RESOLVE SYSTEMS™

splunk>

Find it with Splunk, Fix it with Resolve: Your Solution for Enterprise-Wide Incident Response and Resolution

Splunk Users – Across the Enterprise

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

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

Incidents Impacting Businesses

The ability to respond to incidents and outages is *critical* to your business

This image cannot currently be displayed.

AWS: 5hr outage due to human error takes down Netflix, Reddit, Airbnb and 1000’s of more businesses

Salesforce.com: Site down for 12hrs due to database incident with severe business impact

JP Morgan: 76 million households and 7 million SMB’s impacted by breach

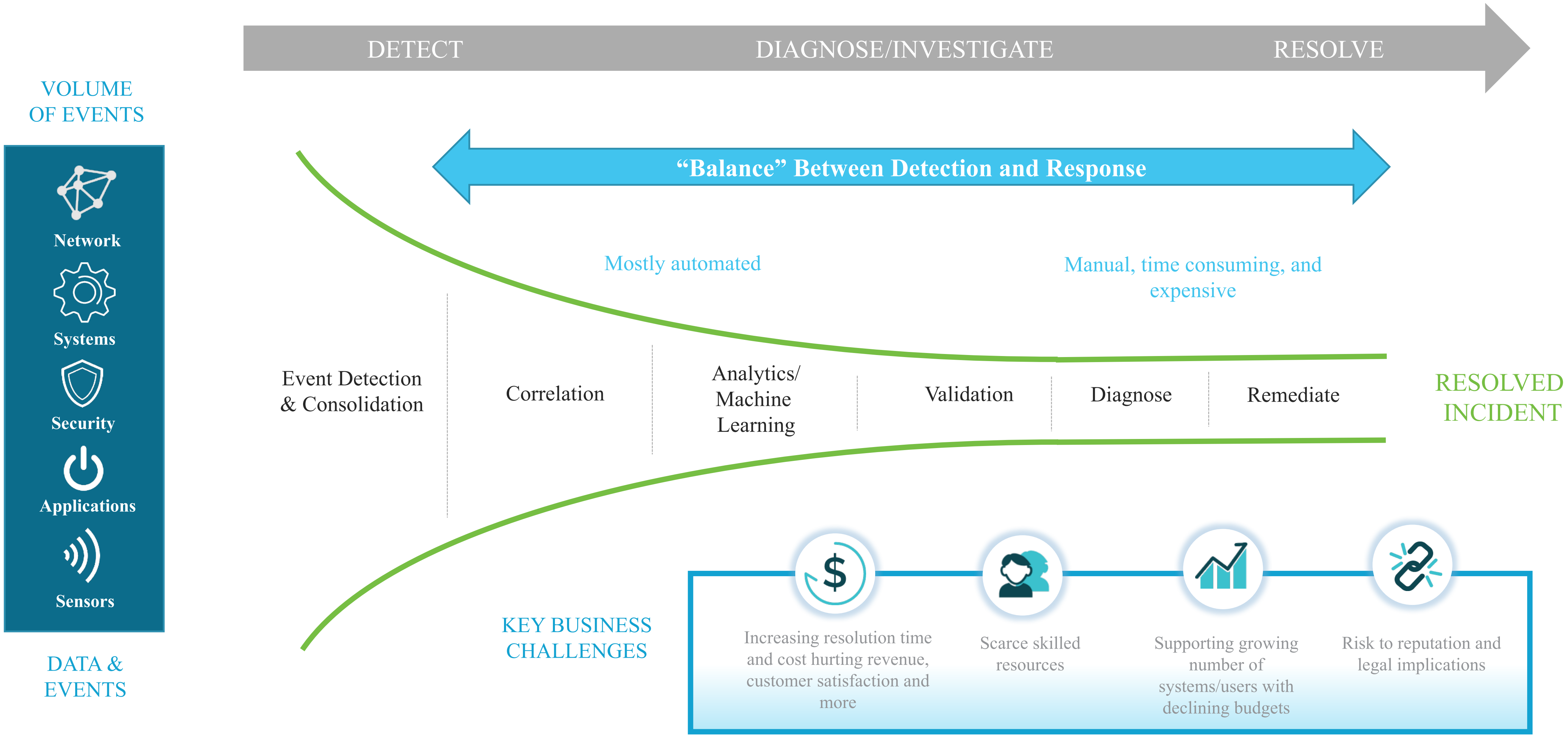
Anthem: 87.6 million individual records compromised by data theft

This image cannot currently be displayed.

Equifax: PII was stolen for 143MM people, which took 2 months to detect

Many more high impact outages and breaches across verticals…

End-to-End Incident Management



DETECT | DIAGNOSE/INVESTIGATE | RESOLVE

VOLUME OF EVENTS

Network

Systems

Security

Applications

Sensors

DATA & EVENTS

“Balance” Between Detection and Response

Mostly automated

Manual, time consuming, and expensive

Event Detection & Consolidation

Correlation

Analytics/ Machine Learning

Validation

Diagnose

Remediate

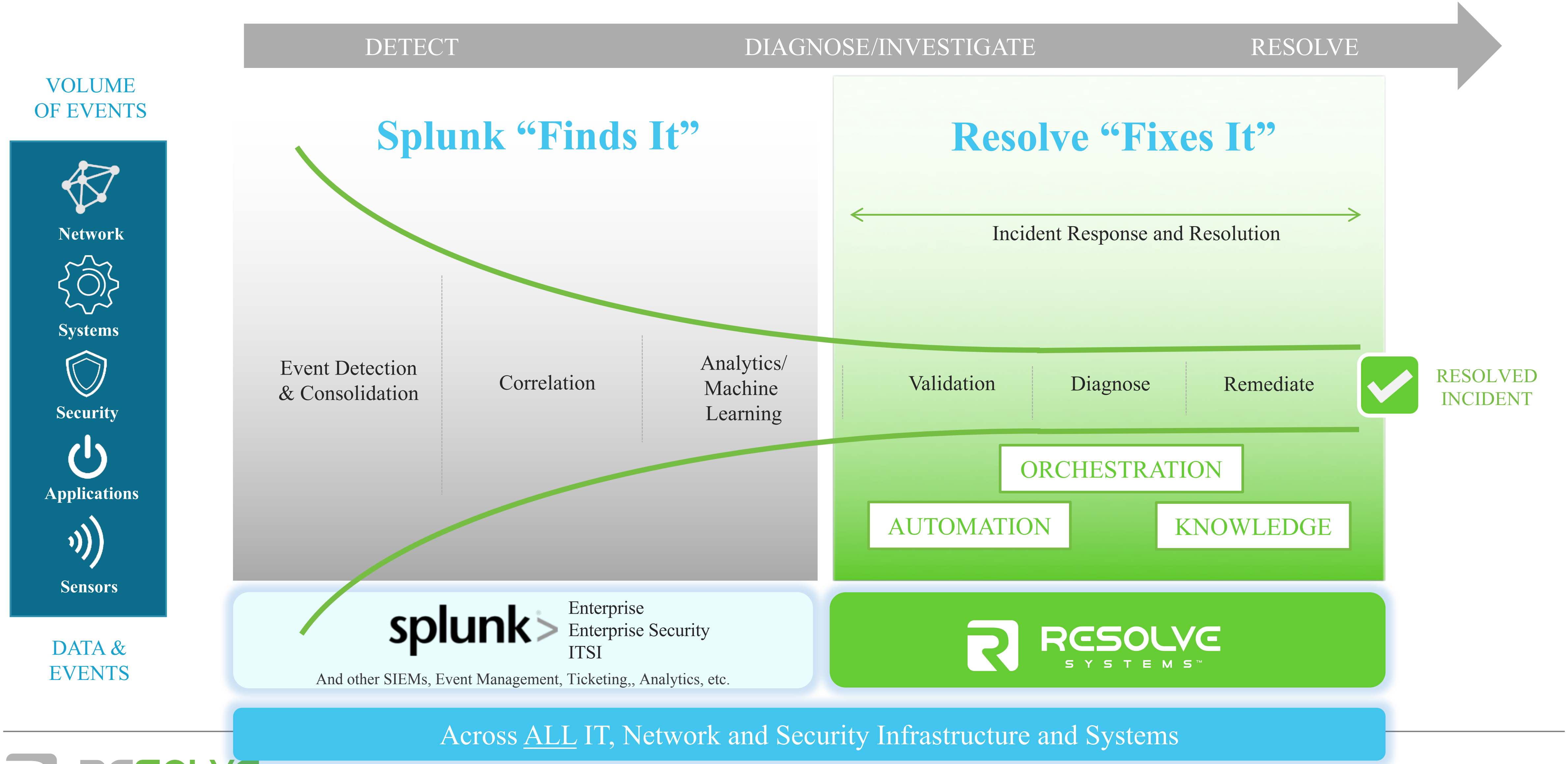
RESOLVED INCIDENT

KEY BUSINESS CHALLENGES

- Increasing resolution time and cost hurting revenue, customer satisfaction and more
- Scarce skilled resources
- Supporting growing number of systems/users with declining budgets
- Risk to reputation and legal implications

RESOLVE SYSTEMS™

Resolve Systems: Incident Response and Automation



DETECT

DIAGNOSE/INVESTIGATE

RESOLVE

VOLUME
OF EVENTS

Network

Systems

Security

Applications

Sensors

DATA &
EVENTS

Splunk “Finds It”

Event Detection
& Consolidation

Correlation

Analytics/
Machine
Learning

splunk>

Enterprise
Enterprise Security
ITSI

And other SIEMs, Event Management, Ticketing,, Analytics, etc.

Resolve “Fixes It”

Incident Response and Resolution

Validation

Diagnose

Remediate

✓ RESOLVED
INCIDENT

ORCHESTRATION

AUTOMATION

KNOWLEDGE

RESOLVE SYSTEMS™

Across ALL IT, Network and Security Infrastructure and Systems

RESOLVE SYSTEMS™

Resolve Systems reduces the amount of time that it takes organizations to respond to, diagnose and remediate incidents *across IT, Network & Security*

- Unified process orchestration and automation platform
- Fully-automated and unique human-guided automation
- Prebuilt integrations, content and playbooks
- "No-code," "drag 'n drop" automation development tools
- Not rip-and-replace; extract significant value from existing investments
- Proven success delivering, enabling and supporting the largest and most complex enterprises

17%
Improvement in OPEX

90%
Improvement in MTTR on P1 issues

5%
YoY Reduction on Global IT Support Spend

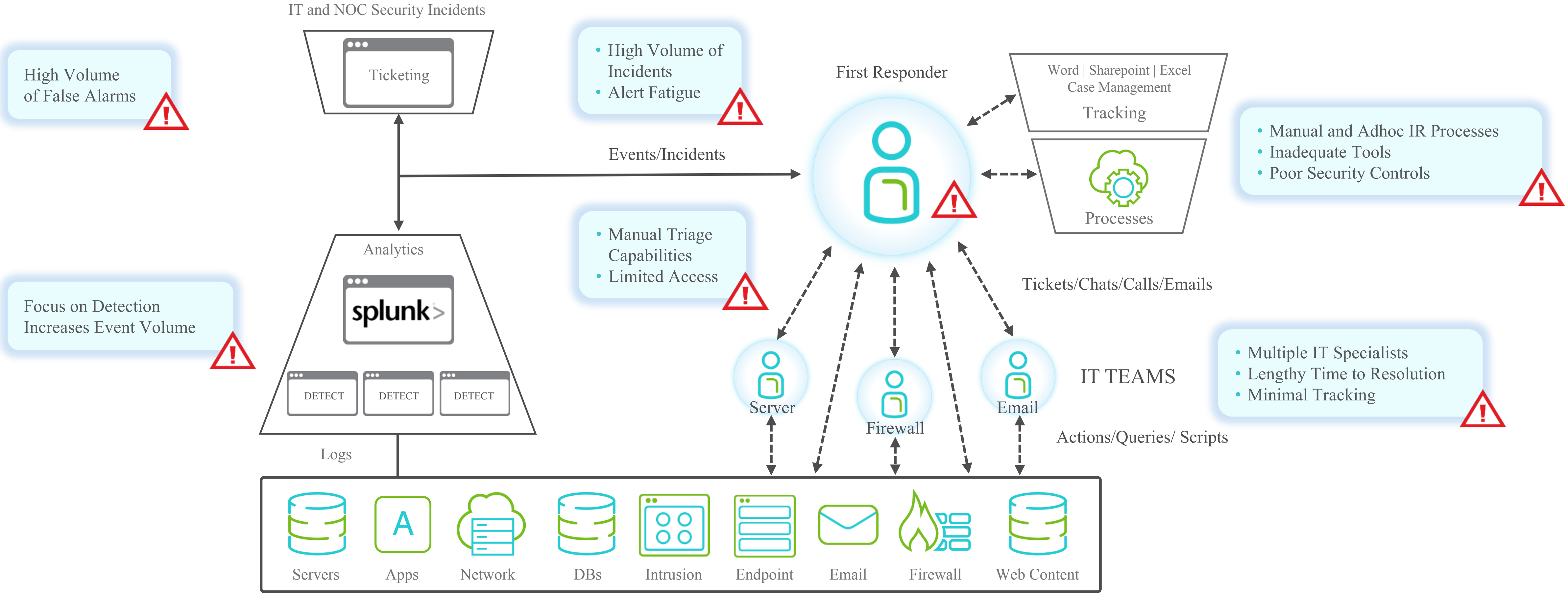
70%
Reduction of Incidents Related to Mission Critical Enterprise Application

30%
Reduction in headcount

CenturyLink™ JPMorganChase T··Mobile RBC Royal Bank Charter Spectrum accenture workday. amadeus FUJITSU

RESOLVE SYSTEMS™

What problem does Incident Response solve?



IT and NOC Security Incidents

Ticketing

High Volume of False Alarms

- High Volume of Incidents
- Alert Fatigue

First Responder

Word | Sharepoint | Excel
Case Management

Tracking

Events/Incidents

Processes

- Manual and Adhoc IR Processes
- Inadequate Tools
- Poor Security Controls

Analytics

splunk>

DETECT

DETECT

DETECT

- Manual Triage Capabilities
- Limited Access

Focus on Detection Increases Event Volume

Tickets/Chats/Calls/Emails

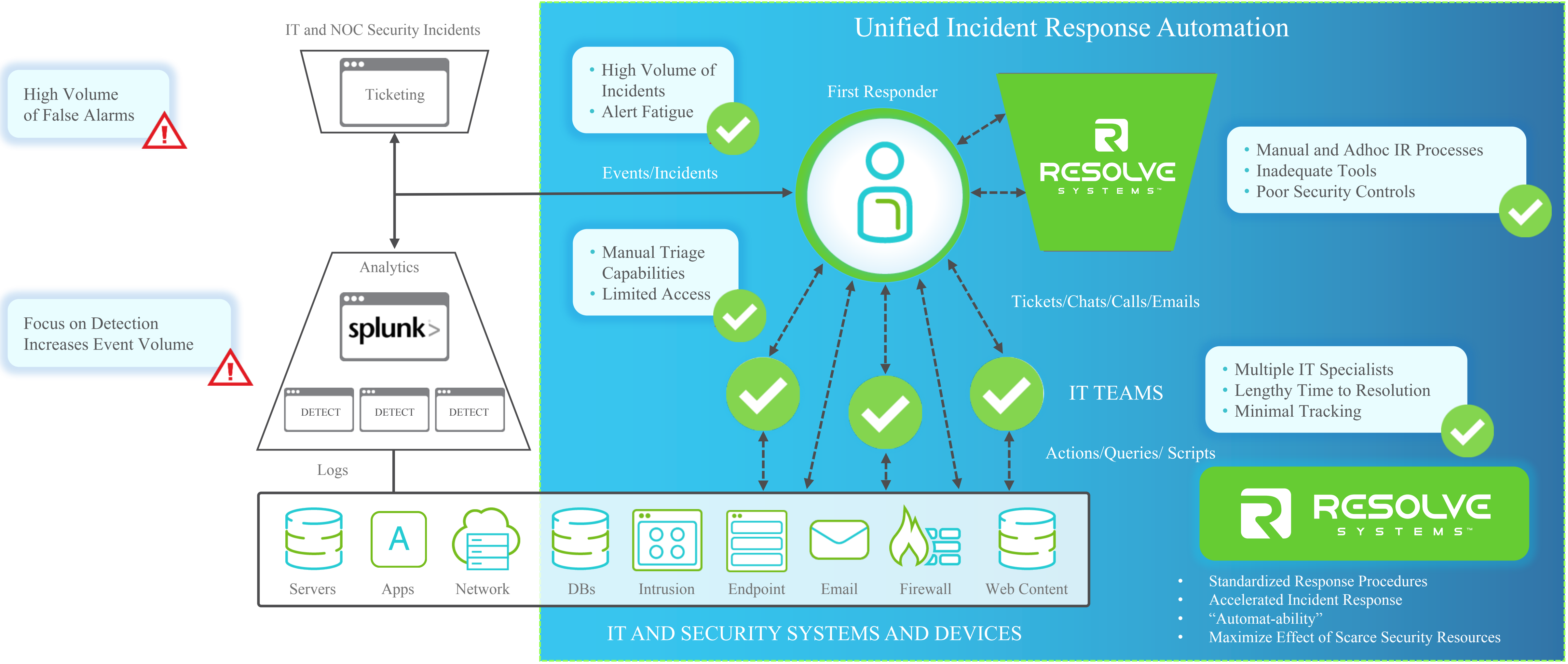
IT TEAMS

- Multiple IT Specialists
- Lengthy Time to Resolution
- Minimal Tracking

Actions/Queries/ Scripts

Logs

What problem does Incident Response solve?



High Volume of False Alarms

Focus on Detection Increases Event Volume

IT and NOC Security Incidents

Ticketing

Analytics

splunk>

DETECT

DETECT

DETECT

Logs

Servers

Apps

Network

DBs

Intrusion

Endpoint

Email

Firewall

Web Content

IT AND SECURITY SYSTEMS AND DEVICES

Unified Incident Response Automation

- High Volume of Incidents
- Alert Fatigue

Events/Incidents

- Manual Triage Capabilities
- Limited Access

First Responder

RESOLVE SYSTEMS

- Manual and Adhoc IR Processes
- Inadequate Tools
- Poor Security Controls

Tickets/Chats/Calls/Emails

IT TEAMS

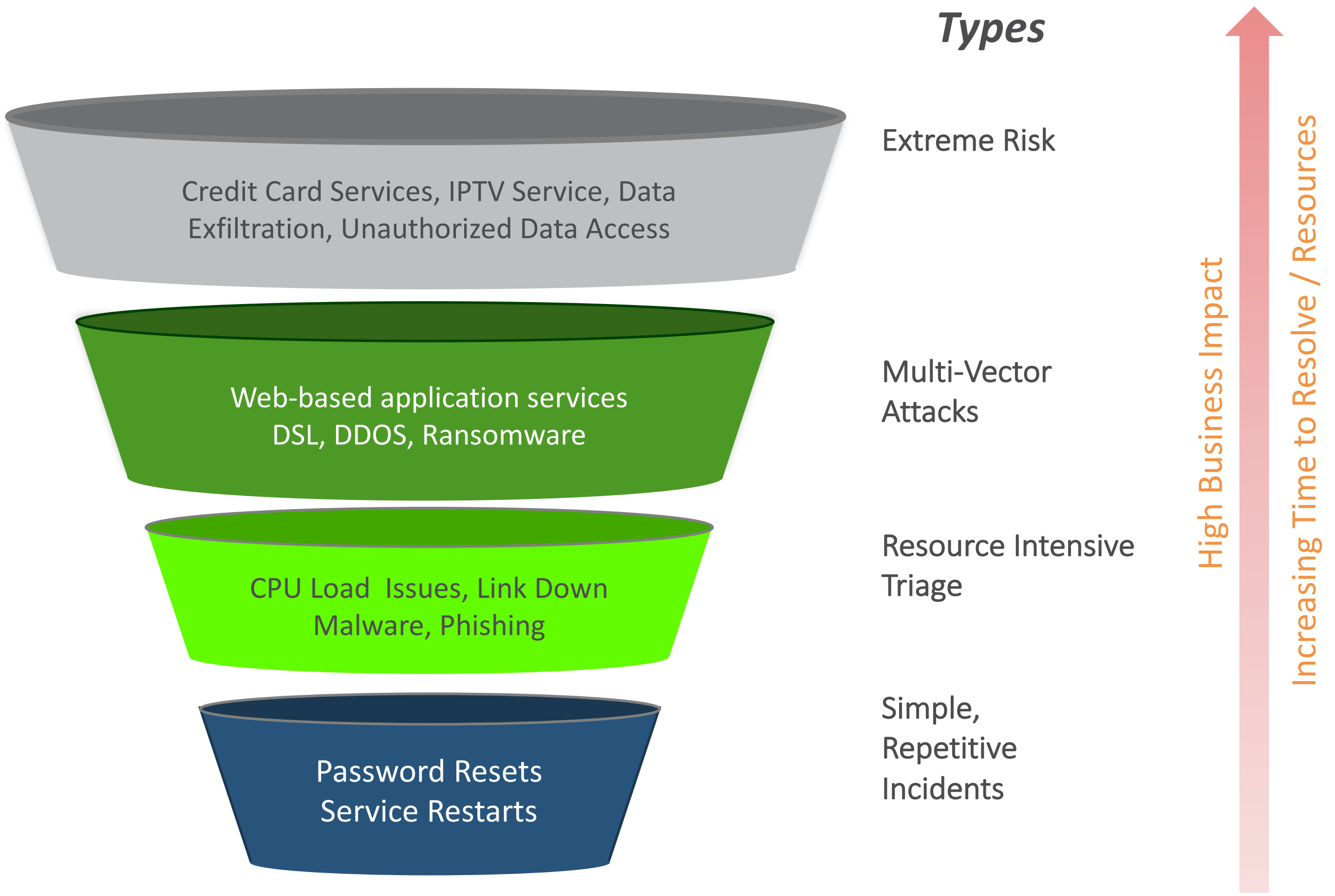
- Multiple IT Specialists
- Lengthy Time to Resolution
- Minimal Tracking

Actions/Queries/ Scripts

RESOLVE SYSTEMS

- Standardized Response Procedures
- Accelerated Incident Response
- “Automat-ability”
- Maximize Effect of Scarce Security Resources

Can all incident types be treated the same?

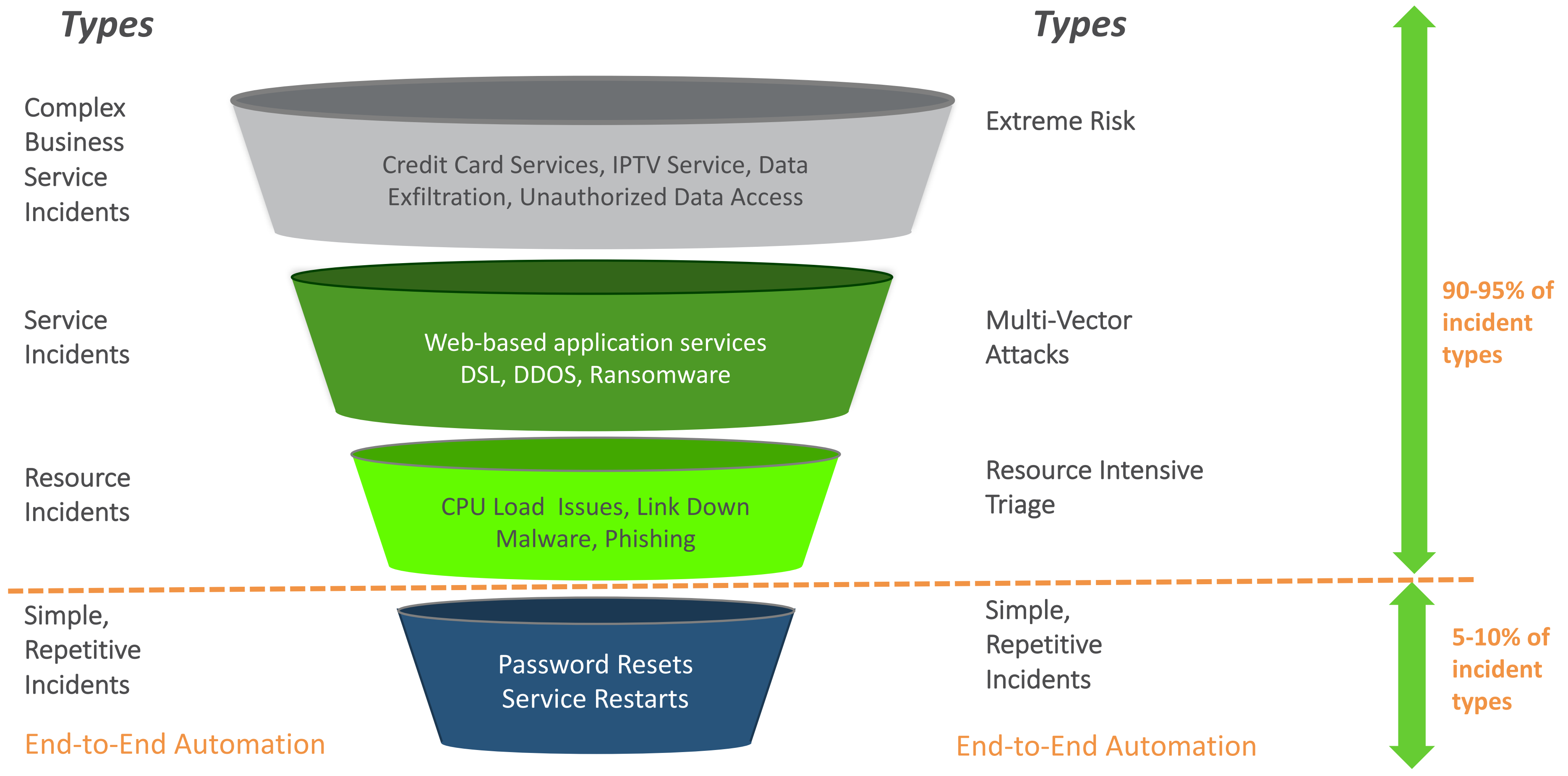


IT Incident Types		***Security Incident Types***
Complex Business Service Incidents	Credit Card Services, IPTV Service, Data Exfiltration, Unauthorized Data Access	Extreme Risk
Service Incidents	Web-based application services DSL, DDOS, Ransomware	Multi-Vector Attacks
Resource Incidents	CPU Load Issues, Link Down Malware, Phishing	Resource Intensive Triage
Simple, Repetitive Incidents	Password Resets Service Restarts	Simple, Repetitive Incidents

Can all incident types be treated the same?

IT Incident Types

Security Incident Types



Complex Business Service Incidents

Credit Card Services, IPTV Service, Data Exfiltration, Unauthorized Data Access

Extreme Risk

Service Incidents

Web-based application services DSL, DDOS, Ransomware

Multi-Vector Attacks

Resource Incidents

CPU Load Issues, Link Down Malware, Phishing

Resource Intensive Triage

90-95% of incident types

Simple, Repetitive Incidents

Password Resets Service Restarts

Simple, Repetitive Incidents

5-10% of incident types

End-to-End Automation

End-to-End Automation

- 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

Resolve: Key Capabilities

Unified Incident Response Experience

Single pane of glass for all Incident Response tasks, investigations, processes, automation and notes

Process Orchestration

Consistent and standards-based process guidance, case management, decision trees and instructions based on NIST SP 800-61 rev2

Automat-ability

Powerful human-guided automation and end-to-end automation to automate incrementally and pragmatically

Playbooks and Automations

Prebuilt processes and automations with most common security and IT systems and “no code” automation design tools

Enterprise-Class Capabilities

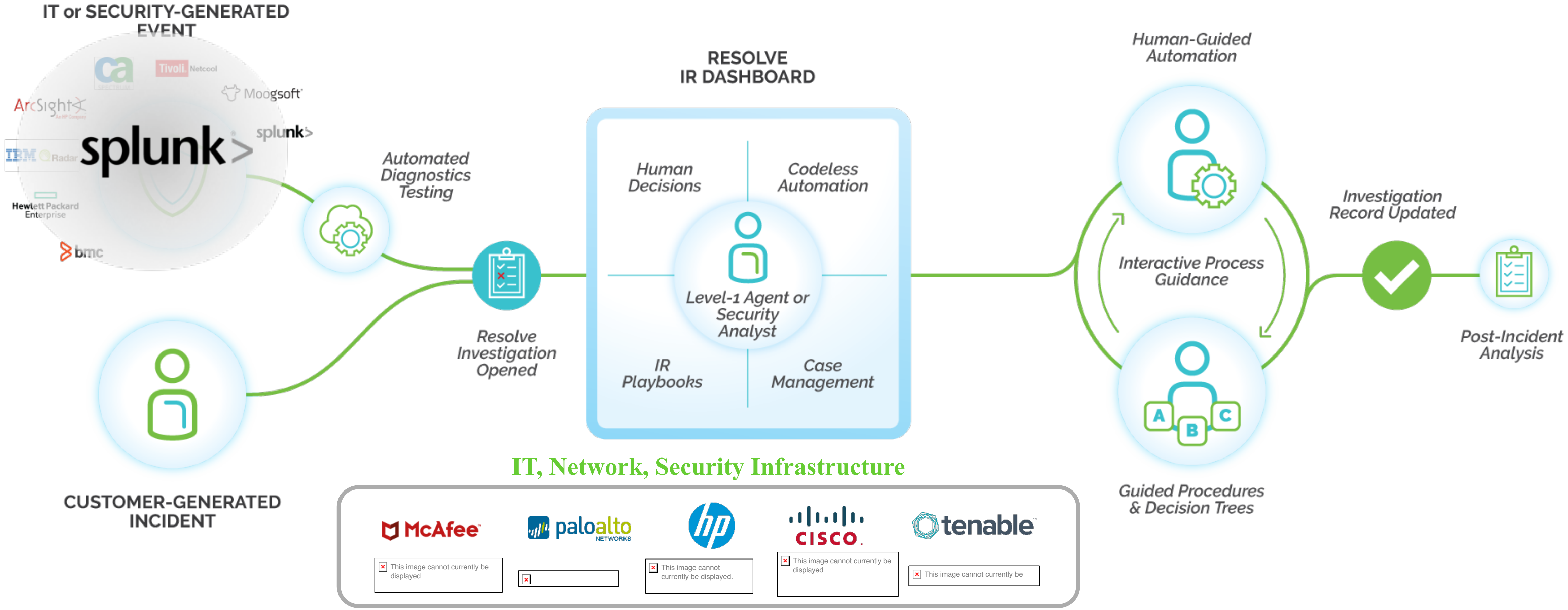
Scalable, redundant and available with proven success in the most complex and largest organizations

Enterprise-Wide Incident Response & Automation Platform

1 **VALIDATE**
Automated Diagnostics

2 **INVESTIGATE**
Incident Response Dashboard

3 **REMEDIATE**
Contain and Eradicate



IT or SECURITY-GENERATED EVENT

Automated Diagnostics Testing

Resolve Investigation Opened

CUSTOMER-GENERATED INCIDENT

RESOLVE IR DASHBOARD

Human Decisions

Codeless Automation

Level-1 Agent or Security Analyst

IR Playbooks

Case Management

Human-Guided Automation

Interactive Process Guidance

Guided Procedures & Decision Trees

Investigation Record Updated

Post-Incident Analysis

IT, Network, Security Infrastructure

This image cannot currently be displayed.

This image cannot currently be displayed.

This image cannot currently be displayed.

This image cannot currently be

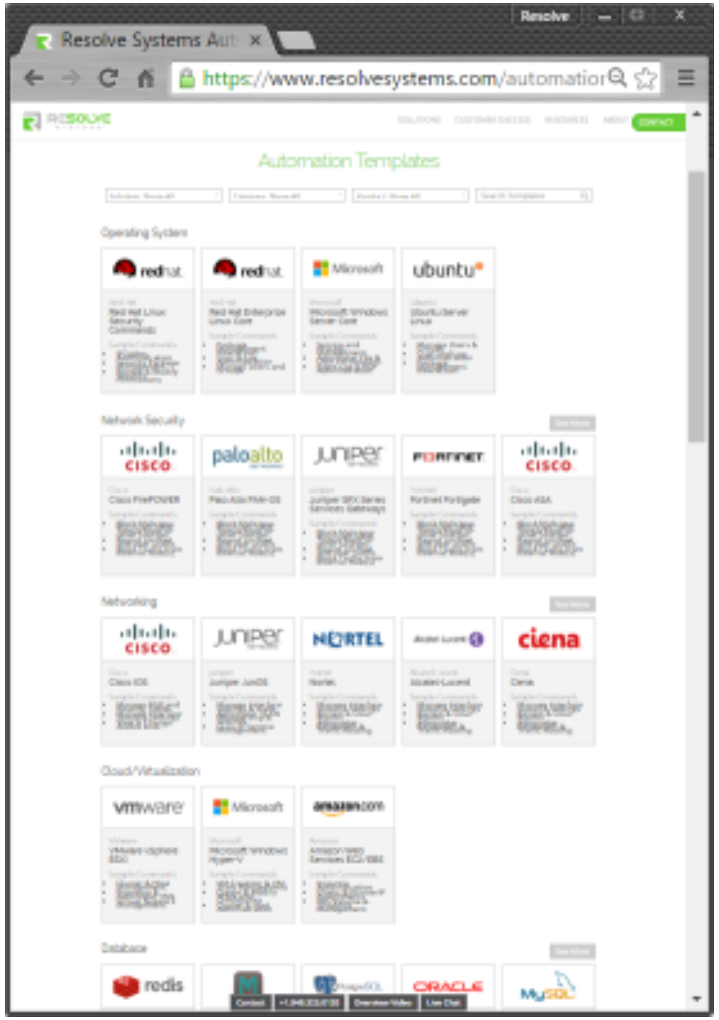
Get Started With Resolve Fast

CONNECTORS

This image cannot currently be displayed.

This image cannot currently be displayed.

AUTOMATION TEMPLATES



Automation Templates

Operating System

- Red Hat Linux Security Commands
- Red Hat Enterprise Linux Core
- Microsoft Windows Server Core
- Ubuntu Server Linux

Network Security

- Cisco FirePOWER
- Palo Alto PAN-OS
- Juniper SRX Series Services Gateways
- Fortinet FortiGate
- Cisco ASA

Networking

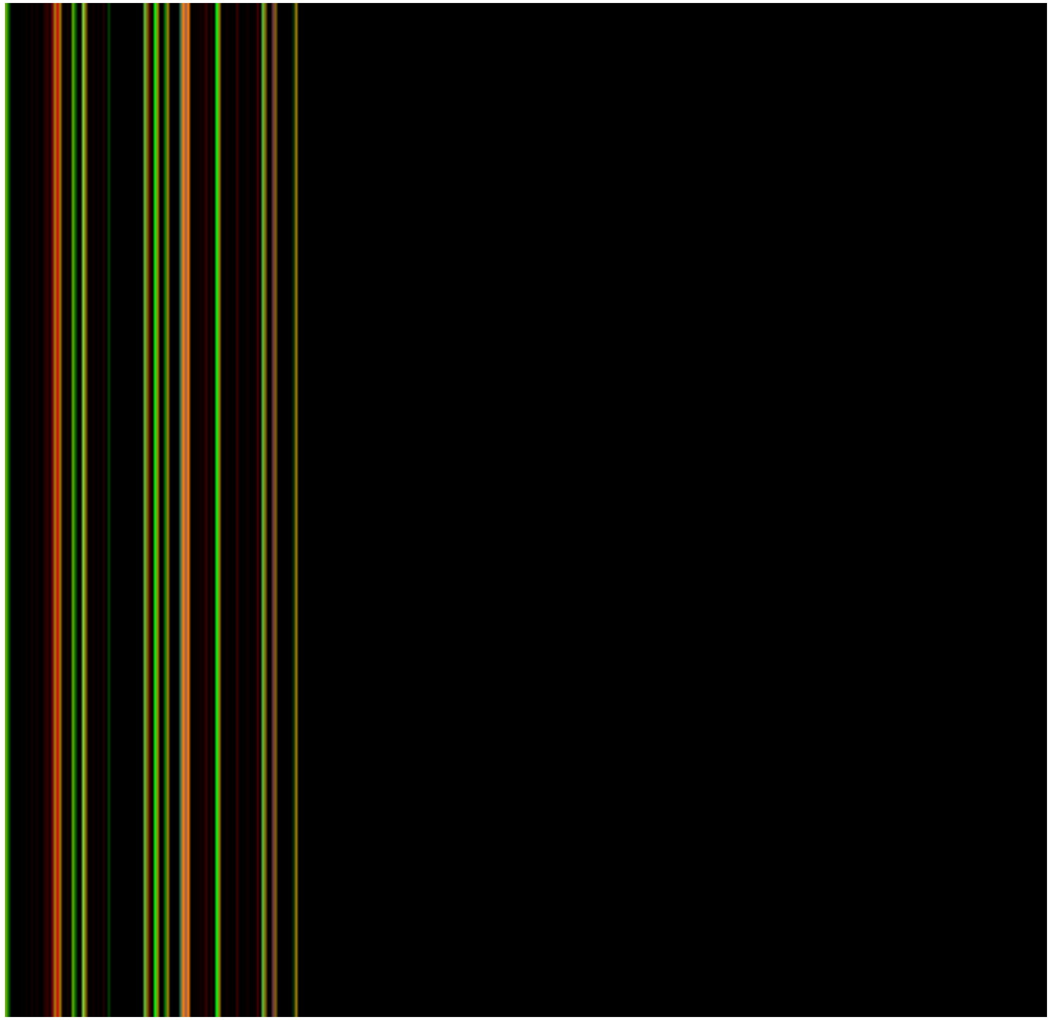
- Cisco IOS
- Juniper JunOS
- Nortel
- Alcatel-Lucent
- Ciena

Cloud/Virtualization

- VMware vSphere ESXi
- Microsoft Windows Hyper-V
- Amazon Web Services EC2/EBS

Database

PLAYBOOKS



Resolve's Easy to Use Tools for Automation & Orchestration

Build within Hours, Deploy within Days

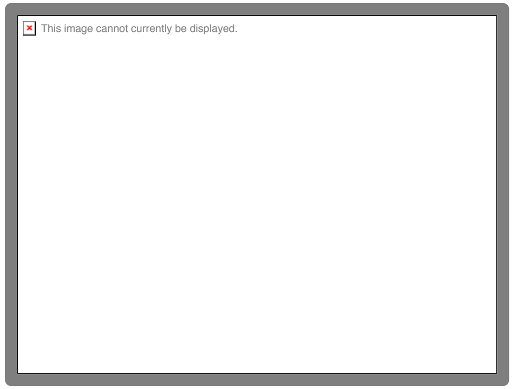
Action Task Builder

- Easily and quickly design and build new automated tasks using a configuration wizard including action and assessment creation
- Game changing intelligent parsing
- Use the same wizards to modify and reuse existing tasks

Decision Tree Builder

- Quickly drag and drop questions, answers and content and let Resolve quickly generate your guided procedures

Page Builder



- Build powerful resolution dashboards using a fully-featured page builder interface

Automation Designer

- Quickly build and test new processes using drag and drop and input/output configuration
- Combine the higher level process and lower level task views in one pane
- Drag and drop new integrated sessions into your process

Find it with Splunk, Fix it with Resolve — Enterprise-Wide Incident Management

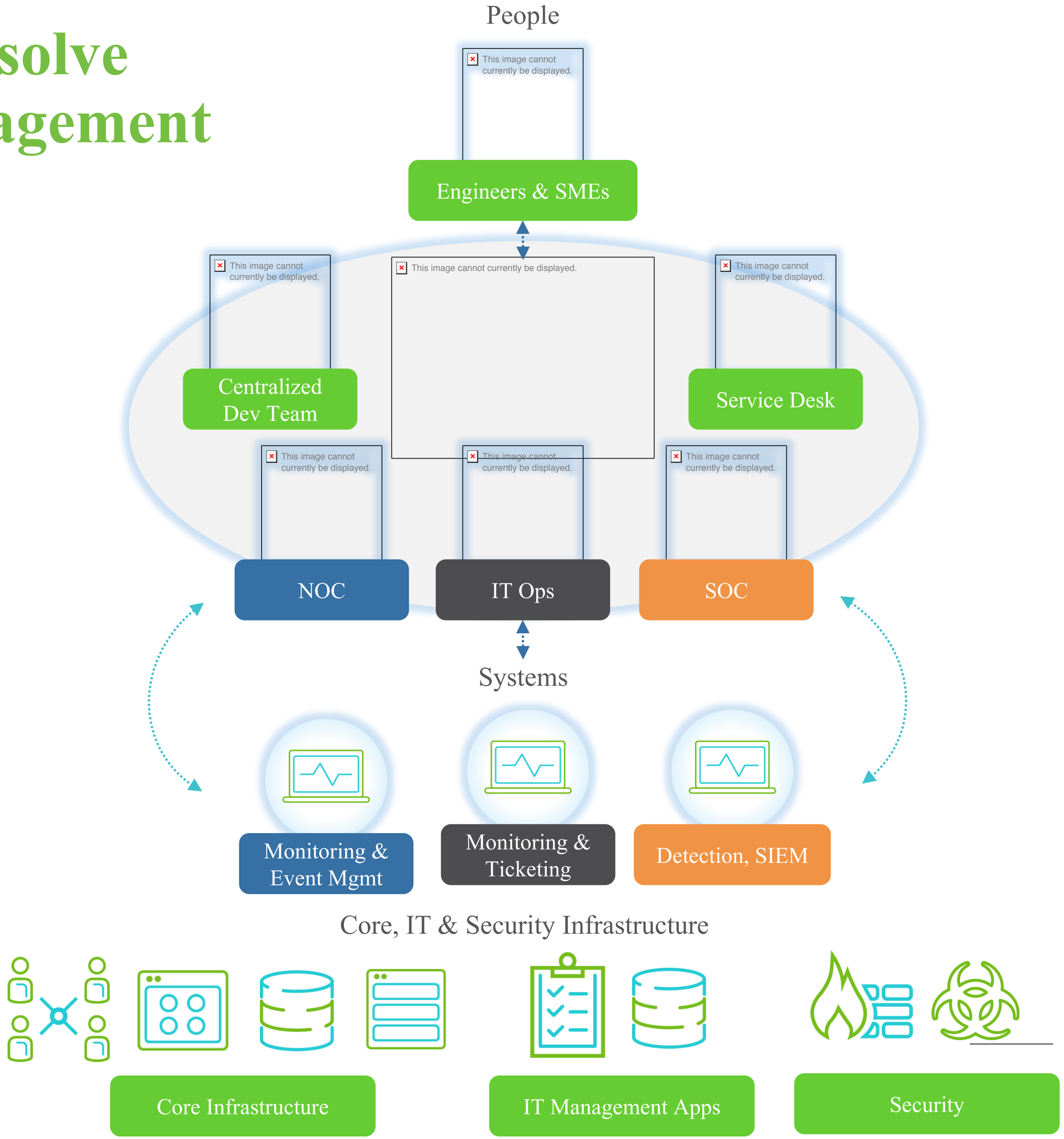
When IT, Network and Security incidents happen:

1. Leverage the same engineers and SMEs to resolve
2. Gather information from the same systems
3. Take actions on the same systems

Centralize Incident Response platform that can be leveraged across the entire enterprise

1. Familiar user interface for all teams
2. Tool that takes actions and automations across enterprise devices/systems
3. Share processes/knowledge from SME resources across the organization
4. Build once and re-usable automations

Shared Incident Response Platform - Processes tailored for each team



RESOLVE SYSTEMS™

The Resolve Advantage

☑ Cohesive Enterprise Incident Response Strategy for IT, Networks & Security

- 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

- 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

- Deployed in largest enterprises and service providers across all verticals
- Handles millions of daily events

5 Splunk Apps Available in Splunkbase today - **Fully Certified!**

RESOLVE

SYSTEMS™