splunk> .conf2017

Ending the Finger-Pointing Between Apps and Network Admins

Using Splunk Stream™ for Fault Isolation

David J. Cavuto, CISSP | Principal Product Manager, Data Ecosystem

Eptember 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.

My Bio

- Bell Labs
  - Principal Engineer - Lucent VPN Firewall
- AT&T
  - Network security and analytics
- Narus
  - Product Manager – Narus Cyber Analytics
- Splunk
  - Sales Engineer, Security SME
  - Principal Product Manager – Splunk App for Stream
  - Principal Product Manager – Data Ecosystem Area

- David J. Cavuto
  dcavuto@splunk.com

Presentation Overview

1. Problem Statement
2. What is Wire Data? What is Splunk Stream?
3. Splunk Stream – Product Overview
4. Splunk Stream – Architecture
5. Fault Isolation Methodologies

Problem Statement

- Many different elements of networks
  - Hosts
    - OS
    - Enterprise Software
    - App Software
  - Infrastructure
    - Routers
    - Switches
    - Wireless
- Often those elements are managed by different teams
- How do you fault isolate?

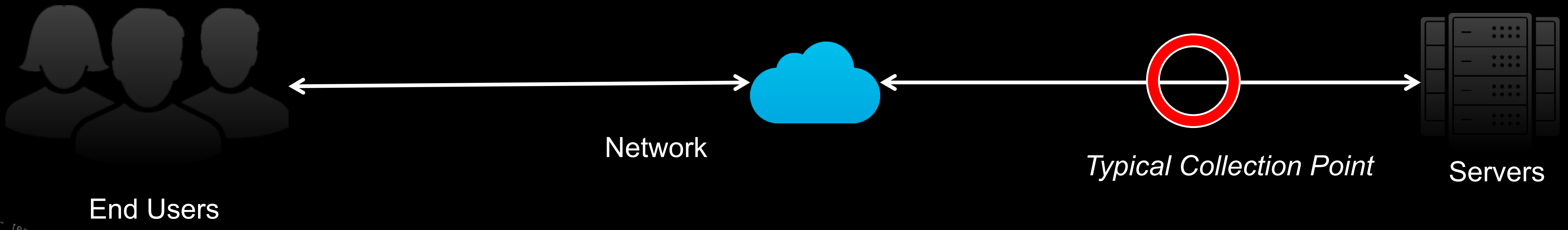
Background on Wire Data and Stream

The Ground Truth

What’s Wire Data?

```
tcpdump -qns 0 -A -r blah.pcap
    20:57:47.368107 IP 205.188.159.57.25 > 67.23.28.65.42385: tcp 480
        0x0000:  4500 0214 834c 4000 3306 f649 cdbc 9f39  E....L@.3..I...9
        0x0010:  4317 1c41 0019 a591 50fe 18ca 9da0 4681  C..A....P.....F.
        0x0020:  8018 05a8 848f 0000 0101 080a ffd4 9bb0  ................
        0x0030:  2e43 6bb9 3232 302d 726c 792d 6461 3033  .Ck.220-rly-da03
        0x0040:  2e6d 782e 616f 6c2e 636f 6d20 4553 4d54  .mx.aol.com.ESMT
        0x0050:  5020 6d61 696c 5f72 656c 6179 5f69 6e2d  P.mail_relay_in-
        0x0060:  6461 3033 2e34 3b20 5468 752c 2030 3920  da03.4;.Thu,.09.
        0x0070:  4a75 6c20 3230 3039 2031 363a 3537 3a34  Jul.2009.16:57:4
        0x0080:  3720 2d30 3430 300d 0a32 3230 2d41 6d65  7.-0400..220-Ame
        0x0090:  7269 6361 204f 6e6c 696e 6520 2841 4f4c  rica.Online.(AOL
        0x00a0:  2920 616e 6420 6974 7320 6166 6669 6c69  ).and.its.affili
        0x00b0:  6174 6564 2063 6f6d 7061 6e69 6573 2064  ated.companies.d
```

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



OSI Stack Model

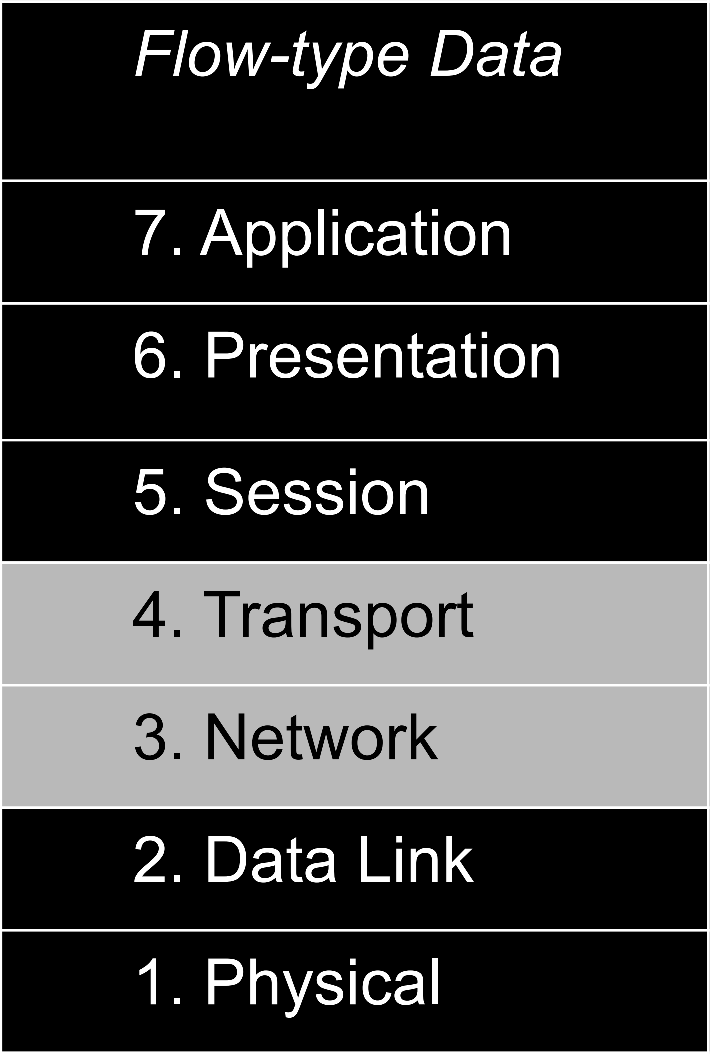
- Open Systems Interconnect (OSI) model
- Published in 1984 by ISO and CCITT (now ITU-T)
- Forms the basis for all modern network communication models
- Hierarchical messages encapsulated as they go down the stack, and get decapsulated as they go up the stack

Layer	*Examples*
7. Application	HTTP, SMTP
6. Presentation	TLS
5. Session	SCP
4. Transport	TCP, UDP
3. Network	IPv4, IPv6
2. Data Link	Ethernet
1. Physical	Ethernet, WiFi

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
- Multidimensional / Multiresolution Data

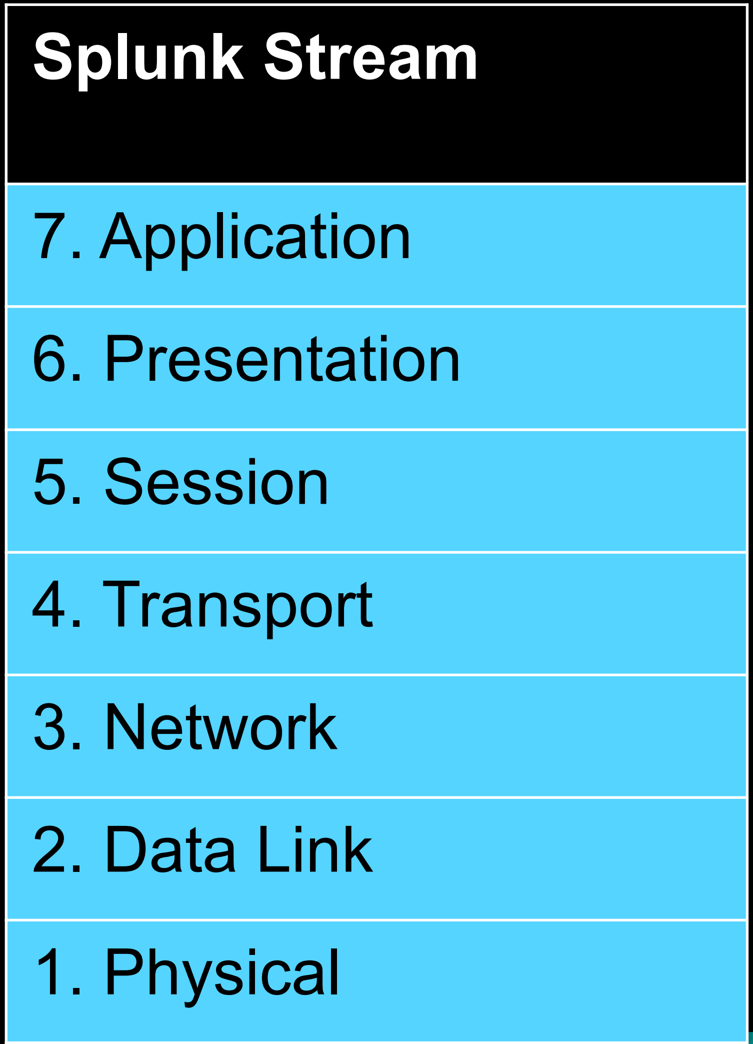
Why Splunk Stream™?



Flow-type Data

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

- Traditional Wire Data flow-type records (such as NetFlow) generally contains only IP addresses and TCP or UDP ports.
- While this can show host-host connections, it doesn't give any insight about the **content** of those conversations (like telephone call records)
- Splunk Stream parses wire data all the way up the stack and generates Events with information at every level (more akin to a written transcript of a phone call)

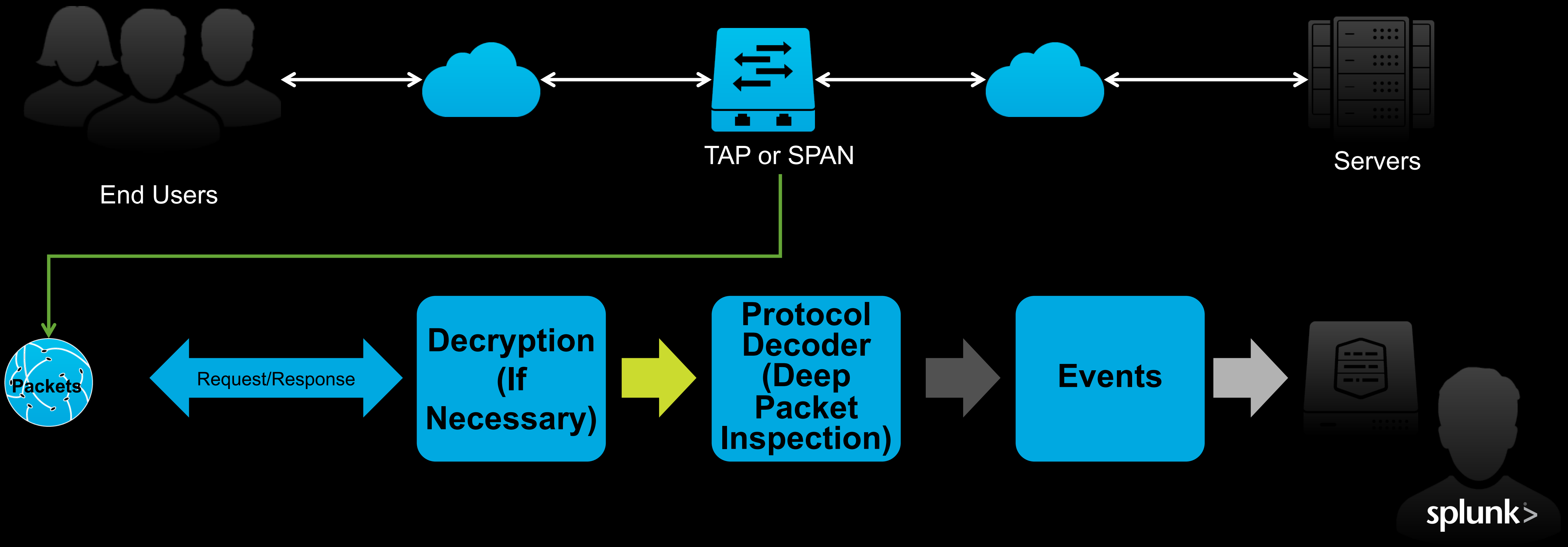


Splunk Stream

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

Product Overview

Wire Data Collection / Metadata Generation


End Users
TAP or SPAN
Servers
Packets
Request/Response
Decryption (If Necessary)
Protocol Decoder (Deep Packet Inspection)
Events
splunk>

Splunk Stream™ (7.1 - GA) Features

STM

- Packet Metadata Collection
  - Collects elements of the application conversation
  - Can use live data from a tap or SPAN port
  - Can extract from PCAP files
  - 1GbE and 10GbE link options
  - Can collect directly on host's inband interface
- Targeted Packet and File Collection
  - Collects "sessionized" bidirectional PCAPs
  - Extracts reassembled File Attachments also
  - Based on L2/3/4/7 Target criteria
  - Saved to customer-supplied NAS
  - Retrieval proxied by SH
- NetFlow Ingestion
  - Explicit Flow Collector for other flow sources
  - NetFlow v5, v9, IPFIX, jFlow, cFlowd, sFlow
  - Can aggregate ingested Flow data
- Estimate Mode
  - Deploy without collecting data
- Commercial App Detection (300+)
  - Works even if the app is encrypted
- TLS/SSL Decryption (with certs)
- Aggregation Mode
  - Statistics generated at endpoint
  - Equivalent to "stats sum(field1), avg(field2)" in SPL
- Filtering at Endpoint (BPF)
- Out-of-Box Content
  - Dashboards for common protocols
- Distributed Forwarder Management
  - All config centrally managed
  - Forwarder Groups

Protocols Parsed with Stream 7.1

Simple Transport

- TCP
- UDP
- IP

Infrastructure

- ARP
- DHCP
- SNMP
- DNS
- ICMP
- IGMP

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
- RTCP

Commercial Application Detection

- Add the many hundreds of applications to be detected to the TCP stream type existing “app” field
- Help diagnose the problem of “what is going over port 80”? And also “what’s taking all of my bandwidth?”
- DOES NOT PARSE applications, simply detects them
  - Will detect encrypted protocols!
  - Will detect vendor-proprietary protocols!
  - Uses empirical patterns, DNS, Cert CNs and other methods
- Current feature supports 300+ applications, many more to be added

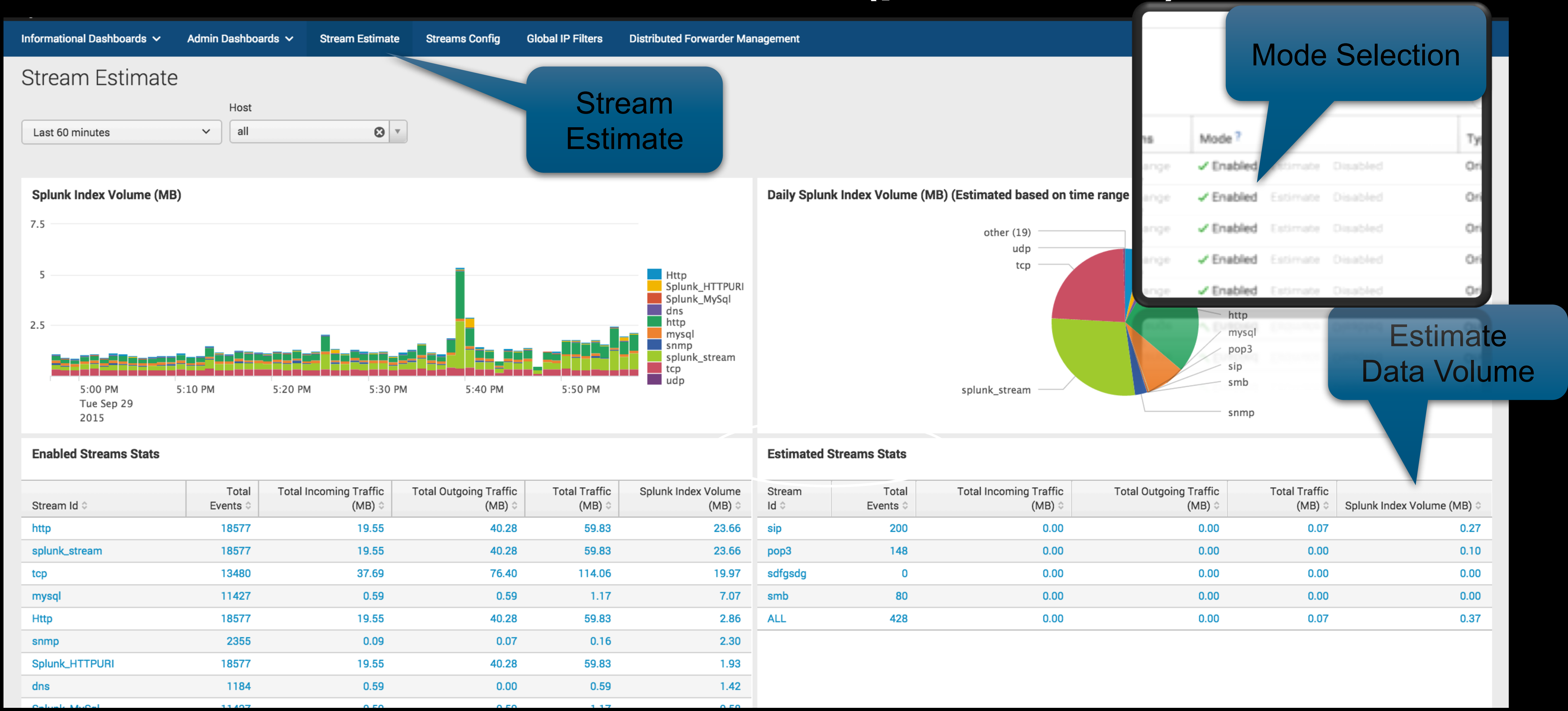
300+ Commercial Applications Detected ☺

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 Airport Apple AirPrint Apple App Store 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 Netwok 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 Twitpic 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 Mail v.2.0 Yahoo Messenger Yahoo Messenger conference service Yahoo Messenger Transfer 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

Application Detection Categories

1. Application Service
2. Audio/Video
3. Authentication
4. Behavioral
5. Database
6. Encrypted
7. ERP
8. File Server
9. File Transfer
10. Forum
11. Game
12. Instant Messaging
13. Mail
14. Middleware
15. Network Management
16. Network Service
17. Peer to Peer
18. Printer
19. Routing
20. Terminal
21. Thin Client
22. Tunneling
23. Web
24. Webmail

Data Estimate Mode (per-Stream)



Stream Estimate

Mode Selection

Estimate Data Volume

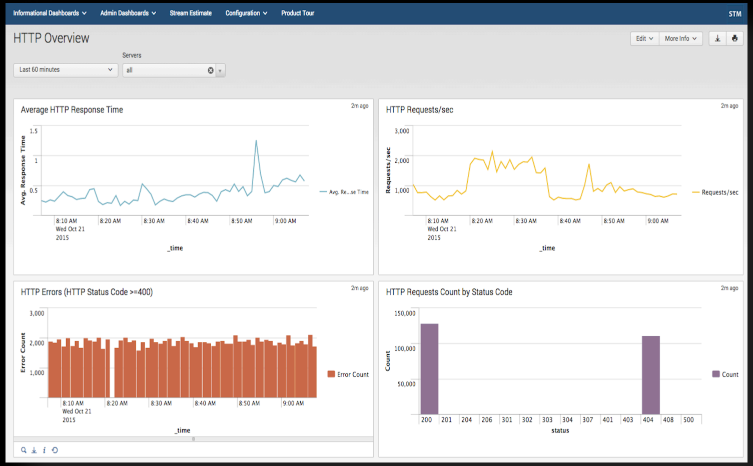
Enabled Streams Stats

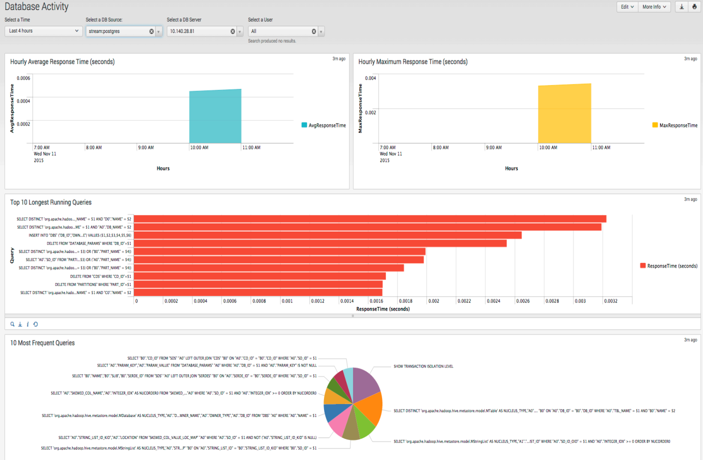
Stream Id	Total Events	Total Incoming Traffic (MB)	Total Outgoing Traffic (MB)	Total Traffic (MB)	Splunk Index Volume (MB)
http	18577	19.55	40.28	59.83	23.66
splunk_stream	18577	19.55	40.28	59.83	23.66
tcp	13480	37.69	76.40	114.06	19.97
mysql	11427	0.59	0.59	1.17	7.07
Http	18577	19.55	40.28	59.83	2.86
snmp	2355	0.09	0.07	0.16	2.30
Splunk_HTTPURI	18577	19.55	40.28	59.83	1.93
dns	1184	0.59	0.00	0.59	1.42
Splunk_MySql	11427	0.59	0.59	1.17	0.58

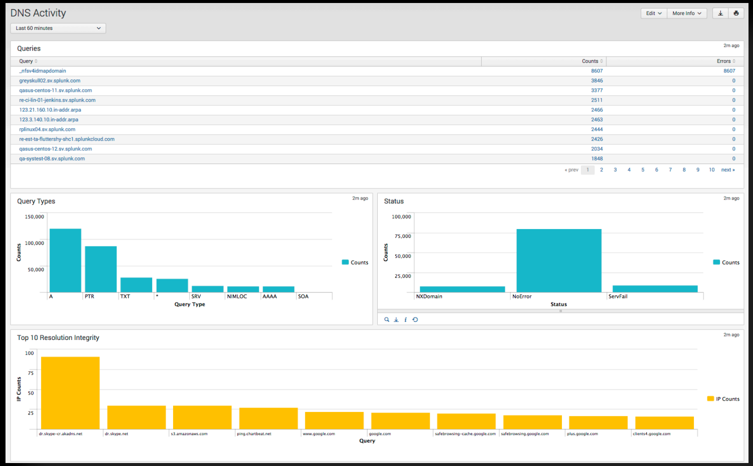
Estimated Streams Stats

Stream Id	Total Events	Total Incoming Traffic (MB)	Total Outgoing Traffic (MB)	Total Traffic (MB)	Splunk Index Volume (MB)
sip	200	0.00	0.00	0.07	0.27
pop3	148	0.00	0.00	0.00	0.10
sdfgsdg	0	0.00	0.00	0.00	0.00
smb	80	0.00	0.00	0.00	0.00
ALL	428	0.00	0.00	0.07	0.37

Prebuilt Reporting







Query	Counts	Errors
_nfsv4idmapdomain	8607	8607
greyskull02.sv.splunk.com	3846	0
qasus-centos-11.sv.splunk.com	3377	0
re-ci-lin-01-jenkins.sv.splunk.com	2511	0
123.21.160.10.in-addr.arpa	2466	0
123.3.140.10.in-addr.arpa	2463	0
rplinux04.sv.splunk.com	2444	0
re-est-ta-fluttershy-shc1.splunkcloud.com	2426	0
qasus-centos-12.sv.splunk.com	2034	0
qa-systest-08.sv.splunk.com	1848	0

Get visibility into applications performance and user experience

Understand database activity and performance without impacting database operation

Improve security and application intelligence with DNS analytics

splunk> .conf2017

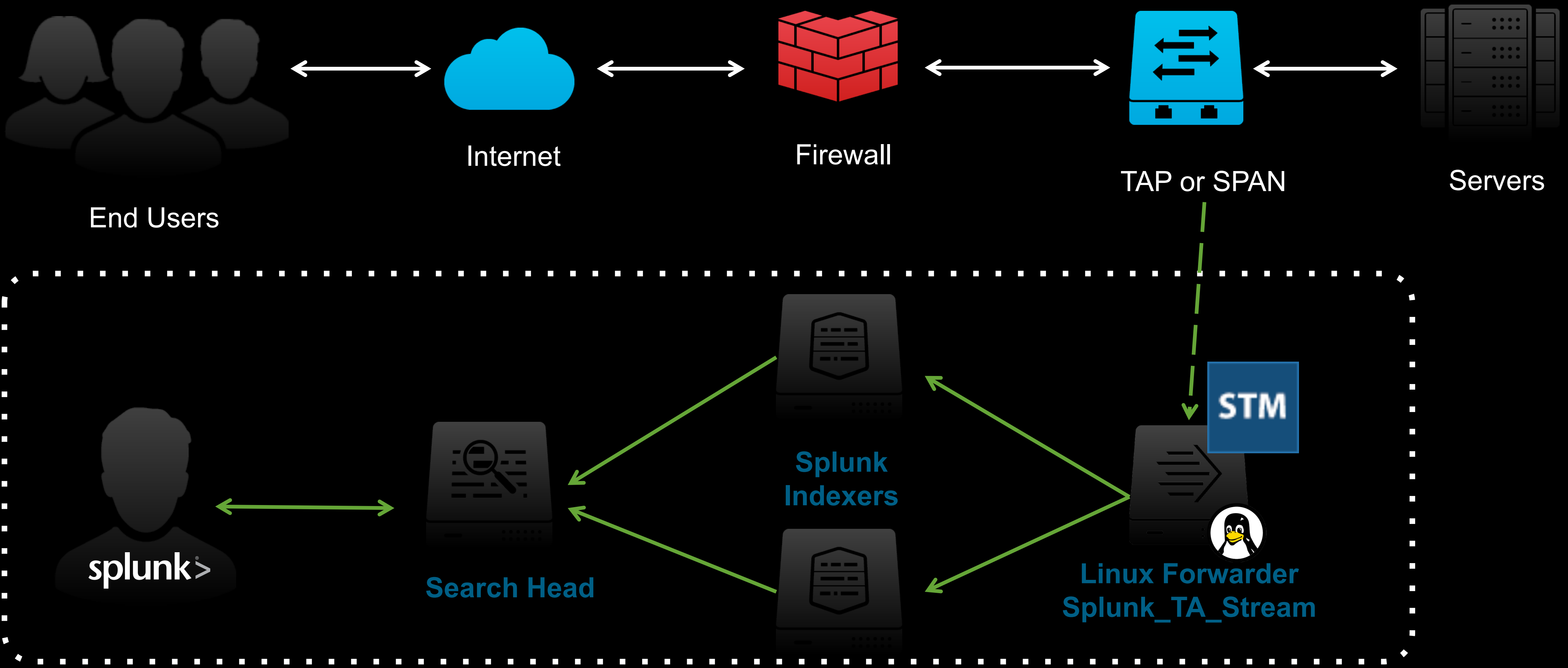
Architecture and Deployment

\

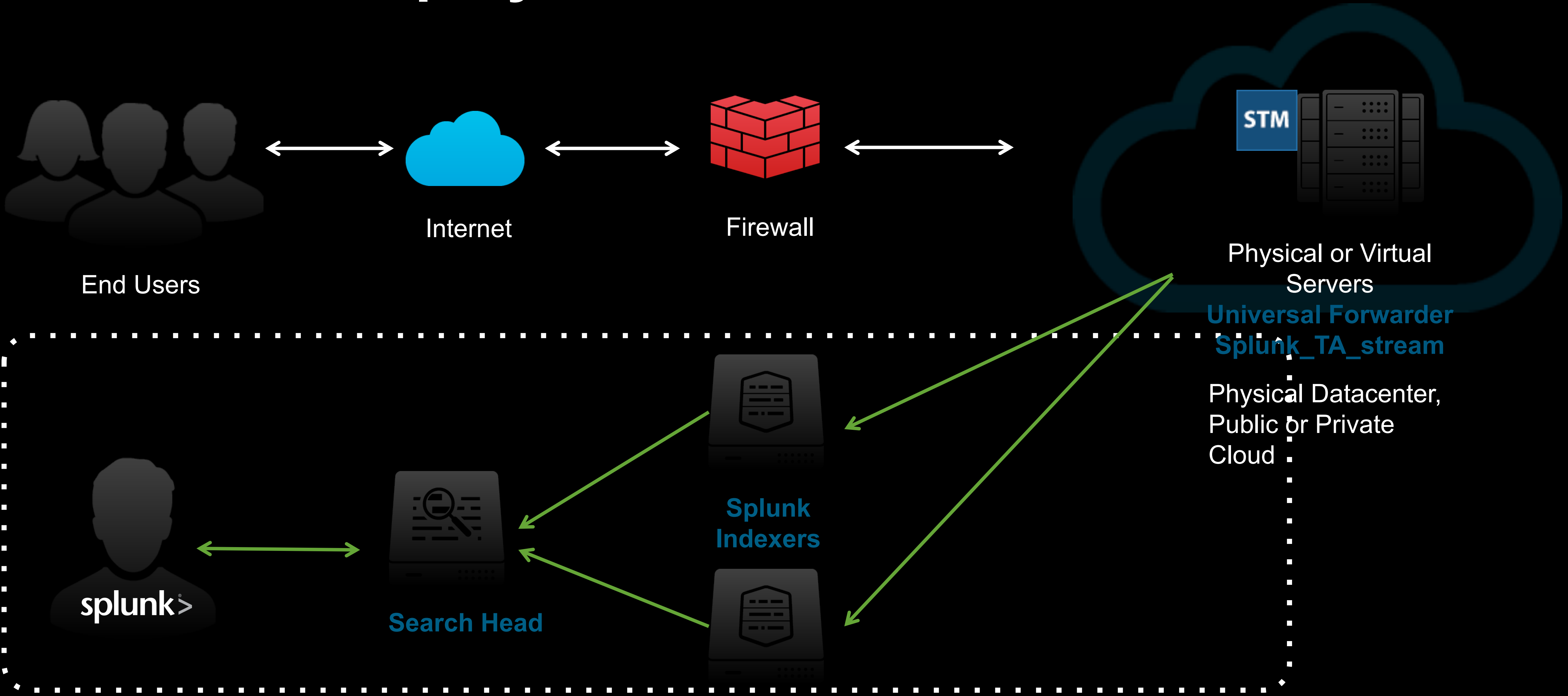
Collect and Monitor Data with Stream

- 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

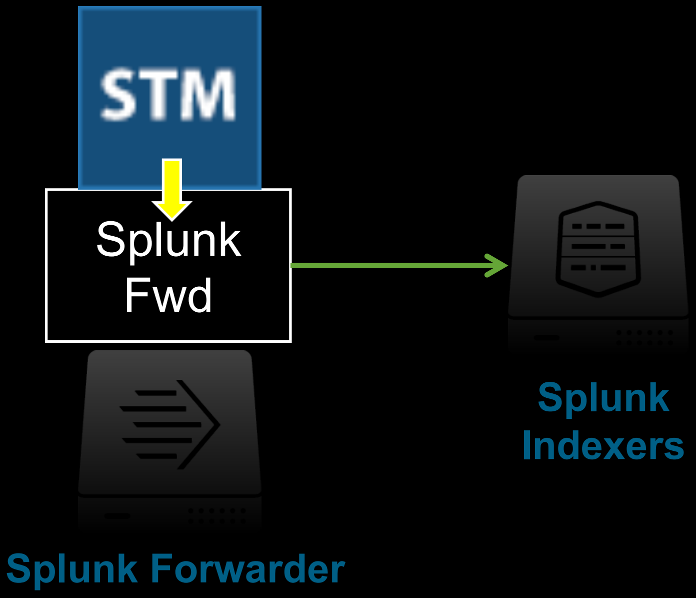


Stream Forwarder Options

Makes it easy to add Stream anywhere in your environment

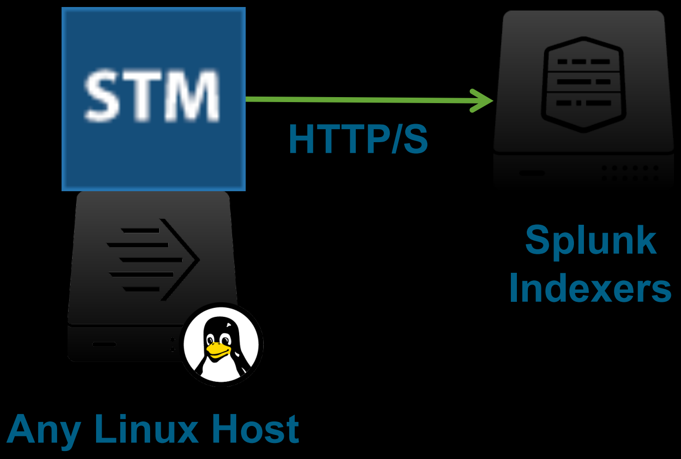
1. Stream TA

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

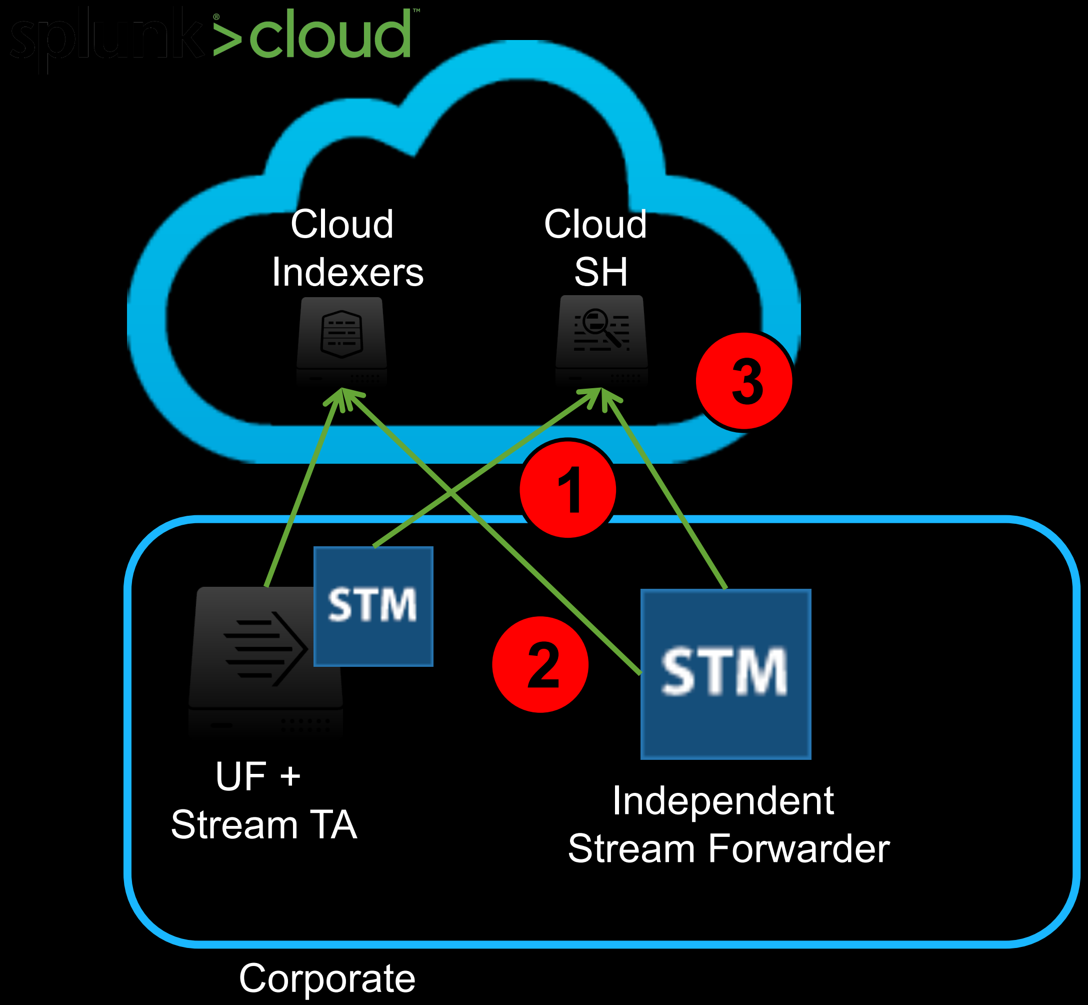


2. Independent Stream Forwarder

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



Splunk Cloud Support for Stream



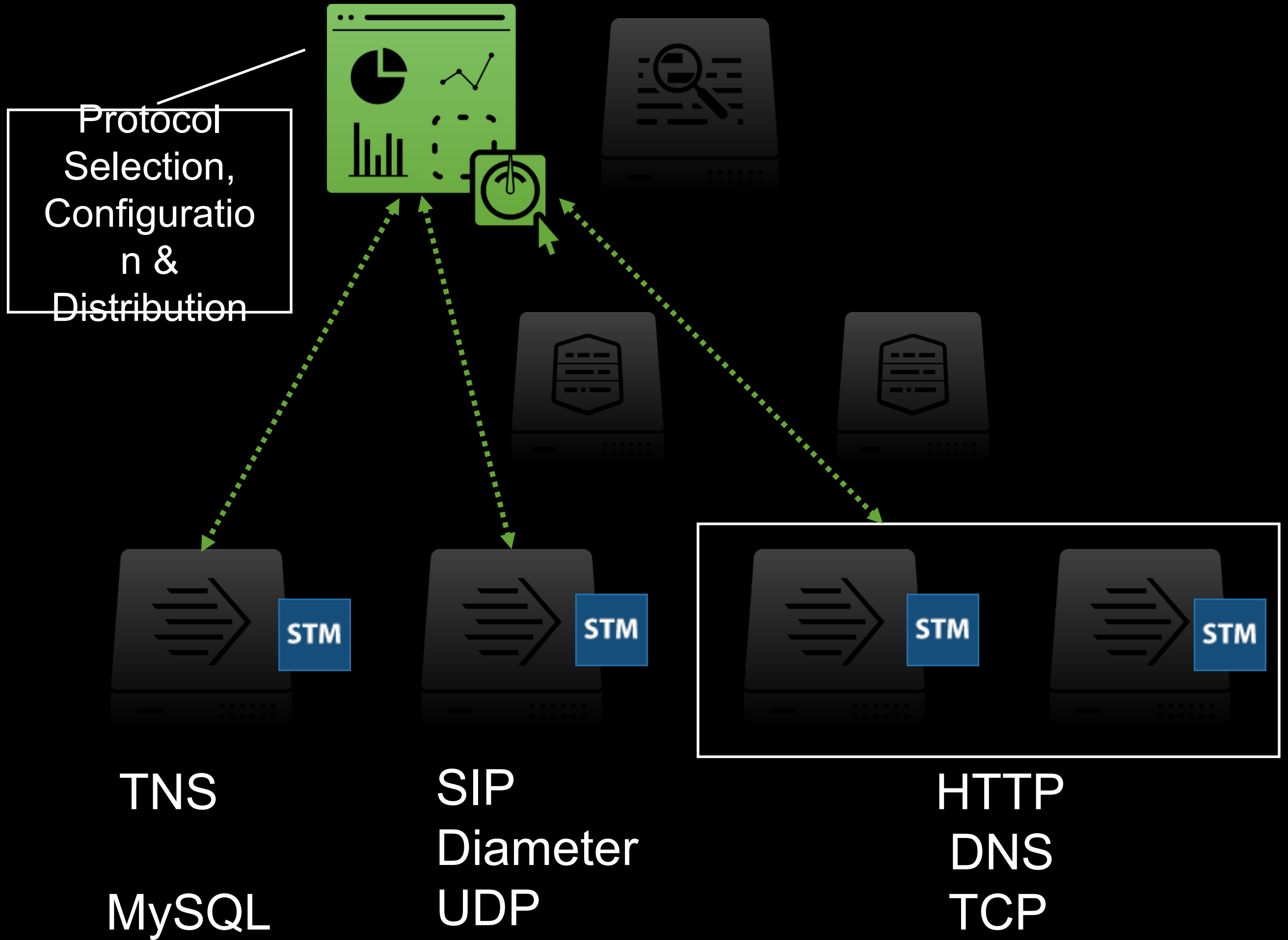
1. Stream forwarders fetch their configuration from the Cloud SH (authenticated)

2. Stream sends metadata back to Cloud indexers via the UF or HEC

3. Analysts connect to Cloud SH to explore the data collected by Stream

Distributed Forwarder Management

- Gain more deployment flexibility
- Increase management efficiency with per-forwarder protocol control
- Tailor data collection by assigning different sets of protocols to groups of forwarders



Protocol Selection, Configuratio n & Distribution

TNS

MySQL

SIP
Diameter
UDP

HTTP
DNS
TCP

New Features in Stream 7.0 and Stream 7.1

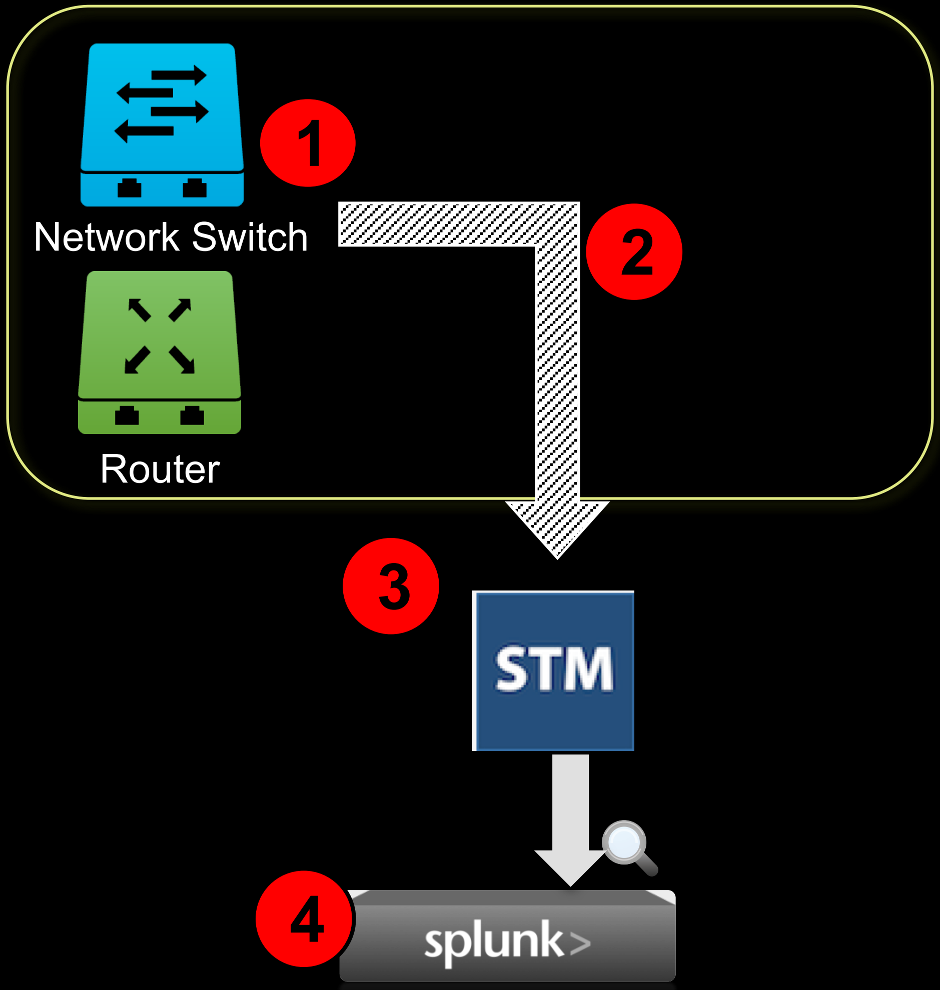
Major New Features in Stream 7.0

- Splunk Stream™ 7.0 was released GA in November 2016
- **NetFlow Collector**
  - NetFlow v5, v9 (with template support), IPFIX (with vendor extensions)
- **MD5 Hashing**
  - Any parsed Stream field, including SMTP attachments and HTTP files
  - Integrates with Enterprise Security – Threat Intelligence Framework
- **Flow Visualization** for all IPv4 space
- **PCAP Upload** via SH and Continuous Directory Monitoring via Forwarder
- **Enhanced Metadata** Fields (eg FlowID, Protocol Stack, Event Name)
- **Configuration Templates**
  - Easier integration with other Splunk products

Flow Collection

- Active Flow listening socket on Stream Forwarder
- Flexible Configuration Options
  - Selectable fields and filtering
  - Can configure multiple, disctinct listening ports on each Stream Forwarder
- Supports most common versions of Flow protocols
  - Cisco NetFlow, Juniper jFlow, HP sFlow, cFlowd
  - NetFlow v5, v9, IPFIX
  - V9 with templates (standard and custom)
  - IPFIX with vendor extensions
- Aggregation of Flow records (pre-indexing) can dramatically reduce the number of Splunk Events created
- Performance **> 465,000 flows/second (on a single Independent Stream Forwarder)**

Flow Collector Data Flow

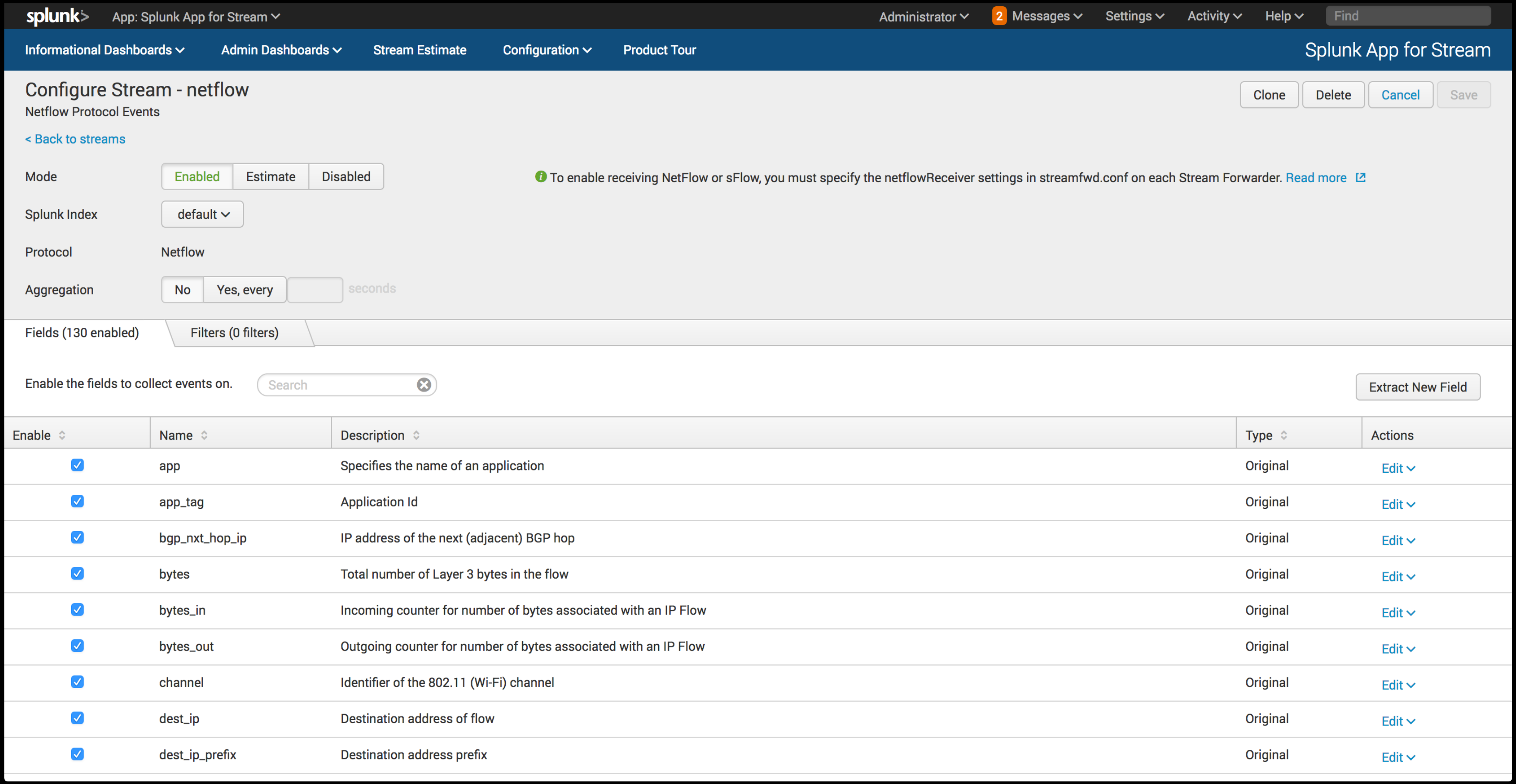


1. Netflow enabled devices
2. Export Netflow (over UDP)
3. NetFlow Metadata captured by Stream
4. Events in Splunk Indexer / Search Head

NetFlow Collector

- NetFlow listening sockets (UDP ports)
- Actively capture Flows from Netflow v5, v9, IPFIX
- Creates Splunk-compatible Flow Records
- Management from Stream Centralized UI

NetFlow and sFlow Streams UX



Configure Stream - netflow

Netflow Protocol Events

Mode: [✓ Enabled] Estimate Disabled

Splunk Index: default

Protocol: Netflow

Aggregation: No | Yes, every ___ seconds

To enable receiving NetFlow or sFlow, you must specify the netflowReceiver settings in streamfwd.conf on each Stream Forwarder. Read more

Fields (130 enabled) | Filters (0 filters)

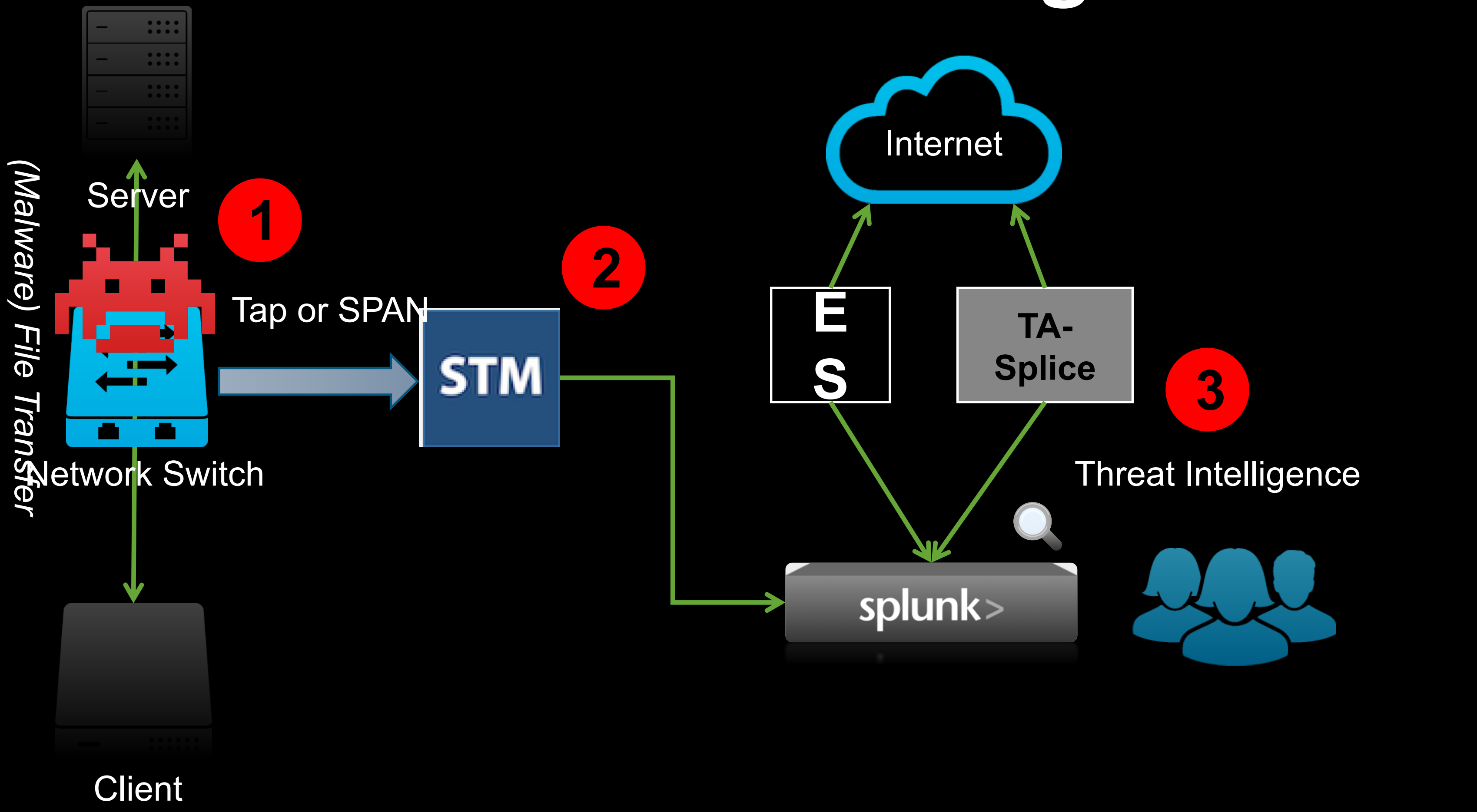
Enable the fields to collect events on.

Enable	Name	Description	Type	Actions
☑	app	Specifies the name of an application	Original	Edit
☑	app_tag	Application Id	Original	Edit
☑	bgp_nxt_hop_ip	IP address of the next (adjacent) BGP hop	Original	Edit
☑	bytes	Total number of Layer 3 bytes in the flow	Original	Edit
☑	bytes_in	Incoming counter for number of bytes associated with an IP Flow	Original	Edit
☑	bytes_out	Outgoing counter for number of bytes associated with an IP Flow	Original	Edit
☑	channel	Identifier of the 802.11 (Wi-Fi) channel	Original	Edit
☑	dest_ip	Destination address of flow	Original	Edit
☑	dest_ip_prefix	Destination address prefix	Original	Edit

MD5 Hashing of Files

- File Hashing provides integrity verification of files, can be used for a number of security use cases
  - inbound malware detection
  - outbound data loss prevention
- Stream generates MD5 hashes equivalent to “md5sum” unix command after decoding content back to binary
- Specifically **for SMTP file attachments** and **HTTP**
- MD5 hashes generated with Stream integrate directly into the Threat Intelligence framework of Enterprise Security, and has been tested with ES
- As a bonus, *any* non-numeric field can be MD5 hashed using the “Extract New Field” option. Field can be length-truncated if desired.

MD5 Hashing Data Flow



MD5 hashing

- Used to enable DLP and Security use cases
- Examines both inbound and outbound data transfer
- Can be used to find IOCs as well as data exfiltration
- Better metric than file names or file types

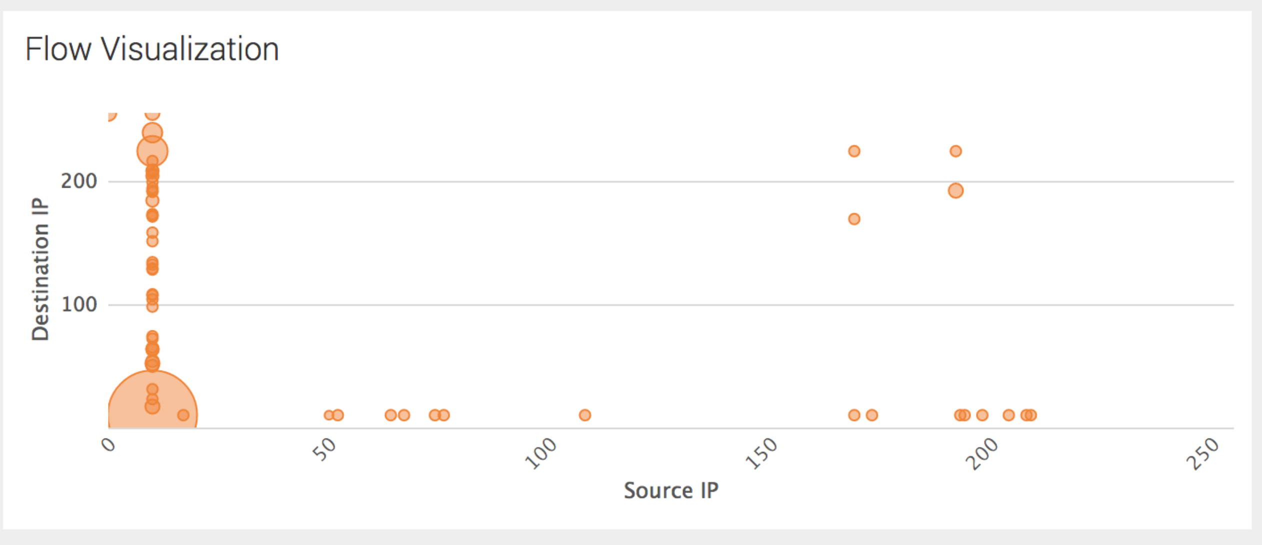
1 File Transfer Traffic between Client and Server directed towards Stream

2 Stream generates MD5 hashes of files, sends to Splunk Indexers

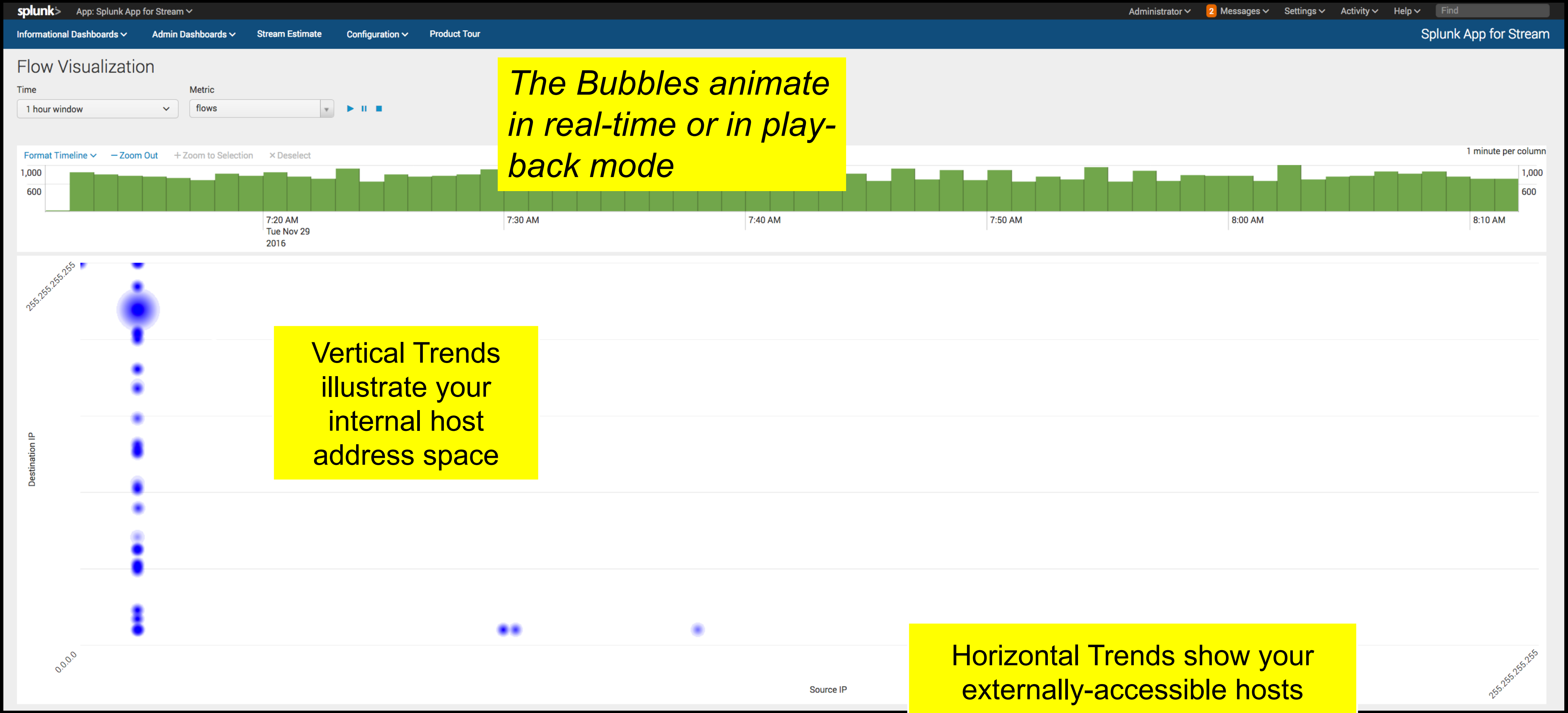
3 MD5 hashes compared against Threat Intel from public databases

Flow Visualization

- Designed to show limited Client->Server interaction for IPv4 address space. Overview and Detail views
- Can be used in real-time, interactive, and forensic modes
- Bubble chart that animates as flows appear (Detail view only)



Flow Visualization Detail View



Flow Visualization

Time: 1 hour window

Metric: flows

The Bubbles animate in real-time or in play-back mode

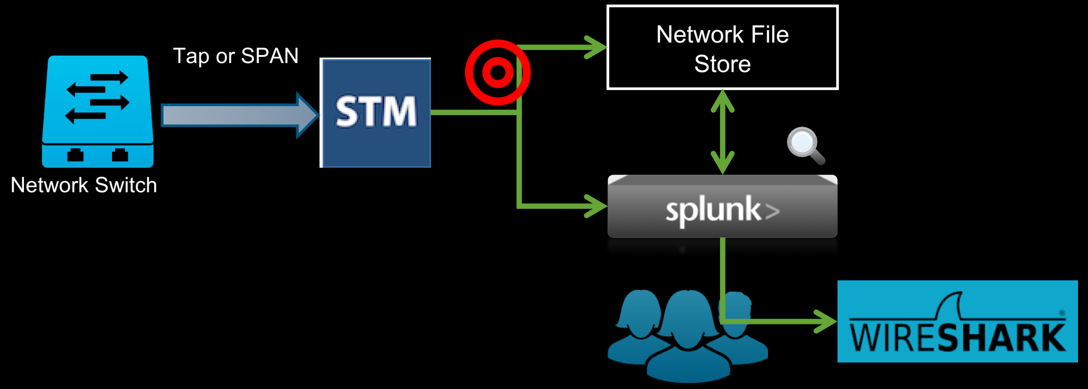
Vertical Trends illustrate your internal host address space

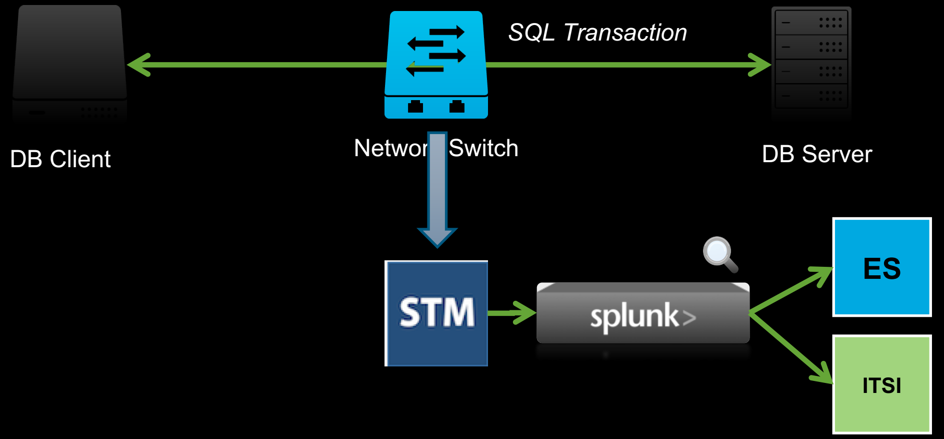
Horizontal Trends show your externally-accessible hosts

Major New Features in Stream 7.1

Stream 7.1 was released GA in March 2017

1. **Targeted Full Packet Capture**
   - Use Case: ES analyst sees anomalous behavior with log or Stream metadata, requests full packet capture. Downloads full packet capture (PCAP) from Search Head into Wireshark for further analysis.
2. **File Extraction**
   - Use Case: File containing malicious attachment is dowoaded via HTTP. MD5 hash automatically generated triggers ES Notable Event via Threat Intel framework. File is extracted and stored on disk for Analyst investigation.
3. **SQL query parsing**
   - Use case: Alert when a user is attempting to execute a SQL command to a table they shouldn't be allowed to access
   - Use case: Look for SQL Injection or other SQL-based attacks

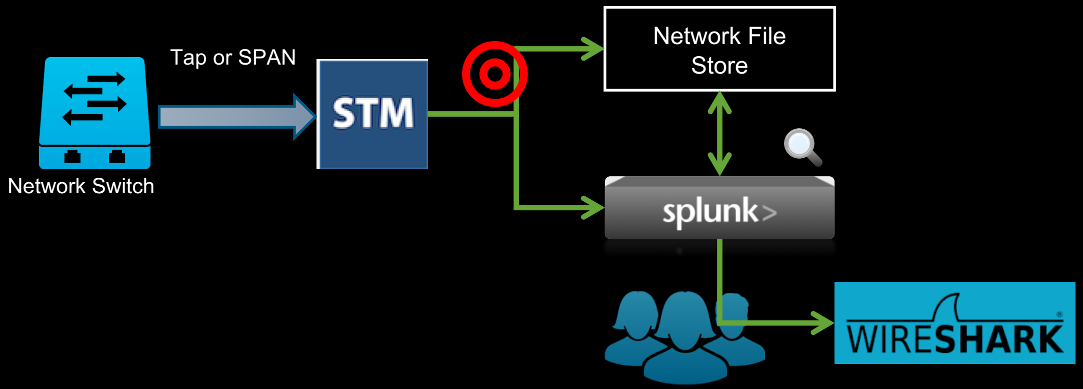




Stream 7.1: Targeted Full Packet Capture

Explanation and Inspiration

- Stream 7.0 and earlier transforms wire data into Splunk events, digesting many packets into a small number of events
- Most of the time, this is advantageous for troubleshooting because it preserves the salient features of the packets but eliminates all the redundancy
- Occasionally, for security and other reasons, analysts need to see the full packets in the conversation →



Targeted Full Packet Capture!

Stream 7.1 Targeted Full Packet Capture

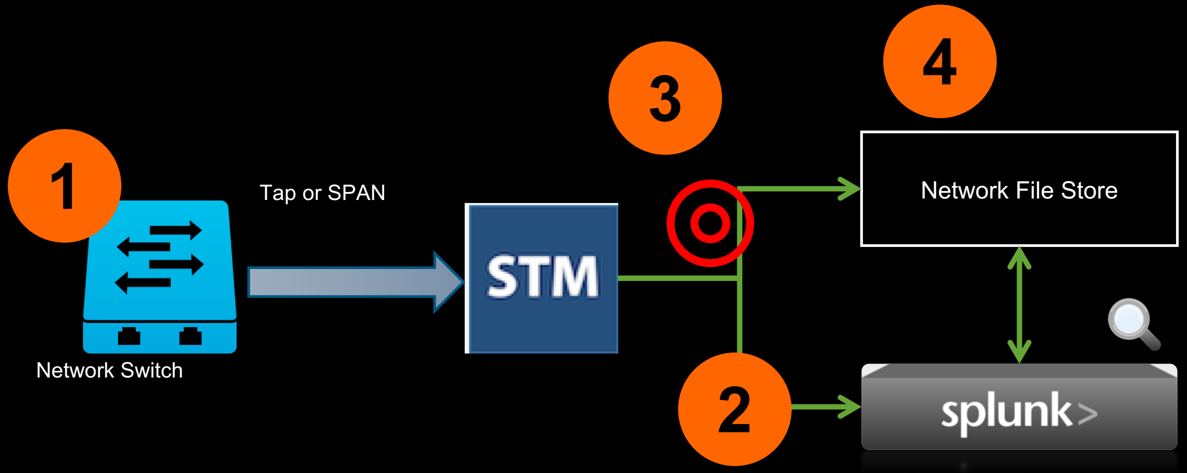
Functional Concepts

- "Targeted" because it doesn't capture every packet it sees. The analyst specifies a set of criteria to use for capturing data, and only conversations that meet those criteria are fully captured
- Full Packet Capture: The full fidelity of the original packet-level conversation observed on the wire is captured and stored to a File Server (ie NAS), **NOT the Splunk indexer**
- Packets are stored in a sessionized format – meaning, the PCAP files on disk represent a single SRC <-> DEST bidirectional conversation
- Metadata (Splunk Events) is still generated and sent to the Splunk Indexer. These events contain links to the File Server where the packet file is stored
- A workflow action is created in the Splunk Search Head to download the packets to the Analyst's browser (and into a PCAP reader, like Wireshark)

Stream 7.1: Targeted Full Packet Capture

Packet Storage Process

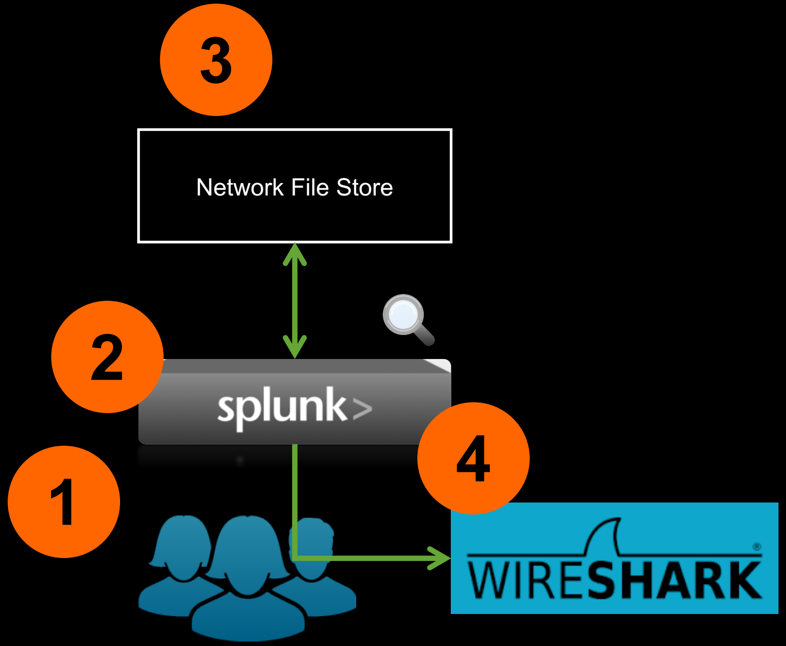
1. Packets are observed by Stream
2. Stream generates Splunk Events (Metadata) for all packets
3. Some packets match Packet Targeting Expression (“Packet Stream”)
4. Conversations containing matching packets are sent across the network from Stream to a File Server using a standard FS protocol (SMB/CIFS, NFS, etc.)



Stream 7.1: Targeted Full Packet Capture

Packet Retrieval Process

1. Analyst explores Stream metadata in Splunk Indexer
2. For metadata that has Packet Stream data, Analyst requests Packet Data via Event Action in Search Head
3. Search Head contacts appropriate File Server, automatically retrieves associated PCAP file
4. Search Head passes PCAP file to browser, which opens file in registered app



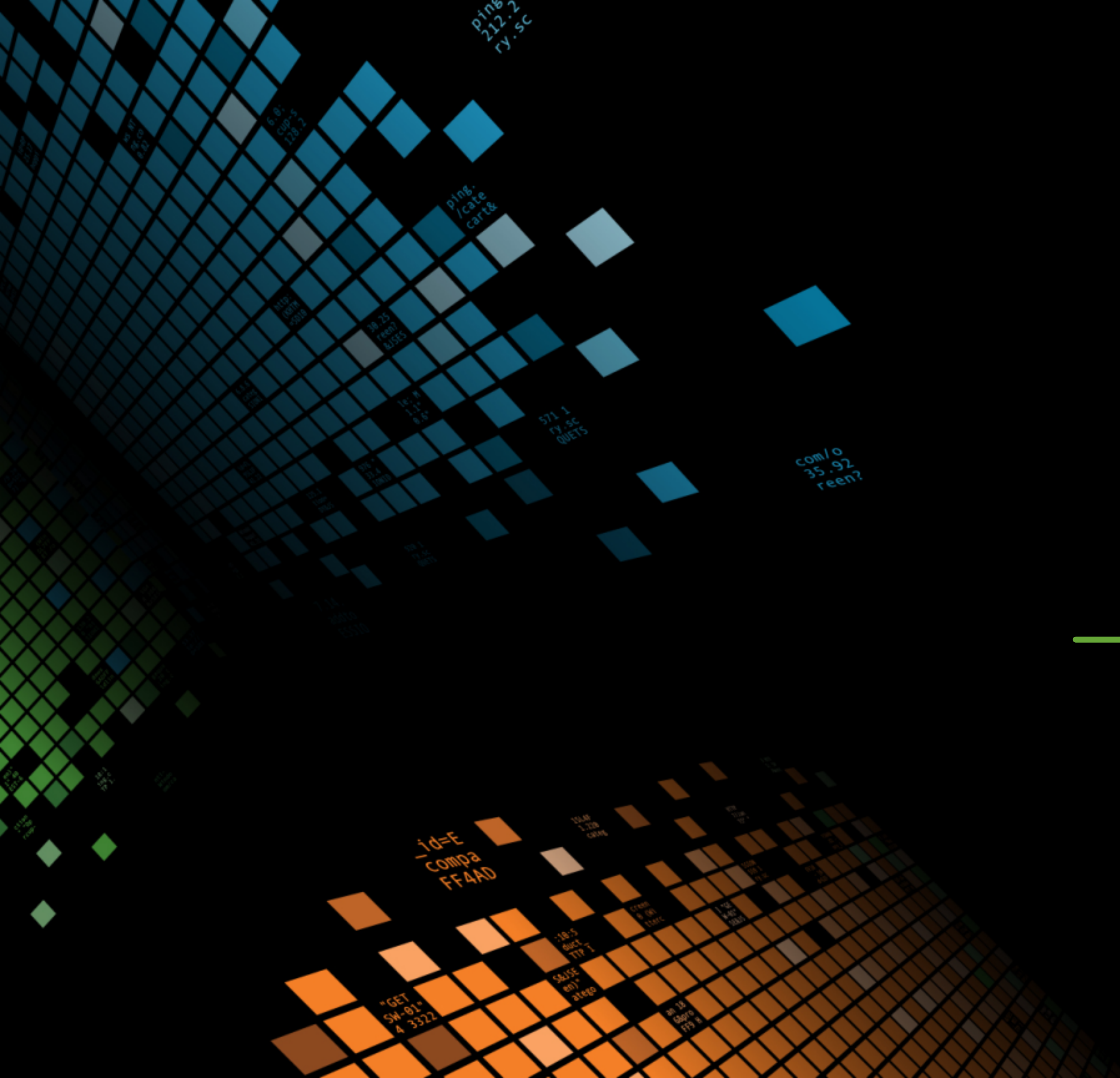
Stream 7.1: File Extraction

- Works in the same manner as Packet Capture
- Extracts files from HTTP and SMTP protocol
- Can simultaneously extract files and generate MD5 hash
- Saves files on File Server and allows Search Head Retrieval

Stream 7.1: SQL Protocol Parser

- Stream now includes a full SQL parser
- Dissects statements 8 different variants of SQL
- Extracts:
  - Command (INSERT, UPDATE, DELETE, SELECT)
  - Stored procedures (XP_*, SP_* etc.)
  - Database DDL (CREATE TABLE, DROP TABLESPACE, etc)
  - Table name(s)
- User name, row count, return code are already included in Stream 7.0

User: Jim executes
DELETE from
TBL_EMPLOYEES where
VALUE="Tom Smith"



Fault Isolation

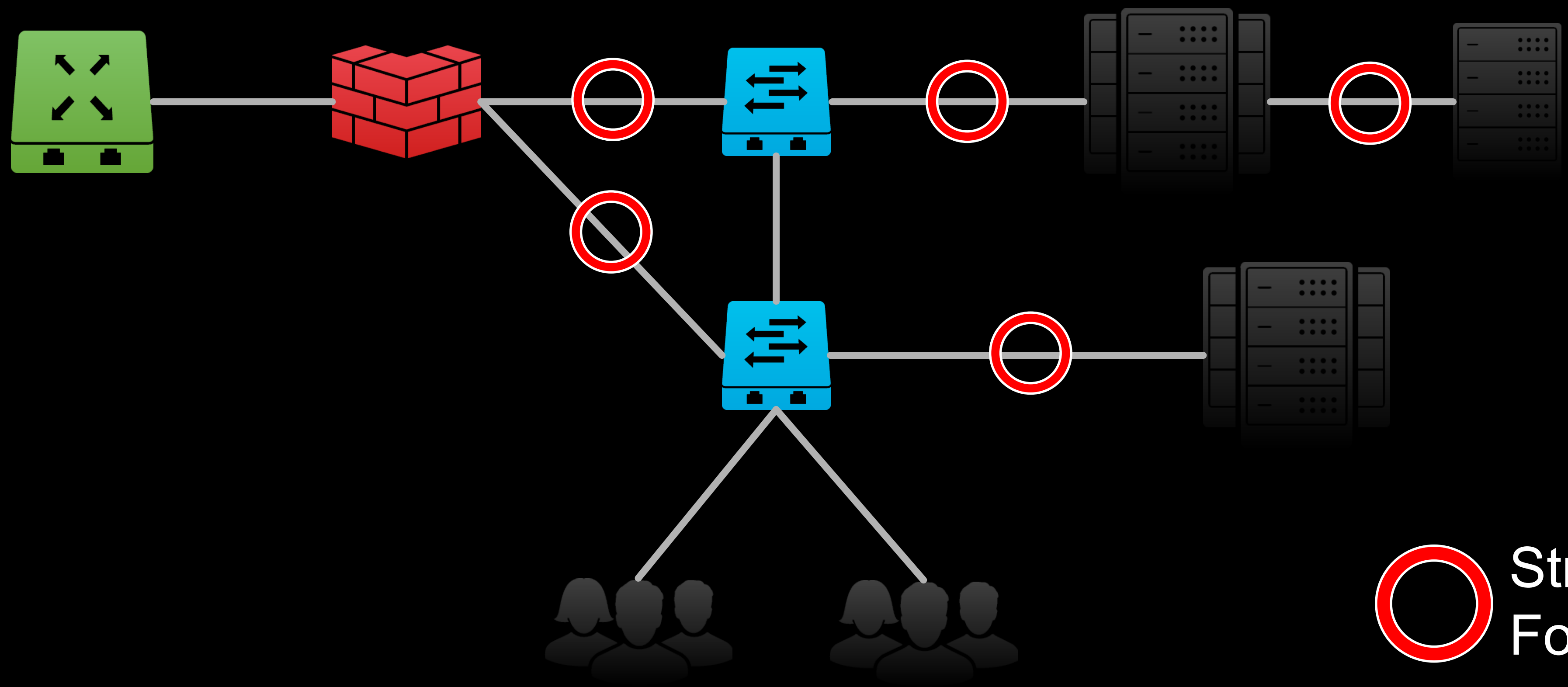
Fault Isolation

Ending Finger Pointing

- Ideally, we’d like to test each element in isolation, to see if any specific element is misbehaving individually
- Two practical problems:
  - 1) Don’t usually have spare equipment to isolate
  - 2) Often the problem is caused by interactions between elements

Isolation Solution Strategy

Use Stream probes to explore traffic between elements



○ Stream Forwarder

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

splunk> .conf2017