Be an Incident Resolution Superhero!

Fight Incidents with Automation & Orchestration: Find it with Splunk, Fix it with Resolve

Larry Lien | Chief Product Officer, Resolve Systems

September 2018

Splunk Users

Across the Enterprise

- Are you using Splunk Enterprise?
- Are you using Splunk ITSI?
- Are you using Splunk Enterprise Security?

Resolve Systems integrates and helps no matter which Splunk product(s) you use today.

The Impact of IT, Network & Security Incidents

Business Risks, Stalled Productivity, High Ops Costs, Unreliable Service Delivery and more

VISA

Credit card system outage leads to millions of failed transactions in Europe

AA AmericanAirlines

Hundreds of cancelled flights due to failure of crew scheduling system. Southwest, Delta, United suffered similar outages

charles SCHWAB

Trading system outage prevents thousands of clients from executing stock transactions

91%
of Enterprises
Experienced major IT incident or outages one or multiple times in a year

$8662/min
Average Cost of Unplanned IT Downtime

78%
of Enterprises
Takes hours to days to Resolve a incident after it is reported

404 error

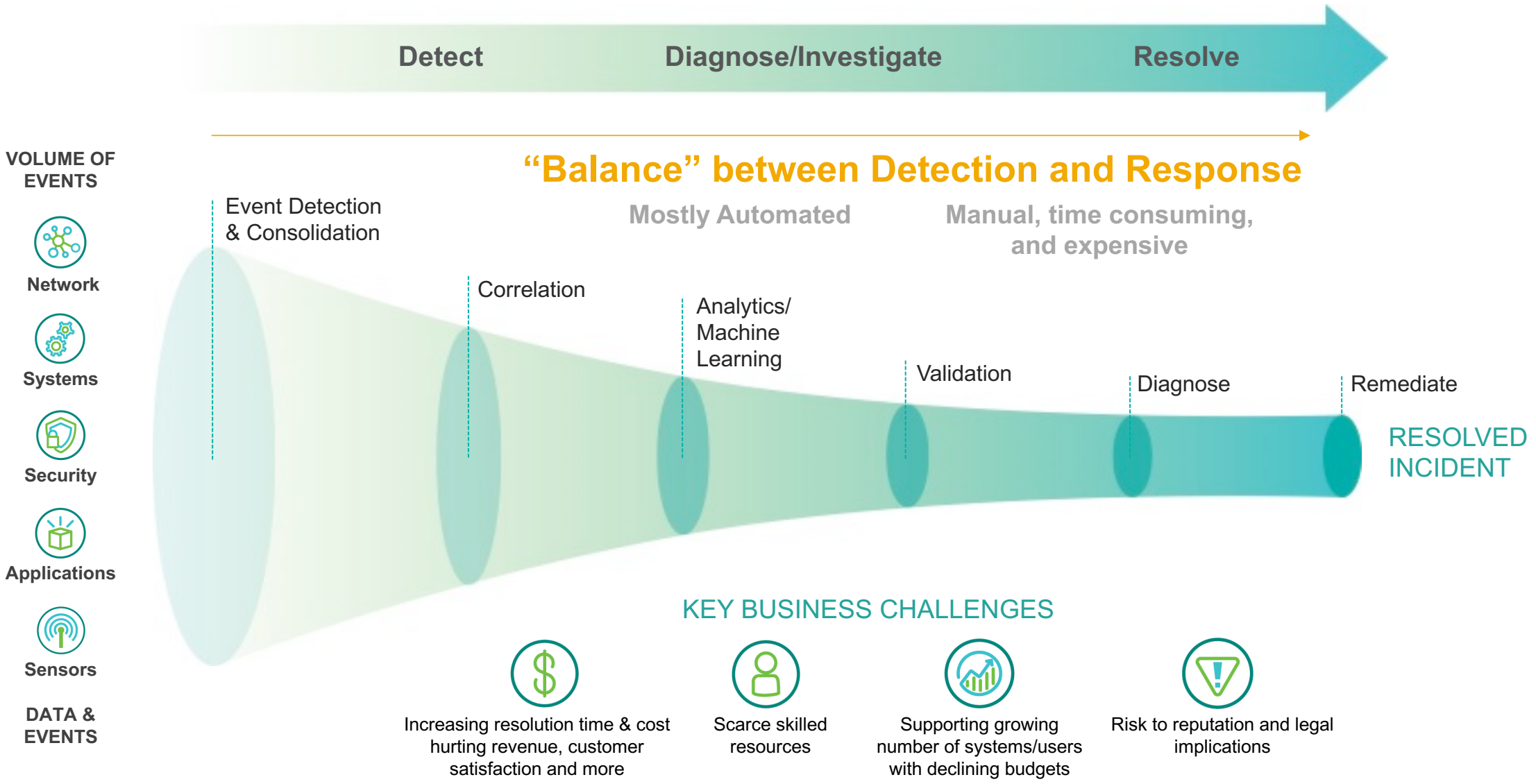
97%
of Enterprises
Human errors are causing network outages

Many more high impact outages across verticals…

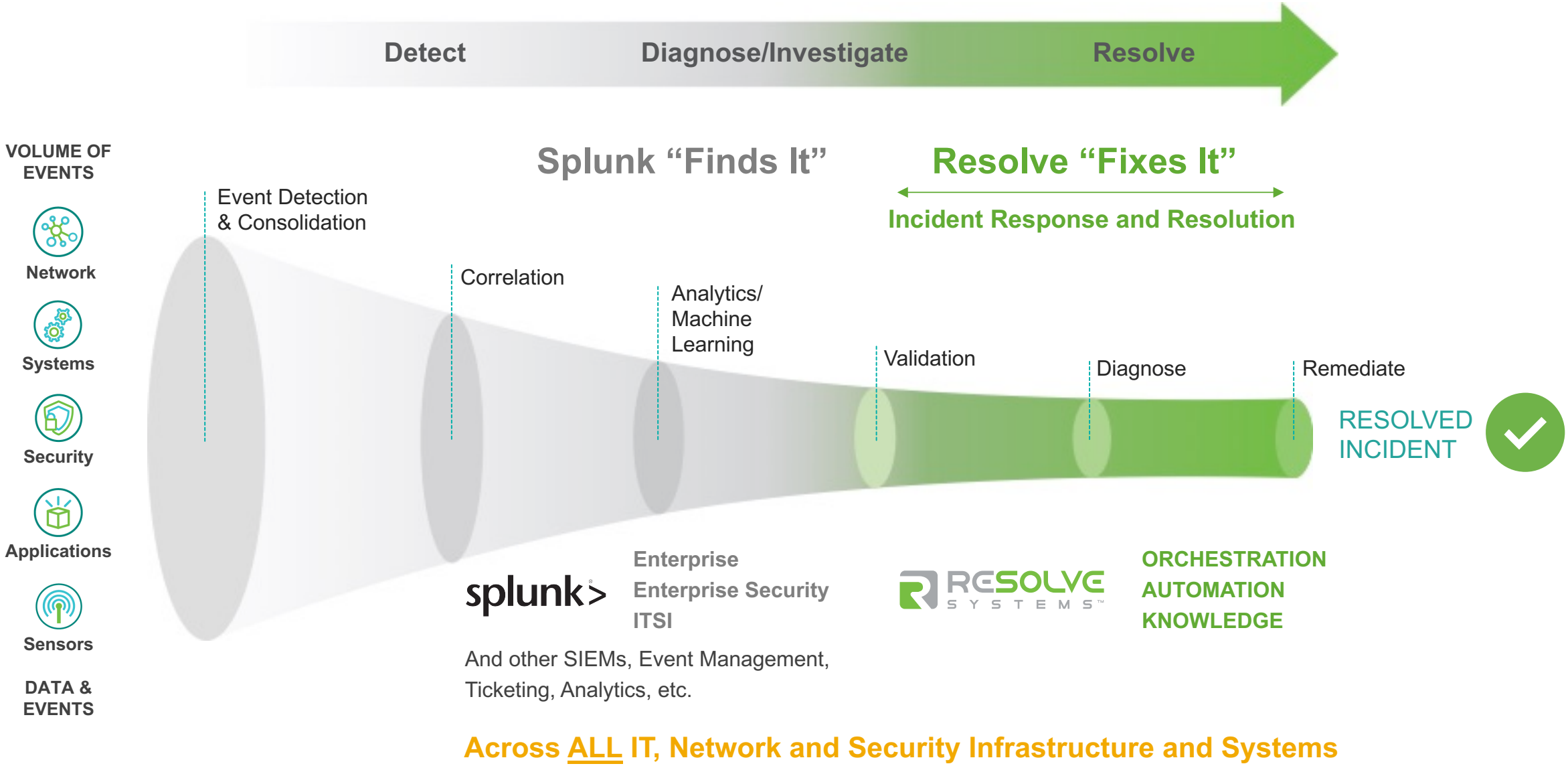
Marketo comcast GitLab Microsoft Square

splunk> .conf18

End-to-End Incident Management



Resolve Systems: Incident Response and Automation



About Resolve Systems

Work Smarter. Work Faster. Work Efficiently.

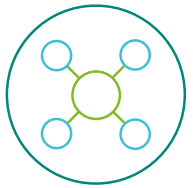
Proven to scale and support the largest and most complex enterprise environments, Resolve Systems is the global leader in delivering incident response and resolution, fully focused on orchestration, automation and incident resolution to help customers address all aspects of the incident response lifecycle. Resolve Systems' focus on human-guided, end-to-end automations makes it the only solution flexible enough to address the full spectrum of use cases whether it be for IT, network or security operations.

Deep Roots in the Industry

Founded by experts with extensive experience with IT Operations, Network Operations, Security Operations and Customer Care.

Worldwide Presence

- North America HQ
  Irvine, California
- EMEA HQ
  London, United Kingdom
- APAC HQ
  Singapore

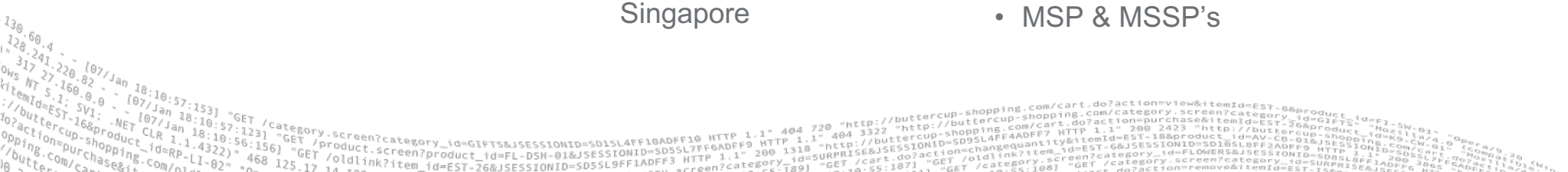


Industries & Markets

- Telecommunications
- Banking & Financial
- High-Tech
- Healthcare
- Oil & Gas
- Retail
- MSP & MSSP's

Financial Stability & Growth

Resolve Systems is majority owned by Insight Venture Partners, a $18B leading global private equity and venture capital firm investing in high-growth technology and software companies.



splunk> .conf18

What We Do

Global 1000 Companies Trust Resolve

T-Mobile · zayo · accenture · CVS · GUARDIAN · Charter Spectrum

CenturyLink · TELUS · LIBERTY GLOBAL · FIS · GYMBOREE

17% Improvement in OPEX

90% Improvement in MTTR on P1 issues

5% YoY Reduction on Global IT Support Spend

70% Reduction of Incidents Related to Mission Critical Enterprise Application

30% Reduction in headcount

Transform Your Organization with Resolve

Incident Resolution Today

- Manual and ad-hoc processes
- Escalations, rely on Tribal Knowledge
- Patchwork of disconnected tools
- Strained cross-team process
- IT Ops limiting business growth

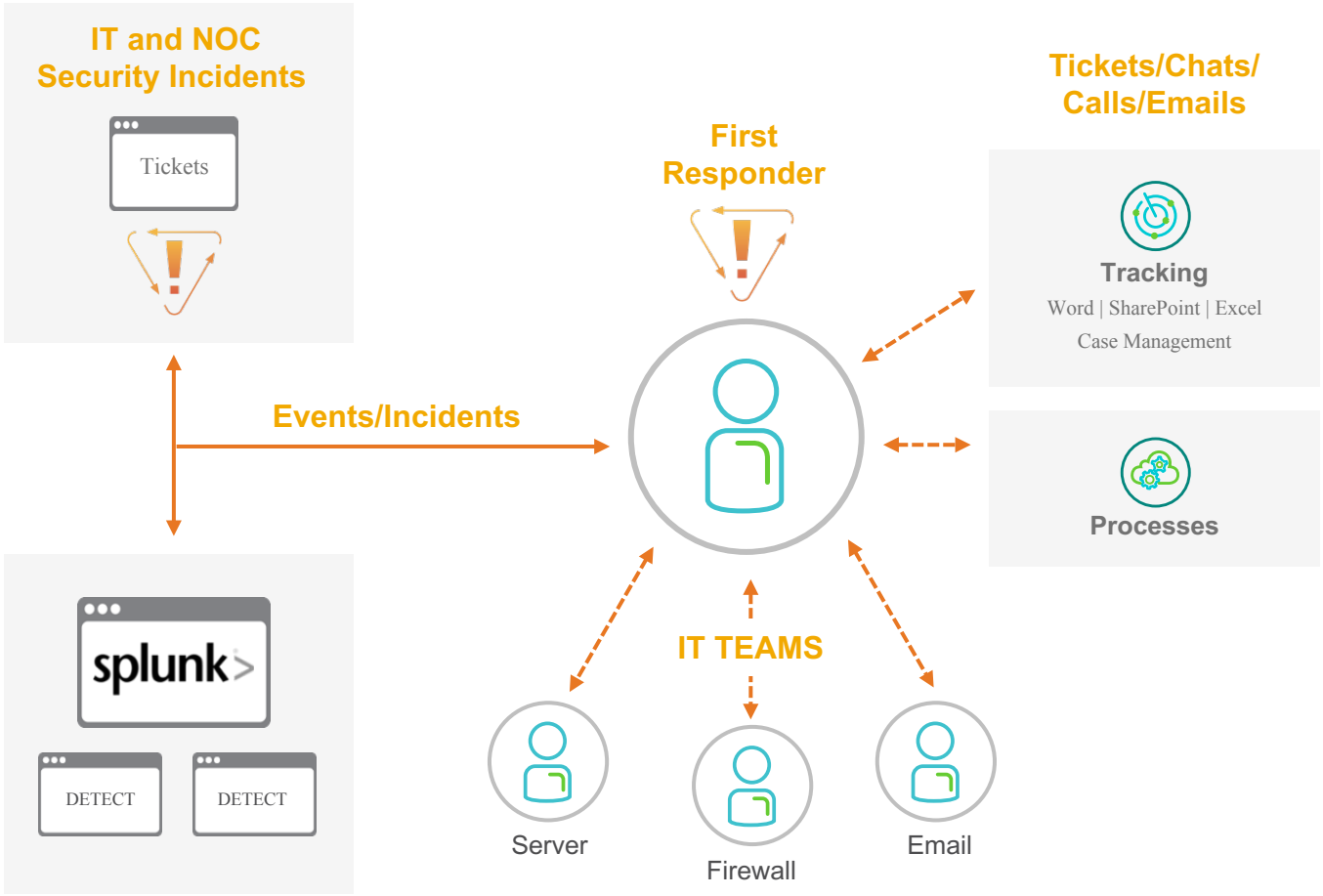
Where You Need to Be

- Highly Automated & Streamlined
- Empowered L1 with SME-approved procedures
- Centralized, Purpose-built for IR
- Tightly connected Ops teams
- IT Ops is strong business enabler

What Problem Does Incident Response Solve?

Current Investments Over-indexed to Detect & Manage

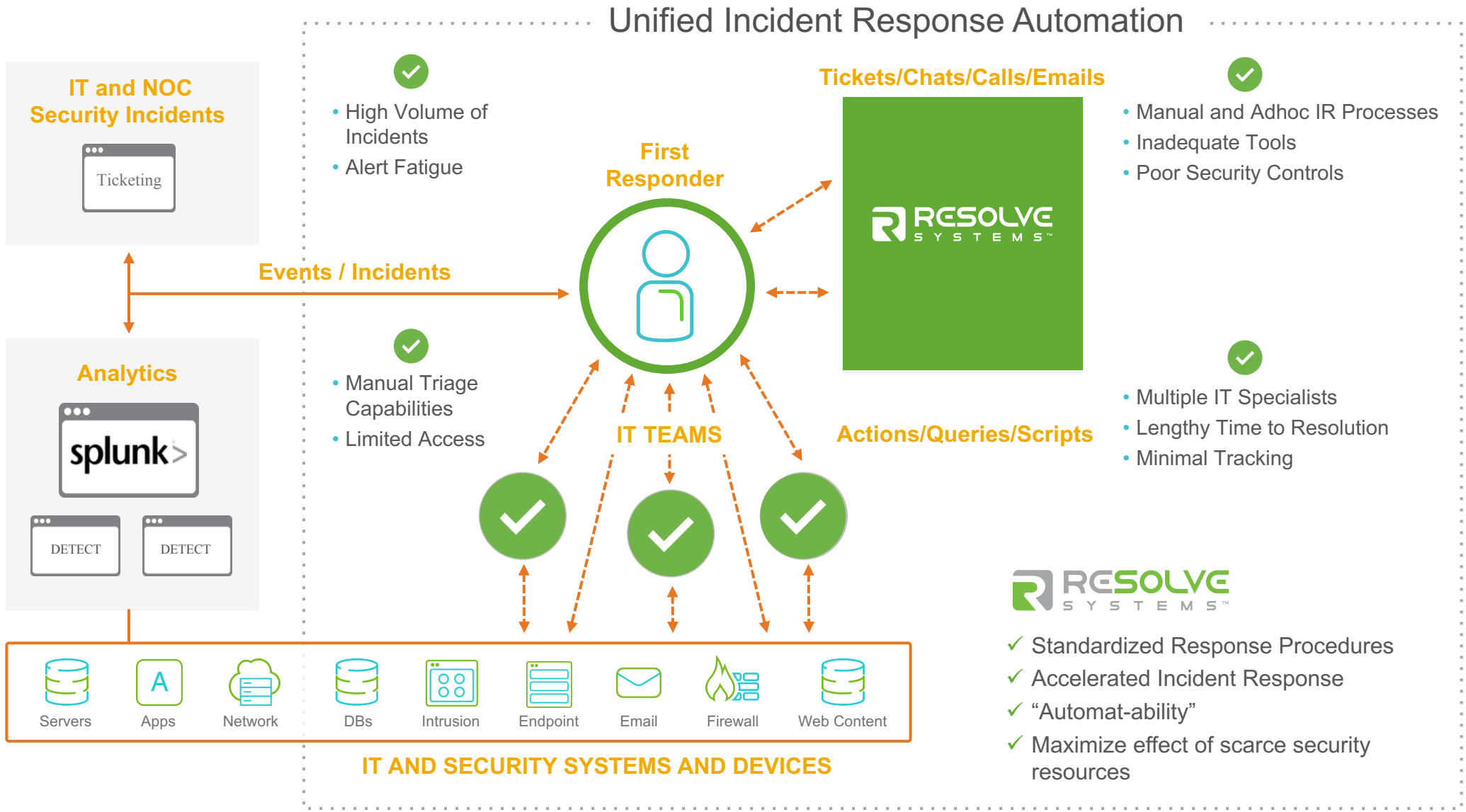
- Alert Fatigue from High Volume of False Alarms
- Lengthy Time to Resolution
- Multiple IT Specialists/Minimal Oversight & Tracking
- Manual & Adhoc IR Processes = Manual Triage Capabilities



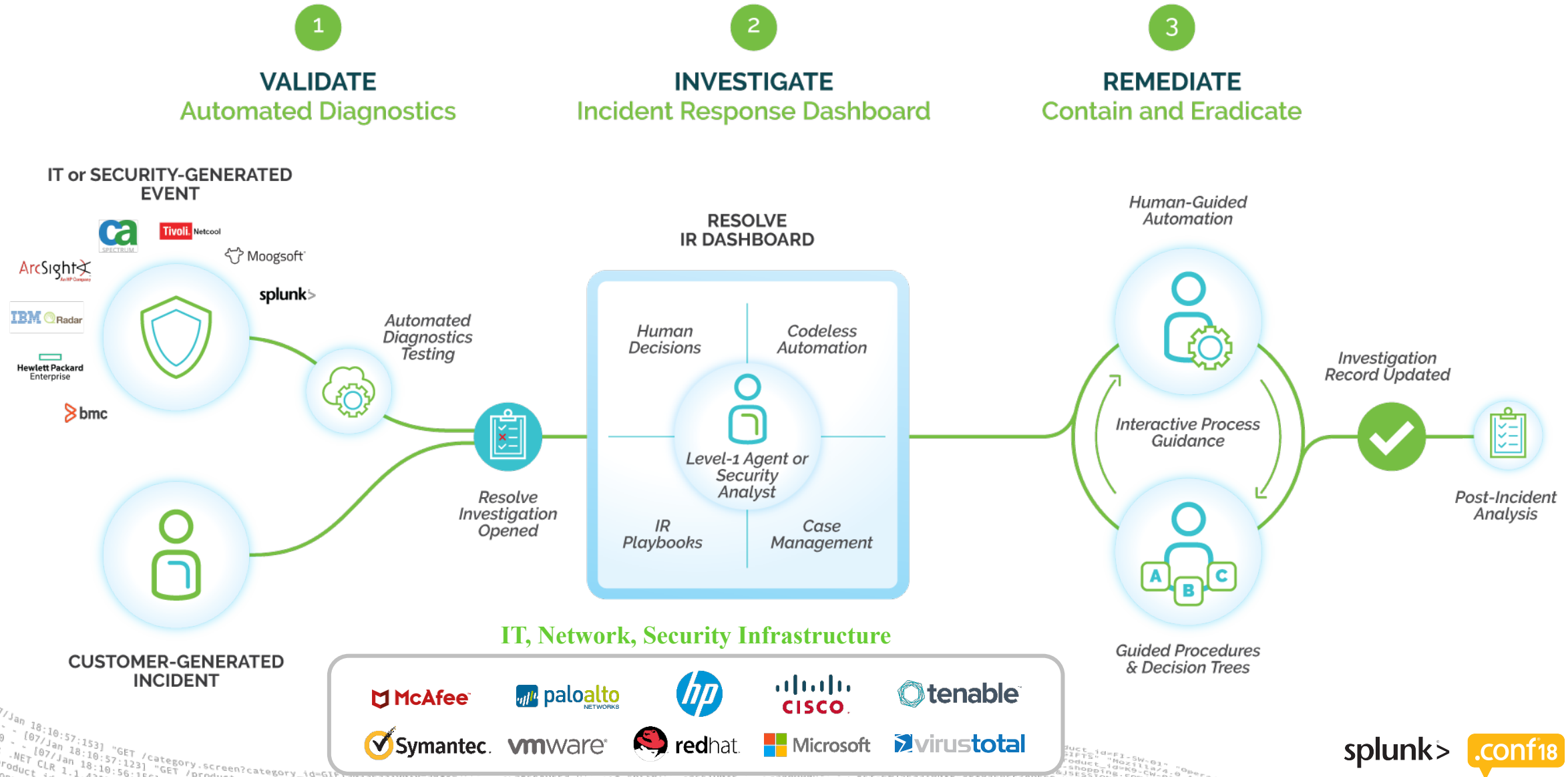
What Problem Does Incident Response Solve?

High Volume of False Alarms

Focus on Detection Increases Event Volume

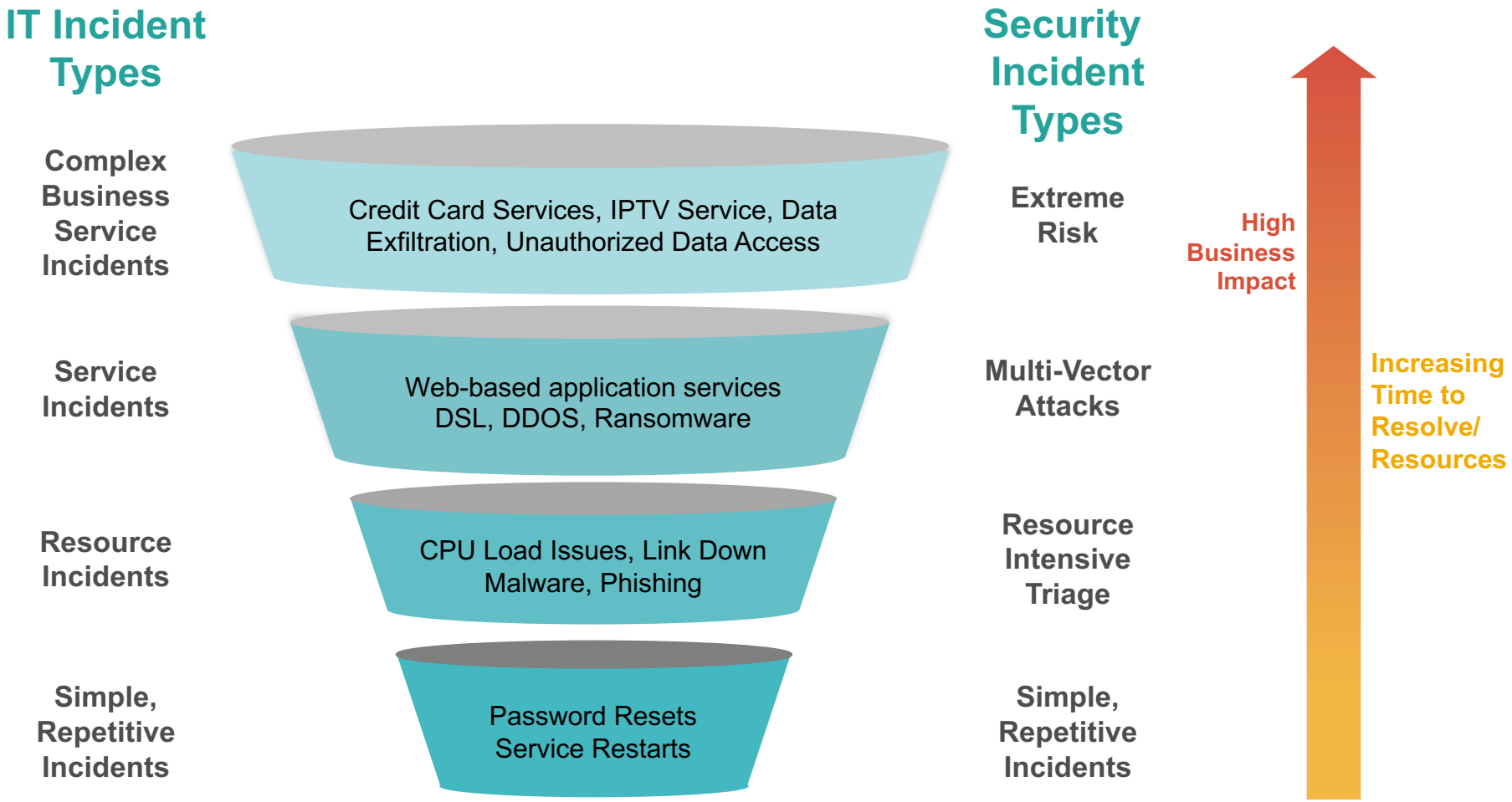


Enterprise-Wide Incident Response and Automation Platform

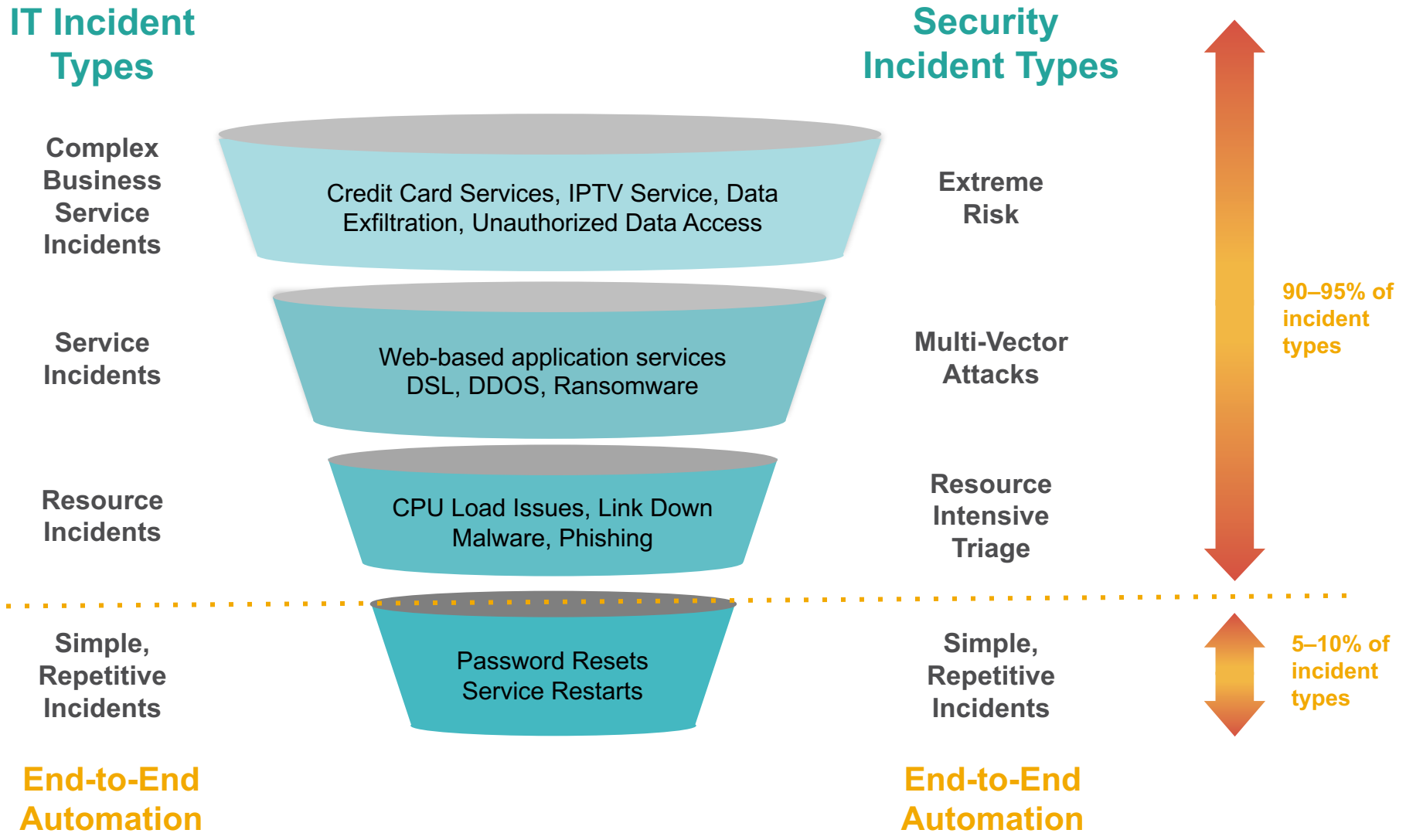


splunk> .conf18

Can All Incident Types Be Treated The Same?



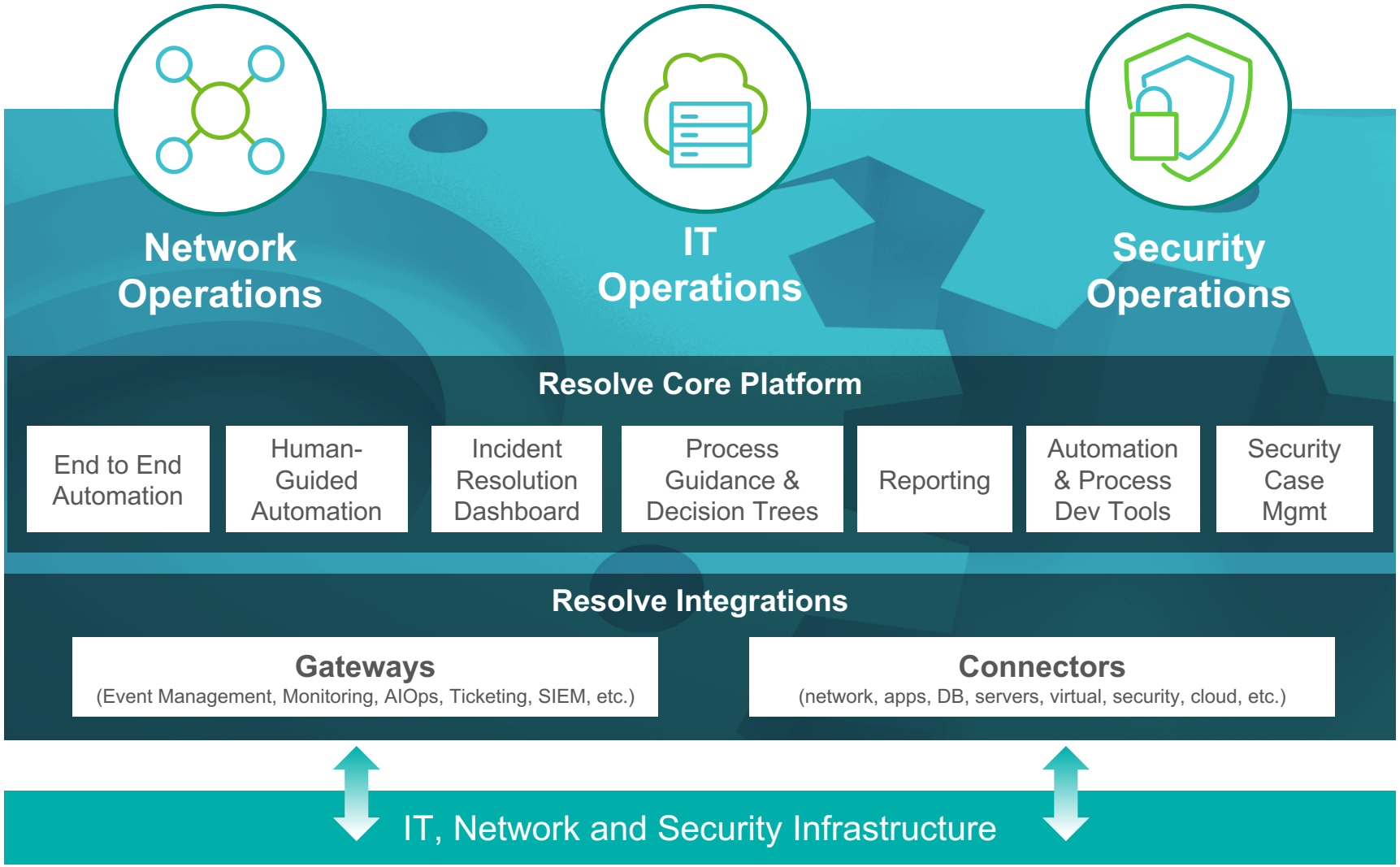
Can All Incident Types Be Treated The Same?



- How do you address the other 90-95% of incident types?
- How can you reduce your Incident Response Time?
- Requires more than just end-to-end automation
- Requires process guidance, knowledge management

splunk> .conf18

The Power of Resolve



Community Content Library

Runbooks / Playbooks

Process Templates

Action Tasks

Why Resolve Systems?

Differentiated Approach

Full and Human Guided Automation

Automation can accelerate simplest to most complex use cases; support for an iterative approach to automation

Ease of Automation & Process Development

Visual tools for fast development of automations, procedures and integrations even by Ops staff and SMEs

Integrates with your Environment

Library of Integration & Automation

5000+ pre-built automations, 150+ Integrations, 100s of process templates with codified best practices

Integrates with Existing Automations

Leverage existing automations in 10's of scripting languages and automation tools including Perl,, Python, Shell scripts, HPOO, CA PAM, BMC AO, and more

Proven Enterprise Ready

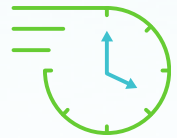
Purpose-built for Incident Resolution

New product capabilities, integrations, reports, content all focused on keeping Resolve best in class for Incident Resolution

Support and Scale Large Complex Environments

Deployed and proven in the more than 50% of Tier-1 Service Providers and globally. Proven to handle million+ daily events

Drives Business Outcomes



Fastest Time to Value

Quick installation and integration (weeks), prebuilt library, reusable automation framework, iterative rollout with quick ROI

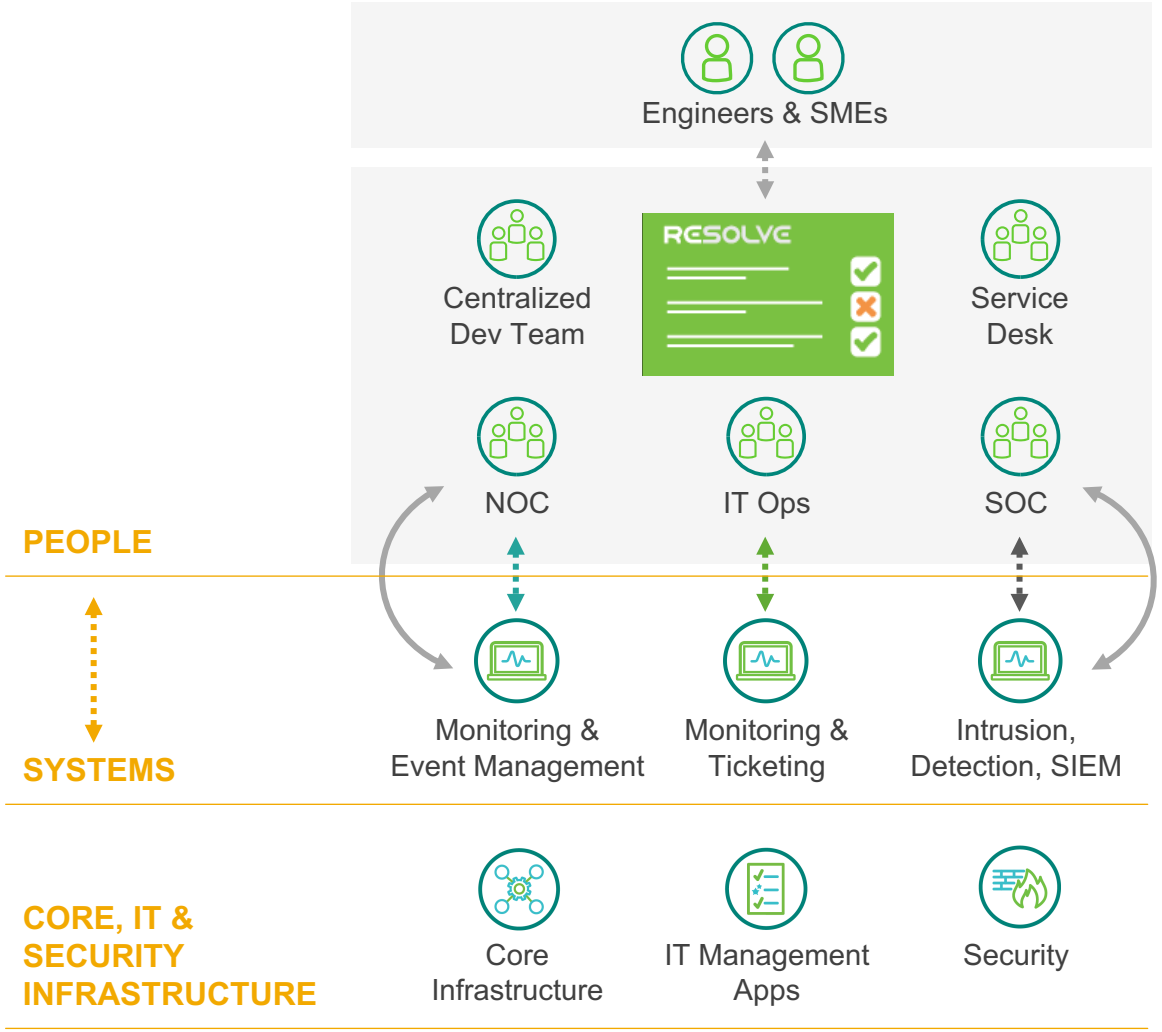
Partner for Success

10+ years of IT & Network experience with codified industry best practices. Business partnership committed to customer success,

splunk> .conf18

Find it With Splunk, Fix it With Resolve

Enterprise-wide



When IT, Network, & Security incidents happen

- Leverage same engineers and SMEs to resolve
- Gather information from the same systems
- Take actions on the same systems

Resolve provides one centralized incident response platform for the entire enterprise

- Unified tool - enables actions and automations to be taken across enterprise devices and systems – IT, Network, or Security
- Processes/knowledge defined and shared from the same SME resources
- Re-usable automations across organizations

Processes tailored for each team with a Platform built and shared by the entire enterprise

The Resolve Advantage

Cohesive Incident Response solution for your entire Enterprise

- Unified Process Orchestration, KM & Automation for faster incident response
- Closed-loop and Human-Guided Automations to address all incident types

Designed for Rapid Time to Value and the Quickest ROI

- NOC/SOC/IT Ops teams are able to quickly reduce MTTR and incident response times
- Out of box Automations, Procedures and Integrations for rapid kick-start
- Next-gen Automation Dev Tools including “no-code” and “drag ‘n drop” for fast custom development

Proven Enterprise Grade Platform and Proven Company

- Deployed in largest and most complex Enterprises and Service Providers - Handles millions of daily events
- Only Incident Response Platform with SaaS offering

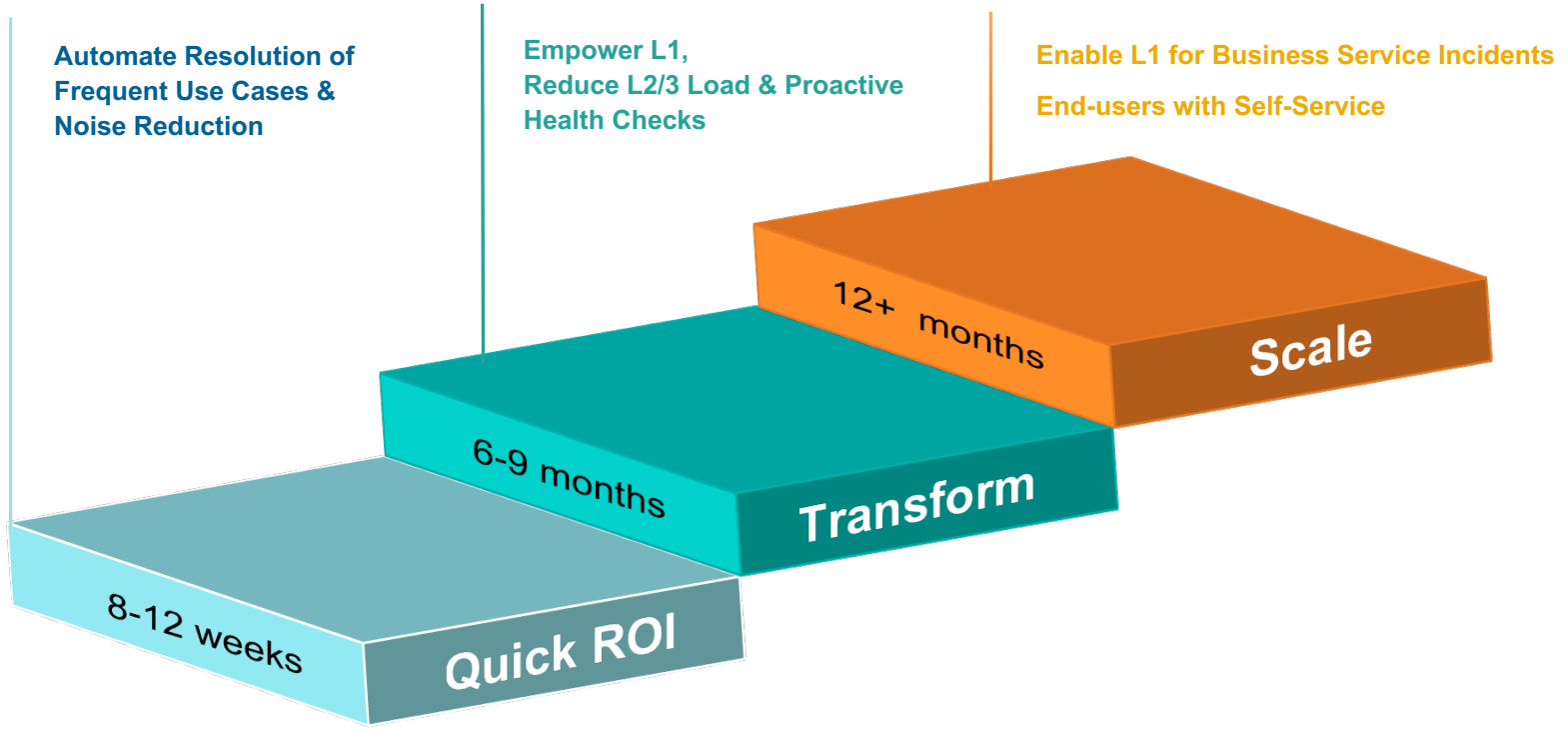
splunk> .conf18

Customer Journey with Resolve

RESOLVE SYSTEMS™

Stop by booth **T2** to learn how to:

- Derive near and long-term business value
- Automate the simple to most complex incidents
- Using Resolve your organization can take a pragmatic and iterative automation approach



Get your questions answered

Get a live demo

Thank You

Don't forget to rate this session in the .conf18 mobile app

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> .conf18

2018 Splunk Section Template Header

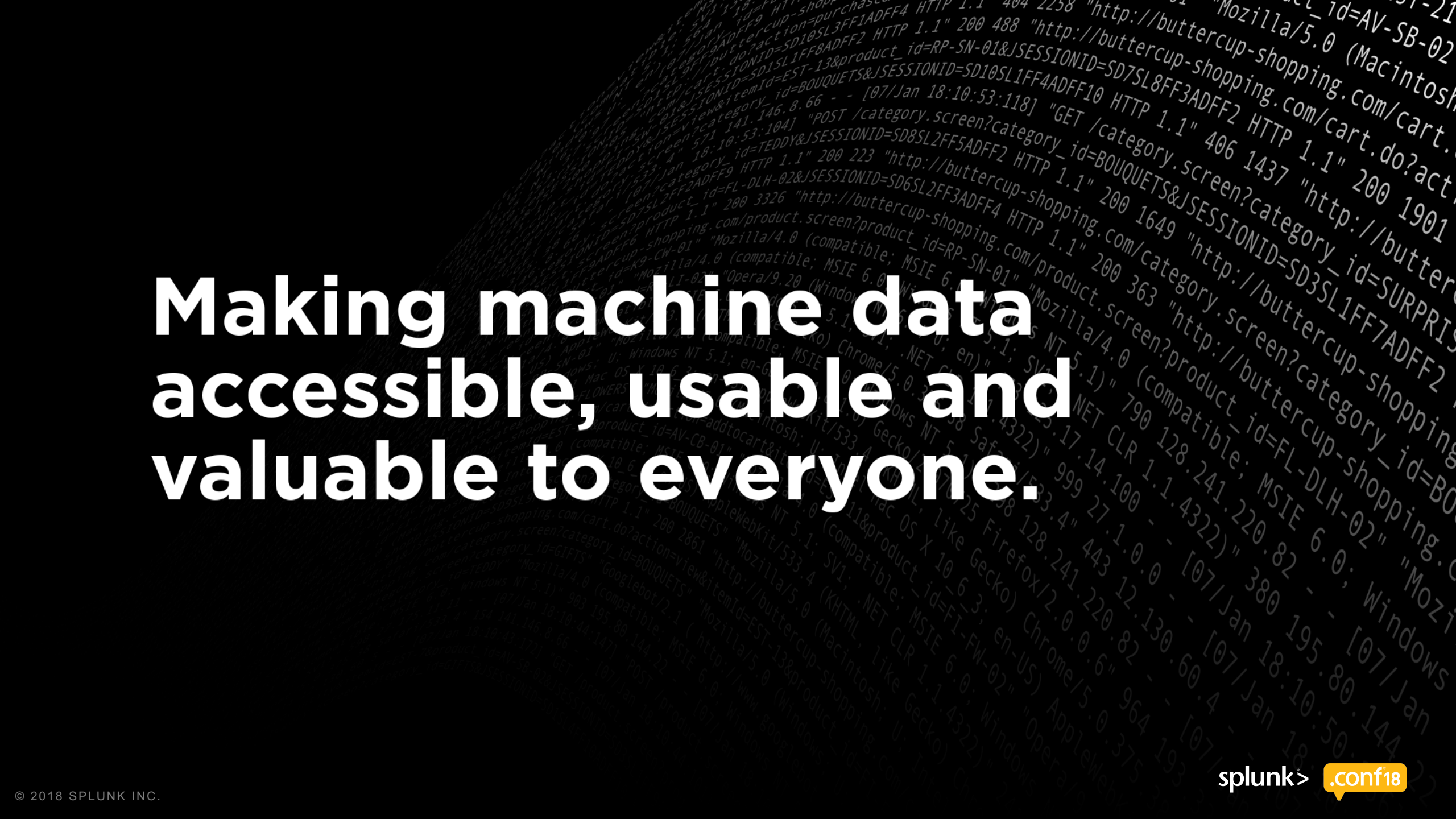
Section subtitle goes here

splunk> .conf18

Key Takeaways

This is where the subtitle goes

1. First level bullets should be sentence case, 28pt
2. First level bullets should be sentence case, 28pt
3. First level bullets should be sentence case, 28pt



Making machine data accessible, usable and valuable to everyone.

splunk> .conf18

Tracks and Sessions

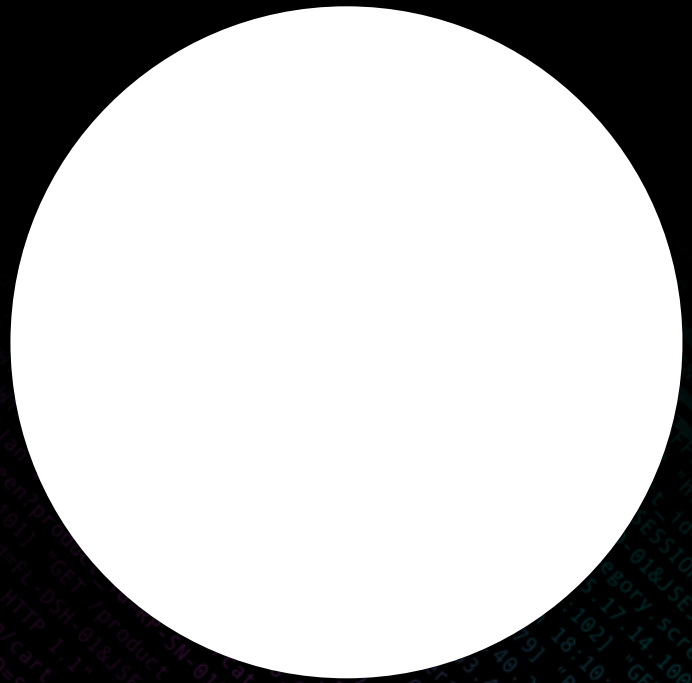
New to Splunk	**11:15 – 12:15**	Splunk Overview	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Getting Started with Splunk Enterprise **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	Data Onboarding	**Presenter Name**, Senior Sales Engineer, Splunk
IT Ops	**11:15 – 12:15**	Happy Apps, Happy Users: Using Splunk APM	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Splunk Enterprise for IT Troubleshooting **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	How to Design, Build and Map IT and Business Services in Splunk	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
Security	**11:15 – 12:15**	Build a Security Portfolio That Strengthens Your Security Posture	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Building an Analytics Driven Security Operation Center using Splunk Enterprise Security	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	An End-To-End Approach: Detect via Behavior and Orchestrate via SIEM	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk
Advanced	**11:15 – 12:15**	The Power of SPL	**Presenter Name**, Senior Sales Engineer, Splunk
	1:30 – 2:30	Advanced Analytics and Machine Learning in Splunk	**Presenter Name**, Senior Sales Engineer, Splunk
	2:45 – 3:45	Ransomware Investigation and Prevention Strategies **(HANDS-ON)**	**Presenter Name**, Senior Sales Engineer, Splunk **Presenter Name**, Senior Sales Engineer, Splunk

BUTTERCUP SPLUNKER

Mascot, Internal Mischief

splunk> .conf18

Our Speakers



BUTTERCUP SPLUNKER

Mascot, Internal Mischief

BUTTERCUP SPLUNKER

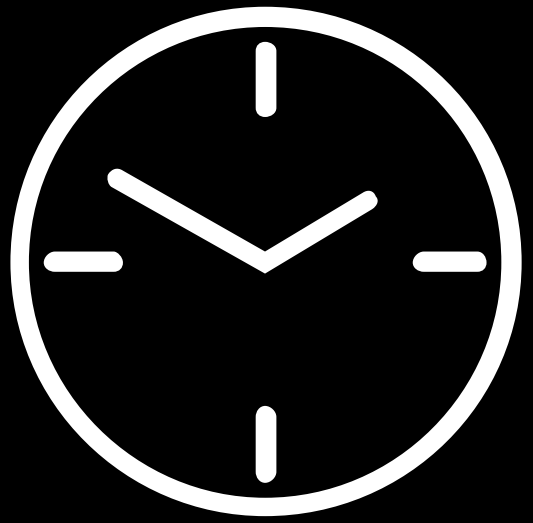
Mascot, Internal Mischief

MODERATED BY GREEN TRACKSUIT

Splunk Demo

Presented by Buttercup Splunker

splunk> .conf18



BREAK

15 MINUTES

Customer Logo Here

Please use an all-white image on a transparent background, like this Splunk logo: splunk>

Join the Pony Poll

ponypoll.com/***

Join us at Splunk .conf18

October 1–4, 2018

Walt Disney World Swan and Dolphin Resort in Orlando

8,750+ Splunk Enthusiasts
300+ Sessions
100+ Customer Speakers

Plus Splunk University:

Three Days: September 29-October 1, 2018
Get CPE credits for CISSP, CAP, SSCP

Register now at conf.splunk.com

Q&A

Participant name | Role

Participant name | Role