

Cisco and Splunk

Innovation through the Power of Innovation

Douglas Hurd	Cisco Security Technical Alliances PM
Colin Lowenberg	Cisco Meraki Platform Partnerships PM
Karthik Karupasamy	Cisco UCS Technical Marketing Engineer
Robert Novak	Cisco Big Data Technical Solutions Architect

September 28, 2017 | 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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

Eight Years of Integration and Innovation

A brief history of Cisco and Splunk together
With Robert Novak

Why Does Hardware Still Matter?

- ▶ Splunk will run on almost anything (even my laptop)
- ▶ Standalone servers have lower admin overhead
- ▶ Build up your clusters and you have to keep them consistent
- ▶ Grow your data sources (and uses) and you have to add servers
- ▶ Cluster constipation is bad, mmmkay?

Why Does Hardware Still Matter?

- ▶ Cisco customer big data pools tend to grow 2-3x/year
- ▶ Cisco customer IT staff doesn't grow as fast
- ▶ The Cisco Unified Computing System (UCS) provides scalable, repeatable, predictable, and manageable deployments across dozens to thousands of servers for any application deployment
- ▶ Pallet to production in hours, not days or weeks
- ▶ Deep engineering integration between Cisco and Splunk with tested and proven configurations

More on this later...

Big Data at a Big Customer: Cisco

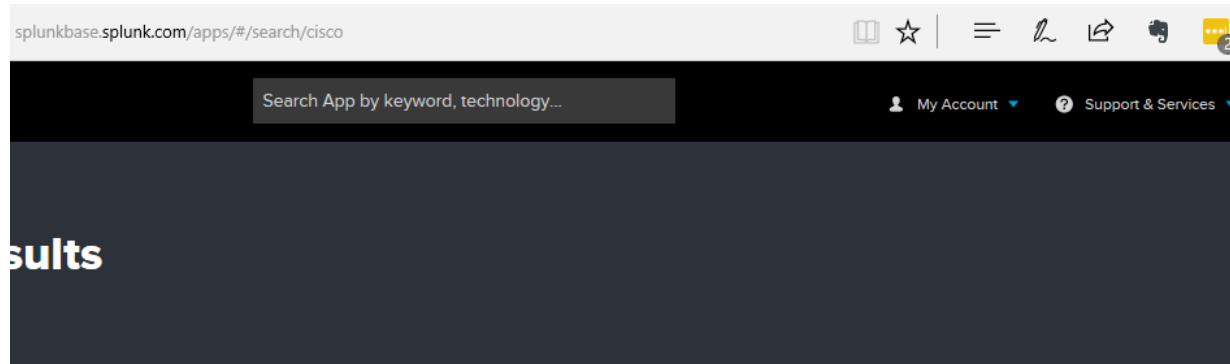
- ▶ 10s of thousands of employees, contractors, devices
- ▶ 100s of offices, business apps, audiences
- ▶ Lots of data in lots of places
- ▶ No one tool (not even Splunk) can do everything for everyone all the time
- ▶ High volume, low value, low shelf life
 - Stealthwatch (formerly Lancope), Hadoop feed into Splunk
- ▶ Low to moderate volume, high value, (any) shelf life
 - Splunk on its own, sometimes with fronting dashboards
- ▶ Additional visualizations with Platfora, Tableau, etc

A closer look at Splunk within Cisco

- ▶ Customer for 8+ years, strategic partner for 4+ years
- ▶ Geographically disparate data collection and analysis
- ▶ Over 70 business applications/use cases across the company
 - Around 20 teams using Splunk including Cisco IT and CSIRT
- ▶ Nearly 10x growth in search volume from 2014-2016



Dozens Of Apps And Add-ons At Splunkbase



Search: cisco x

Showing 1-20 of 47 results

Best Match v

 Cisco Security Suite 2064 Installs	 Cisco Networks App for Splunk 1839 Installs	 Cisco Networks Add-on for Splunk 2974 Installs	 Cisco ACI App for Splunk Enterprise 103 Installs
 Cisco ACI Add-on for Splunk 107 Installs	 Splunk Add-on for Cisco ASA 5249 Installs	 Splunk Add-on for Cisco FireSIGHT 5306 Installs	 Splunk Add-on for Cisco IPS 563 Installs

Always more being added and updated, by Cisco, Splunk, partners, third party developers, and end users!

Splunk and Cisco API-based Integrations

Programmable Operational Analytics at Scale



Security



Identity Services
(ISE/pxGrid)



FirePOWER Next
Gen Firewall



Umbrella (DNS)



CloudLock



ThreatGrid*

Infrastructure



Cisco UCS



ACI / APIC



Nexus 9k



Meraki Wireless / CMX

Tetration

Collaboration Business Analytics



Call Manager



Spark

and many more here <https://splunkbase.splunk.com/apps/#/search/Cisco/>

Cisco Security Integrations

Making sense of a broad security platform
using Cisco and Splunk technologies

With Douglas Hurd

Splunk & Cisco Security – “Better Together”



Security Breadth, Customer Reach, Infrastructure for Automation

- Largest security footprint in the industry
- Produces broad range of security telemetry across most security technologies
- Ubiquitous network footprint enables bi-directional integration for executing security automation
- High investment in Splunk apps for serving joint customers



Analytics Efficacy, Ability to Automate, Committed Customers

- Voluminous, context-rich Cisco data sources drive license volumes while enabling improved security & compliance, more effective SIEM use cases and new use cases beyond security
- Automated actions in Cisco network environs
- Proven, supported integrations accelerate time to value

Cisco Splunk Integrations

Security

IPS
Identity Services Engine/pxGrid
FireSIGHT (including AMP)
ASA/PIX/FWSM Firewalls
Web Security Appliance (WSA)
Email Security Appliance (ESA)
Stealthwatch
Umbrella Investigate
Cloud Web Security (CWS)
AnyConnect
CloudLock
ThreatGrid

Cisco Security
Suite App

Data Center / ACI

Cisco UCS
UCS Director Express for Big Data
Application Centric Infrastructure (ACI - APIC)
Nexus 9K
Tetration (planned)

Enterprise Networking

Nexus and Catalyst Switches
Nexus 1000V
NGN Routers (CRS, ASR, ISR)
Meraki Wireless
Open SDN Network Controller
CMX Wireless
Network Data Platform (planned)

Cisco Networks
App

Collaboration

Call Manager
Spark
AppDynamics

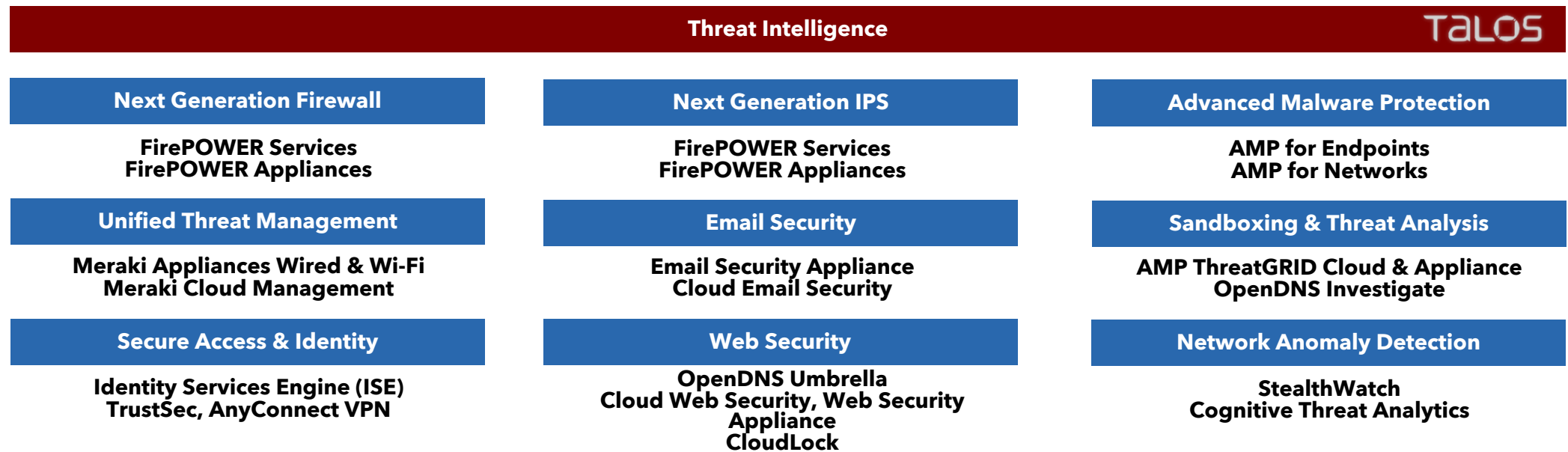
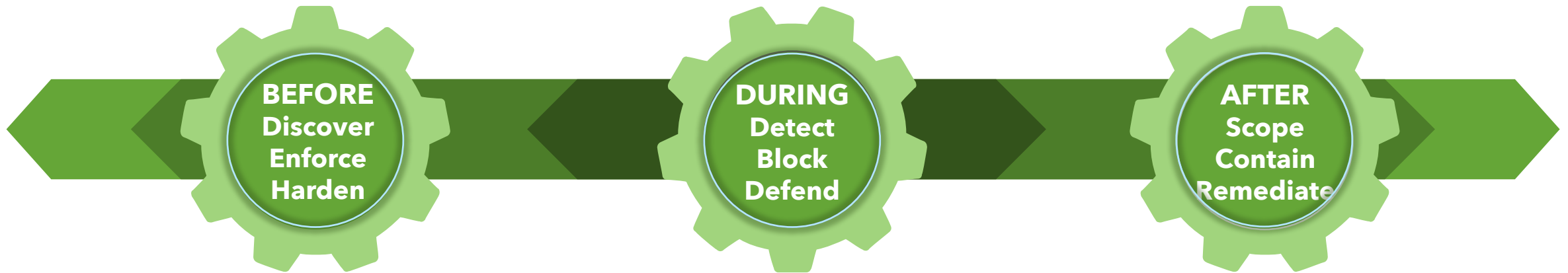
- ✓ Inaugural SIEM & Threat Defense Partner
- ✓ Inaugural pxGrid partner
- ✓ Inaugural member of Cisco Security Tech Alliances program
- ✓ Inaugural ACI Partner
- ✓ Inaugural Data Analytics Partner

- ✓ **CVD:** Cisco UCS Integrated Infrastructure for Splunk Enterprise (Distributed Deployment, High Capacity) ([link](#))
- ✓ **CVD:** Cisco Application Centric Infrastructure with Splunk ([link](#))
- ✓ Splunk on UCS Reference Architecture ([link](#))
- ✓ Cisco Cloud Security for VMDC 1.0 Design Guide ([link](#))

Cisco Firepower & Splunk

Douglas Hurd / Cisco Security Technical Alliances

Threat Defense Security



Threat Defense Security

[Overview](#)
[Analysis](#)
[Policies](#)
[Devices](#)
[Objects](#)
[Deploy](#)
[System](#)
[Help](#)
[Global \ dohurd](#)

[Dashboards](#)
[Reporting](#)
[Summary](#)

Summary Dashboard (6.2.0)

Provides a summary of activity on the appliance

[Network](#)
[Threats](#)
[Intrusion Events](#)
[Status](#)
[Geolocation](#)
[QoS](#)

Show the Last 1 hour

Add Widgets

Top Attackers

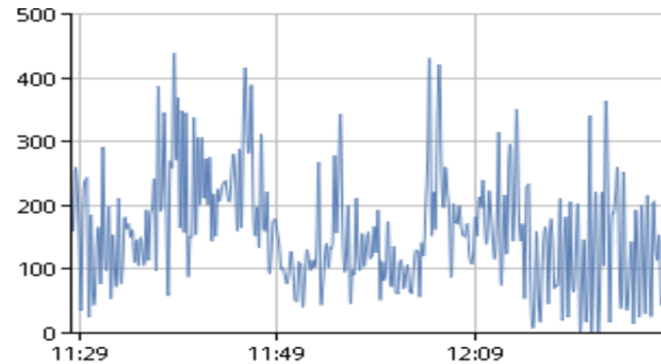
Source IP	Count
192.168.199.132	20,722
192.168.199.133	7,643
220.231.10.124	3,965
186.107.10.124	1,723
172.149.41.1	1,453
172.91.41.1	1,441
12.100.10.50	1,263
220.231.10.75	1,102
220.231.10.21	1,068
192.168.199.254	1,020

Last updated 4 minutes ago

Top Targets

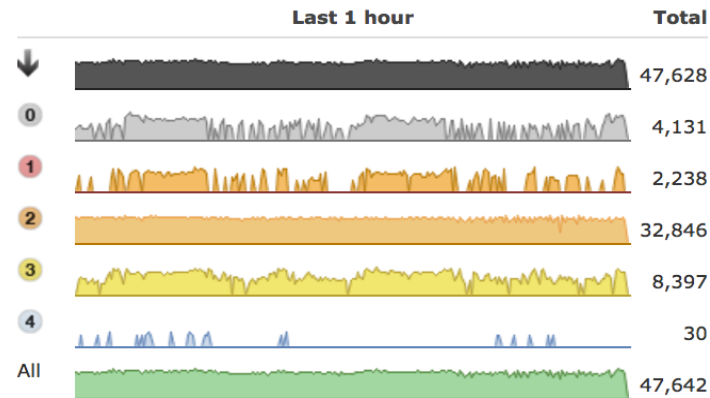
Destination IP	Count
224.0.0.22	26,122
192.168.199.133	2,312
10.0.10.124	2,164
10.0.10.21	1,937
10.0.10.75	1,741
10.110.10.12	1,723
192.38.41.133	1,453
192.89.41.133	1,441
10.0.10.122	1,266
192.168.199.132	1,020

All Intrusion Events



Last updated 4 minutes ago

Intrusion Events



Total Events by Application Protocol

Application	Total Events
IGMP	52,114
SNMP	23,070
ICMP	12,248
HTTP	386
ICMP for IPv6	204
FTP	16
SMTP	16
IMAP	12
LDAPS	12
SSH	10

Last updated 4 minutes ago

Impact 1 Events by Application Protocol

Application	Impact 1 Events
SNMP	2,346
ICMP	10

Threat Defense Security

Overview Analysis Policies Devices Objects Deploy System Help Global \ dohurd

Dashboards Reporting Summary

Summary Dashboard (6.2.0)

Provides a summary of activity on the appliance

Network Threats Intrusion Events Status Geolocation QoS +

Top Attackers

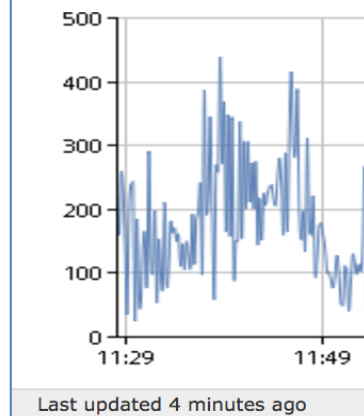
Source IP	Count
192.168.199.132	20,722
192.168.199.133	7,643
220.231.10.124	3,965
186.107.10.124	1,723
172.149.41.1	1,453
172.91.41.1	1,441
12.100.10.50	1,263
220.231.10.75	1,102
220.231.10.21	1,068
192.168.199.254	1,020

Last updated 4 minutes ago

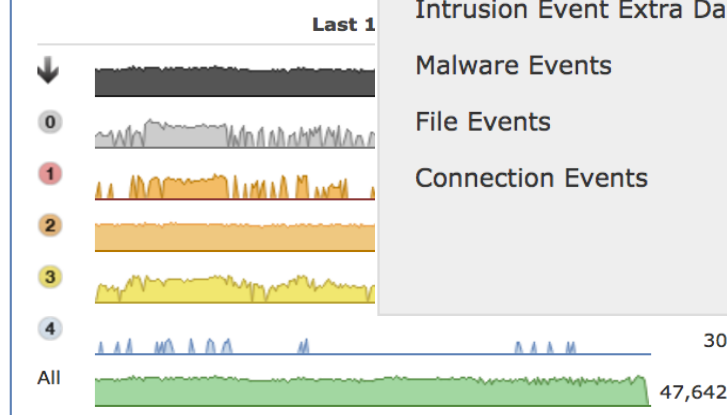
Top Targets

Destination IP	Count
224.0.0.22	26,122
192.168.199.133	2,312
10.0.10.124	2,164
10.0.10.21	1,937
10.0.10.75	1,741
10.110.10.12	1,723
192.38.41.133	1,453
192.89.41.133	1,441
10.0.10.122	1,266
192.168.199.132	1,020

All Intrusion Events



Intrusion Events



eStreamer Event Configuration

Select the types of events that will be sent to connected eStreamer clients

- Discovery Events ☒
- Correlation and White List Events ☒
- Impact Flag Alerts ☒
- Intrusion Events ☒
- Intrusion Event Packet Data ☒
- User Activity ☒
- Intrusion Event Extra Data ☒
- Malware Events ☒
- File Events ☒
- Connection Events ☒

Save

Show the Last 1 hour

Add Widgets

by Application Protocol

Application	Total Events
HTTP	52,114
HTTPS	23,070
SSH	12,248
FTP	386
for IPv6	204
SMTP	16
POP3	16
IMAP	12
LDAP	12
SNMP	10

Events by Application Protocol

Application	Impact 1 Events
HTTP	2,346
HTTPS	10

Background on Firepower and Splunk

- ▶ Firepower-Splunk mutual customer base expanding
 - ASA to Firepower Threat Defense – More FMCs
- ▶ Add-Ons for Firepower available on Splunkbase
- ▶ Cisco's Firepower TA & App built in 2014, based on v.5.4
 - Over 6000 downloads
 - *Not recommended with FMC V6.x*
- ▶ 'Community Supported' model facing challenges
- ▶ Focused on new business model for this critical integration
- ▶ Resources directed at Firepower 6.x customers

The screenshot shows the Splunkbase interface for the 'Cisco eStreamer for Splunk' app. At the top, there's a search bar and navigation links for 'My Account' and 'Support & Services'. The app card features the title 'Cisco eStreamer for Splunk', a 4-star rating from 9 reviews, and a thumbnail image of the app's interface. Below the card, the 'Overview' tab is selected, showing a description of the app as a Sourcefire eStreamer log collection tool. It lists supported Sourcefire event types: Intrusion Events, Intrusion Event Packet Data (optional), Intrusion Event Extra Data, Malware Events, File Events, Connection Logs and Security Intelligence Events (optional), Correlation and White List Events, Impact Flag Alerts, and Connection Events (optional). A note states that the app is for Unix platforms only and is not officially supported by Cisco. To the right, statistics show 435 installs and 4,275 downloads, with a 'LOGIN TO DOWNLOAD' button. Further down, a 'Release Notes' section for version 2.2.2 is visible, dated Sept. 23, 2016. On the far right, a sidebar lists metadata including version (2.2.2), category (Security, Fraud & Compliance), product support (Splunk Enterprise), content type (App), Splunk versions (6.4, 6.1, 6.0), licensing (Cisco eStreamer End User License Agreement), platforms (Platform Independent), community support (Questions on SplunkAnswers, File a case, Flag as inappropriate), and the builder (douglas hurd). At the bottom right are 'Subscribe' and 'Share' buttons.

splunkbase Search App by keyword, technology... My Account Support & Services

Cisco eStreamer for Splunk

★★★★★ 9 reviews

Overview Details

Sourcefire eStreamer log collection and comprehensive selection of dashboards optimized for Sourcefire System 5.2+ and Splunk 6.

The supported Sourcefire event types are:

- Intrusion Events
- Intrusion Event Packet Data (optional)
- Intrusion Event Extra Data
- Malware Events
- File Events
- Connection Logs and Security Intelligence Events (optional)
- Correlation and White List Events
- Impact Flag Alerts
- Connection Events (optional)

Please note this app was developed for, and tested on, Unix platforms only. Windows support is not currently available.

This app is written and maintained by Sourcefire, now part of Cisco, but is only community supported – no official support is available. Be sure to visit the Documentation tab for initial assistance with setup, configuration, important notes, and a version change log.

eStreamer for Splunk is copyright © 2013-2014 Cisco and/or its affiliates. All rights reserved. Sourcefire is now part of Cisco.

Release Notes Version 2.2.2

Version: 2.2.2

Sept. 23, 2016, 6:07 p.m.
Platform Independent
6.4, 6.1, 6.0

435 Installs 4,275 Downloads

[LOGIN TO DOWNLOAD](#)

VERSION
2.2.2

CATEGORY
Security, Fraud & Compliance

PRODUCT SUPPORT
Splunk Enterprise

CONTENT TYPE
App

SPLUNK VERSIONS
6.4
6.1
6.0

LICENSING
[Cisco eStreamer End User License Agreement](#)

PLATFORMS
Platform Independent

COMMUNITY SUPPORTED
[Questions on SplunkAnswers](#)
[File a case](#)
[Flag as inappropriate](#)

BUILT BY
douglas hurd

[Subscribe](#) [Share](#)

Background on Firepower and Splunk

- ▶ Firepower-Splunk mutual customer base expanding
 - ASA to Firepower Threat Defense – More FMCs
- ▶ Add-Ons for Firepower available on Splunkbase
- ▶ Cisco's Firepower TA & App built in 2014, based on v.5.4
 - Over 6000 downloads
 - *Not recommended with FMC V6.x*
- ▶ 'Community Supported' model facing challenges
- ▶ Focused on new business model for this critical integration
- ▶ Resources directed at Firepower 6.x customers

The screenshot shows the Splunkbase interface for the 'Cisco eStreamer eNcore Add-on for Splunk'. The header includes the Splunkbase logo, a search bar, and links for 'My Account', 'My Splunk', and 'Support & Services'. The app card displays the Cisco logo, the app name, a 2-star rating from 2 users, and a blue bar with 'ADMINISTRATOR TOOLS: Manage App | View App | View Analytics'. Below the card, the 'Overview' tab is active, showing a description of the app as an eStreamer client with a Splunk plugin for event forwarding from Firepower Management Center (FMC) versions 6.x to Splunk Enterprise and Splunk Enterprise Security. It lists supported event types: Discovery Events, Correlation and White List Events, Impact Flag Alerts, Intrusion Events, Intrusion Event Packet Data, User Activity, Intrusion Event Extra Data, Malware Events, File Events, and Connection Events. A note states the app is for Linux only. On the right, a summary box shows 105 installs and 324 downloads, with 'Download' and 'Rate this App' buttons. Further down, it lists the version as 3.0.0, built by 'douglas hurd', categorized under 'Security, Fraud & Compliance', and compatible with Splunk Enterprise products and versions 6.6 and 6.5.

splunkbase

Search App by keyword, |

My Account > My Splunk > Support & Services

Cisco eStreamer eNcore Add-on for Splunk

★ ★ ★ ★ ★ 2 ratings

ADMINISTRATOR TOOLS: Manage App | View App | View Analytics

Overview Details

Cisco eStreamer eNcore Add-on for Splunk is an eStreamer client with a Splunk plugin that provides comprehensive event forwarding from all 6.x versions of Firepower Management Center to Splunk Enterprise and Splunk Enterprise Security.

The following event types are supported with complete schema coverage through the eStreamer API specification for FMC version 6.2.

- Discovery Events
- Correlation and White List Events
- Impact Flag Alerts
- Intrusion Events
- Intrusion Event Packet Data
- User Activity
- Intrusion Event Extra Data
- Malware Events
- File Events
- Connection Events

This app was developed for and tested on Linux platforms only. Windows support is not currently available. Please check with Cisco for any change in status.

Release Notes

105 Installs 324 Downloads

Download Rate this App

VERSION 3.0.0

BUILT BY douglas hurd

CATEGORY & CONTENTS

Categories: Security, Fraud & Compliance

App Type: Add-on

COMPATIBILITY

Products: Splunk Enterprise

Splunk Versions: 6.6, 6.5

Platform: Platform Independent

Data Consumption – Eat In or Delivery?

Expectations and User Roles are Changing



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03" "Opera/9.20 (Win
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Comodo11.4.0
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D5L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CW-01" "Comodo11.4.0
item_id=EST-16&product_id=RP-LI-02" "0
buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0
buttercup-shopping.com/cart.do?action=purchase&itemId=EST-16&product_id=RP-LI-02" "0

New Cisco eStreamer 'eNcore' for Splunk

- ▶ Scalable app with major improvements
- ▶ TAC Support option will be offered
 - Free for customers that do not want TAC support
 - Chargeable for customers that want TAC support
- ▶ Official GA Release: End of June
- ▶ Beta II underway during May thru June 2017
- ▶ PID: FP-SPLUNK-SW-K9
- ▶ Description: "Cisco eStreamer eNcore for Splunk"
 - Software downloads: software.cisco.com

	Free Version	Pay Version
App Cost	Free	\$\$\$
Community Support	Yes	Yes
TAC Support	No	Yes
App Updates	Yes	Yes

Improvements and Enhancements

Feature	Benefit
Built from scratch in Python	- No Perl dependencies - Python very popular - Completely up to date with entire 6.2 API schema
Multi-process	Highly scalable
Multi-FMC Support	- Connect multiple FMCs to one instance - Reduce complexity
Fully Qualified Event Output	Encoded event info is written out in text
Event de-duplication (Future)	- Avoid paying Splunk for redundant event data - Gives Firepower HA configurations more flexibility
TAC Supported option available	End to End support for Firepower Splunk customers
Forward Compatible	Ongoing maintenance to support new eStreamer API versions

PXGrid?

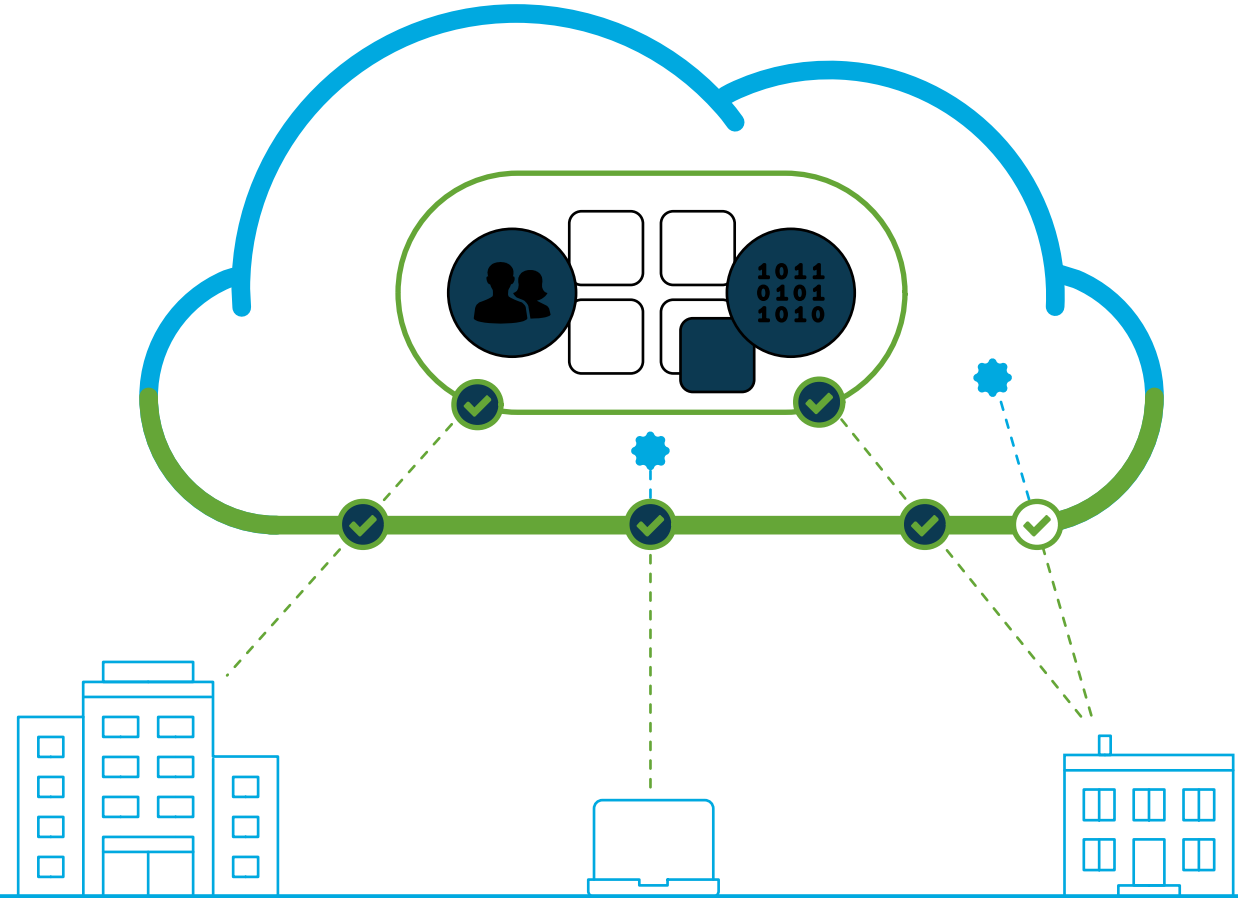
Cisco Cloud Security and Splunk

Cisco Cloud Security

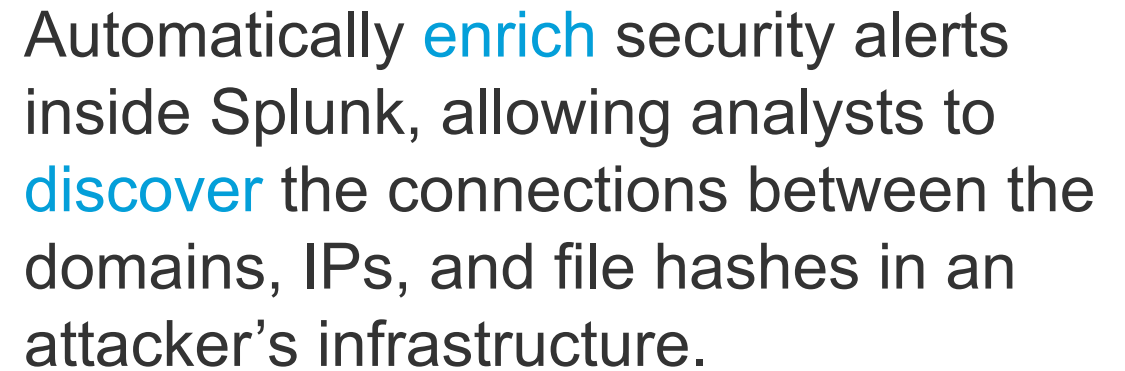
Umbrella

Cloudlock

Investigate

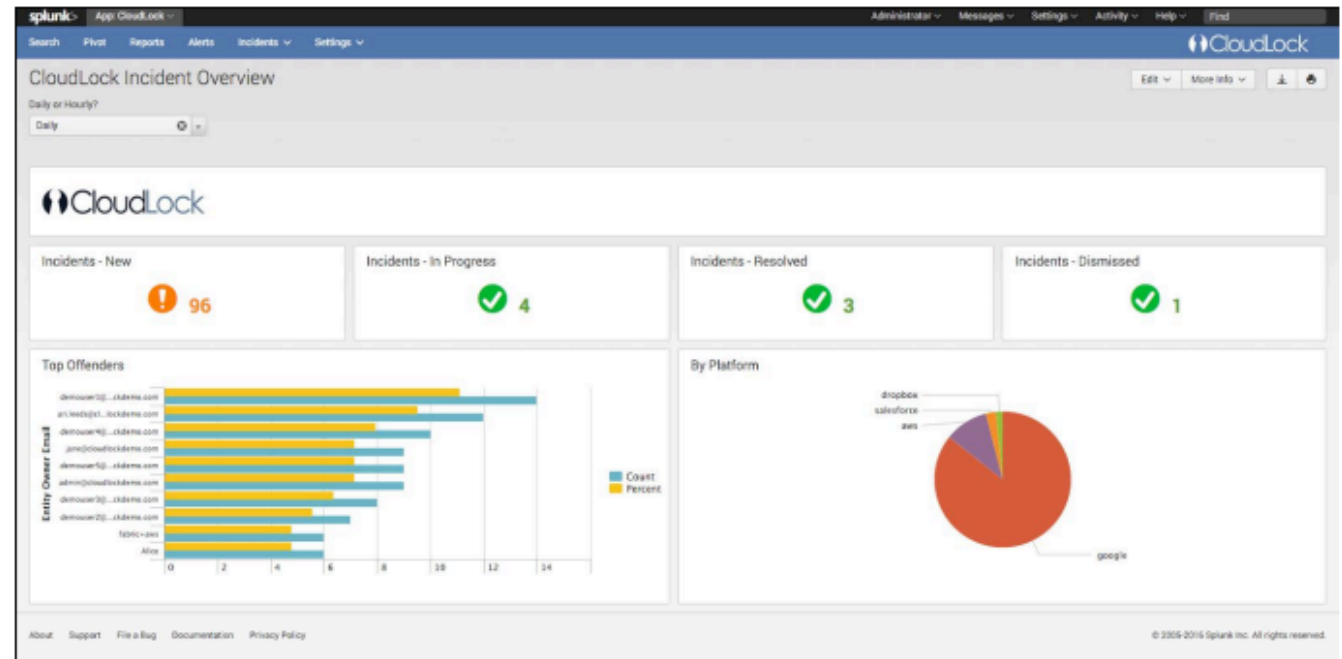


130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D5SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D5SL7FF6ADFF9 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=AV-CB-01&JSESSIONID=5D5SL7FF6ADFF9" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5SL9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0"
125.17.14.118 - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D5SL9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D5SL9FF1ADFF3" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_0; rv:53.0) Gecko/20100101 Firefox/53.0"

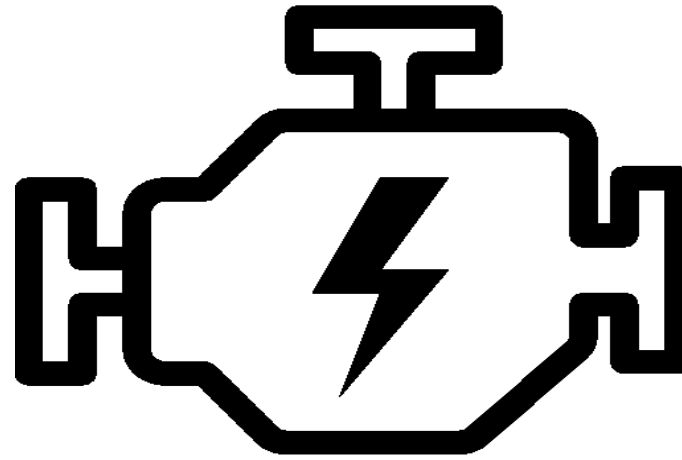


Splunk App for Cisco Cloudlock

- ▶ Manage Cloud Security incidents within Splunk
- ▶ Seamless extend Security Operations to cloud environments while maintaining existing workflows
- ▶ Leverage Splunk's rich data visualization, alerting and reporting functionality
- ▶ Two leaders - Partnership Strength

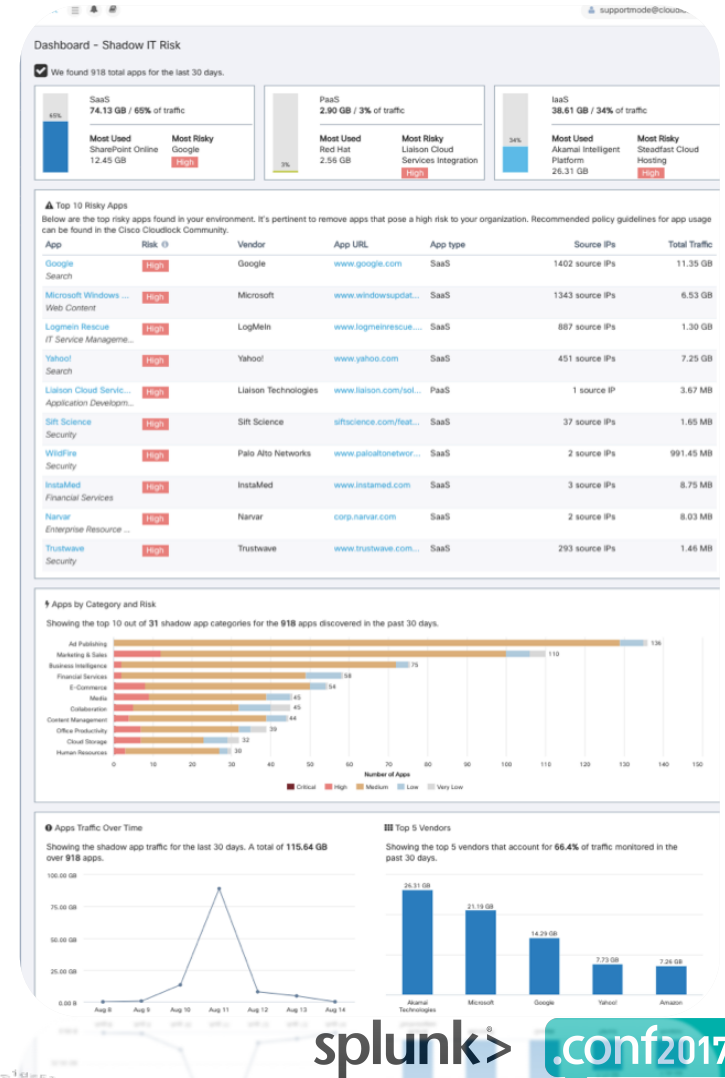


ShadowIT for Cisco FP and Splunk Customers



SIEM: **splunk**>

**DESIGNED TO SUPPORT
ANY DATA SOURCE**

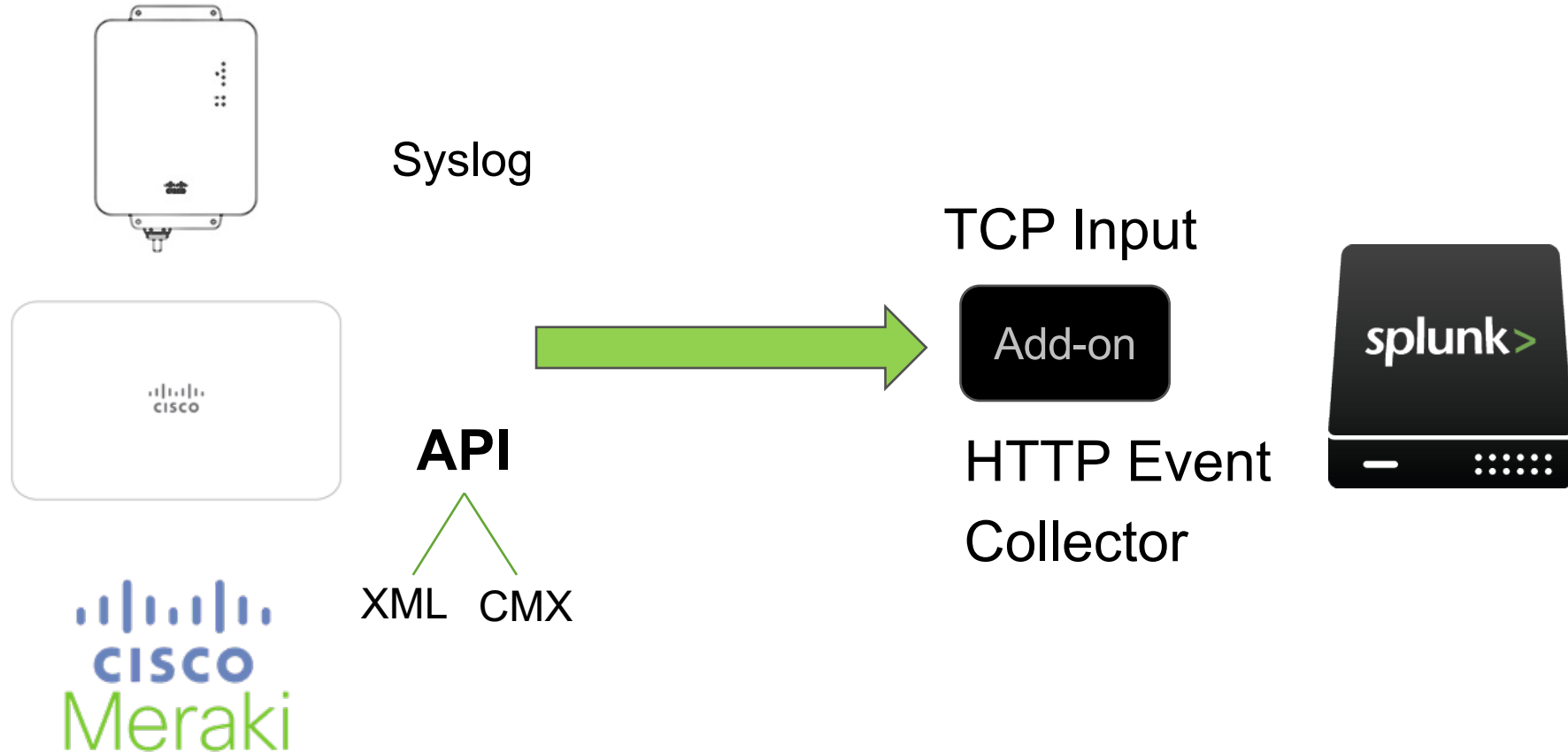


Correlating Network And Infrastructure Data Around The World

Using open APIs monitor and manage connectivity and
security for the largest Latin American country

Colin Lowenberg

Collecting Meraki Data Into Splunk





MÉXICO
CONECTADO

- ▶ Managed WiFi in all Mexican Gov't buildings: libraries, health centers, community buildings, etc.
- ▶ Indoor and outdoor APs for gov't and public use
- ▶ 22K+ sites across Mexico



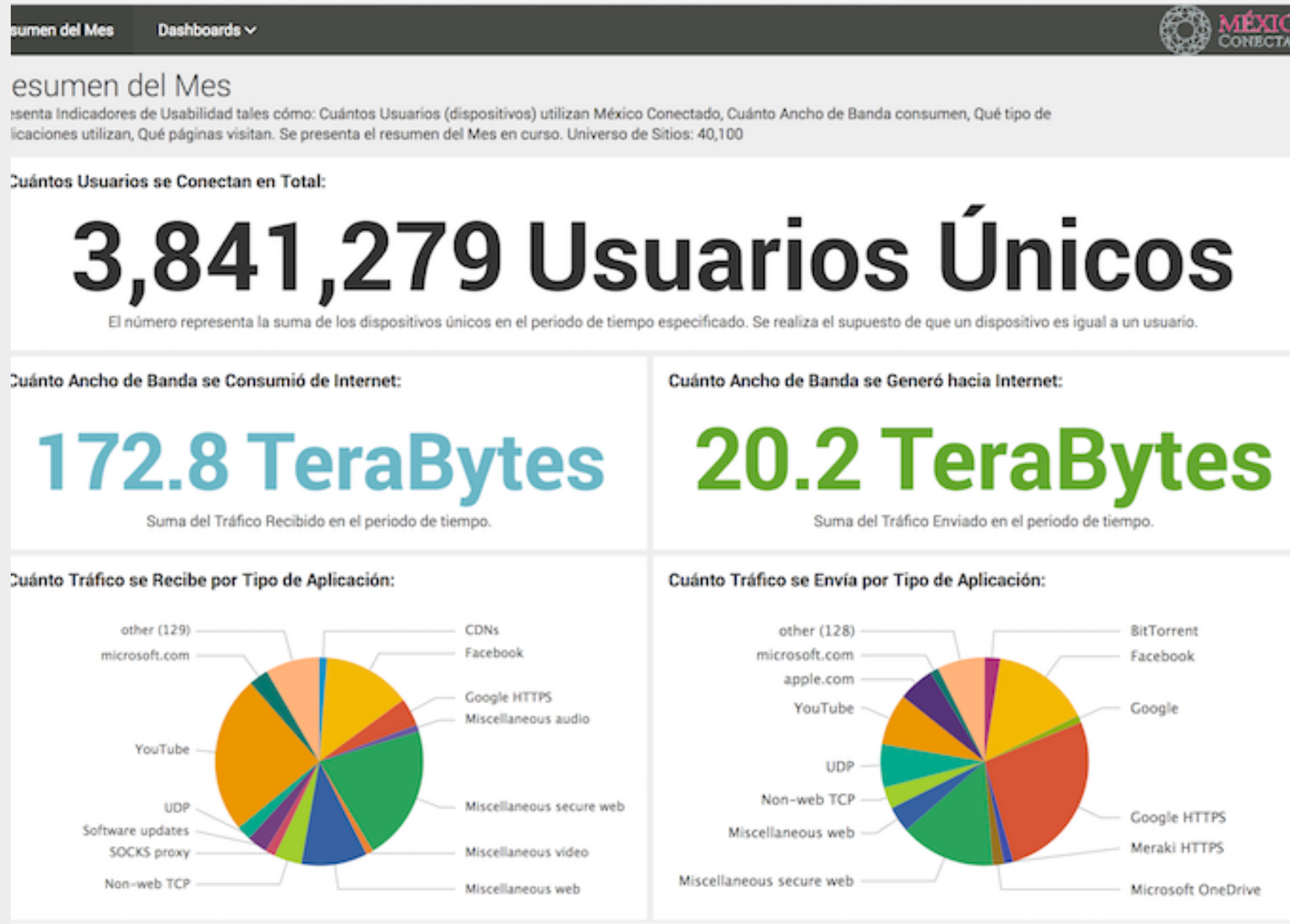
Smart Cities & Government Analytics

The Mexico Conectado
Project

Country Digitization
Analytics Platform

CDAP

(powered by Splunk)



Your Splunk Environment: Better on Cisco UCS

Automate deployment, correlate with your entire datacenter, and optimize for management and scalability

With Karthik Karupasamy

Cisco UCS Add-On for Splunk Enterprise

Splunk Add-On for Cisco UCS

- ▶ Splunk-built rewrite of original UCS add-on
- ▶ 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




Accelerated Troubleshooting with Splunk & UCS



See demo on Youtube at bit.ly/splunk-ucs-mtti

Cisco Unified Computing System

A differentiated, revolutionary approach



Simplified Architecture

- ▶ Networking with fewer components
- ▶ Lower cost and easier scaling
- ▶ Fewer management touch points
- ▶ Stateless: any resource, any time
- ▶ Better TCO/ROI



Unified Management

- ▶ Faster deploy/provision
- ▶ Unification leads to reduced complexity
- ▶ Management via a single interface



Higher Performance

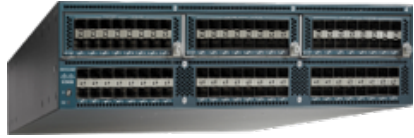
- ▶ Brings out the best of x86 architecture
- ▶ Optimized resource utilization for compute, networking, and management



Scale

- ▶ Ultimate Scalability
Enhanced design capability
- ▶ Designed for the future, today

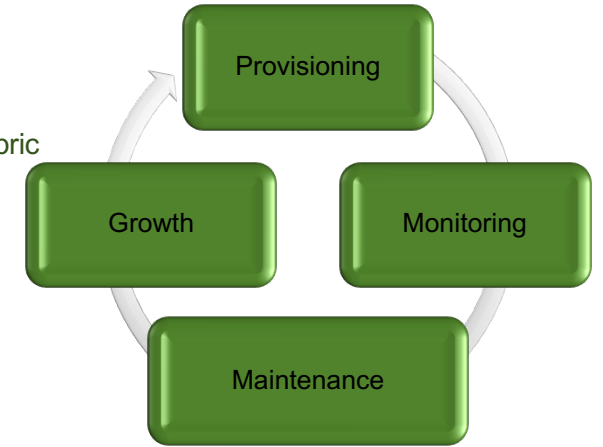
Cisco UCS Integrated Infrastructure for Big Data Topology



Support for direct connectivity to Fabric Interconnects

SingleConnect: LAN, SAN and Management

UCS 6200 and 6300 Series Fabric Interconnects, Installed in pairs, active-active. UCS Manager is embedded



Pre-tested and pre-validated configuration

Fabric-based infrastructure integrates computing, networking, and storage resources

Designed for high performance and availability



Cisco UCS Director Express for Big Data

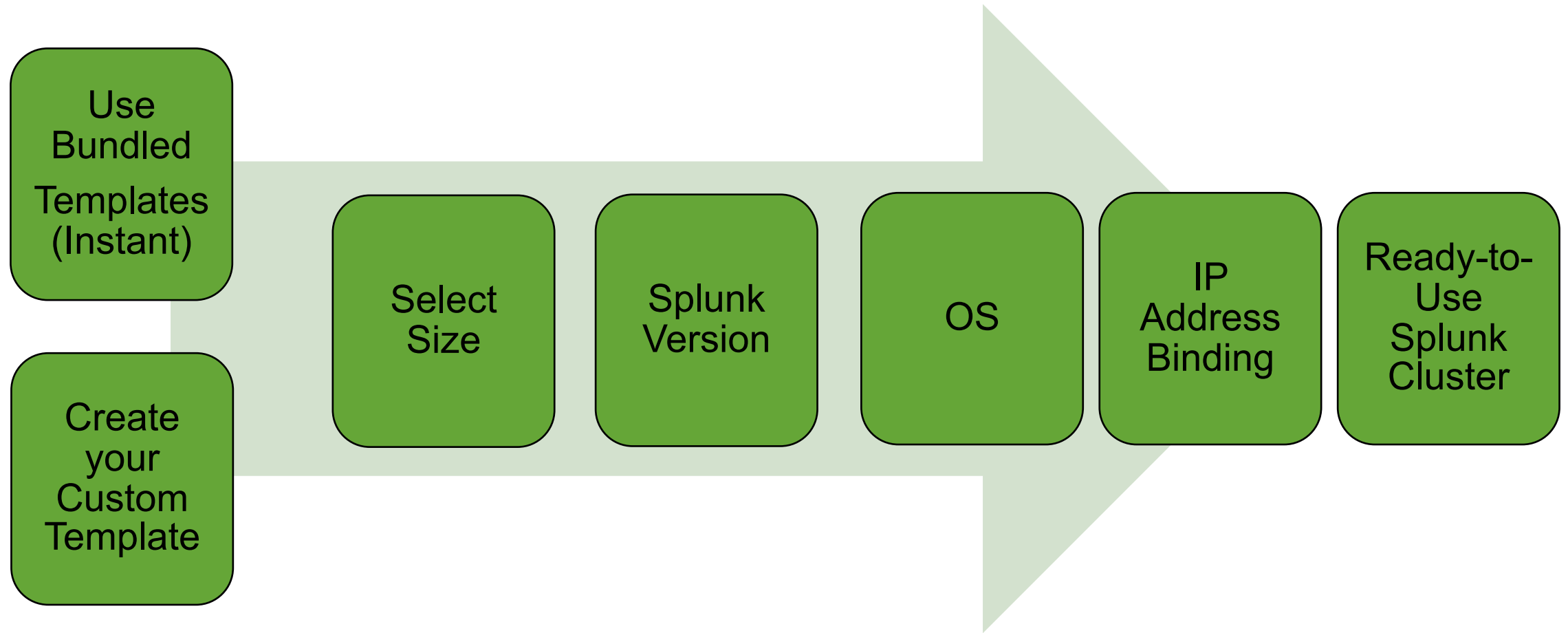
Deploy your Splunk Enterprise Cluster in hours – not in days or weeks

- ▶ Complete automation of industry-leading validated solution for Splunk Enterprise
- ▶ Indexer clustering – customizable Replication and Search Factors
- ▶ Search Head clustering
- ▶ Shared License Master, Deployer for SHC
- ▶ Ability to grow the Search head, Indexer clusters.
- ▶ Monitoring console

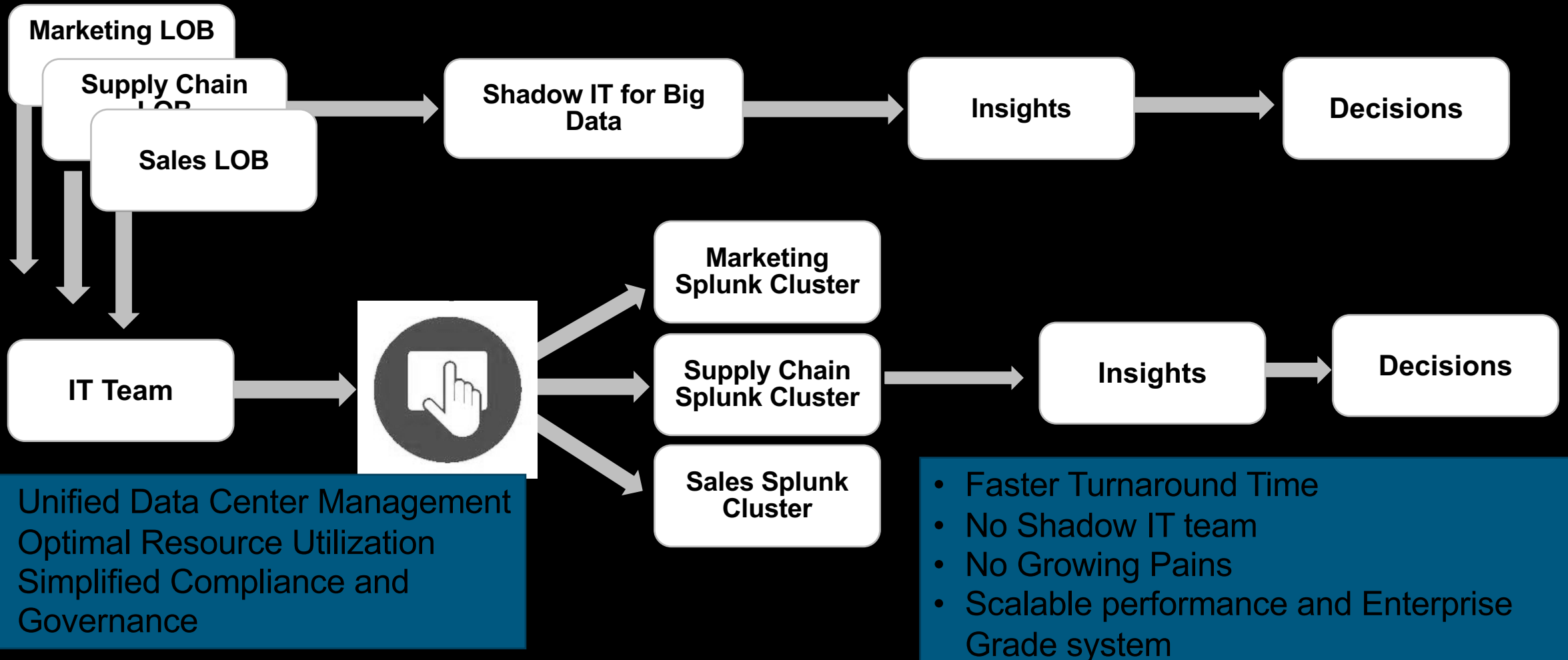
- ▶ Complete automation of industry-leading validated solution for Splunk Enterprise
- ▶ Indexer clustering – customizable Replication and Search Factors
- ▶ Search Head clustering
- ▶ Shared License Master, Deployer for SHC
- ▶ Ability to grow the Search head, Indexer clusters.
- ▶ Monitoring console

UCSD Express For Big Data – Two Ways to Create

Unified Management Platform for Highly Available Distributed Splunk Clusters

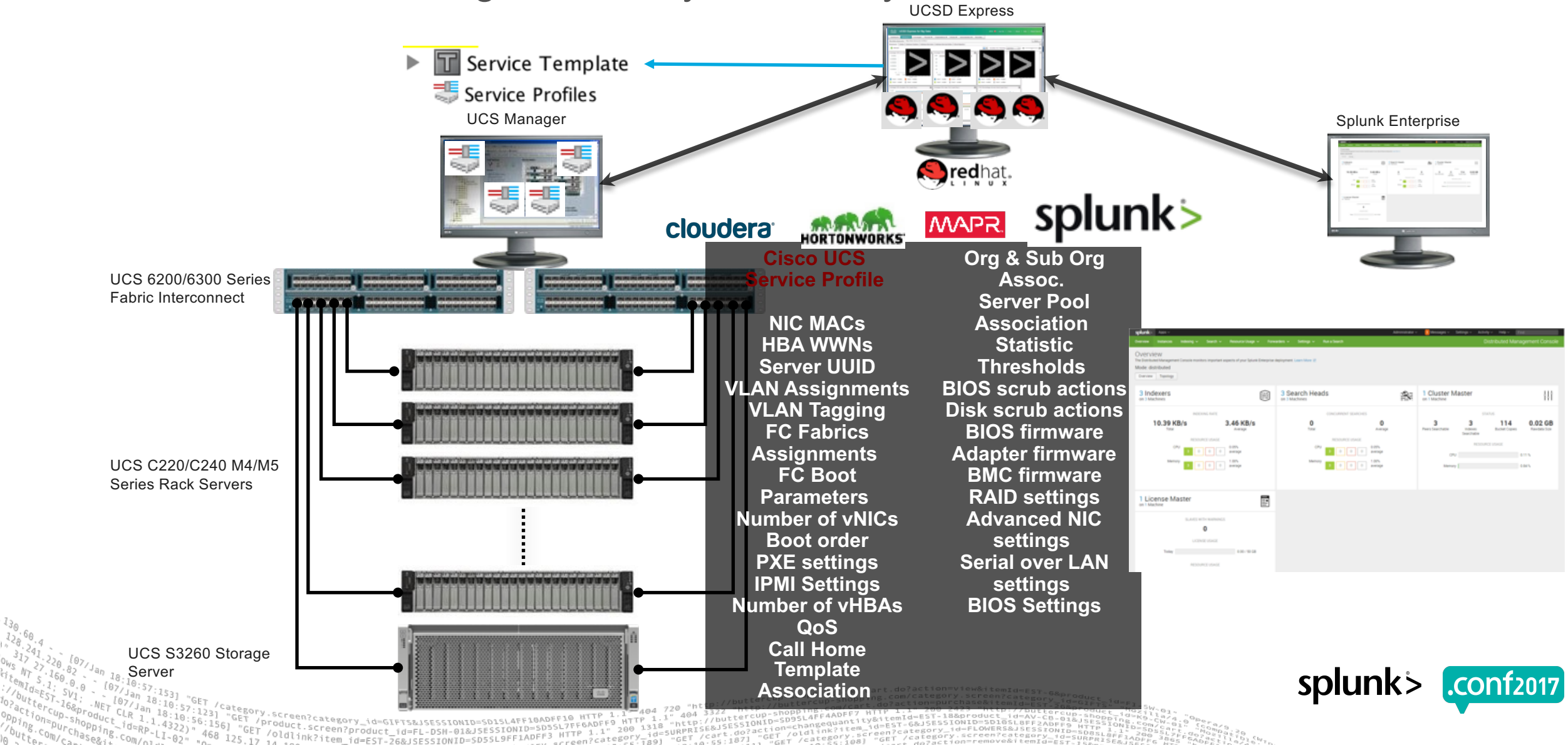


Instant Splunk Cluster Under One Management



Unified Management with UCS Director Express for Big Data

Programmability, Scalability and Automation



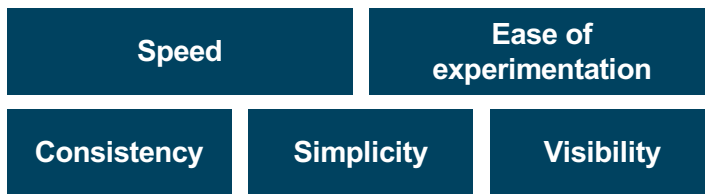
Programmable Infrastructure

Policy based Management

Abstraction of all configuration and identity information into a service profile speeds deployment, reduces errors, lowers costs



UCS Management Software provides:



UCS Manager

- Industry leading tool to provision, manage and monitor all software and hardware components
- Policy and model-based management, with service profiles, that improves agility and reduces risk
- Utilizes auto-discovery to detect, inventory, manage, and provision system components
- Offers a comprehensive open XML API, which facilitates integration with third-party management tools

UCS Central

- Manages multiple, globally distributed Cisco UCS domains with thousands of servers from a single pane
- Provides global configuration capabilities for pools, policies, and firmware

UCS Director

- Delivers a unified converged infrastructure management solution
- Provides programmable application containers across computing, networking, and storage resources and extend automation benefits to the entire infrastructure stack

UCS Director Express for Big Data

- Delivers scalable and reliable Hadoop deployment on UCS Big Data clusters
- Offers centralized visibility across Hadoop and physical infrastructure
- Provides greater IT agility resulting in increased IT impact on business

UCS Director Express for Big Data

End-to-end provisioning, deployment and management

1

Subject Matter Expert
Define Policies



Hadoop SME Storage SME Server SME Network SME

Create Infrastructure
Profile

Create Hadoop Profile

Create Hadoop
Application Profile

2

Policies Used to Create
Hadoop and Infrastructure
Service Profile Templates

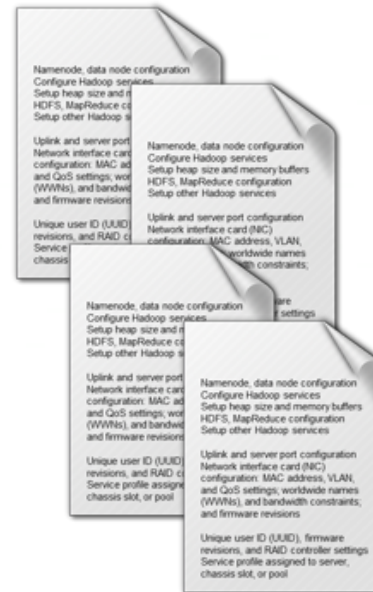
Namenode, data node configuration
Configure Hadoop services
Setup heap size and memory buffers
HDFS, MapReduce configuration
Setup other Hadoop services

Uplink and server port configuration
Network interface card (NIC)
configuration: MAC address, VLAN,
and QoS settings; worldwide names
(WWNs), and bandwidth constraints;
and firmware revisions

Unique user ID (UUID), firmware
revisions, and RAID controller settings
Service profile assigned to server,
chassis slot, or pool

3

Service Profile Templates
Create Service Profiles



4

Associate Hadoop and
Infrastructure Profiles to
create Hadoop Clusters



Creating and Managing Splunk clusters

Splunk Cluster customizations

Select physical infrastructure options

UCSD Express for Big Data

Containers UCS SP Template

Create UCS SP Template for Big Data

UCS SP Template Specification

Template Name* Production

Template Description

Template Type* Updating Template

Container Type* splunk

Use vNIC Bonding ☐

Use Multiple vNIC ☐

Next Cancel Next

Optionally add another NIC for Replication Traffic

UCSD Express for Big Data

Containers UCS SP Template

Create UCS SP Template for Big Data

UCS SP Template Specification

Create vNIC Policy

vNIC Name	Fabric	Enable Failover	VLANs	MTU	Pin Group	Adapter Policy	Dynamic vNIC Connection Pol.	QoS Pol.	Network Control Policy
eth0	A	true	MGMT	9000	<not set>	Linux	<not set>	QoSSP	default
eth1	A	true	Replication	9000	<not set>	Linux	<not set>	QoSBest	default

When you delete the vNICs, ensure that at least one vNIC is available per fabric interconnect

Back Cancel Next

Select custom RAID policy for each Role

UCSD Express for Big Data

Containers UCS SP Template

Create UCS SP Template for Big Data

UCS SP Template Specification

Local Disk Configuration Policy

Local Disk Configuration Details

Use LVM For Disk Configuration ☐

Partition Configuration

Configure Splunk RAID Policy

Node Type	RAID Level(OS)	RAID Level(Hot Data)	RAID Level(Cold Data)	RAID Level(Frozen Data)
Indexer	RAID1	RAID10	Same Disk As Hot Data	Same Disk As Cold Data
Search Head	RAID1	NA	NA	NA
Admin	RAID1	NA	NA	NA
Archival No...	RAID1	NA	NA	RAID10

Total 4 items

Back Cancel Submit

Customize Storage Tiers

Containers UCS SP Template

Edit Configure Splunk RAID Policy Entry

Disks for Hot Data

RAID Level(Hot Data)* RAID10

Disks Per Group* 24

Write Mode* Write back

Read Mode* Read ahead

Use Cache ☐

Use Cache if Bad BBU ☐

Strip Size(MB)* 128

Data Disks for Cold Data

Same Disk As Hot Data ☒

Data Disks for Frozen Data

Same Disk As Cold Data ☒

Creating a Splunk cluster

- ▶ Cluster Name
- ▶ OS (RHEL)
- ▶ Splunk version
- ▶ UCS Manager
- ▶ Organization

The screenshot shows the 'UCSD Express for Big Data' interface. The left sidebar contains navigation icons. The main content area is titled 'Cluster Deploy Templates' and 'Customized Splunk Cluster Creation'. The form includes the following fields:

Field	Value
Big Data Account Name*	prod1
UCSM Policy Name Prefix*	prod1
SSH (root) Password*	
Confirm SSH Password*	
Splunk Manager Password*	
Confirm Splunk Manager Password*	
OS Version*	RHEL7.2
Splunk Distribution Version*	splunk-6.5.2
Multi UCSM	☐
UCS Manager Account*	UCSM1
Organization*	root

At the bottom of the form are 'Cancel' and 'Submit' buttons.

Creating a Splunk Cluster

- Server-pools (per role)
- Map vNIC to IP-Pools.
 - Mgmt, (and ingest)
 - Data1 for Replication (optional),
- Click **Submit**

Replication
Factor,
Search
Factor

PXE VLAN

Server
Pools

Networking

UCSD Express for Big Data

Containers Cluster Deploy Templates

Customized Splunk Cluster Creation

UCS Manager Account* UCSM1

Organization* root

[+] UCS SP Template

PXE VLAN ID* 104
[4048-4093],[1-3967]

Replication Factor* 2

Search Factor* 2

[--] Splunk Server Roles*

Node Type	Node Count	Host Name Pre...	Validate Page	SSD Boot Drives Available for ...	Search Head to be part of clus...	Deploy
Indexer	4	prod-idx	false	false	true	true
Search Head	3	prod-srch	false	false	true	true
Admin	1	prod-admin	true	false	true	true
Archival No...			false	false	false	true

Total 4 items

[--] vNIC Template*

vNIC Name	IP Pool	MAC Address Pool	VLAN ID
eth0	Pool1:50.1.1.1	Mgmt	101
eth1	Pool2:0.0.0.0	Data1	220

Total 2 items

When you use vNIC bonding, ensure that you assign IP Pool, MAC Address Pool and VLAN ID to the first vNIC in the vNIC Template table.

Cancel Submit

Creating a Splunk Cluster -- Server Pool Selection

Server
Count

Server
Pools

Hostname
Prefix

Containers Cluster Deploy Templates

Edit Splunk Server Roles Entry

Node Type Indexer

Node Count* 4

Host Name Prefix* prod-idx

[--] Server Pool* (UCSM1;org-root/compute-pool-Indexer;5)

	ID	Server Pool	Server Pool Policy Qualificati...	Assign...	Size
☐	UCSM1;org-root/compute-pool-default;0	default		1	1
☐	UCSM1;org-root/compute-pool-ucs;8	ucs		3	11
☐	UCSM1;org-root/compute-pool-960gb-ssd;0	960gb-ssd		1	1
☒	UCSM1;org-root/compute-pool-Indexer;5	Indexer		2	7
☐	UCSM1;org-root/compute-pool-Search;4	Search		2	6
☐	UCSM1;org-root/compute-pool-Admin;1	Admin		1	2
☐	UCSM1;org-root/compute-pool-C220;3	C220		2	5
☐	UCSM1;org-root/compute-pool-Admin1;1	Admin1		0	1
☐	UCSM1;org-root/compute-pool-rack6-13;7	rack6-13		1	8

Cancel Submit

Creating a Splunk Cluster -- VNIC configuration

- Map vNIC to IP-Pools.

NOTE: eth0 → MGMT pool binding shown.

- Click **Submit**

Containers Cluster Deploy Templates

Edit vNIC Template Entry

vNIC Name eth0

IP Pool* Pool1(50.1.1.150 - 50.1.1.180)

MAC Address Pool* Mgmt (503)

VLAN ID* 101

[4048-4093],[1-3967]

(MGMT VLAN)

Cancel Submit

UCSD Express for Big Data

Containers Cluster Deploy Templates

Customized Splunk Cluster Creation

UCS Manager Account* UCSM1

Organization* root

[+] UCS SP Template

PXE VLAN ID* 104

[4048-4093],[1-3967]

Replication Factor* 2

Search Factor* 2

[--] Splunk Server Roles*

Node Type	Node Count	Host Name Pre...	Validate Page	SSD Boot Drives Available for ...	Search Head to be part of clus...	Deploy
Indexer	4	prod-idx	false	false	true	true
Search Head	3	prod-srch	false	false	true	true
Admin	1	prod-admin	true	false	true	true
Archival No...			false	false	false	true

Total 4 items

[--] vNIC Template*

vNIC Name	IP Pool	MAC Address Pool	VLAN ID
eth0	Pool1:50.1.1.1	Mgmt	101
eth1	Pool2:0.0.0.0	Data1	220

Total 2 items

When you use vNIC bonding, ensure that you assign IP Pool, MAC Address Pool and VLAN ID to the first vNIC in the vNIC Template table.

Cancel Submit

Flexible RAID config via UCS HW Profiles

- ▶ Splunk Cluster is powered by Underlying UCS HW Template
- ▶ Splunk's UCS HW Template comes with Flexible RAID Policy
- ▶ RAID Policies Supported:
 - RAID1, RAID0
 - RAID5, RAID6
 - RAID10 (**default**)
 - Future (RAID50, RAID60)
- ▶ Separate RAID policies for HOT/WARM, COLD and Frozen

Splunk UCS HW Template – RAID Policy

The screenshot shows the 'UCSD Express for Big Data' interface. The left sidebar contains a list of configuration options: UCS SP Template Sp..., Create QoS Policy, Create VLAN Policy, Create vNIC Policy, Create UCS BIOS Policy, and Local Disk Configurati... (selected). The main panel is titled 'UCS SP Template for Big Data - Local Disk Configuration Policy'. It includes a 'Local Disk Configuration Details' section with a checkbox for 'Use LVM For Disk Configuration'. Below this is a 'Partition Configuration' section with a table of mount points and sizes. At the bottom, there is a link to 'Configure Splunk RAID Policy' and buttons for 'Back', 'Cancel', and 'Submit'.

UCSD Express for Big Data

Containers UCS SP Template

Modify UCS SP Template for Big Data

- UCS SP Template Sp...
- Create QoS Policy
- Create VLAN Policy
- Create vNIC Policy
- Create UCS BIOS Policy
- Local Disk Configurati...

UCS SP Template for Big Data - Local Disk Configuration Policy

Local Disk Configuration Details

Use LVM For Disk Configuration ☐

[-] Partition Configuration

+ / ✎

Mount Po...	Size(GB)
/boot	1
/	1 with grow
/tmp	5
/var/tmp	5
swap	2
/home	5

[+] Configure Splunk RAID Policy

Back Cancel Submit

Custom
Partitions

RAID
Policy

Splunk UCS HW Template – Inside the RAID Policy

The screenshot shows the 'Edit Configure Splunk RAID Policy Entry' window. On the left is a sidebar with a list of configuration steps: UCS SP Template Specification, Create QoS Policy, Create VLAN Policy, Create vNIC Policy, Create UCS BIOS Policy, Local Disk Configuration Policy, and Edit Configure Splunk RAID Policy Entry (which is selected). The main area is divided into two columns. The left column contains settings for 'Disks for Hot Data' (RAID Level, Disks Per Group, Write Mode, Read Mode, Use Cache, Use Cache if Bad BBU, Strip Size) and 'Data Disks for Cold Data' (Same Disk As Hot Data). The right column contains settings for 'Data Disks for Frozen Data' (Same Disk As Cold Data). The 'RAID Level' is set to RAID10, 'Disks Per Group' is 24, 'Write Mode' is Write back, 'Read Mode' is Read ahead, 'Strip Size' is 128, 'Use Cache' is unchecked, 'Use Cache if Bad BBU' is unchecked, 'Same Disk As Hot Data' is checked, and 'Same Disk As Cold Data' is checked.

Section	Setting	Value
Disks for Hot Data	RAID Level[Hot Data]*	RAID10
	Disks Per Group*	24
	Write Mode*	Write back
	Read Mode*	Read ahead
	Use Cache	☐
	Use Cache if Bad BBU	☐
	Strip Size(MB)*	128
Data Disks for Cold Data	Same Disk As Hot Data	☒
Data Disks for Frozen Data	Same Disk As Cold Data	☒

RAID10 for
HOT/WARM

Cold data
on the same
RAID group

Splunk UCS HW Template – Inside the RAID Policy

UCSD Express for Big Data

Containers UCS SP Template

Edit Configure Splunk RAID Policy Entry

✓ UCS SP Template Sp ...	RAID Level[Hot Data]*	RAID10
✓ Create QoS Policy	Disks Per Group*	16
✓ Create VLAN Policy	Write Mode*	Write back
✓ Create vNIC Policy	Read Mode*	Read ahead
✓ Create UCS BIOS Policy	Use Cache	☐
✓ Local Disk Configurati ...	Use Cache If Bad BBU	☐
✓ Edit Configure Splunk ...	Strip Size(MB)*	128
Data Disks for Cold Data		
	Same Disk As Hot Data	☐
	RAID Level[Cold Data]*	RAID5
	Disks Per Group*	8
	Write Mode*	Write back
	Read Mode*	Read ahead
	Use Cache	☐
	Use Cache If Bad BBU	☐
	Strip Size(MB)*	128
Data Disks for Frozen Data		
	Same Disk As Cold Data	☒

Cancel Submit

RAID10 for
HOT/WARM

RAID5 for
COLD

Typical Big Data Deployment Challenges

- ▶ Paralysis by HW analysis
- ▶ Inconsistent configurations
- ▶ Repeatable results
- ▶ Justifiable costs/TCO/footprint
- ▶ Scalability and sustainability

Cisco UCS Delivers

- ▶ Accelerated Sales cycle/time to production
- ▶ Reduced architectural planning and calculation for the customer
- ▶ Consistent, repeatable results
- ▶ Comprehensive automated deployment
- ▶ Facilitates Splunk expansion at a reduced footprint



ACI and Tetratation

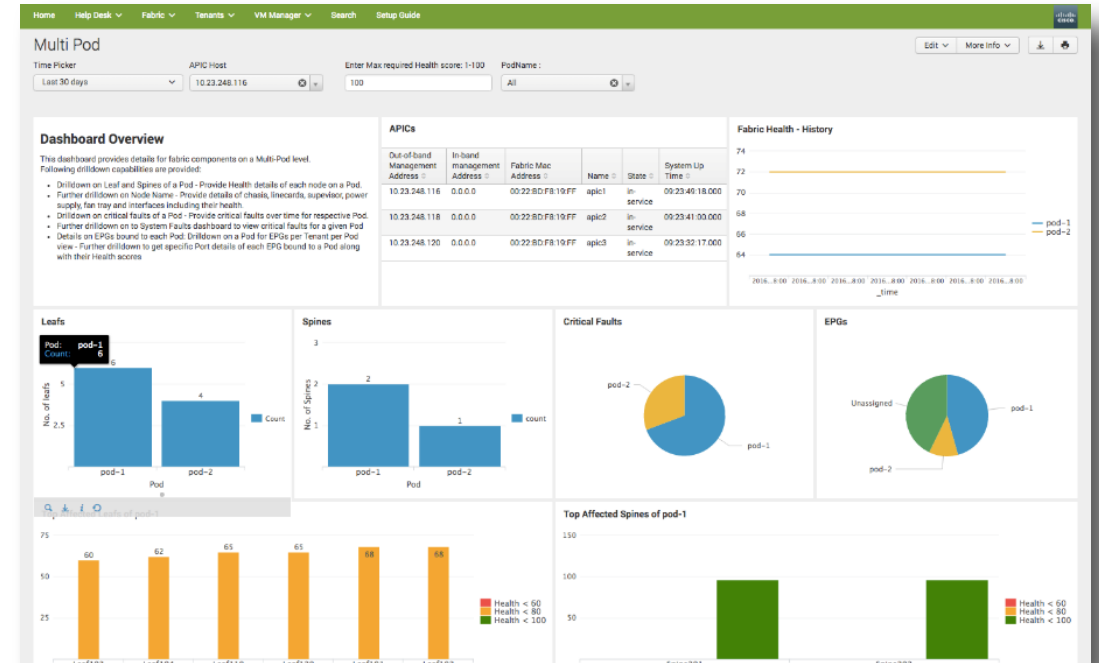
Aci-splunk: What Is New?

Cisco ACI App & Add-on for Splunk Enterprise version 4.0 – Splunk Certified



Splunk Certified

Available on [splunkbase](https://splunkbase.splunk.com)



Supported on APIC 1.3 and higher

Compatible with Splunk 6.4 & above

Multiple APIC monitoring

Multi-Pod visibility

Micro-Segmentation support

Enhanced user interface with drill down capabilities

ACI App Center integration

Log data snippet showing HTTP requests and responses, including headers like 'Host: 10.23.248.116' and 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2; rv:53.0) Gecko/20100801 Firefox/53.0'.

Tetration Analytics App for Splunk

Cisco Tetration App & Add-on for Splunk Enterprise version 1.0

Use Tetration APIs to receive ADM,
Endpoints, Inventory data



Send Configuration data, health & performance
metrics, syslog and fault information
Enforce policies using Tetration sensors

Cisco Tetration
Analytics

Real-time Application
Monitoring

Accelerated RCA & deeper visibility

Policy Enforcement

Why You Never See Tacos Mounted On Drones In The Real World

Wrapping up the Cisco and Splunk innovation story

With Robert Novak

Thank You

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

splunk> .conf2017

Supplemental Information



Cisco Technology	Description	SplunkBase URL
Cisco Security Suite	The Cisco Security Suite provides a single pane of glass interface into Cisco security data.	https://splunkbase.splunk.com/app/525/
Cisco Firepower™ Management Center	Splunk Add-on for Cisco FirePower Management Center leverages data collected via Cisco eStreamer to allow a Splunk Admin to analyze and correlate reports from Cisco through the Splunk Common Information Model.	https://splunkbase.splunk.com/app/1808
Cisco eNcore for Splunk	Comprehensive eStreamer ‘Client’ or Splunk ‘TA’ that collects all ten event types in their entirety from Firepower Management Center 6.x	https://splunkbase.splunk.com/app/3662/
Cisco Umbrella	Automatically enrich security alerts inside Splunk, allowing analysts to discover the connections between the domains, IPs, and file hashes in an attacker’s infrastructure	https://splunkbase.splunk.com/app/3324/
Cisco ISE	Splunk App for Cisco ISE. Collects data from ISE via Syslog and provides Adaptive Network Control (ANC) Mitigation Actions via pxGrid.	https://splunkbase.splunk.com/app/1589/ https://splunkbase.splunk.com/app/1915/
Cisco CloudLock	The CloudLock Cloud Access Security Broker harnesses crowd-sourced, actionable cybersecurity intelligence to enable enterprises to securely leverage the cloud.	https://splunkbase.splunk.com/app/3043/ https://www.cloudlock.com/blog/tag/cloudlock-for-splunk/
Cisco eStreamer	eStreamer log collection and comprehensive selection of dashboards optimized for Sourcefire System 5.2+ and Splunk 6.	https://splunkbase.splunk.com/app/1629/
Cisco IPS	The Splunk Add-on for Cisco IPS allows a Splunk software administrator to consume, analyze, and report on Cisco IPS data that conforms to the Security Device Event Exchange (SDEE) standard.	https://splunkbase.splunk.com/app/1903
Cisco CWS	The Cisco Cloud Web Security (CWS) Add-on for Splunk allows a Splunk administrator to analyze and correlate Cisco Cloud Web Security (CWS) log data through the Common Information Model in Splunk Enterprise	https://splunkbase.splunk.com/app/2791
Cisco ESA	The Splunk Add-on for Cisco ESA allows a the Splunk software administrator to leverage Textmail, HTTP, and Authentication logs of Cisco ESA.	https://splunkbase.splunk.com/app/1761
Cisco AnyConnect	The Cisco AnyConnect Network Visibility (NVM) App for Splunk allows IT administrators to analyze and correlate user and endpoint behavior in Splunk Enterprise.	https://splunkbase.splunk.com/app/2992/
Cisco ASA	The Splunk Add-on for Cisco ASA allows a Splunk software administrator to map Cisco ASA devices, Cisco PIX, and Cisco FWSM events to the Splunk CIM.	https://splunkbase.splunk.com/app/1620