

Disclaimer

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 the 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.

Cavuto Bio

General Awesomeness

Adorable Headshot

Presentation Overview

- Problem Statement
- 2. What is Wire Data? What is Splunk Stream?
- 3. Using Wire data from Stream in ITSI
- 4. Automatic Anomaly Detection using Wire Data in ITSI
- 5. Where to go from here

Problem Statement

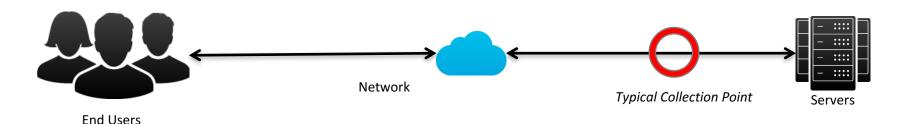
- Applications may not accurately report their own performance accurately, for a number of reasons
 - Heavily loaded
 - Mistaken measurements
 - Developer error
 - It Died!
 - No access to data (politically, organizationally)
 - They're lying! ☺
- Insert quote about trusting something to monitor itself

Why Wire Data with Splunk Stream?

- Use Wire Data provided by Splunk Stream to monitor application and network performance
- Direct ingest into Splunk (no props/transforms) makes it simple
- Stream is not a dedicated APM / NPM tool, but has aspects of both
- In most cases, Stream will do everything you need to isolate faults and pinpoint the trouble spot(s)
- It's Free!

What's Network (Wire) Data?

- Machine data
- Poly-structured data
- Authoritative record of real-time and historical communication between machines and applications



Splunk App for Stream (6.6)



- Metadata Collection
 - Collects essential elements of the application conversation
 - Eliminates redundancy of duplicate packet headers
- Live Interface Collection Option
 - Collect directly on hosts
 - Also from a tap or SPAN port
- Estimate Mode
 - Deploy Stream without collecting data (or affecting license)
 - Test data volume

- Aggregation Mode
 - Statistics generated at endpoint
 - Similar to "stats sum(x)" in SPL
- Filtering at Endpoint
- Out-of-Box Content
 - Dashboards for common protocols
- Distributed Forwarder Mgt
 - Similar to Splunk UF mgt
 - All config centrally managed
 - Forwarder Groups

How will Wire Data help Solve Problem?

- Wire data represents capture of true conversations between endpoints
- It has the "omniscient view" of what actually transpired
- The conversations contain the details about each transaction, including the time of occurrence
- Less chance of interference
 - Intentional / Malicious
 - Load or resource based

Protocols Parsed with Stream 6.6

Simple Transport

- TCP
- UDP
- IP

Infrastructure

- SNMP
- DHCP
- DNS
- ICMP

File Transfer

- FTP
- HTTP

File Service

- NFS
- SMB

Email

- IMAP
- MAPI
- POP3
- SMTP

Messaging

- AMQP
- IRC
- SMPP
- XMPP

Authentication

- Diameter
- LDAP
- RADIUS

Database

- MYSQL
- Postgres
- TDS (Sybase / MS-SQL)
- TNS (Oracle SQL*Net)

VoIP

- SIP
- RTP

Examples of What's Available From the Streaming Network/Wire Data

Performance Metrics
Round Trip Time
Client Request Time
Server Reply Time
Server Send Time
Total Time Taken
Base HTML Load Time
Page Content Load Time
Total Page Load Time

Application Data
POST Content
AJAX Data
Section
Sub-Section
Page Title
Session Cookie
Proxied IP Address
Error Message

Business Data
Product ID
Customer ID
Shopping Cart ID
Cart Items
Cart Values
Discounts
Order ID
Abandoned?

How to Collect and Monitor Data

Stream has two deployment architectures and two collection methodologies

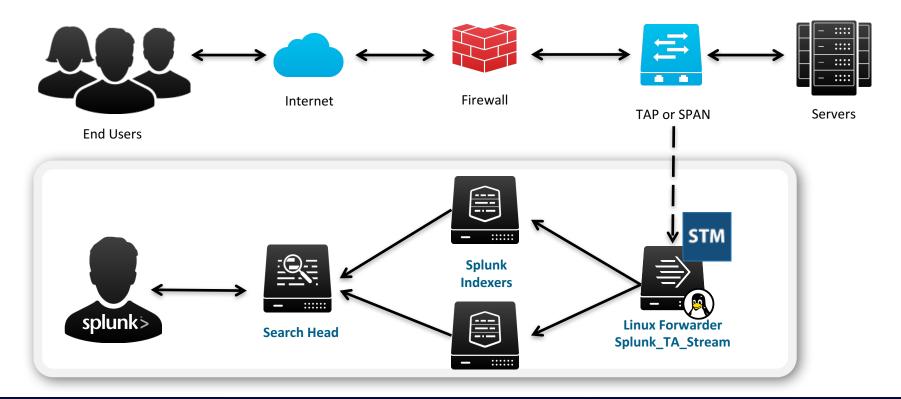
Deployment:

- Out-of-band (stub) with tap or SPAN port
- In-line directly on monitored host

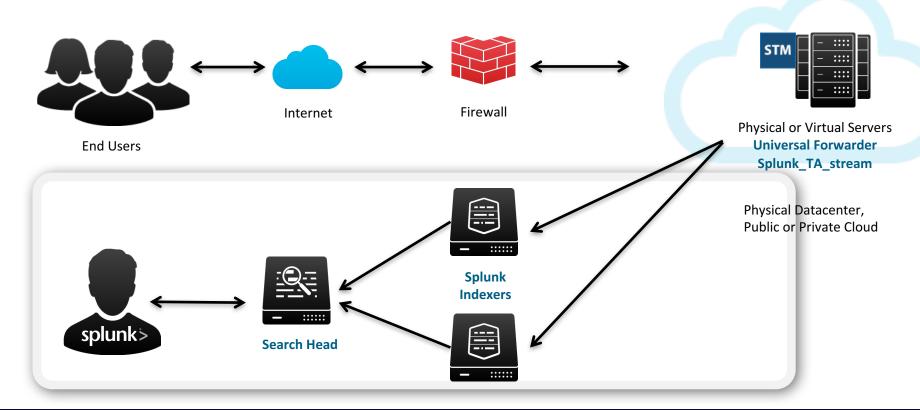
Collection:

- Technical Add-On (TA) with Splunk Universal Forwarder (UF)
- Independent Stream Forwarder using HTTP Event Collector (HEC)

Deployment: Dedicated Collector



Deployment: Run on Servers

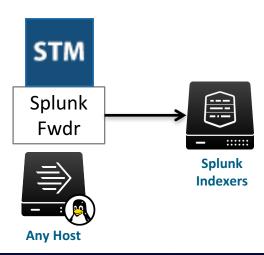


Stream Forwarder Options

Makes it easy to add Stream anywhere in your environment

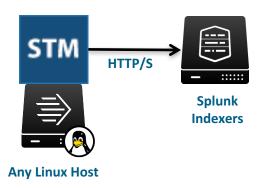
1. Stream TA

 Stream deploys as a modular input on top of your Splunk Forwarders.



2. Independent Stream Forwarder

- Stream deploys as a stand-alone binary and communicates via HEC.
- Requires >= Splunk 6.3.1



300+ Commercial Applications Detected ©



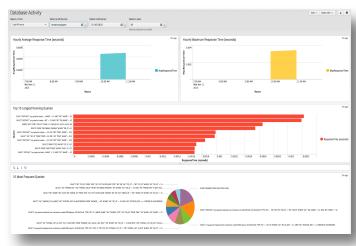
Adobe Flash Plugin Update Adobe Update Manager AIM express AIM Transfer AllMusic.com Altiris Amazon Ad System Amazon Cloud Drive Amazon Generic Services Amazon MP3 Amazon Video Amazon Web Services/Cloudfront CDN Android connectivity Manager Aol AOL Instant Messenger (formerly OSCAR) Apple AirPlay Apple AirPrint Apple AirPrint Apple Apple FaceTime Apple Generic Services Apple HTTP Live Streaming Apple Location Apple Maps Apple Music Apple Push Notification Service Apple SIRI Apple Update ASProxy Atlassian Background Intelligent Transfer Service Baidu Player Baidu wallet Baidu.com Bet365.com Bitcoin client BitTorrent Bittorrent Apps BitTorrent Bleep (aka BitTorrent Chat) BlackBerry Locate BlackBerry Messenger BlackBerry Messenger Audio BlackBerry Messenger Video BlackBerry.com Border Gateway Protocol CARBONITE CCProxy ChatON Chatroulette.com Chrome Update Cisco Discovery Protocol Cisco MeetingPlace Cisco Netflow Common Unix Printer System Crackle craigslist Data Stream Interface DB2 Debian/Ubuntu Update Dropbox Download Dropbox Upload Dropbox.com eBay.com Edonkey Evernote.com EverQuest - EverQuest II Facebook Facebook Messenger FarmVille Find My iPhone Firefox Update Flickr Generic Routing Encapsulation GitHub Gmail Basic Gmail drive Gmail Mobile GNUnet Gnutella Google Accounts Google Analytics Google App Engine Google Cache Google Calendar Google Chat Google Cloud Messaging Google Cloud Storage Google Documents (aka Google Drive) Google Earth Google Generic Google groups Google GStatic Google Hangouts (formerly Google Talk) Google Mail Google Maps Google Picasa Google Play Music, Google Play Musique Google Play Store Google Plus Google Safe Browsing Google Tag Manager Google Toolbar Google Translate Google.com GoToDevice Remote Administration GoToMeeting Online Meeting GoToMyPC Remote Access GPRS Tunneling Protocol GPRS Tunneling Protocol version 2 Half-Life Hi5.com High Entropy Hot Standby Router Protocol HP Printer Job Language Hulu HyperText Transfer Protocol version 2.HTTP/2 I2P Invisible Internet Project IBM Informix IBM Lotus Sametime IBM SmartCloud IBM Websphere MQ iCloud (Apple) iHeartRADIO iMessage File Download Imgur.com Independant Computing Architecture (Citrix) Instagram Internet Group Management Protocol Internet Printing Protocol Internet Security Association and Key Management Protocol Internet Small Computer Systems Interface iOS over-the-air (OTA) update IP Payload Compression Protocol IP-in-IP tunneling IPsec Encapsulating Security Payload IRC File Transfer Data iTunes Jabber File Transfer Java Update JEDI (Citrix) Kazaa (FastTrack protocol) KIK Messenger King Digital Entertainment LinkedIn.com Live hotmail for mobile Livestream.com LogMeIn Rescue magicJack Mail.ru Agent Maktoob mail Media Gateway Control Protocol Message Session Relay Protocol Microsoft ActiveSync Microsoft Lync Microsoft Lync Online Microsoft Office 365 Microsoft Remote Procedure Call Microsoft Service Control Microsoft SharePoint Microsoft SharePoint Administration Application Microsoft SharePoint Blog Management Application Microsoft SharePoint Calendar Management Application Microsoft SharePoint Document Management Application Multi Protocol Label Switching data-carrying mechanism Nagios Remote Data Processor Nagios Remote Plugin Executor Name Service Provider Interface Netflix.com NetMeeting ILS Network Time Protocol Nintendo Wi-Fi Connection Nortel/SynOptics Network Management Protocol OkCupid Online Certificate Status Protocol Oovoo Open Shortest Path First Opera Update Orkut.com Outlook Web Access (Office 365) Outlook Web App PalTalk Paltalk audio chat PalTalk Transfer Protocol Paltalk video Pandora Radio Pastebin Pastebin posting PCAnywhere Photobucket.com Pinterest.com Playstation Network Plenty Of Fish QIK Video QQ QQ File Transfer QQ Games QQ Mail QQ WeiBo QQ.com QQDownload QQLive Network Player QQMusic QQStream Quake quic QVOD Player RapidShare.com Real Time Streaming Protocol Remote Desktop Protocol (Windows Terminal Server) Remote Procedure Call RetroShare Routing Information Protocol V1 Routing Information Protocol V2 Routing Internet Protocol ng1 Rovio Entertainment RSS Salesforce.com SAP SecondLife.com Secure Shell Session Traversal Utilities for NAT SharePoint Online Silverlight (Microsoft Smooth Streaming) Simple Object Access Protocol Skinny Client Control Protocol Slacker Radio Slingbox Snapchat SOCKet Secure v5 SoMud Bittorrent tracker SoundCloud SourceForge SPDY Spotify SquirrelMail Steampowered.com Symantec Norton AntiVirus Updates Syslog Systems Network Architecture Teamspeak v2 TeamSpeak v3 TeamViewer Telnet Teredo protocol Terminal Access Controller Access-Control System Plus TIBCO RendezVous Protocol Tor2web Tumblr Twitch Twitter UStream uTorrent uTP (Micro Transport Protocol) UUSee Protocol VEVO Viber Vimeo.com Vine Virtual Router Redundancy Protocol VMWare vmware horizon view Waze Social GPS Maps & Traffic WebEx WhatsApp Messenger WHOIS WiiConnect24 Wikipedia.com Windows Azure CDN Windows Internet Naming Service Windows Live File Storage Windows Live Groups Windows Live Hotmail Windows Live Hotmail Attachements Windows Live SkyDrive Windows Live SkyDrive Login Windows Marketplace Windows Update WordPress.com World of Warcraft Xbox Live Xbox Live Marketplace Xbox Music Xbox Video (Microsoft Movies and Tv) xHamster.com Yahoo groups Yahoo Mail classic Yahoo Messenger Yahoo Messenger Cransfer Protocol Yahoo Messenger Video Yahoo Search Yahoo webmail for mobile Yahoo Webmessenger Yahoo.com Yellow Page Bind Yellow Page Passwd Yellow Pages Server Youtube.com

Analyzing Wire Data using Splunk

 Once data is collected, use normal SPL to generate dashboards to analyze data

Pros:

- Flexible and Detailed analytics
- Simple drill-downs to raw data
- Cons:
 - SPL is hard!
 - Long Time-to-Value

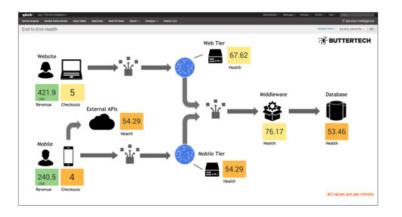


Splunk ITSI

- IT Service Intelligence solution Design "Services" comprised of KPIs
- Specifies, Extracts, and Monitors Key Performance Indicators (KPIs) in your Splunk data
- Glass tables allows you to visualize KPIs on an intuitive layout with color changes and other indicators
- Deep Dives illustrate time-series correlations between KPIs to show elements at fault or temporal causality
- Built in Anomaly Detection with Machine Learning allows

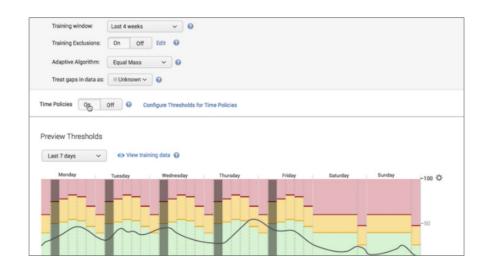
ITSI for Application and Network Monitoring

- Stream + ITSI = APM / NPM ??
- Not quite, but many of the elements
- Monitor the Application
 - Response Time
 - Connections
 - Response Codes
 - Simultaneous
- Monitor the Network
 - Bandwidth
 - Latency
 - Extraneous Traffic



Automatic Anomaly Detection with ITSI

- How do you know when something has gone wrong?
- Typically, anomaly detection takes much tuning, is delicate
- ITSI automatically learns the patterns in your data so anomaly detection happens automatically too!
- Dynamic Machine Learning not simple static thresholds



Demo



Art of the Possible

What else can we do with Stream + ITSI?

- Automatically alert when a new Commercial Application is seen on the network and track the source user
- Dynamically let you know when an unusual number of customer transactions (high or low) are occurring on your eCommerce platform
- Alert when the delay accessing a critical server exceeds a threshold, and then help isolate the source of the trouble (network, host, storage, etc.)

THANK YOU



