



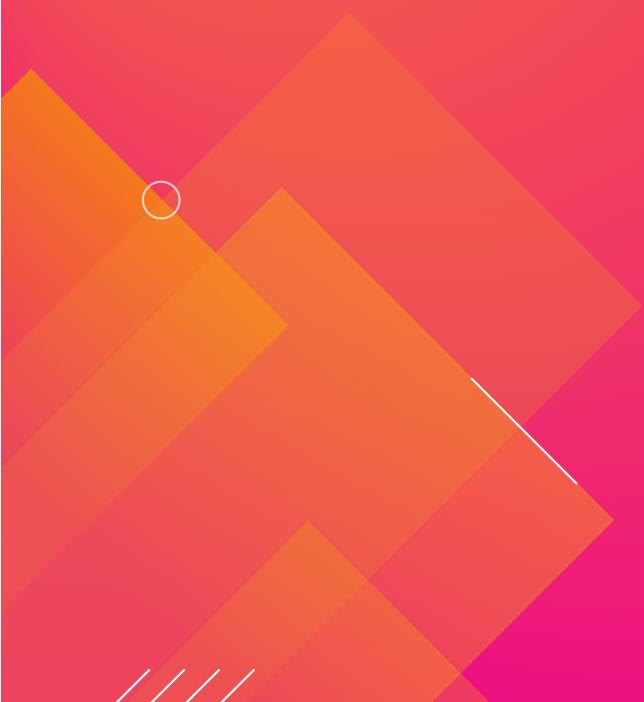
Product Vision for Autodesk

February 18, 2020

Jon Tran, Solutions Engineer
Jimmy Huang, Regional Sales Manager

splunk[®] turn data into doing™

Forward-Looking Statements



During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. 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, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, 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. © 2020 Splunk Inc. All rights reserved.

Agenda

1

Discuss the
Broader Data
Landscape

2

Present Splunk's
Premium Solutions

3

Share Splunk's
Unique Approach
to Improving
Observability and
Action and How
We are Designing
for the Future

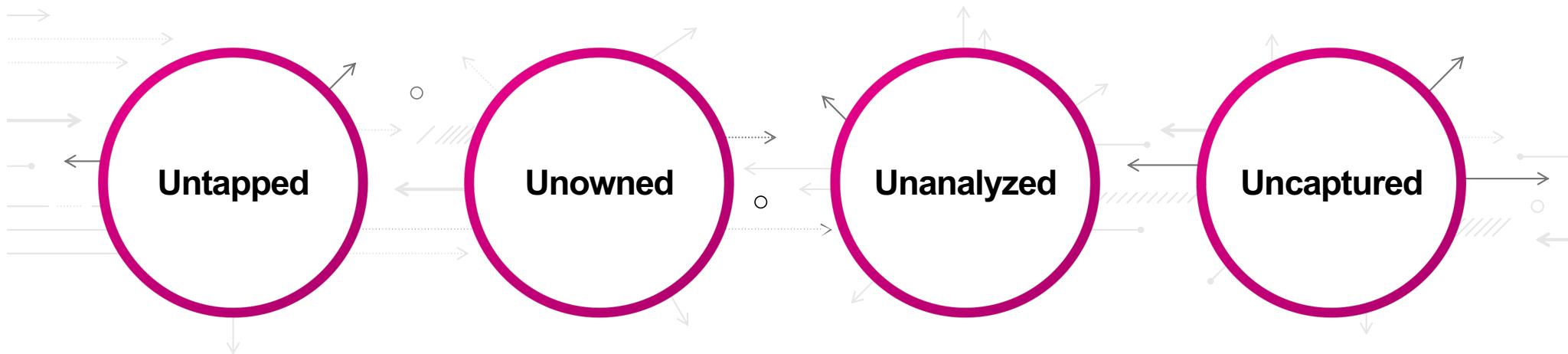
4

Agree Upon
Next Steps

Most Organizations' Data is Still Dark Data

60%

of organizations report
that the majority of
their data is still dark*

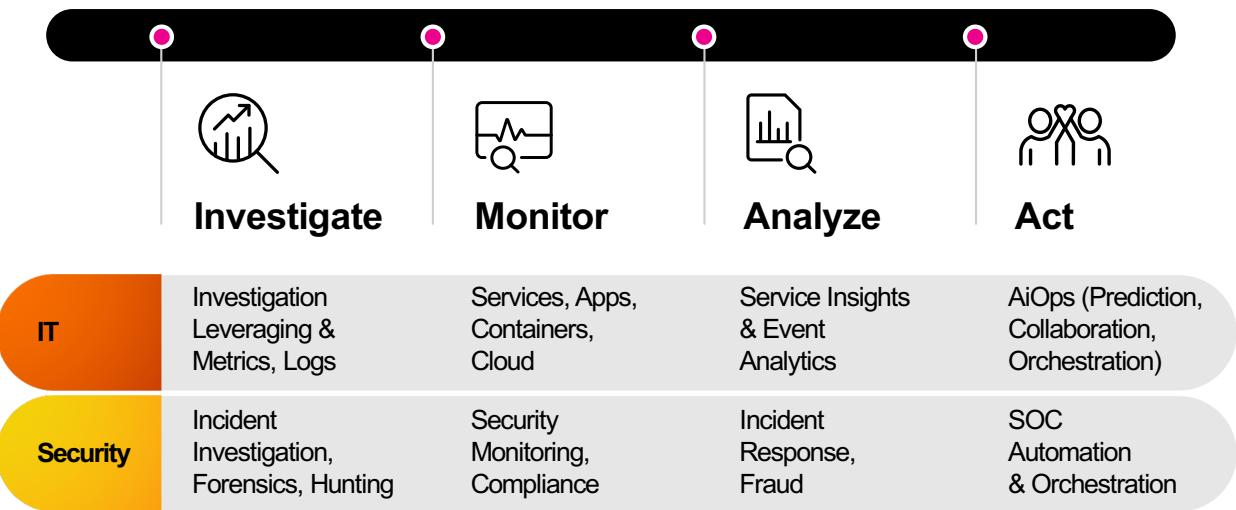


*Splunk Inc., "State of Dark Data Report", May 2019

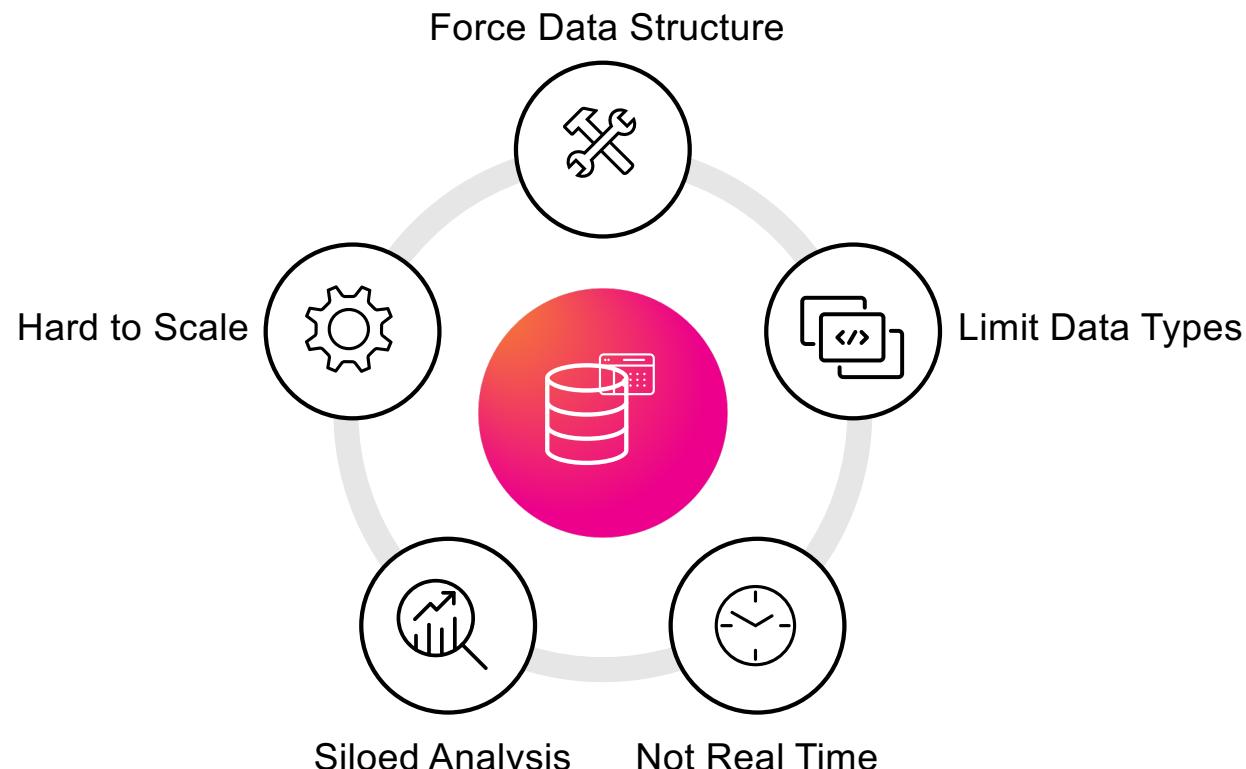
splunk > turn data into doing

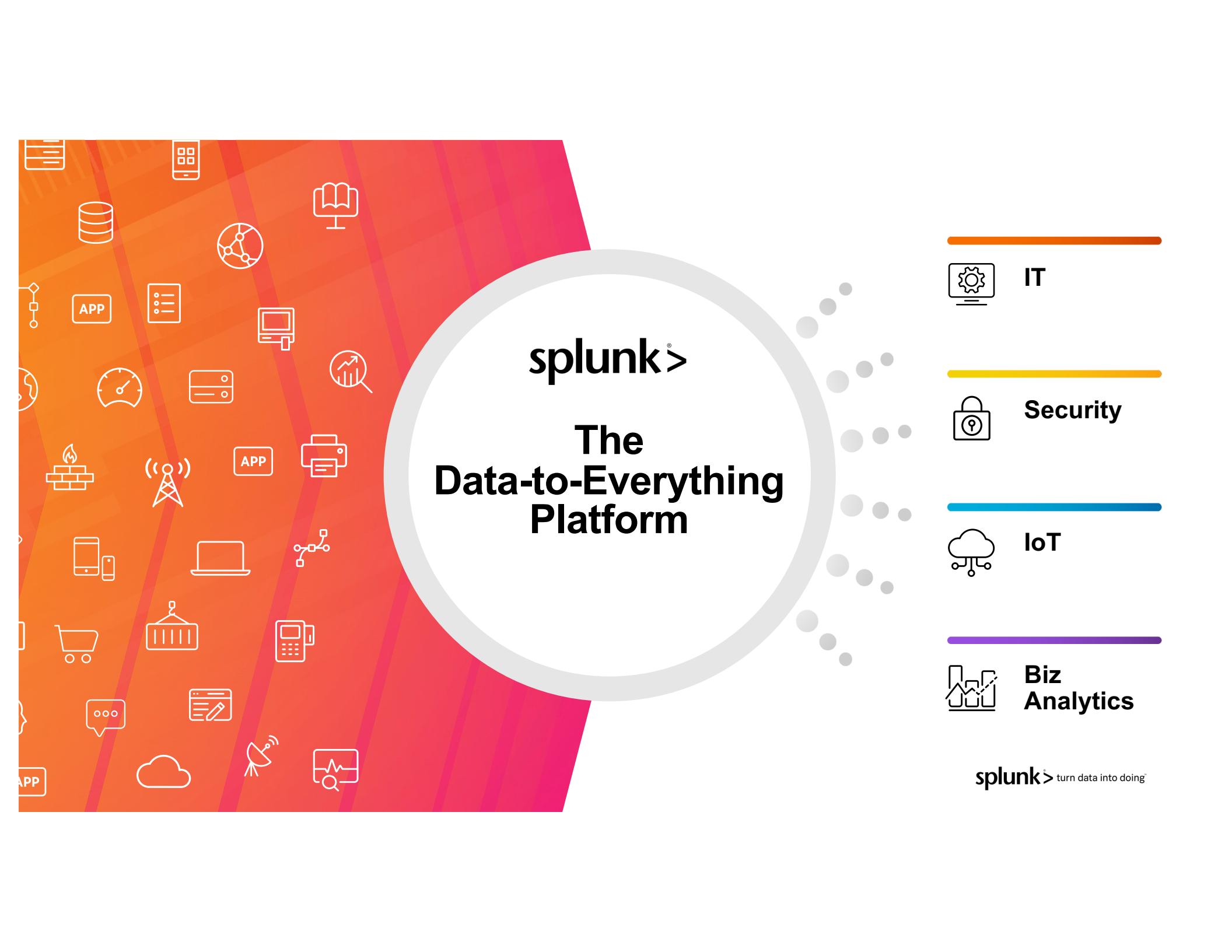


IT and Security Data Journeys



Traditional Data and Analysis Solutions No Longer Solve the Problem





The graphic features a central white circle containing the "splunk>" logo and the text "The Data-to-Everything Platform". To the left of this circle is a large orange and red radial background filled with various white line-art icons representing different data sources and technologies, such as databases, mobile devices, clouds, and network components. To the right of the central circle is a grey dotted line that curves upwards and to the right, with several grey dots trailing off. The entire graphic is set against a white background.

splunk®

The Data-to-Everything Platform



IT



Security



IoT



Biz
Analytics

splunk> turn data into doing

Splunk Premium Solutions



Splunk IT Service
Intelligence™



Splunk Enterprise
Security™



Splunk User Behavior
Analytics™



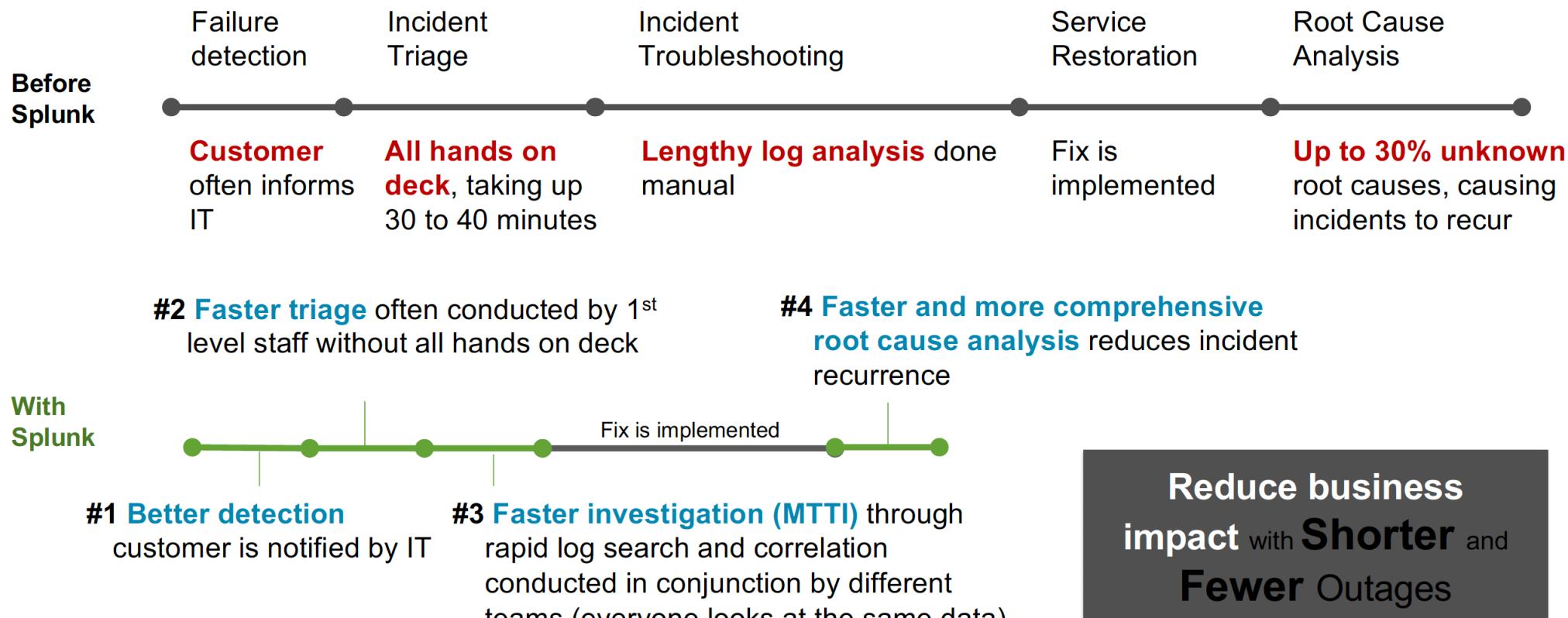
Splunk for Industrial
Internet of Things

splunk>
VictorOps

splunk>
phantom

splunk> turn data into doing®

TOP 4 Value Drivers for IT Ops



IT Service Intelligence (ITSI)

IT OPS

DESCRIPTION

- ▶ Data-driven insights across your services, apps, and infrastructure so you can predict and prevent problems before they impact revenue and customer experience.

ITSI SUCCESS PLANS

- ▶ Success Plans include SW license and support
- ▶ Choose Standard or Premium options
- ▶ **Support sold separately for perpetual licenses**

LICENSING

- ▶ **Volume:** We license by amount of data indexed in a 24 hour period
- ▶ Complimentary product. Customers must have an equivalent license of Splunk Enterprise or Splunk Cloud subscription.
(same GB volume level).

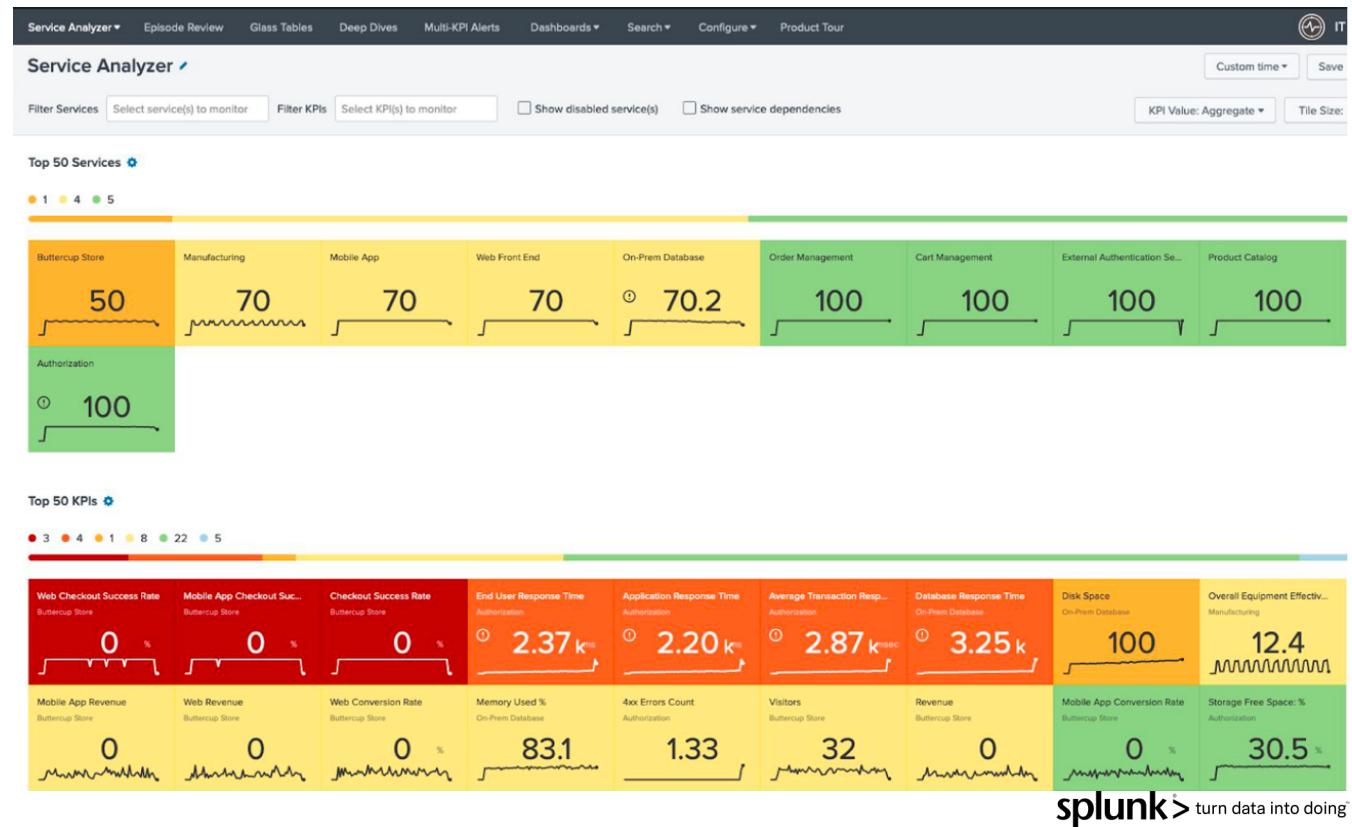


splunk > turn data into doing

IT Service Intelligence (ITSI)

IT Operations

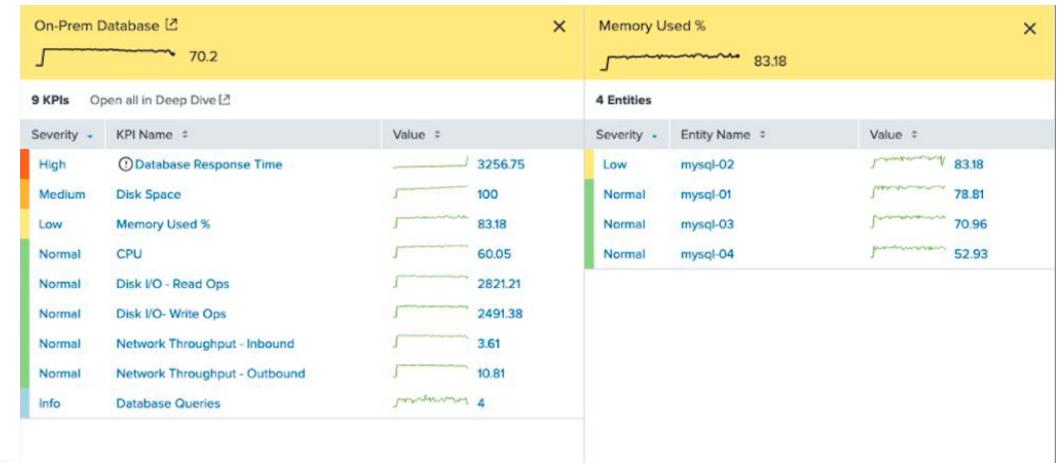
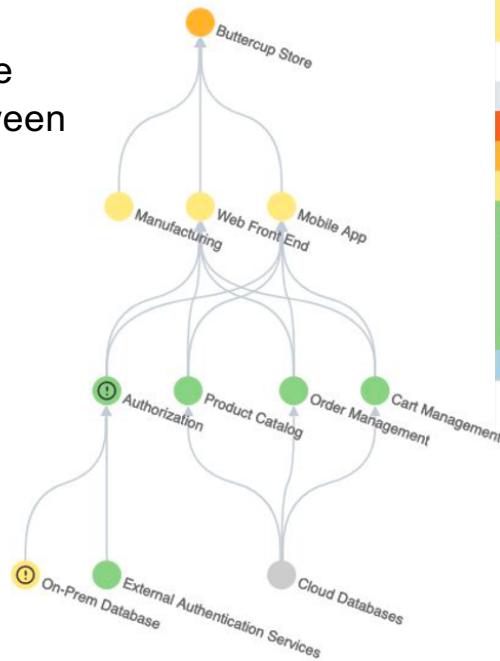
Service Analyzer provides a high-level view of the health of your services and KPIs



IT Service Intelligence (ITSI)

IT Operations

Deep Dive: See the dependencies between services



IT Service Intelligence (ITSI)

IT Operations

Episode Review: Group events to reduce noise

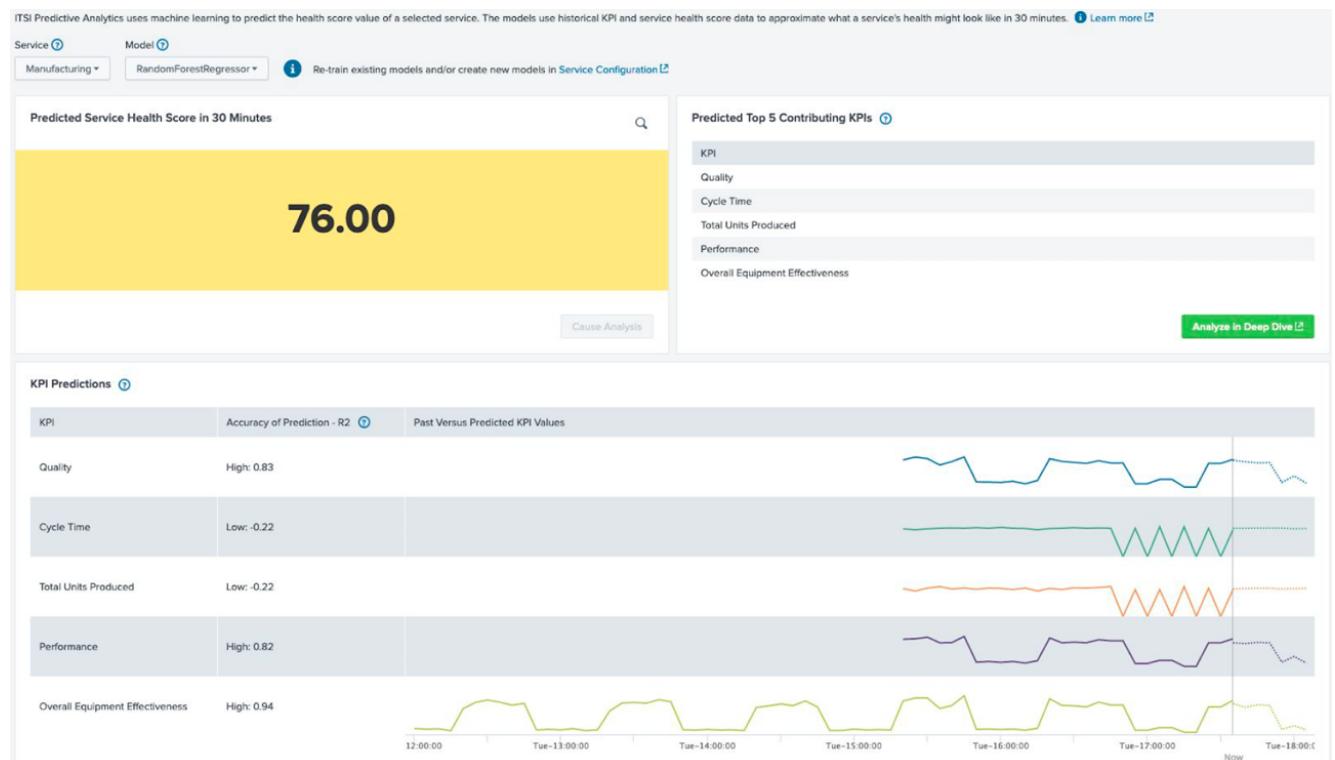
The screenshot shows the Splunk Episode Review interface. At the top, there are navigation links: Service Analyzer, Episode Review (which is active), Glass Tables, Deep Dives, Multi-KPI Alerts, Dashboards, Search, Configure, and Product Tour. Below the navigation is a search bar with the placeholder "search". A button labeled "Add Filter" is also present. The main area is titled "Episode Review" and displays a table of 221 events. The table has columns for Title, Time, Owner, and Severity. The events are sorted by time, with the most recent at the top. Many events are grouped together, indicating they are part of a single episode. The severity of the events varies, with some being Low and others Medium.

Title	Time	Owner	Severity
SNOW Change Request: completed	4/9/2019 3:03:41 AM	Unassigned	Low
Windows Event Log: Security on mysql-02	4/9/2019 3:33:27 AM	Unassigned	Low
New Relic Login API: status = orange	4/9/2019 5:22:41 AM	Unassigned	Medium
Windows Event Log: Security on mysql-02	4/9/2019 5:33:36 AM	Unassigned	Low
New Relic Login API: status = orange	4/9/2019 5:35:43 AM	Unassigned	Medium
Windows Event Log: Security on mysql-02	4/9/2019 6:33:40 AM	Unassigned	Low
New Relic Cart API: status = orange	4/9/2019 6:38:47 AM	Unassigned	Medium
Windows Event Log: Security on mysql-02	4/9/2019 7:33:44 AM	Unassigned	Low
New Relic Cart API: status = orange	4/9/2019 7:35:51 AM	Unassigned	Medium
Windows Event Log: Security on mysql-02	4/9/2019 8:33:48 AM	Unassigned	Low
New Relic Login API: status = orange	4/9/2019 8:35:55 AM	Unassigned	Medium
Windows Event Log: Security on mysql-02	4/9/2019 9:33:52 AM	Unassigned	Low
New Relic Cart API: status = orange	4/9/2019 9:34:59 AM	Unassigned	Medium
Nagios Service Check: check_disk on mysql-02	4/9/2019 9:44:59 AM	Unassigned	Medium
Host: mysql-02 Metric: disk Value: 90.33	4/9/2019 9:44:59 AM	Unassigned	Medium

IT Service Intelligence (ITSI)

IT Operations

Predictive Analytics:
Use historical data to predict the future state of services



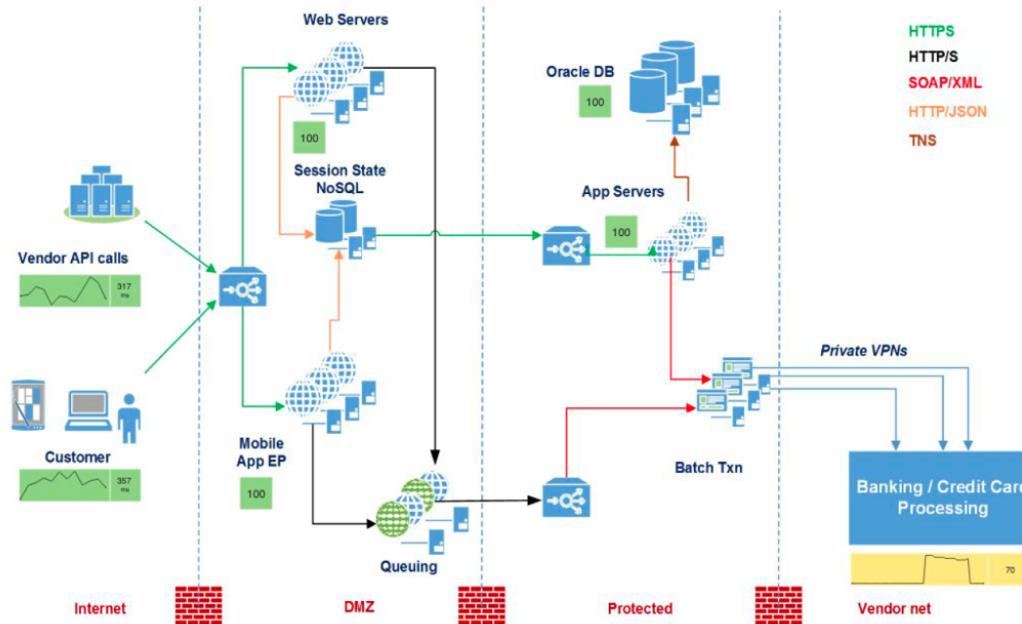
splunk > turn data into doing

IT Service Intelligence (ITSI)

IT Operations

OnLine Transaction Service ✓ Now ▾ Edit

Glass Tables: Use an existing network diagram and annotate it with the health of the services involved



VictorOps

IT Operations

DESCRIPTION

- ▶ Deliver the right alerts to the right people, reducing time to acknowledge and resolve problems
- ▶ Empower Dev Ops teams with collaboration and data
- ▶ Make on-call suck less for your developers and operations teams

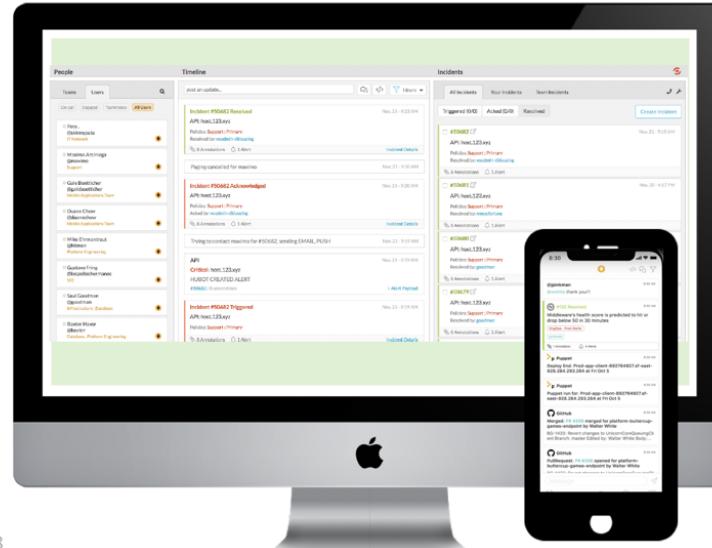
VictorOps SUPPORT

- ▶ Support included in the VictorOps subscription

LICENSING

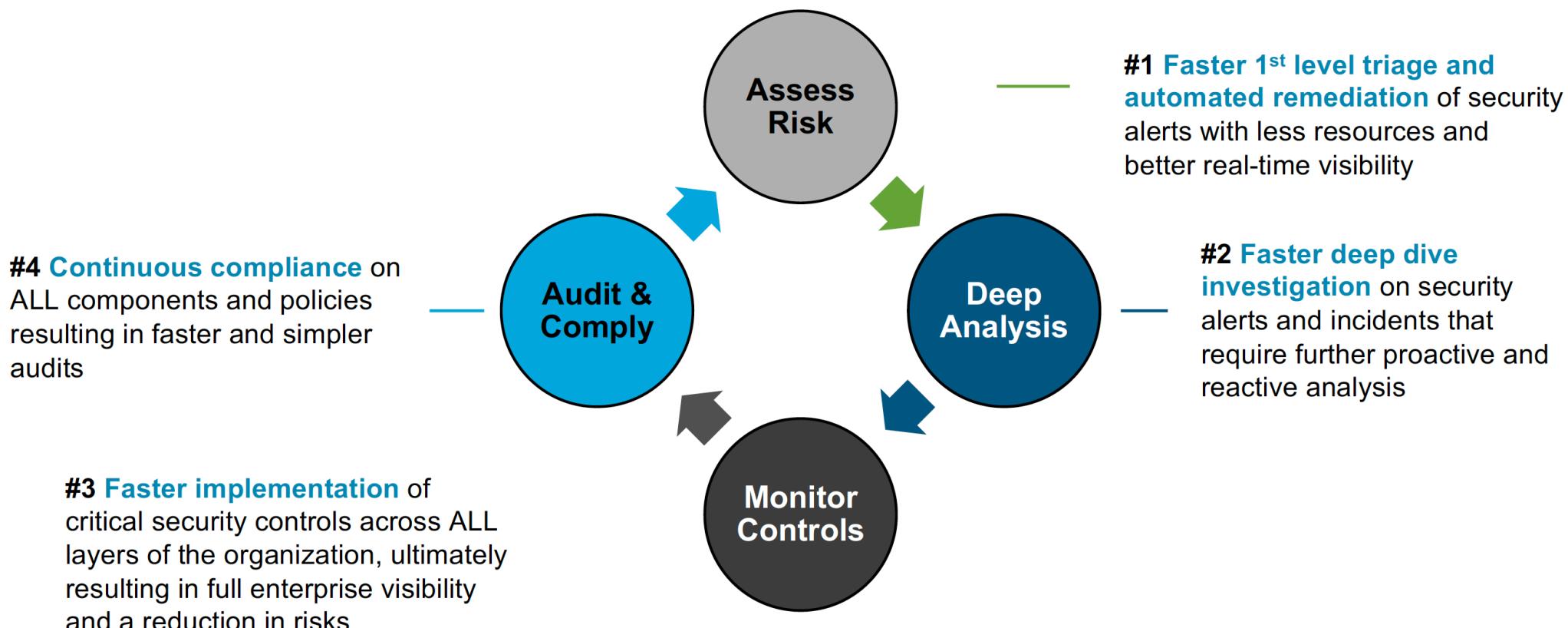
Seats: VictorOps is licensed on a per-seat (user) basis.

Tiers: VictorOps offers an entry, growth and enterprise tier to offer a great fit for all kinds of accounts



splunk > turn data into doing

TOP 4 Value Drivers for Security



Enterprise Security (ES)

Security

DESCRIPTION

- ▶ **Analytics-Driven SIEM.** Use to Monitor, Detect, Analyze, Investigate and Respond to Threats and Attacks.



Splunk Enterprise
Security™

ES SUCCESS PLANS

- ▶ Success Plans include SW license and support
- ▶ Choose Standard or Premium options
- ▶ **Support sold separately for perpetual licenses**

LICENSING

- ▶ **Volume:** We license by amount of data indexed in a 24 hour period
- ▶ Complimentary product. Customers must have an equivalent license of Core Splunk (same GB volume).



splunk > turn data into doing

Enterprise Security (ES)

Security

Security Posture: At-a-glance information about what's taking place throughout the entire organization



Enterprise Security (ES)

Security

Incident Review: Single comprehensive view for analyst to conduct investigations

Incident Review

Urgency

CRITICAL	92
HIGH	233
MEDIUM	918
LOW	3125
INFO	0

Status

Owner

Search

Security Domain

Time

Last 24 hours

Tag

Submit

7,261 events (2/16/20 5:00:00:000 PM to 2/17/20 5:20:27.000 PM)

Format Timeline ▾ Zoom Out +Zoom to Selection X Deselect Job ▾ Smart Mode ▾

1 hour per column

3,500

6:00 PM Sun Feb 16 2020 12:00 AM Mon Feb 17 6:00 AM 12:00 PM

3,500

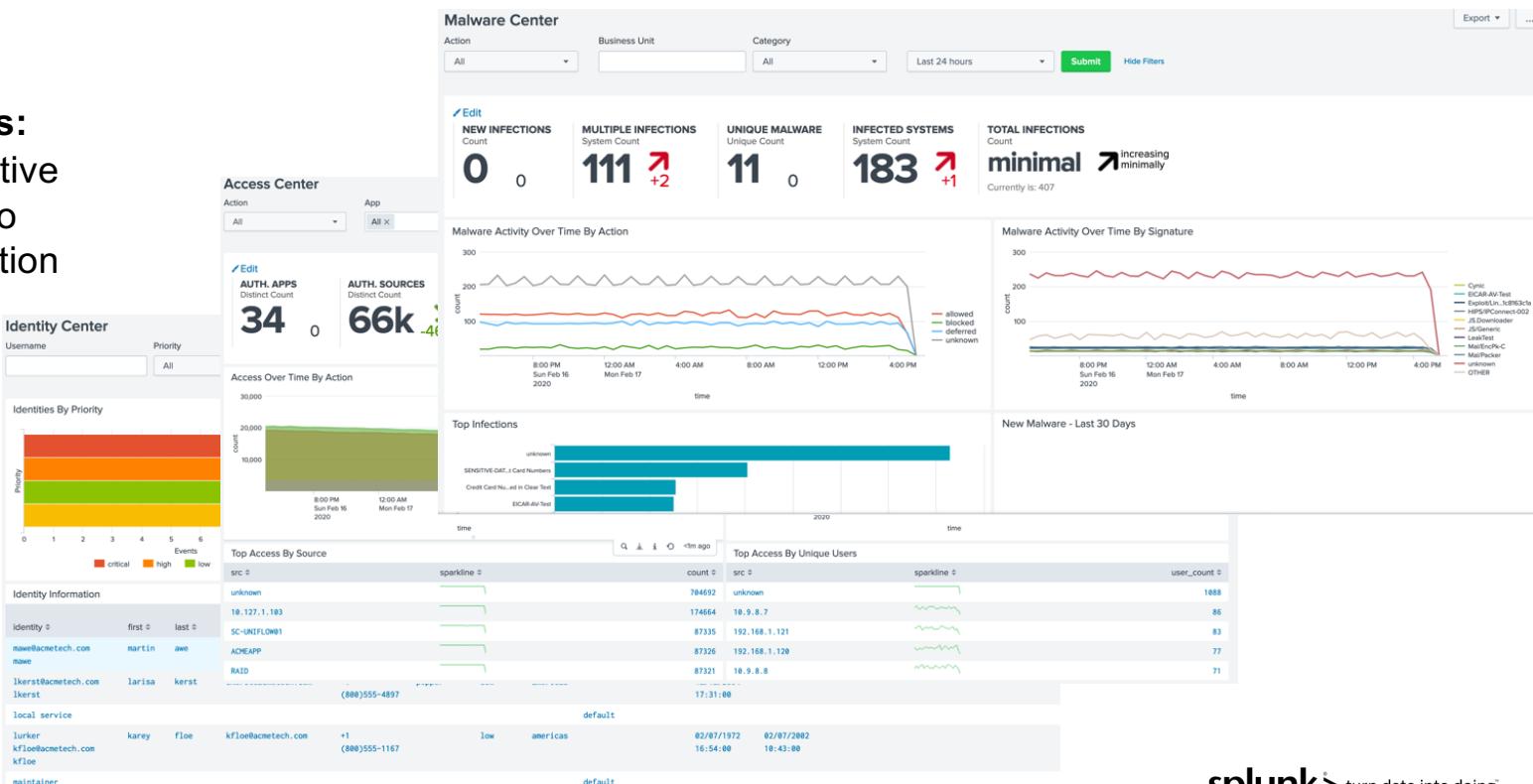
[Edit Selected](#) | [Edit All 7261 Matching Events](#) | [Add Selected to Investigation](#)

i	Time	Urgency	Security Domain	Title	Description	Status	Risk Score	Owner	Actions
>	2/17/20 5:20:15.000 PM	⚠️ High	Endpoint	Host With Multiple Infections (87.240.128.18)	The device 87.240.128.18 was detected with multiple (2) infections.	New	640	unassigned	▼
>	2/17/20 5:20:13.000 PM	⚠️ Medium	Access	Account Deleted	User (ACME-001) deleted account (Domain_B\user_...) on system (ACME-001)	New	9240	unassigned	▼
>	2/17/20 5:20:12.000 PM	⚠️ High	Endpoint	Host With Multiple Infections (27.175.11.11)	The device 27.175.11.11 was detected with multiple (3) infections. ▾	New	640	unassigned	▼
>	2/17/20 5:20:12.000 PM	⚠️ High	Endpoint	Host With Multiple Infections (10.11.36.42)	The device 10.11.36.42 was detected with multiple (2) infections.	New	900	unassigned	▼
>	2/17/20 5:20:12.000 PM	⚠️ Critical	Endpoint	Host With Multiple Infections (10.11.36.28)	The device 10.11.36.28 was detected with multiple (2) infections.	New	1040	unassigned	▼
>	2/17/20 5:20:12.000 PM	⚠️ Critical	Endpoint	Host With Multiple Infections (10.11.36.14)	The device 10.11.36.14 was detected with multiple (2) infections.	New	900	unassigned	▼
>	2/17/20 5:19:51.000 PM	⚠️ Medium	Access	Default Account Activity Detected	User account GUEST is a default account that successfully authenticated to HOST-005 at 1581959719. Please verify this activity conforms with your information security policy.	New	9480	unassigned	▼

Enterprise Security (ES)

Security

Security Domains:
 Wealth of prescriptive content provided to expedite investigation monitoring



Enterprise Security (ES)

Security Content:
Created by Splunk's
dedicated Security
Research Team that
proactively monitors and
designs content to stay
on top of the latest
security risks

- Framework base:
- CIS Top 20
- Kill Chain Phases
- Mitre ATT&CK Chain

User and Entity Behavior Analytics (UEBA)

Security

DESCRIPTION

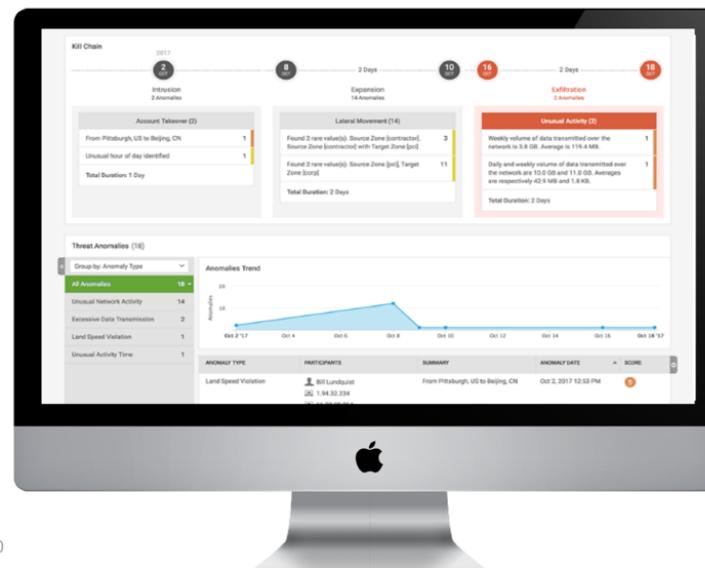
Detect cyber-attacks and insider threats using data science, machine learning, behavior baseline, peer group analytics, and advanced correlation.

UBA SUPPORT

- ▶ Term license include SW license and support
- ▶ Choose Standard or Premium options
- ▶ **Support sold separately for perpetual licenses**

LICENSING

Users: number of authorized users (the number of users or system accounts in Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) or any similar service that is used to authenticate users inside the network). Can be sold with Content Subscription service.



splunk > turn data into doing

Phantom

Security

DESCRIPTION

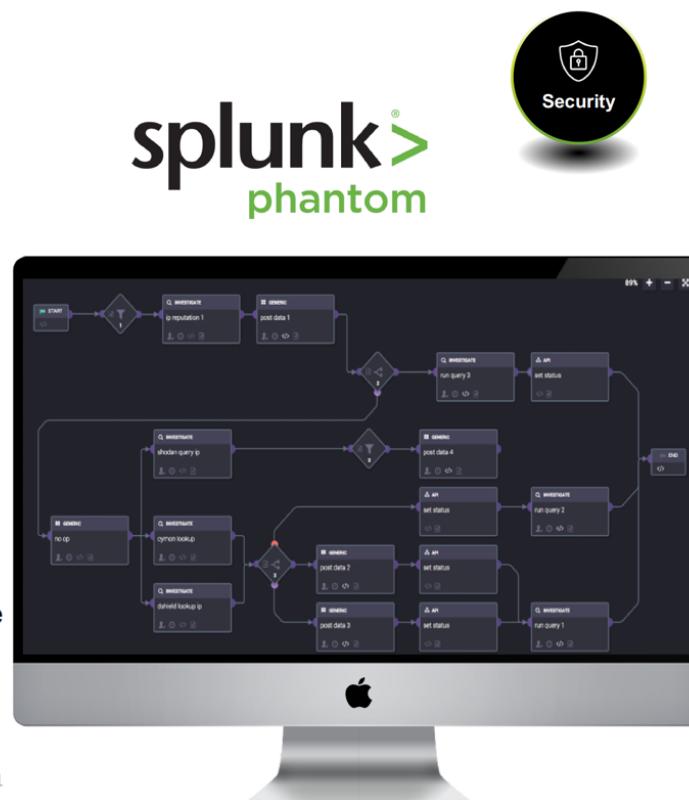
- ▶ **SOAR (Security Orchestration, Automation & Response):** Integrate teams, processes and tools to accelerate SOC workflows, force multiply existing resources, and strengthen defenses.

PHANTOM SUPPORT

- ▶ Term license include SW license and support
- ▶ Choose Standard or Premium options
- ▶ **Support sold separately for perpetual licenses**

LICENSING

- ▶ Term subscription license – multi-year terms available
- ▶ Pricing via Event Volume Tiers – 25, 150, 350, 500, 750, 1500, 3000, 5000
- ▶ Currently, no charge for overages



Machine Learning Tool Kit (MLTK)

Predict Numeric Fields

Predict Categorical Fields

Detect Numerical Outliers

Detect Categorical Outliers

Forecast Time Series

Cluster Events

Overview

Welcome to the Machine Learning Toolkit and Showcase. Click on the dashboards or examples below to explore the kinds of analytics this app enables. Each dashboard includes both end-to-end examples with datasets we have provided, as well as the ability to apply the dashboard to your own data. You can inspect the dashboard panels and other code to see how each one works and then create custom dashboards to suit your needs. Everything you see was implemented on the Splunk platform using public interfaces, so you can bring similar functionality to your own organization's Splunk instance; there's nothing hidden up our sleeves.

Predict Numeric Fields

Predict the value of a numeric field using a weighted combination of the values of other fields in that event. A common use of these predictions is to identify anomalies: predictions that differ significantly from the actual value may be considered anomalous. IT admins could predict the values of sensors that were malfunctioning; security analysts could predict how much data a user is likely to transfer and flag unusually high prediction errors; and business analysts could predict the likely spending habits of customers.

Algorithm: Linear Regression

Examples:

- Predict Median House Value
- Predict Baseball Runs
- Predict App Usage from Other Apps

Predict Categorical Fields

Predict the value of a categorical field using the values of other fields in that event. A common use of these predictions is to identify anomalies: high-confidence predictions that turn out to be incorrect may be considered anomalous. IT admins could predict the correct values of missing configuration variables; security analysts could predict what actions a user is likely to perform and raise an alert when the user behaves unexpectedly; and business analysts could predict customer churn based on other factors.

Algorithm: Logistic Regression

Examples:

- Predict Telecom Customer Churn
- Predict Species of Iris from Physical Measurements
- Predict Incidence of Diabetes from Health Metrics

Detect Numeric Outliers

Find values that are far from previous values. IT admins could look for machines with unusually high resource utilization; security analysts could look for employees transferring unusually large amounts of data; and business analysts could identify big spenders.

Algorithm: Distribution statistics

Examples:

- Detect Outliers in Server Response Time

Detect Categorical Outliers

Find events that contain unusual combinations of values. IT admins could look for unusual machine configurations; security analysts could look for employees performing an atypical combination of activities; and business analysts could identify rare purchasing habits.

Algorithm: Probabilistic measures

Examples:

- Detect Outliers in Mortgage Contract Data
- Detect Outliers in Congressional Voting Records

174.51.216.216:8090/en-US/app/Splunk_ML_Toolkit/showcase_classification?ml_toolkit_dataset=Diab

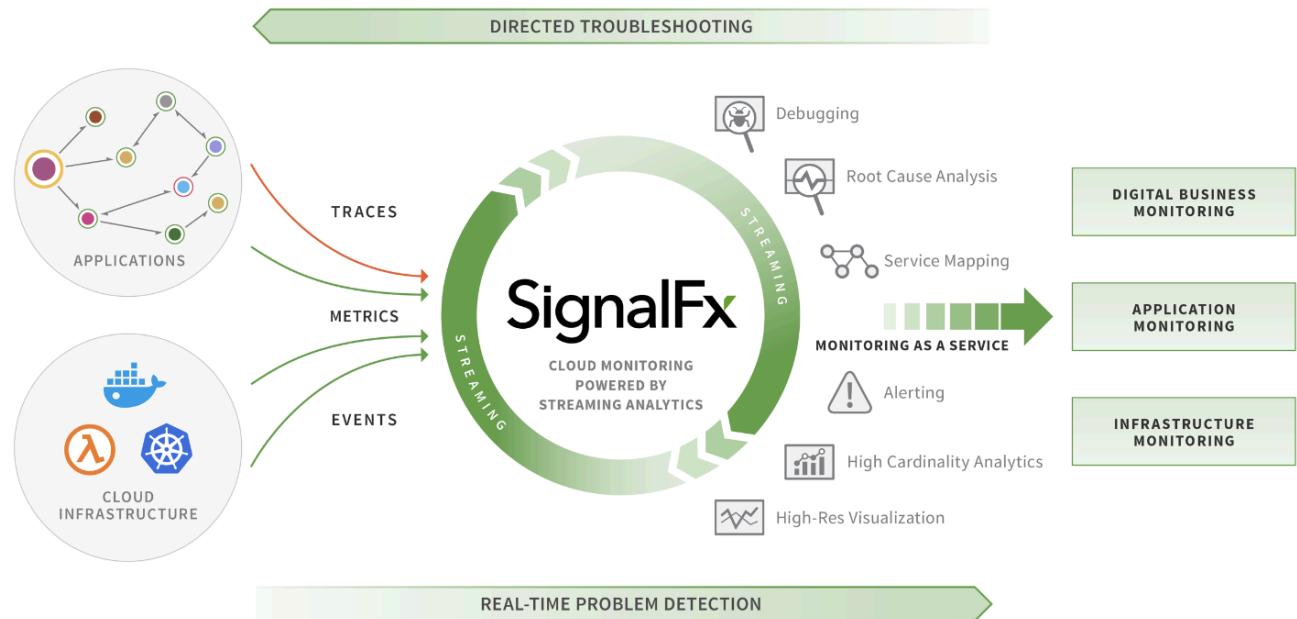
SignalFx

Application Monitoring

MICROSERVICES APM (μ APM)

Key Features

- Real-Time, Stream Processing SaaS
- Public cloud infrastructure monitoring
 - Uses an agent to gather metric on premises. Data pushed to the cloud
- APM covers -> Java, Ruby, Python
- Monitor Kubernetes , Containers, Micro Services , Rest APIs
- Great feature for discovery services and building graph of service dependencies
- Propose dashboards at Application and Service level



What's New: Observability and Action Across the Enterprise

Data Stream Processing | Data Fabric Search | Natural Language Processing | Connected Experiences



IT

Expanded infrastructure monitoring (IT Service Intelligence 4.4)
Engage on-call teams (VictorOps GA)
Unified Service Insights & Collaboration on Mobile



Developers

Collaborative Investigation (Splunk Investigate)
Analyze end-to-end user behavior (Splunk Business Flow GA)
Observability for modern cloud applications (SignalFx*)

*Pending Acquisition Close



Security

Monitoring and remediation in a single pane of glass (Splunk Mission Control)
Expanded security monitoring (Splunk Enterprise Security 6.0)
Mobile response (Splunk Phantom 4.6 w/Mobile)

Splunk Connected Experiences

Delivering Contextual Insights, the Missing Link Between Data and Outcomes



Extends Splunk analyses to even more users via devices they use most.



Empowers consumption and action on information via dashboards, the Apple Watch app, or Splunk TV.



Augmented Reality extends Splunk Dashboards by scanning QR codes or NFC tags for on demand insights.