

# splunk > live!

## Splunk for Enterprise Security featuring User Behaviour Analytics

SplunkLive Sydney 2016

Vlado Vajdic, Sr SE

# whoami

> **Vlado Vajdic** vlado@splunk.com

- 1 year as a Splunk Sales Engineer
- 15+ years in IT security
- Trend Micro, RSA, ... , Sun Microsystems
- First used Splunk in 2010
- GCFA, but don't take this against me

# LEGAL NOTICE

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.

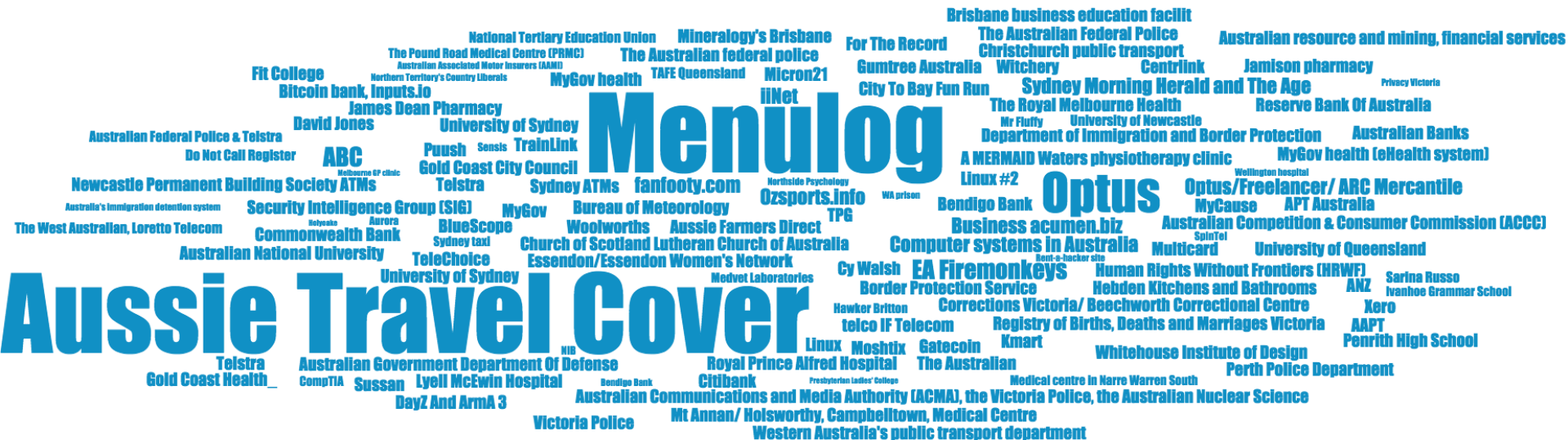
# Agenda

Splunk Security Update

Enterprise Security 4.2

User Behavior Analytics 2.3

# Data Breaches in Australia



# 2016 Cost of Data Breach Study

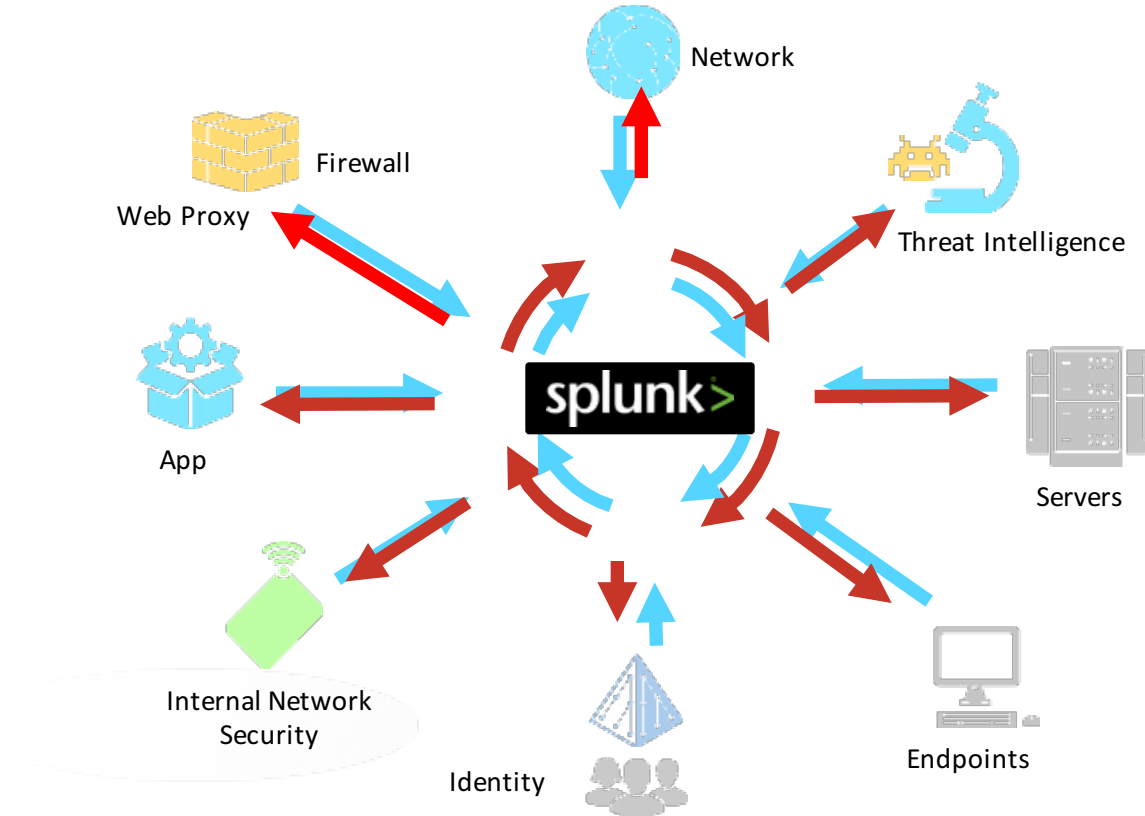
- The cost of a data breach continues to rise: \$158 per record
- The largest component of the total cost of a data breach is lost business
- “Time to Identify” and “Time to Contain” a data breach is critical
- Malicious or criminal attacks were the primary root causes of a data breach.
- Average total cost of data breach in Australia is \$2.64 million
- Key factor to reduce the cost of a data breach is enabling incident response
- Data breaches in regulated industries are more costly

Source:



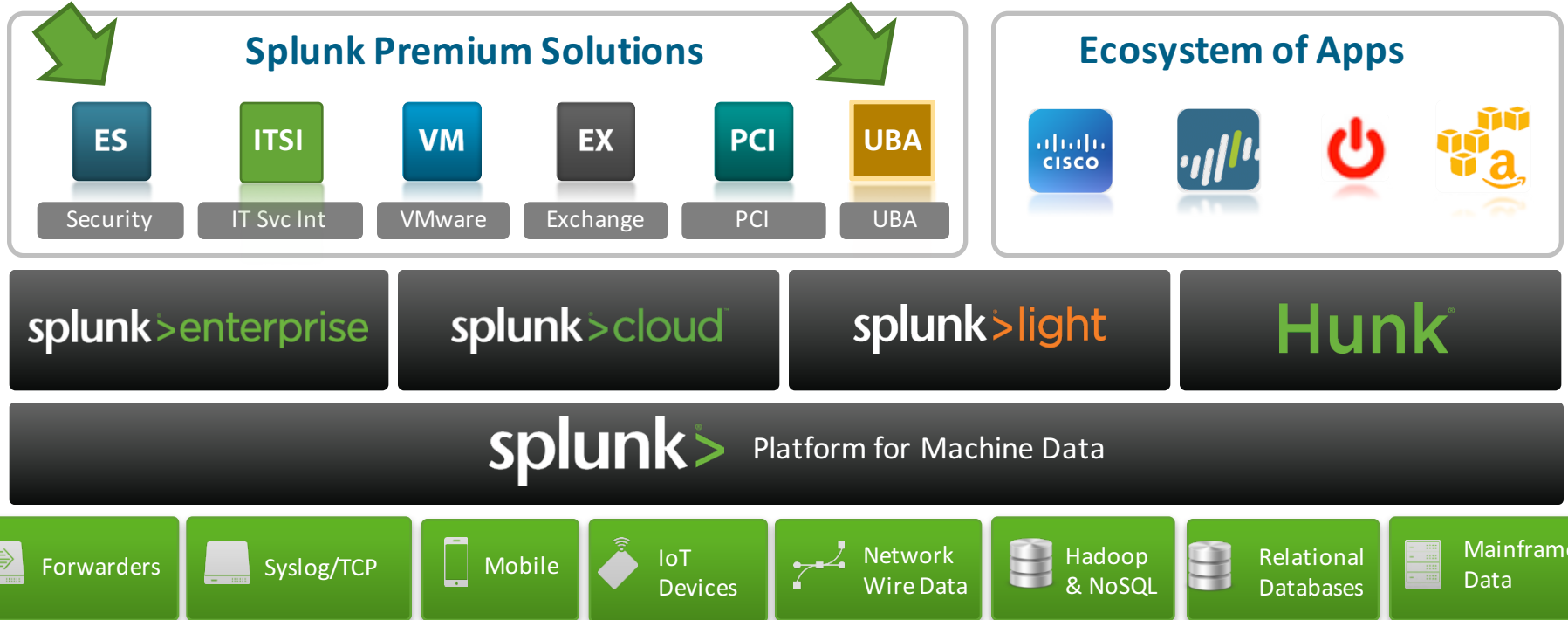
June 2016

# Splunk: the Security Nerve Center for the Enterprise



# Splunk Solutions

Across Data Sources, Use Cases and Consumption Models





# Splunk for Security



DETECTION OF  
INSIDER THREATS



DETECTION OF  
CYBERATTACKS



INVESTIGATION  
OF THREATS AND  
INCIDENTS



OPTIMIZED  
INCIDENT  
RESPONSE AND  
BREACH ANALYSIS



SECURITY &  
COMPLIANCE  
REPORTING

**SPLUNK UBA**

**SPLUNK ES**

# Splunk Security Ecosystem

## Threat Intelligence



## Network



## Endpoint

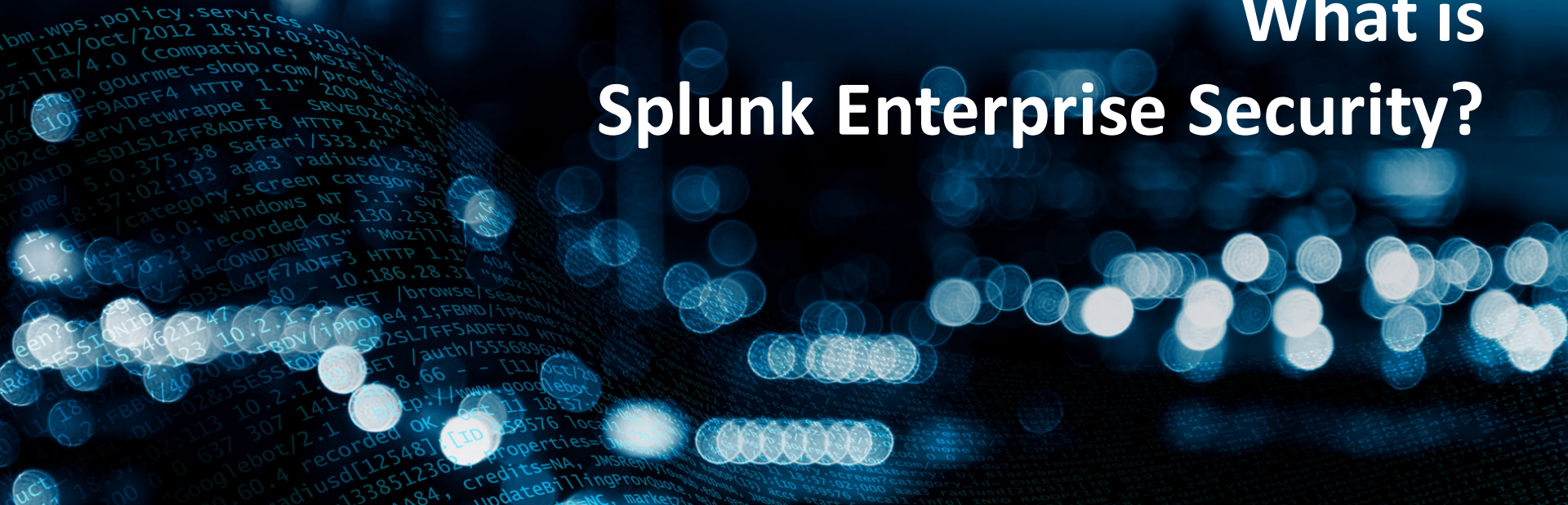


## Identity and Cloud



# splunk > live!

## What is Splunk Enterprise Security?



# Splunk Enterprise Security

Analytics-driven Security



Monitor and  
Detect Threats



Investigate Threats  
and Incidents



Optimize Response  
using Workflows



Security and  
Compliance Reporting



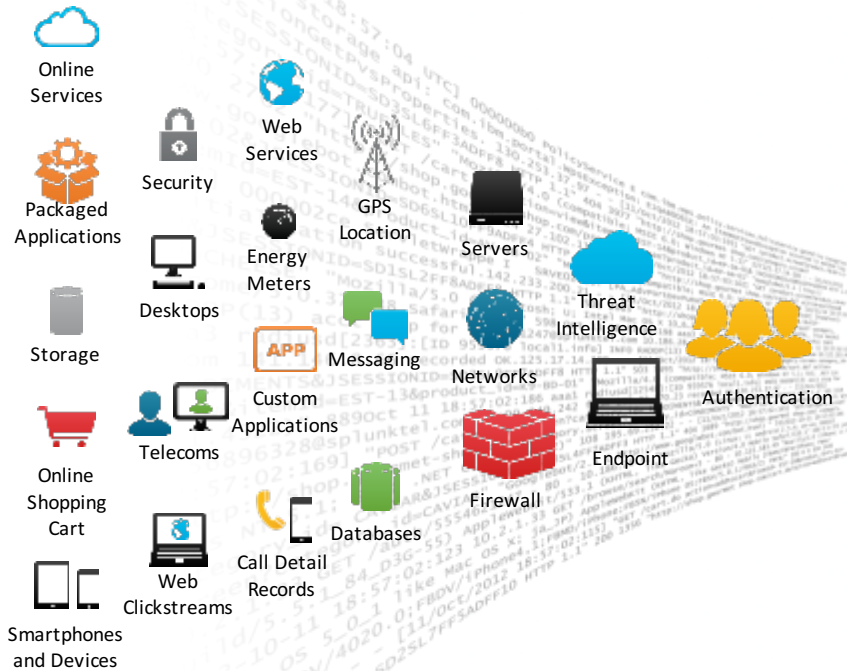
Splunk Enterprise  
Security™

splunk>enterprise

splunk>cloud

splunk> Platform for Machine Data

# Security Intelligence



Ad hoc search



Monitor and alert



Report and analyze



Custom dashboards



Developer Platform

Search-time Data Normalization



Data Enrichment



# Splunk ES in the Gartner SIEM Magic Quadrant

**2015** - Leader (the only vendor to improve its visionary position)

**2014** - Leader

**2013** - Leader

**2012** - Challenger

**2011** - Niche Player

\*Gartner, Inc., SIEM Magic Quadrant 2011-2015. Gartner does not endorse any vendor, product or service depicted in its research publication and not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



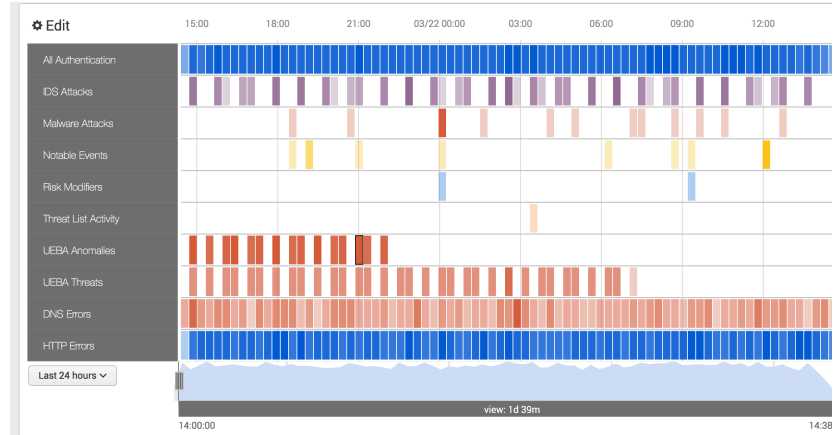
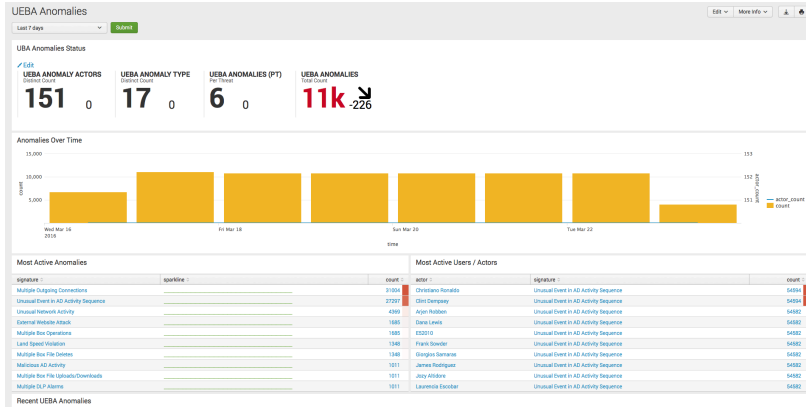


# splunk > live!

## What's New Splunk Enterprise Security v4

# Behavioral Analytics in the SIEM Workflow

- All UBA anomalies now available in ES
- SOC Manager: UBA Reporting within ES
- SOC analyst: UBA anomaly data available for enhanced correlation
- Hunter/Investigator: Ad-hoc searching/pivoting

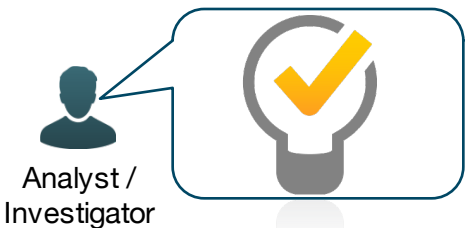


Detect and Investigate faster using ML integrated with SIEM

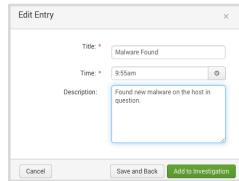


# Attack and Investigation Timelines

Adding content to timeline:

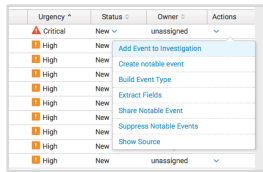


**Memo :**  
- Investigator's memos inserted in desired timeline



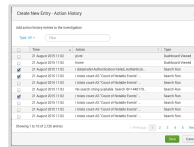
Investigator Memo

**Incident :**  
- Notable events from Incident Review



Urgency	Status	Owner	Actions
Critical	New	unassigned	
High	New		Add Event to Investigation
High	New		Create notable event
High	New		Build Event Type
High	New		Extract Fields
High	New		Share Notable Event
High	New		Suppress Notable Events
High	New		Show Source
High	New	unassigned	

Incident Review



Time	Object	Type
10:21:10	ess_security_posture	Dashboard Viewed
10:21:10	ess_security_posture	Panel Filtered
10:21:10	ess_security_posture	Search Run
10:21:10	ess_security_posture	Notable Status Change
10:21:10	ess_security_posture	Notable Event Suppressed

Action History

**Actions :**

- Search Run
- Dashboard Viewed
- Panel Filtered
- Notable Status Change
- Notable Event Suppressed



# Splunk ES - MSSP Partners

- **Verizon**

“Splunk is enabling our next generation platform. With these new capabilities, we are arming our clients with the tools and systems necessary to shift the balance and make it harder for cybercriminals to succeed.”

**Vinny Lee**, Director of Product Management, Verizon Enterprise Solutions.

- **Herjavec Group**

"Splunk's solutions are cutting edge - changing the way security teams operate at every level. That is why Splunk is such a key contributor to our security operations center and managed services practice,"

**Robert Herjavec**, Founder and CEO, Herjavec Group.

- **Accenture**

“Our alliance with Splunk is another strong example of how Accenture is impacting our clients' businesses with ‘new IT.’”

**Bhaskar Ghosh**, Group Chief Executive, Accenture Technology Services.

# splunk > live!

ES Demo



# splunk > live!

## What is Splunk UBA?



# ENTERPRISE SECURITY OPS CHALLENGES



## THREATS

External, Insiders, Hidden  
And/Or Unknown



## PEOPLE

Availability of  
Security Expertise



## EFFICIENCY

False Positives vs True  
Positives



# Splunk UBA: **TECHNOLOGY**



REAL TIME & BIG DATA  
ARCHITECTURE



BEHAVIOUR  
MODELING



UNSUPERVISED  
MACHINE LEARNING



ANOMALY DETECTION



THREAT  
DETECTION

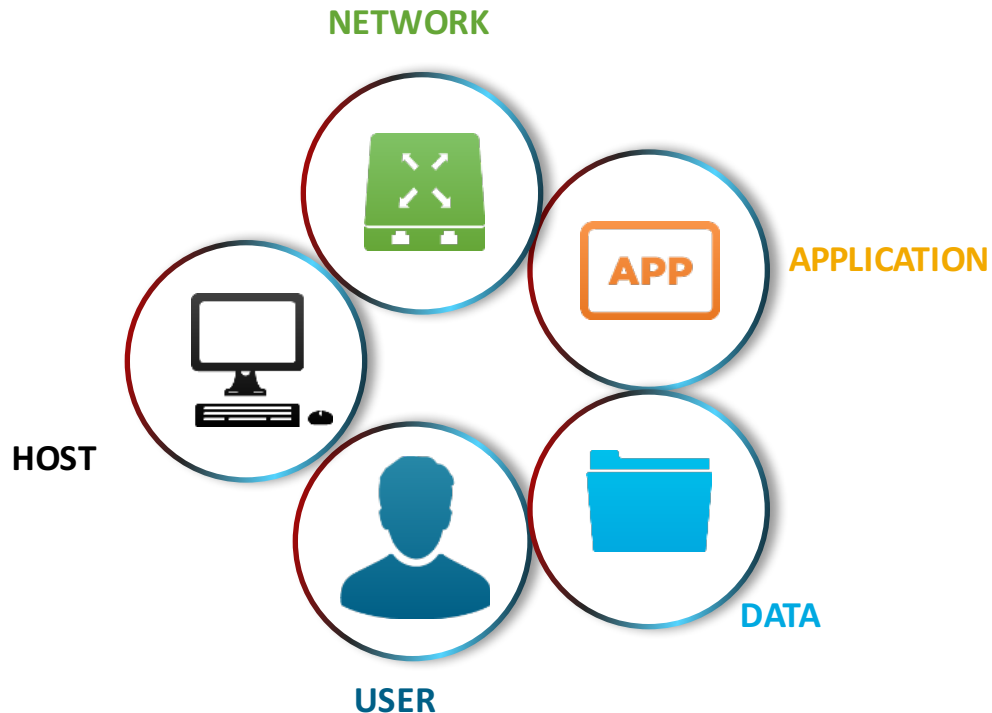


REAL-TIME, BIG DATA  
ARCHITECTURE

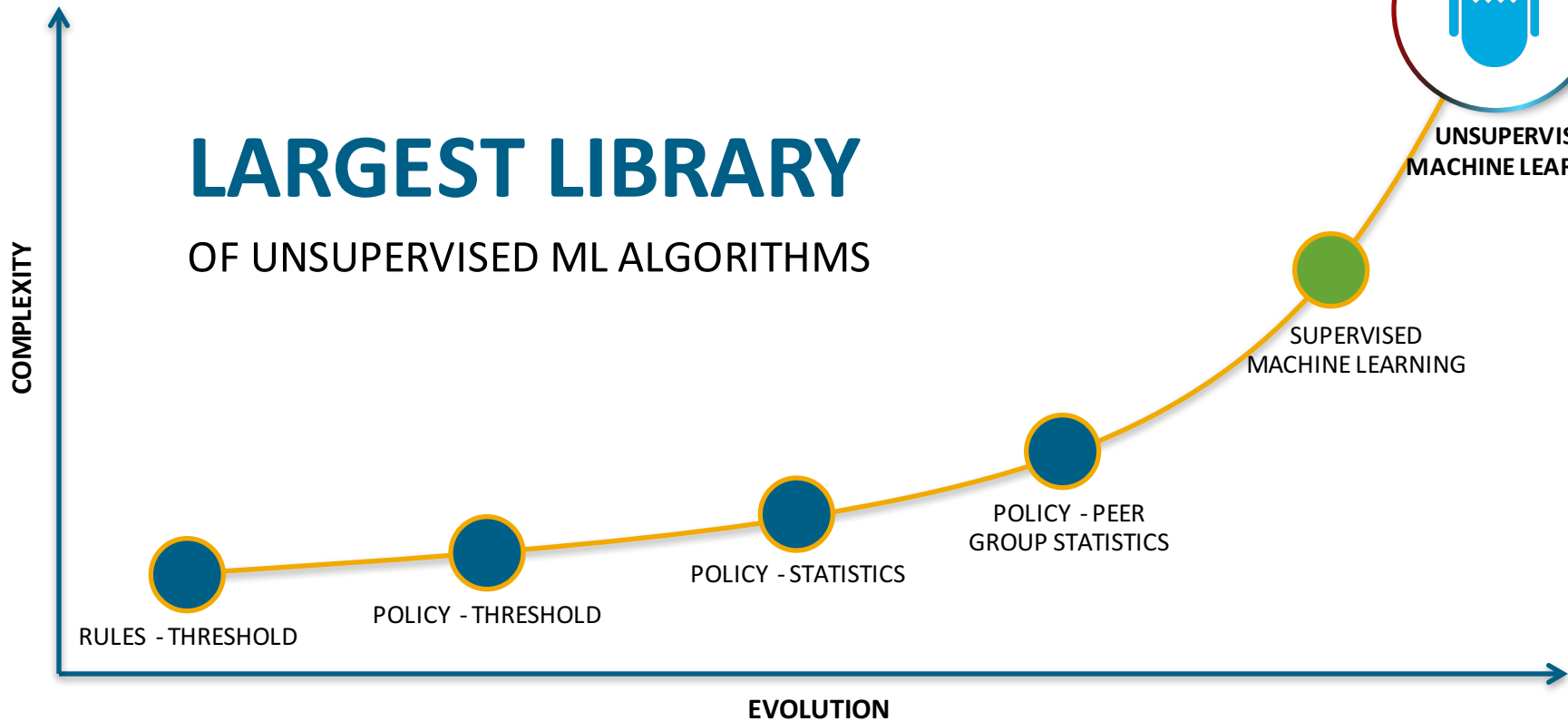
SCALABLE  
ARCHITECTURE

500M  
EVENTS/NO  
DE/DAY

# MULTI-ENTITY BEHAVIORAL MODEL







# LARGEST LIBRARY

## OF UNSUPERVISED ML ALGORITHMS



ANOMALY DETECTION

APPLYING ML AGAINST  
BEHAVIOUR BASELINES

DESIGNED FOR A  
HUNTER   
ANALYST



THREAT DETECTION

ML-DRIVEN AUTOMATED  
OR RULES BASED  
ANOMALY CORRELATION

DESIGNED FOR A  
SOC ANALYST

# THREATS UNCOVERED

---



## ACCOUNT TAKEOVER

- Privileged account compromise
- Data loss



## LATERAL MOVEMENT

- Pass-the-hash kill chain
- Privilege escalation



## INSIDER THREATS

- Misuse of credentials
- IP theft



## MALWARE ATTACKS

- Hidden malware activity
- Advanced Persistent Threats (APTs)



## BOTNETS, C&C

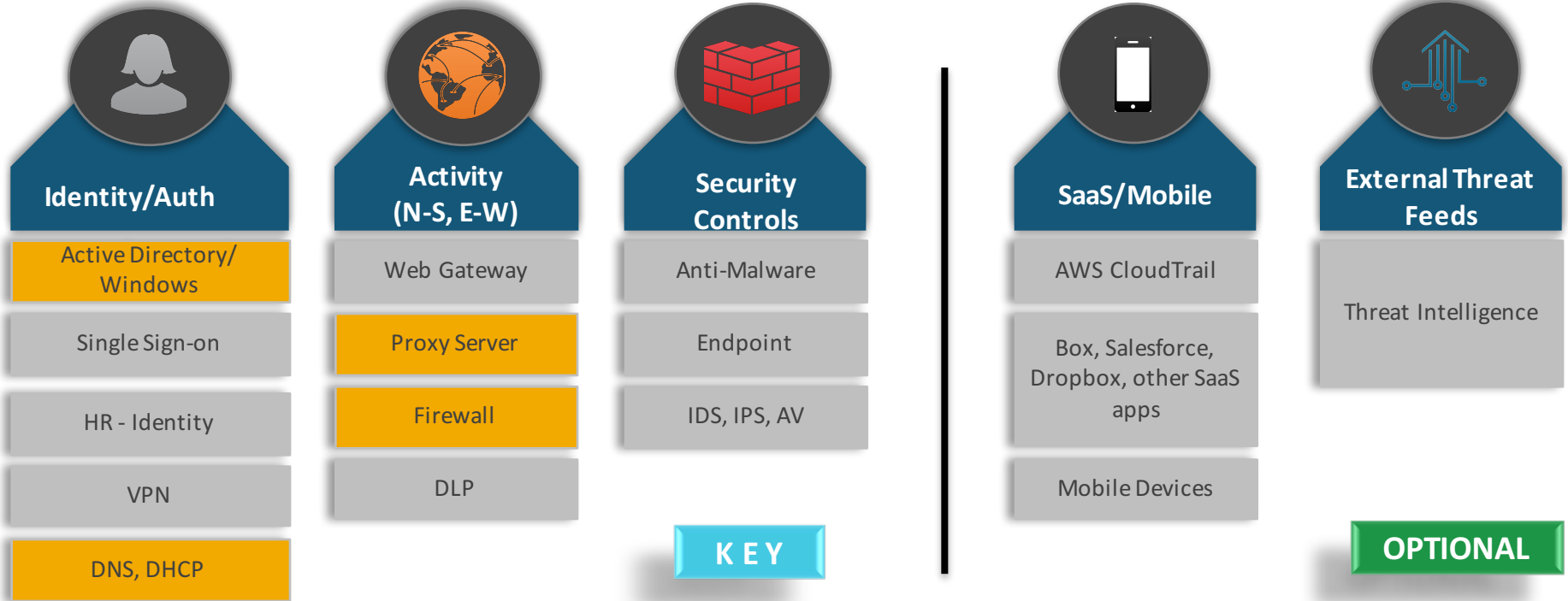
- Malware beaconing
- Data exfiltration



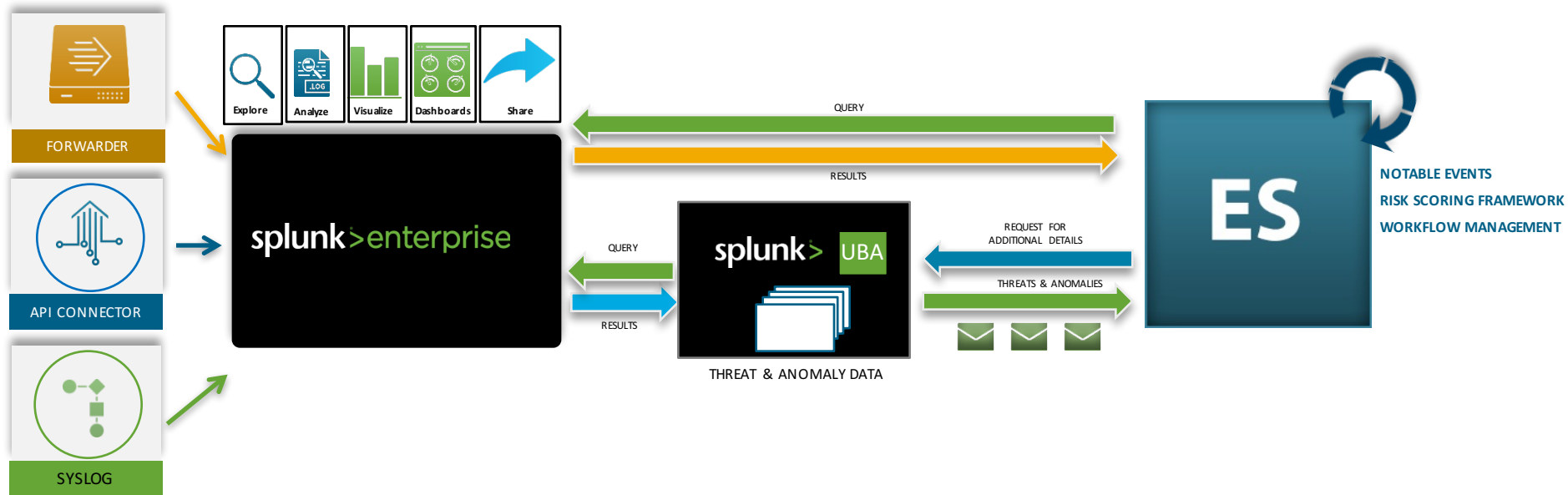
## USER & ENTITY BEHAVIOR ANALYTICS

- Login credential abuse
- Anomalous behaviour

# DATA SOURCES for UBA



# Data Flows: Splunk ES/UBA



# splunk > live!

## What's New in UBA v2

# Enhanced Threat Detection

## Threat Modeling Framework

Create **custom threats** using **60+** anomalies. Examples:

- Compromised Account: Accessed **blacklisted domain** followed by **outgoing connection** along with **unusual geo locations**
- Compromised Device: **Beaconing** followed by **outgoing connections** along with **unusual geo locations**

The collage displays six steps of a threat modeling framework:

- Step 1 of 6 : Rule Properties**: Shows fields for 'Rule Name' (containing 'Rules Creation Example') and 'Rule Description' (containing 'The description of the rule goes here.').
- Step 2 of 6 : Select Participant**: Shows three options: 'User' (selected), 'Device', and 'Session'. A note states: 'A threat is generated for each participant that matches the criteria specified in the following steps.'
- Step 3 of 6 : User Filters**: Shows a sidebar with 'Users' selected. A legend indicates score ranges: Any Score (0-10), Critical (8-10), Major (5-7), and Minor (1-4). A score bar shows a value of 1.
- Step 4 of 6 : Threat Conditions**: Shows a search bar and a list of anomalies with checkboxes: 'Any Anomaly Type', 'Exploit Chain', 'External Alarm', 'External Website Attack', 'Land Speed Violation', 'Machine Generated Beacon', 'Malicious AD Activity', and 'Malicious Domain'. A 'Count' field shows '(0)'. A note says: 'Add conditions on the anomalies that make up the threat.'
- Step 5 of 6 : Processing Times**: Shows a field for 'Anomalies interval of time' set to '1' with a unit dropdown set to 'Hours'. Two radio buttons are present: 'Process Future Anomalies' (selected) and 'Process Anomalies in a Date Range'.
- Step 6 of 6 : Generated Threats**: Shows a 'Threat Description' field, a 'Threat Recommendation' field with 'Suggestions on next possible steps.', and a 'Threat Score' bar with a value of 6. Below the bar are radio buttons for 'Use Existing Threat Type' (selected) and 'Create New Threat Type'. A dropdown menu shows 'RIF\_Candidate\_Client'.

**Threat Customization using ML generated anomalies**



# Enhanced Threat Detection

**30+**  
new metrics

Visibility and baseline metrics for users, devices, applications and protocols, dynamic peer groups, assess the individual user risk, new/enhanced models: device model, USB activity, unusual activity time, lateral movement, and unusual file access

USER CENTRIC



DEVICE CENTRIC



APPLICATION CENTRIC



PROTOCOL CENTRIC

# splunk > live!

## UBA Demo



The 7<sup>th</sup> Annual Splunk Worldwide Users' Conference

**SEPT 26-29, 2016**

**WALT DISNEY WORLD, ORLANDO  
SWAN AND DOLPHIN RESORTS**



- 5000+ IT & Business Professionals
- 3 days of technical content
- 165+ sessions
- 80+ Customer Speakers
- 35+ Apps in Splunk Apps Showcase
- 75+ Technology Partners
- 1:1 networking: Ask The Experts and Security Experts, Birds of a Feather and Chalk Talks
- NEW hands-on labs!
- Expanded show floor, Dashboards Control Room & Clinic, and MORE!



**PLUS Splunk University**

- Three days: Sept 24-26, 2016
- Get Splunk Certified for FREE!
- Get CPE credits for CISSP, CAP, SSCP
- Save thousands on Splunk education!

# splunk > live!

Thank You!