- Data Source Strategies
- Usage Maturity & Staffing Readiness
- Enterprise Adoption Roadmaps

2000+

Engagements Worldwide Since 2013

Common Questions

- What data should we index?
- How can we use this data?
- What value can we realize?
- Cloud vs. On-premises?

- Can data be reused across groups?
- Who else can benefit from this data?
- Do we have the right skills to scale?

- How much value are we realizing today?
- Are we underutilizing Splunk?
- Are we indexing the right data?
- Can we get more value from our data?

- How do we compare with other customers?
- How can we plan our next adoption phase?

splunk> .conf2017

Key Value Drivers

As reported by Splunk Customers through 2000+ engagements worldwide

IT Operations & App Support

70-90% reduction in incident investigation time

15-45% reduction in high priority incidents

67-82% reduction in business impact

5-20% increase in infrastructure capacity utilization

Security & Compliance

70-90% faster detection and triage of security events

70-90% faster investigation of security incidents

70-90% reduction in compliance reporting time

10-50% lower risk of data breach, IP theft and fraud

Application Development

70-90% reduction in time for QA test failure analysis

70-90% reduction in time for pre-prod defect investigation

80-90% faster development of reports and dashboards

10-50% improvement in time to market

splunk> .conf2017

Key Data Sources

Documented through 2000+ engagements worldwide

IT Operations & App Support

70-90% reduction in incident investigation time

15-45% [illegible]priority

67-82% [illegible]ss

5-20% increase in infrastructure capacity utilization

25+ data sources

Security & Compliance

70-90% faster detection and triage of security events

70-90% [illegible]n of

70-90% [illegible]iance

10-50% lower risk of data breach, IP theft and fraud

40+ data sources

Application Development

70-90% reduction in time for QA test failure analysis

70-90% [illegible]for pre-[illegible]ation

80-90% [illegible]of [illegible]boards

10-50% improvement in time to market

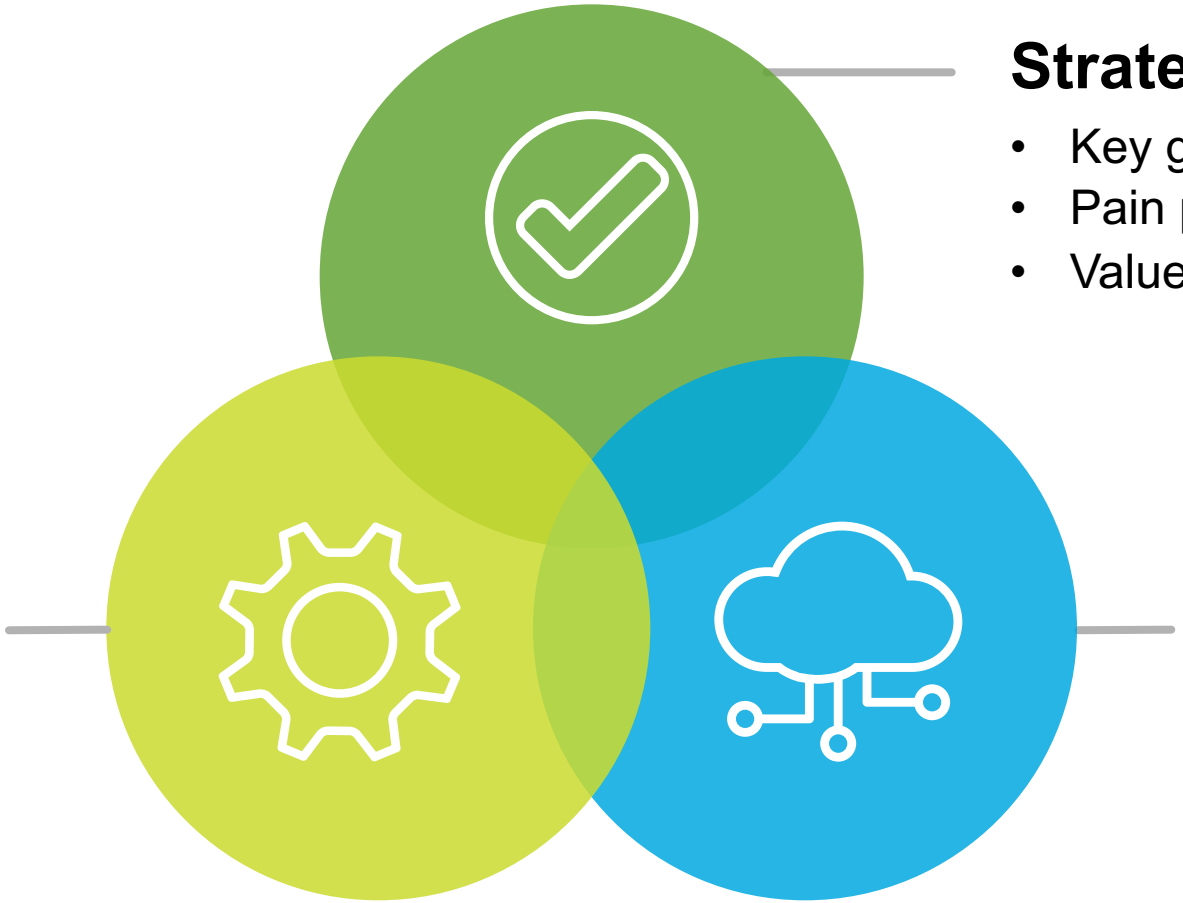
25+ data sources

splunk> .conf2017

Ingredients for a Successful Data Strategy

Strategic initiatives

- Key goals
- Pain points
- Value drivers



Your data

- Inventory of your configured items
- Available data sources in your environment by item

Data Mappings

- Between groups and common data sources
- Between common data sources and key use cases, correlation rules, dashboards, killchain, ITIL, CSC 20, etc…

Simple Best Practice Steps

Step 1

Identify key goals and use cases to be addressed by your data source strategy

Step 2

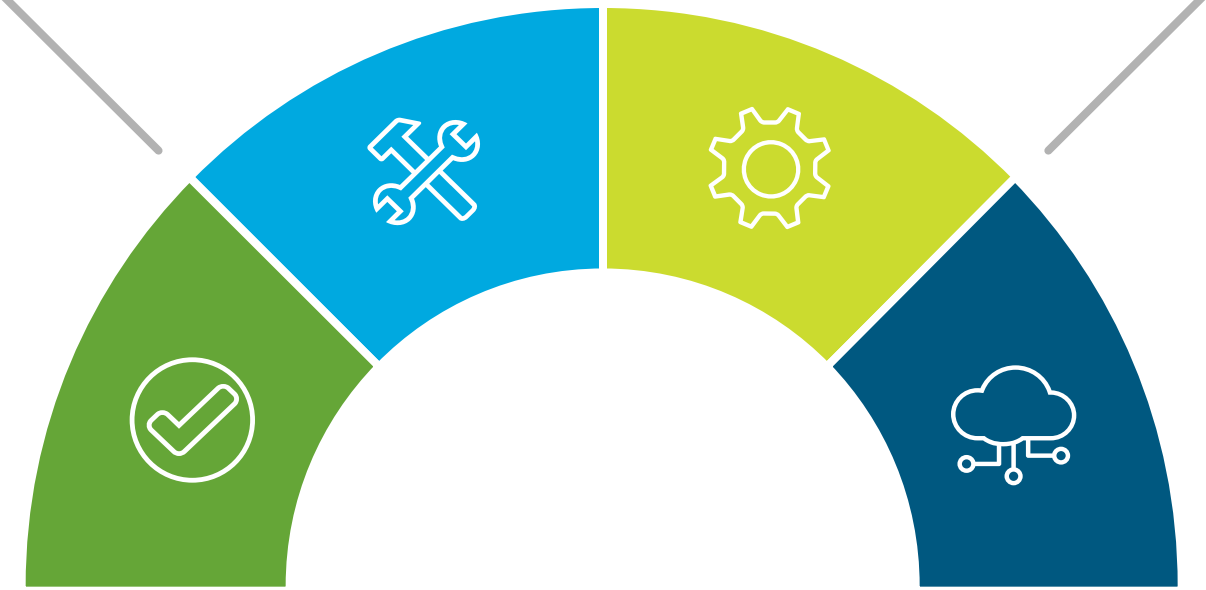
Create a baseline by identifying data sources within your environment

Step 3

Use data maps to confirm the right data sources and potential gaps

Step 4

Design an adoption plan that maximizes data reuse across your organization



DSA – Data Source Assessment

Using a simple process that involves each team

- **Pre-configured lists** of most common data sources to help you document your environment
- **Data dependency maps** for 120+ correlations and dashboards to help you design your data plan
- **Visual dashboards** to assess data indexed and use case adoption and data overlap between groups
- Quickly surface areas where **additional value** can be realized with **existing data**
- **Align your data with key objectives** by focusing on relevant value drivers
- Identify **missing data sources** required to better support key objectives

Identify your Top Value Drivers

Understanding your value drivers will enable alignment with data sources

SAMPLE

IT Ops and App Support

- ❑ Become more proactive
- ❑ Resolve incidents faster
- ❑ Improve root cause analysis
- ❑ Improve HW capacity utilization
- ❑ Automate routine tasks
- ❑ Reduce escalations

Security & Compliance

- ❑ Improve detection of security events
- ❑ Investigate security incidents faster
- ❑ Streamline compliance activities
- ❑ Reduce risk of data breach
- ❑ Reduce risk of IP theft
- ❑ Reduce risk of Fraud

Application Development

- ❑ Develop faster reports and dashboards
- ❑ Analyze test failures faster
- ❑ Investigate pre-production bugs faster
- ❑ Accelerate time to market
- ❑ Reduce time and effort of release

Business Analytics

- ❑ Improve quality of business processes
- ❑ Improve efficiency of business processes
- ❑ Improve measurement of processes
- ❑ Improve audit of processes
- ❑ Improve customer experience

splunk> .conf2017

Document your Environment

1 section per team to achieve value drivers

SAMPLE

Server **750** CONFIGURED ITEMS **154 GB/day** TOTAL REQUIRED DATA PER DAY **35%** INDEXED **54 GB/day** INDEXED

Work with the server admin team to **identify data source items required to achieve key goals** and provide an estimate for the total number of items, an approximation of their daily log size, and a ballpark % of data currently indexed by Splunk. Add missing items as needed to better reflect your environment.

Configured Item	*Total Items*	*% Indexed*	*Best Practice Data Source Types*	*% Data Source Types Indexed*	*Est. Log Size per Item*	*Typical*	*Total Projected Data per Day*	*Current Total Indexed*
Windows - *Production Servers (physical and virtual)*	350	50%	*perfmon, event logs, snare, antivirus, patch logs, etc*	70%	250 *MB/day per item*	250 MB/day per item	85.4 GB/day	29.9 GB/day
Windows - *Non Prod Servers (Dev, Test, etc)*	250	50%	*perfmon, event logs, snare, antivirus, patch logs, etc*	70%	150 *MB/day per item*	150 MB/day per item	36.6 GB/day	12.8 GB/day
Unix - *Production Servers (physical and virtual)*	100	50%	*syslog, top, iostat, netstat, securelog, snare, antivirus, sar, patch logs*	70%	250 *MB/day per item*	250 MB/day per item	24.4 GB/day	8.5 GB/day
Unix - *Non Prod Servers (Dev, Test, etc)*	50	50%	*syslog, top, iostat, netstat, securelog, snare, antivirus, sar, patch logs*	70%	150 *MB/day per item*	150 MB/day per item	7.3 GB/day	2.6 GB/day
Virtual Infrastructure Servers *(ESX servers, vCenters)*	-	0%	*Logs from VMWare ESX servers, vCenter servers*	0%	250 *MB/day per item*	250 MB/day per item	-	-
Cloud Services - *Azure*	-	0%	*WADLogs, WADEventLogs, WADPerformanceCounter, WADDiagnostInfra*	0%	250 *MB/day per item*	250 MB/day per item	-	-
Cloud Services - *AWS*	-	0%	*AWS CloudTrail, CloudWatch, Config, S3, etc*	0%	250 *MB/day per item*	250 MB/day per item	-	-
Other	-	0%		0%	- *MB/day per item*		-	-
Other	-	0%		0%	- *MB/day per item*		-	-
Other	-	0%		0%	- *MB/day per item*		-	-

Other Logs: Could the SERVER team deliver better services if they had access to these logs?

Storage *(SAN, NAS, EMC, NetApp logs, etc)*	YES	Test and Dev *(Non-Prod Web, App and Middleware logs)*	NO
Network *(Switches, Routers, FWs, VPNs, Proxies, LDAPs, FTP, etc)*	YES		
Database *(Prod and Non-Prod Oracle, SQL/Server, MySQL, RDBMS logs)*	NO		
Application *(Prod Web, App and Middleware logs, mobile logs)*	NO		
End-User *(Desktops, AD, Mail, Domain Controlers, etc)*	NO		

Order Mgmt (ERP logs, custom trx logs)	NO		
Billing & Invoicing (ERP logs, custom trx logs)	NO		
Customer Service (ERP logs, custom trx logs)	NO		
Procurement (ERP logs, custom trx logs)	NO		
Product Delivery (ERP logs, custom trx logs)	NO		

Is Splunk in use by the SERVER team to achieve the following functions for SERVERs currently indexed:

Proactive monitoring	YES
Level 1 triage of potential incidents	PARTIAL
Incident investigation	NO
Post incident root cause analysis	NO
Performance monitoring	NO
Monitor capacity utilization of system resources	NO
Routine task automation like system log reviews	PARTIAL
Analyze pre-production issues and defects	NO
Compliance monitoring and reporting	YES

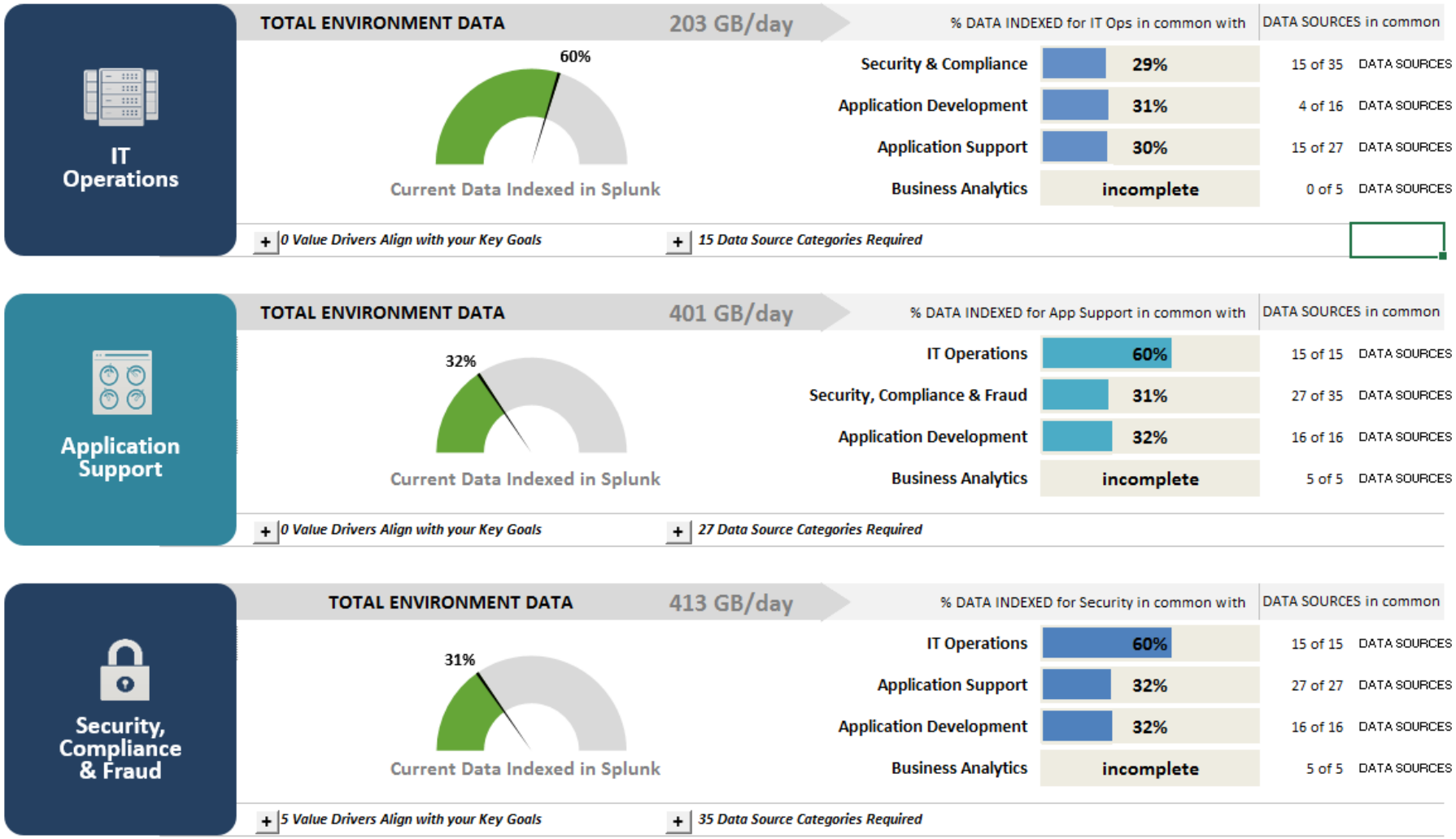
What type of value has the SERVER team realized from using Splunk so far?

Reduced time to investigate incidents by	70%	typically 70-90%
Reduced the number of high priority incidents by	20%	typically 15-45%
Reduced time for post-incident root cause analysis by	0%	typically 70-90%
Reduced time for manual compliance activities by	0%	typically 70-90%
Increased in server capacity utilization by	0%	typically 5-20%
Reduced time to investigate pre-prod defects by	0%	typically 70-90%

Analyze your Deployment

Dashboard to Assess Current/Future Deployment

SAMPLE



- **Key metrics** show total data required vs. actual data indexed
- **Overlap factors** between groups and data already indexed can help you plan your next adoption phase

splunk> .conf2017

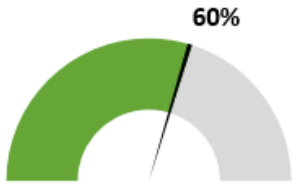
Confirm the Right Data Sources

Visualize which Data Sources are Indexed vs. Not Indexed

SAMPLE

IT Operations

TOTAL ENVIRONMENT DATA 203 GB/day



Current Data Indexed in Splunk

	% DATA INDEXED for IT Ops in common with	DATA SOURCES in common
Security & Compliance	29%	15 of 35 DATA SOURCES
Application Development	31%	4 of 16 DATA SOURCES
Application Support	30%	15 of 27 DATA SOURCES
Business Analytics	incomplete	0 of 5 DATA SOURCES

\+ 0 Value Drivers Align with your Key Goals

\- 15 Data Source Categories Required

Data Source Category	Items	Configured Items	Data Source Types	Log	Size	% Indexed	ITOps
Network	20	Switches	Ethernet and virtual switch logs, netflow data	150	MB per day per Item	50%	x
Network	30	Routers	cisco_cdr, cisco:asa, cisco_syslog, clavister, netflow, etc	250	MB per day per Item	50%	x
Network	20	Trusted FWs	Palo Alto, Cisco, Check Point, etc	250	MB per day per Item	50%	x
Network	12	DMZ FWs	Perimiter FWs	500	MB per day per Item	50%	x
Network	50	VPNs	Citrix NetScaler Nitro, Citric NetScaler IPFIX, Cisco, etc	250	MB per day per Item	50%	x
Network	40	Proxies	Bluecoat, Fortinet, Juniper:idp, Netscreen:firewall, Pan, etc	250	MB per day per Item	50%	x
Network	10	LDAP Directory Services		250	MB per day per Item	25%	x
Network	5	FTP Servers	vsftpd	250	MB per day per Item	25%	x
Network	10	DNS systems	BIND, PowerDNS, Unbound, Dnsmasq, Erl-DNS	150	MB per day per Item	25%	x
Network	2	SNMP systems	LogicMonitor, ManageEngine, Spiceworks, Ruckus Idera	100	MB per day per Item	25%	x
Network	5	DHCP	DHCP Insight, Linux DHCP	100	MB per day per Item	0%	x
Server	350	Windows - Production Servers (physical and virtual)	perfmon, event logs, snare, antivirus, patch logs, etc	250	MB per day per Item	100%	x
Server	250	Windows - Non Prod Servers (Dev, Test, etc)	perfmon, event logs, snare, antivirus, patch logs, etc	150	MB per day per Item	100%	x
Server	100	Unix - Production Servers (physical and virtual)	syslog, top, iostat, netstat, securelog, snare, antivirus, sar, patc	250	MB per day per Item	100%	x
Server	50	Unix - Non Prod Servers (Dev, Test, etc)	syslog, top, iostat, netstat, securelog, snare, antivirus, sar, patc	150	MB per day per Item	100%	x

splunk> .conf2017

Take an Enterprise Approach

Provide a Perspective on Current/Future Use Cases

SAMPLE

● Splunk **FULLY** in use ○ Splunk **PARTIALLY** in use ✚ Splunk **NOT IN USE** however >20% data is **ALREADY INDEXE** ◯ Splunk **NOT IN USE** but can deliver value with **NEW** data

TOTAL DATA PER DAY	1,469 GBs	42%	IT Operations & Application Support							Security, Compliance and Fraud				Application Development			Business Services				
Groups	Required Data / Day	% of Data Indexed	Proactive Monitoring	Level 1 Triage	Incident Response	Root Cause Analysis	Performance Monitoring	Capacity Mgmt	Routine Task Automation	Event Detection	SOC Triage	Deep Dive Investigation	Compliance Monitoring & Reporting	Report & Dashboard Development	QA Test Failure Analysis	Defect Remediation, Debugging Code	Business Service Efficiency	Business Service Quality	Business Service Speed	Business Service Measurement	Business Service Audit
Server Admin	304 GBs	36%	●																		
Storage Admin	289 GBs	38%																			
Network Admin	59 GBs	69%	●	●	○																
Database Admin	1,036 GBs	45%	○		○	○	○		●												
Application Support	754 GBs	47%																			
End-User Support	136 GBs	0%	◯	◯	◯	◯	◯		◯												
Security Engineers	1,191 GBs	41%								○	○	○									
Fraud Team	563 GBs	48%																			
Testers and Developers	1,036 GBs	45%												●							
Order Mgmt	98 GBs	50%																			
Billing & Invoicing	20 GBs	0%	◯	◯	◯	◯	◯	◯	◯					◯	◯	◯	◯	◯	◯	◯	◯
Customer Service	124 GBs	39%																			
Procurement	1 GBs	0%	◯	◯	◯	◯	◯	◯	◯					◯	◯	◯	◯	◯	◯	◯	◯
Product Delivery	2 GBs	0%	◯	◯	◯	◯	◯	◯	◯					◯	◯	◯	◯	◯	◯	◯	◯

splunk> .conf2017

Take an Enterprise Approach

Provide a Perspective on Current/Future Use Cases

SAMPLE

● Splunk **FULLY** in use ○ Splunk **PARTIALLY** in use ✚ Splunk **NOT IN USE** however >20% data is **ALREADY INDEXE** ◯ Splunk **NOT IN USE** but can deliver value with **NEW** data

TOTAL DATA PER DAY	1,469 GBs	42%	IT Operations & Application Support							Security, Compliance and Fraud				Application Development			Business Services				
Groups	Required Data / Day	% of Data Indexed	Proactive Monitoring	Level 1 Triage	Incident Response	Root Cause Analysis	Performance Monitoring	Capacity Mgmt	Routine Task Automation	Event Detection	SOC Triage	Deep Dive Investigation	Compliance Monitoring & Reporting	Report & Dashboard Development	QA Test Failure Analysis	Defect Remediation, Debugging Code	Business Service Efficiency	Business Service Quality	Business Service Speed	Business Service Measurement	Business Service Audit
Server Admin	304 GBs	36%	●	✚	✚	✚	✚	✚	✚						✚	✚					
Storage Admin	289 GBs	38%	✚	✚	✚	✚	✚	✚	✚												
Network Admin	59 GBs	69%	●	●	○	✚	✚		✚												
Database Admin	1,036 GBs	45%	○	✚	○	○	○	✚	●						✚	✚					
Application Support	754 GBs	47%	✚	✚	✚	✚	✚	✚	✚					✚	✚	✚					
End-User Support	136 GBs	0%	◯	◯	◯	◯	◯		◯												
Security Engineers	1,191 GBs	41%							✚	○	○	○	✚		✚						
Fraud Team	563 GBs	48%								✚	✚	✚	✚								✚
Testers and Developers	1,036 GBs	45%												●	✚	✚					
Order Mgmt	98 GBs	50%	✚	✚	✚	✚	✚	✚	✚					✚	✚	✚	✚	✚	✚	✚	✚
Billing & Invoicing	20 GBs	0%	◯	◯	◯	◯	◯	◯	◯					◯	◯	◯	◯	◯	◯	◯	◯
Customer Service	124 GBs	39%	✚	✚	✚	✚	✚	✚	✚					✚	✚	✚	✚	✚	✚	✚	✚
Procurement	1 GBs	0%	◯	◯	◯	◯	◯	◯	◯					◯	◯	◯	◯	◯	◯	◯	◯
Product Delivery	2 GBs	0%	◯	◯	◯	◯	◯	◯	◯					◯	◯	◯	◯	◯	◯	◯	◯

splunk> .conf2017

Assess your Current Data Maturity

Visualize your current state compared to other Splunk Customers

SAMPLE

*52 Security Correlations possible with **current data**,*
*indexing an average of **50%** of commonly required data sources*

Security Use Cases	% Data Indexed
Abnormally High Number of Endpoint Changes By User	41%
Account Deleted	41%
Activity from Expired User Identity	38%
Anomalous Audit Trail Activity Detected	41%
Anomalous New Listening Port	52%
Anomalous New Process	52%
Anomalous New Service	52%
Asset Ownership Unspecified	38%
Brute Force Access Behavior Detected	30%
Brute Force Access Behavior Detected Over One Day	30%
Cleartext Password At Rest Detected	30%
Completely Inactive Account	30%
Concurrent Login Attempts Detected	30%
Default Account Activity Detected	34%
Default Account At Rest Detected	38%
Excessive DNS Failures	50%
Excessive DNS Queries	50%
Excessive Failed Logins	30%
Expected Host Not Reporting	30%
Geographically Improbable Access Detected	30%
High Number of Hosts Not Updating Malware Signatures	56%
High Number Of Infected Hosts	56%
High Or Critical Priority Host With Malware Detected	47%
High or Critical Priority Individual Logging into Infected Machine	41%

Security Use Cases	% Data Indexed
High Process Count	52%
High Volume Email Activity to Non-corporate Domains by User	44%
High Volume of Traffic from High or Critical Host Observed	24%
Host Sending Excessive Email	50%
Host With A Recurring Malware Infection	56%
Host With High Number Of Listening ports	52%
Host With High Number Of Services	52%
Host With Multiple Infections	56%
Host With Old Infection Or Potential Re-Infection	56%
Inactive Account Activity Detected	34%
Insecure Or Cleartext Authentication Detected	30%
Multiple Primary Functions Detected	52%
Network Change Detected	41%
Network Device Rebooted	41%
New User Account Created On Multiple Hosts	41%
Outbreak Detected	56%
Same Error On Many Servers Detected	46%
Short-lived Account Detected	39%
Should Timesync Host Not Syncing	43%
Substantial Increase In Events	75%
Substantial Increase In Port Activity	43%
Threat Activity Detected	100%
Unapproved Port Activity Detected	26%
Unroutable Host Activity	43%
Unusual Volume of Network Activity	43%
Vulnerability Scanner Detected (by events)	75%
Vulnerability Scanner Detected (by targets)	75%
Web Uploads to Non-corporate Sites by Users	24%

splunk> .conf2017

Verify your Planned Data

Compare your data strategy against other Splunk customers

SAMPLE

based on the machine data available in our environment,
*62 Security correlations will have an average of **~80%** of commonly required data sources*

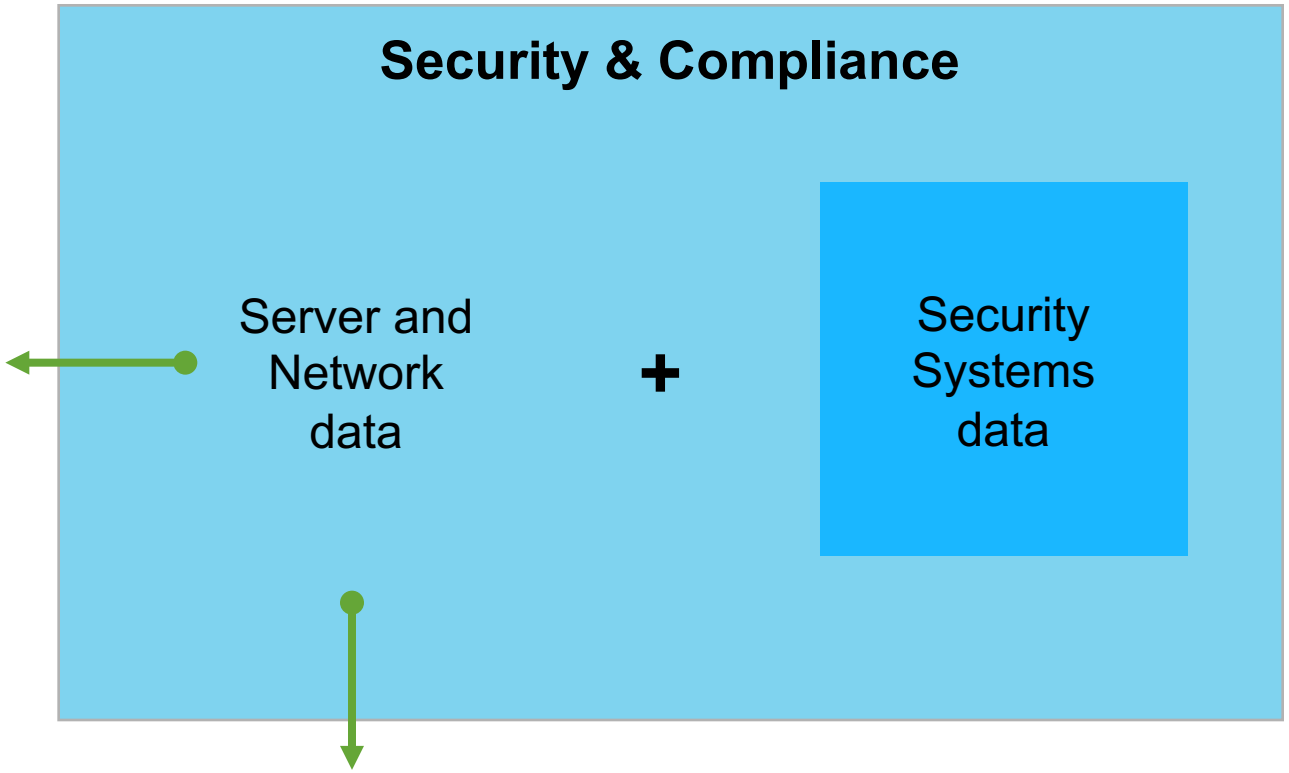
Security Use Cases	% Data Indexed
Abnormally High Number of Endpoint Changes By User	79%
Abnormally High Number of HTTP Method Events By Src	30%
Account Deleted	79%
Activity from Expired User Identity	69%
Anomalous Audit Trail Activity Detected	79%
Anomalous New Listening Port	89%
Anomalous New Process	89%
Anomalous New Service	89%
Asset Ownership Unspecified	69%
Brute Force Access Behavior Detected	62%
Brute Force Access Behavior Detected Over One Day	62%
Cleartext Password At Rest Detected	62%
Completely Inactive Account	62%
Concurrent Login Attempts Detected	62%
Default Account Activity Detected	66%
Default Account At Rest Detected	69%
Excessive DNS Failures	100%
Excessive DNS Queries	100%
Excessive Failed Logins	62%
Excessive HTTP Failure Responses	30%
Expected Host Not Reporting	62%
Geographically Improbable Access Detected	62%
High Number of Hosts Not Updating Malware Signatures	88%
High Number Of Infected Hosts	88%
High Or Critical Priority Host With Malware Detected	78%
High or Critical Priority Individual Logging into Infected Machine	73%
High Process Count	89%
High Volume Email Activity to Non-corporate Domains by User	85%
High Volume of Traffic from High or Critical Host Observed	50%
Host Sending Excessive Email	100%

Security Use Cases	% Data Indexed
Host With A Recurring Malware Infection	88%
Host With High Number Of Listening ports	89%
Host With High Number Of Services	89%
Host With Multiple Infections	88%
Host With Old Infection Or Potential Re-Infection	88%
Inactive Account Activity Detected	66%
Insecure Or Cleartext Authentication Detected	62%
Multiple Primary Functions Detected	89%
Network Change Detected	79%
Network Device Rebooted	79%
New User Account Created On Multiple Hosts	79%
Outbreak Detected	88%
Potential Gap in Data	100%
Prohibited Process Detected	100%
Prohibited Service Detected	100%
Same Error On Many Servers Detected	90%
Short-lived Account Detected	74%
Should Timesync Host Not Syncing	85%
Substantial Increase In Events	100%
Substantial Increase In Port Activity	100%
Threat Activity Detected	100%
UEBA Threat Detected	100%
UEBA Threat Detected (Risk)	100%
Unapproved Port Activity Detected	94%
Unroutable Host Activity	100%
Untriaged Notable Events	100%
Unusual Volume of Network Activity	100%
Vulnerability Scanner Detected (by events)	100%
Vulnerability Scanner Detected (by targets)	100%
Watchlisted Event Observed	100%
Web Uploads to Non-corporate Sites by Users	50%

splunk> .conf2017

Consider Data Reuse to Plan your Next Adoption

On average 80% of the data required for Security & Compliance is **CRITICAL for IT OPS** to achieve full value with infrastructure teams

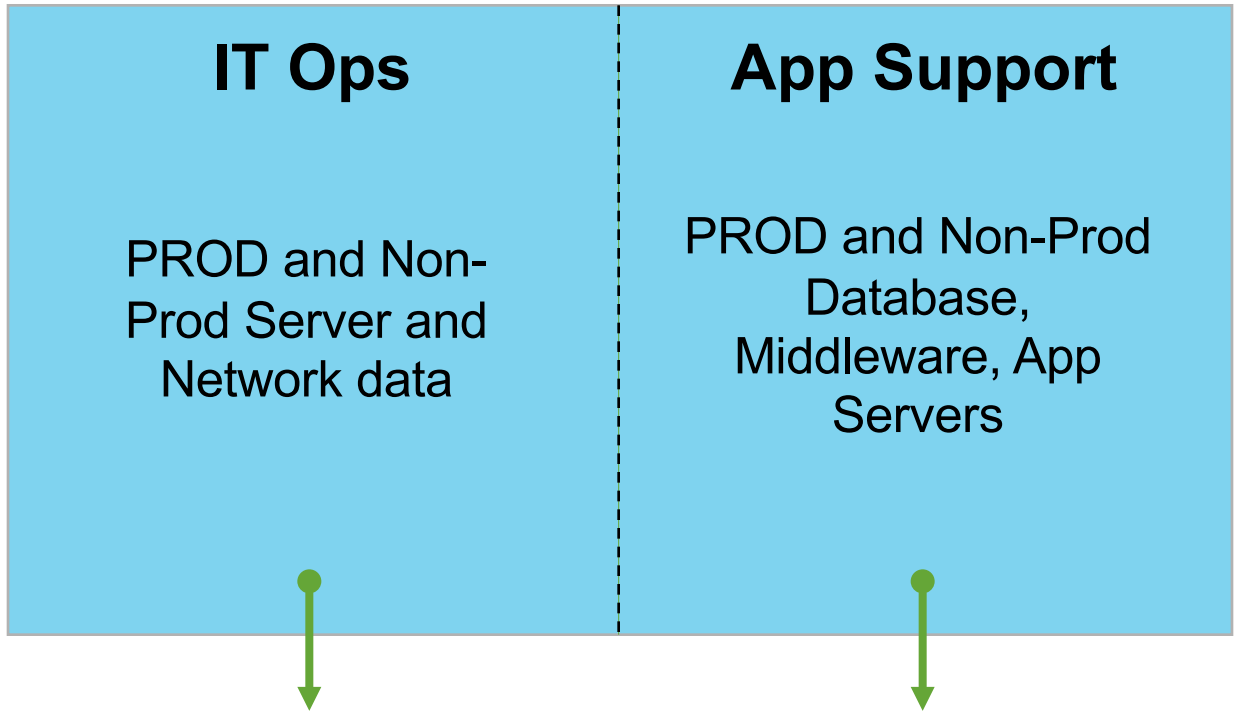


Common Scenario

Data Reuse = Faster Results + Higher Value per GB indexed

On average, 80% of the data required for Security & Compliance is of **HIGH** value for **Application Support teams** to enable End to End visibility once Database, Middleware and Application data is indexed

Reusing IT Ops and App Support Data



80%
data reuse

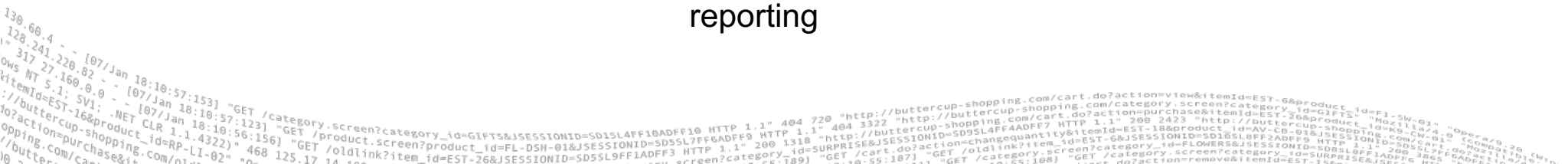
Data Reuse =
Faster Results +
Higher Value per
GB indexed

On average, >80% of the data required for IT Ops and Application Support also

ENABLES Application Delivery teams to produce faster release cycles with less errors

Data Reuse Typically Enables Broader Key Goals

Continuously Secure the Environment	Reduce and/or Avoid IT Expenditures	Improve Internal Efficiencies	Increase Revenue	Accelerate Time to Market	Improve Business Services
Better detection of cyber attacks	Infrastructure cost avoidance through improved capacity management	Labor savings with common IT processes	Avoid revenue impact from fewer critical outages	Faster test failure analysis	Minimize business disruptions
Faster response to security incidents	Future headcount avoidance	Faster incident investigation and root cause analysis	Faster delivery of real-time business analytics	Faster remediation of bugs and defects	Improved & more consistent SLA's
Continuous compliance monitoring	Tools consolidation	Proactive automation of key business processes	Improved innovation value for key business initiatives	Fewer developer disruptions	More reliable business services leads to better brand
Reduction in risk for data breach, fraud and IP theft		Better visibility & reporting		Faster, more robust code deployments	Faster response to customer requirements



splunk> .conf2017

Recap

Your Data Source Strategy should…

1. **Align** with key initiatives/programs
2. Leverage common **data source maps**
3. Surface new use cases possible with **current data**
4. Identify **missing data** to drive better content and new use cases
5. Factor **data reuse** to plan your next adoption phase

What's Next

Common Questions…

- Can you assist me with a data source assessment?
- Will I get a copy of the DSA tools?
- Can I get a copy of this Presentation?

YES

Come see us at the "**Business Value Consulting**" booth, or work with your Splunk account team

splunk> .conf2017

Thank You

Don't forget to rate this session in the .conf2017 mobile app