Splunk for Zero Trust

splunk> turn data into doing™

Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

A discussion of factors that may affect future results is contained in our most recent annual report on Form 10-K and subsequent quarterly reports on Form 10-Q, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov, including descriptions of the risk factors that may impact us and the forward-looking statements made in this presentation. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Agenda

What is Zero Trust

Why is Zero Trust Relevant

How Does Splunk Help

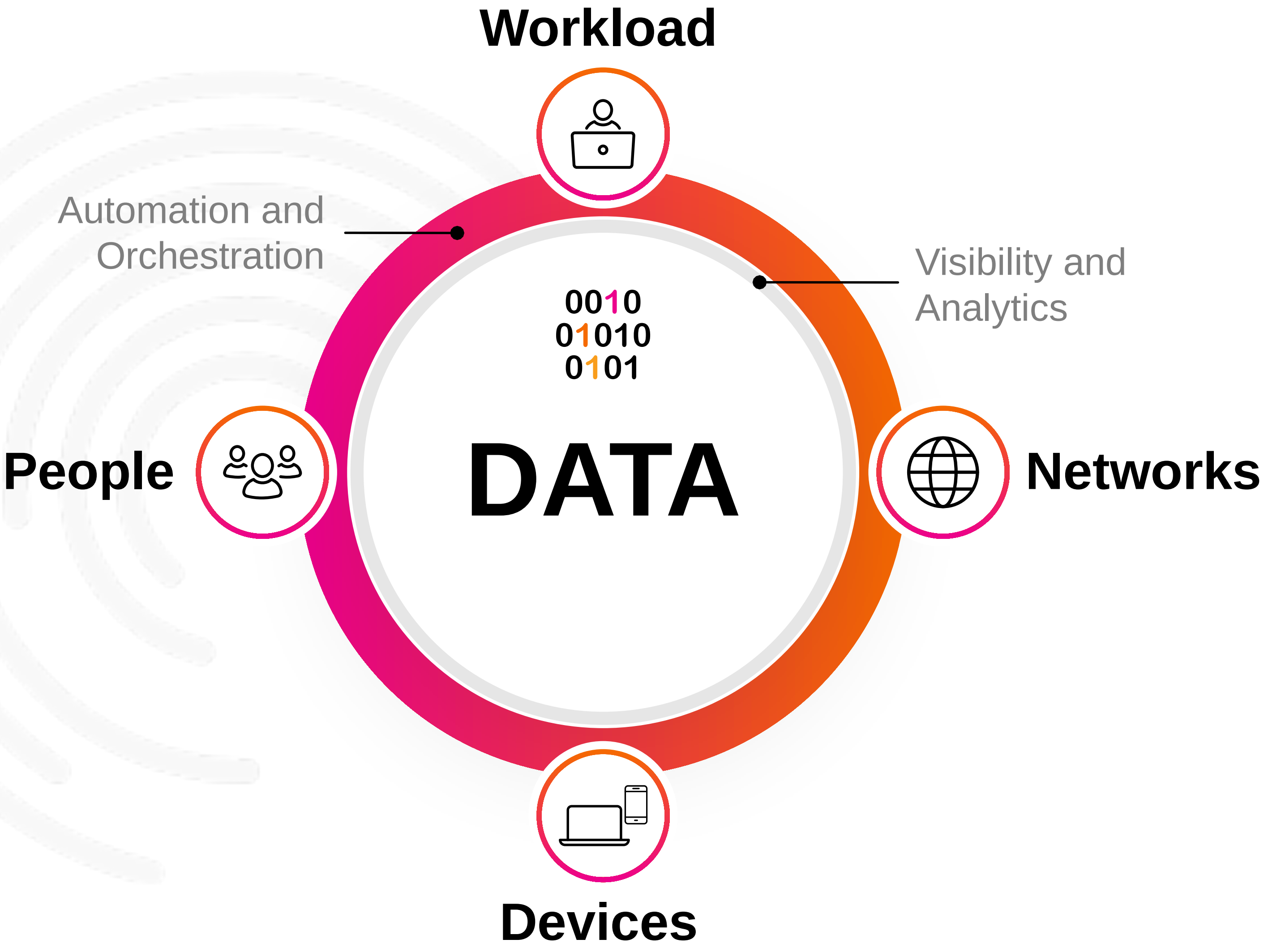
How to Get Started

Introduction

What is zero trust & why is it important

splunk> turn data into doing™

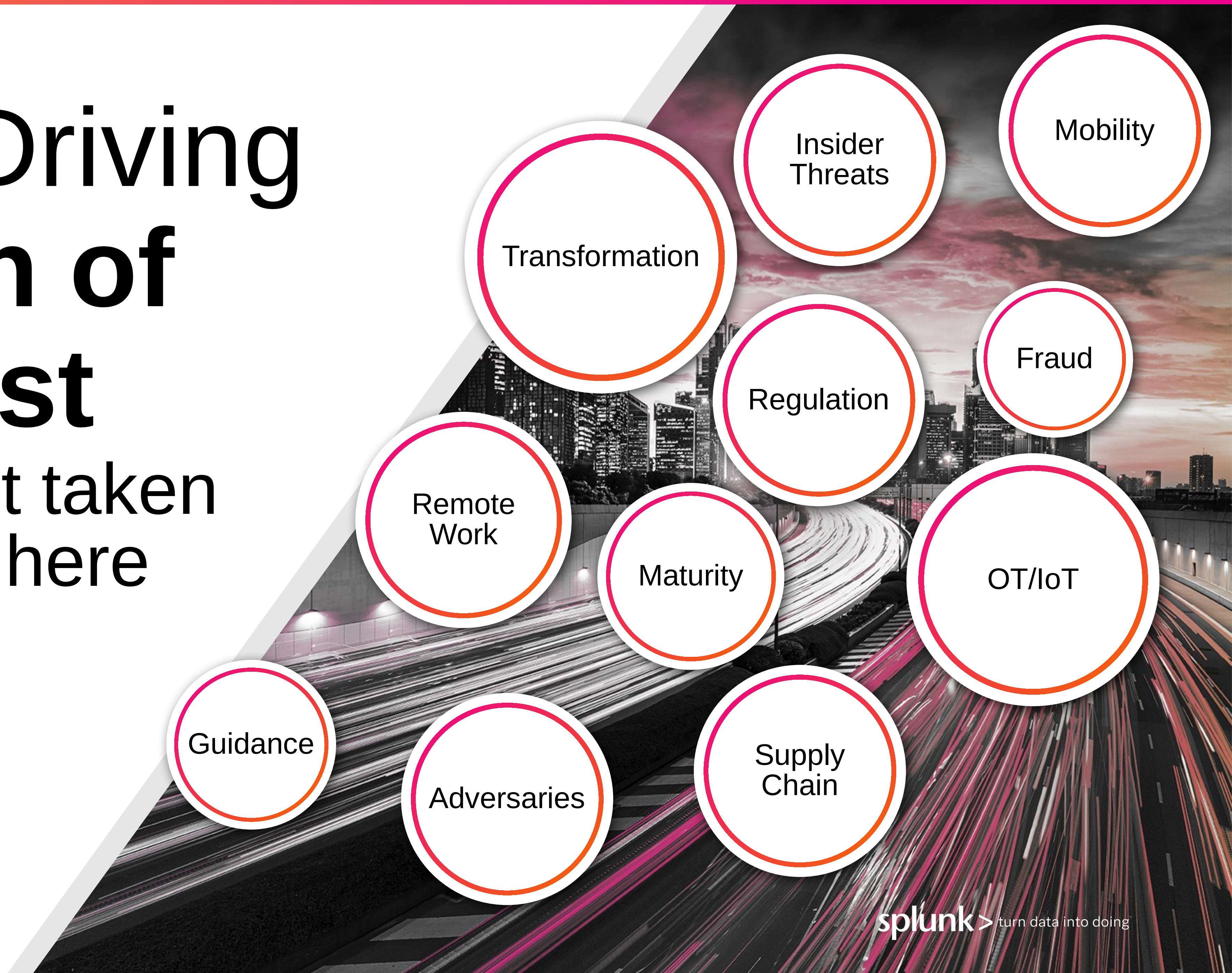
Let’s Agree... What Is **Zero Trust?**



Source: The Zero Trust eXtended (ZTX) Ecosystem, Forrester

What Is Driving **Adoption of Zero Trust**

And why has it taken so long to get here



Mobility

Insider Threats

Transformation

Fraud

Regulation

Remote Work

Maturity

OT/IoT

Guidance

Supply Chain

Adversaries

splunk> turn data into doing

Six Pillars of a Zero Trust Architecture

Data is the fundamental enabler of Zero Trust

1 Users

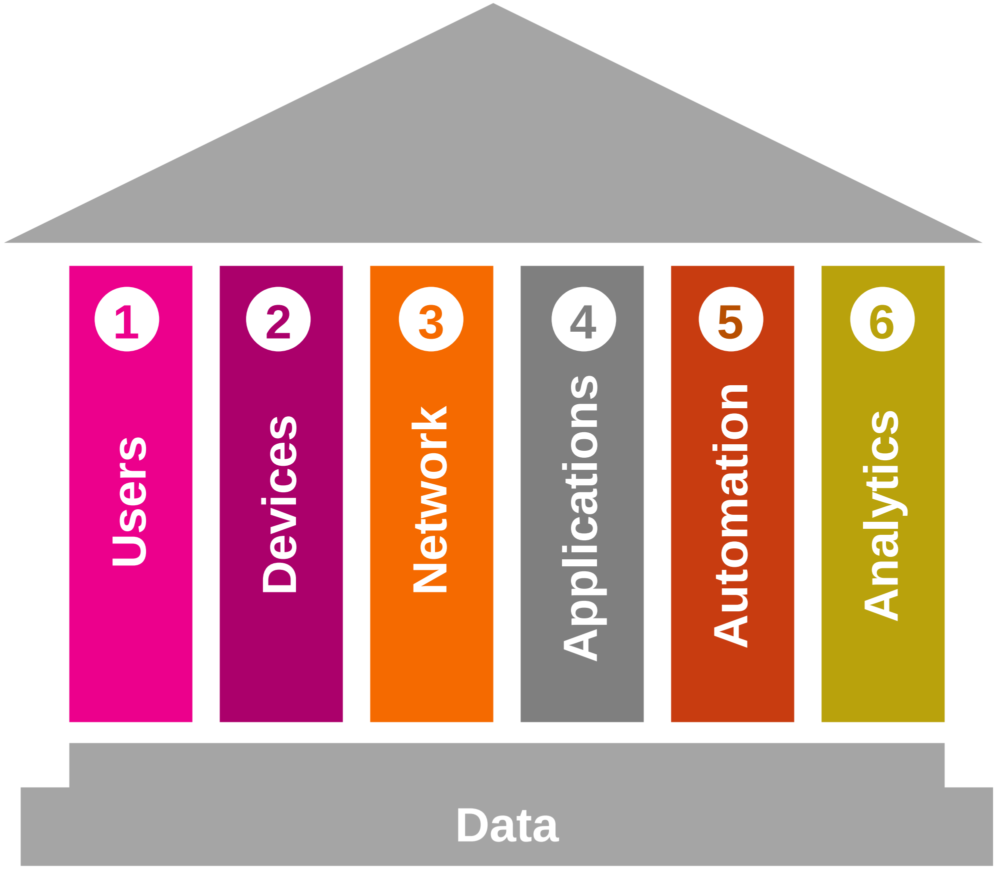
Ongoing authentication of trusted users. Continuous monitoring and validating user trustworthiness to govern their access and privileges.

2 Devices

Real-time cybersecurity posture and trustworthiness of devices

3 Network

The ability to segment, isolate, and control the network, including Software Defined Networks, Software Defined Wide Area Networks and internet-based technologies continues to be a pivotal point of security



4 Applications

Securing and properly managing the application layer as well as compute containers and virtual machines plus the data provided by these applications

5 Automation

Security Automation and Orchestration - automate tasks across products through workflows while allowing for end-user oversight and interaction

6 Analytics

Visibility and Analytics - tools like security information management, advanced security analytics platforms, security user behavior analytics, and other analytics systems to enable security experts to observe in real time what is happening and orient defenses more intelligently

splunk> turn data into doing

Source: Zero Trust Cybersecurity Current Trends, April 18, 2019, ACT-IAC

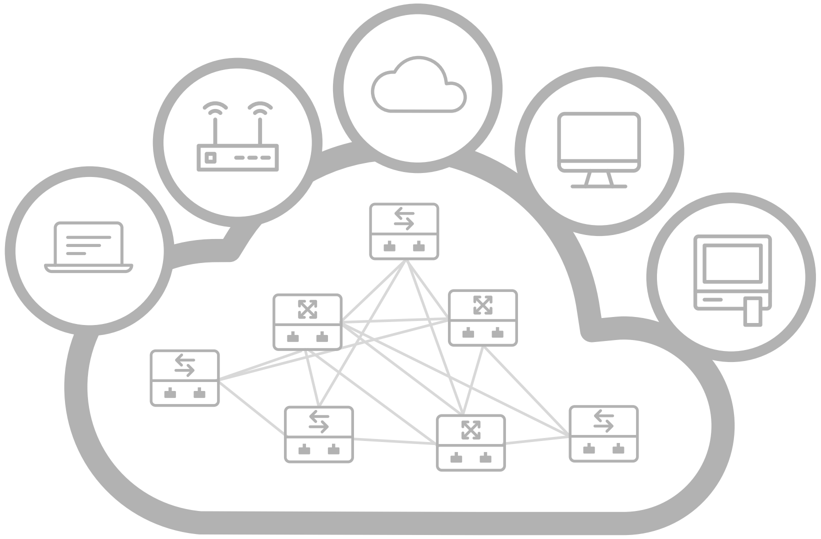
How Does Splunk Help?

splunk> turn data into doing™

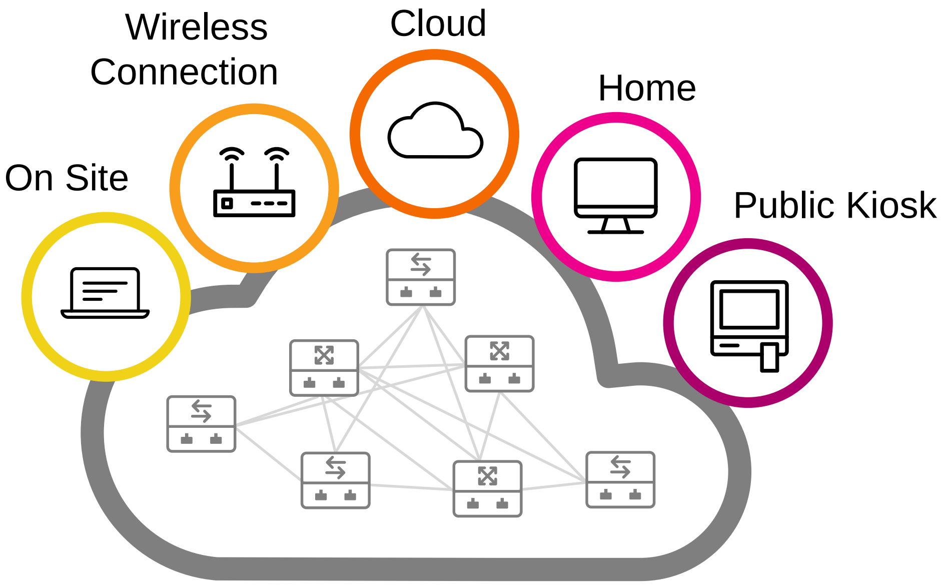
Data Access in Zero Trust

The level of risk determines the access

Traditional Network



Zero Trust Network



Data Sensitivity

Lower Sensitivity/Less Restrictions 🟨🟧🟧🟥🟪 Higher Sensitivity/More Restrictions

Data Categorization

Data is not all equally important. Different data needs to be categorized based on sensitivity and mission criticality.

Traditional Classification

Threat Vectors

Network Infrastructure

Servers

Data Storage

Same Types of Protection

Employee Vacation Schedules

company Budget

Sensitive Messages

Zero Trust Classification

Threat Vectors

Network Infrastructure

Servers

Data Storage

Cloud

0010
01010
0101
Big Data (Data Correlation)

Containers

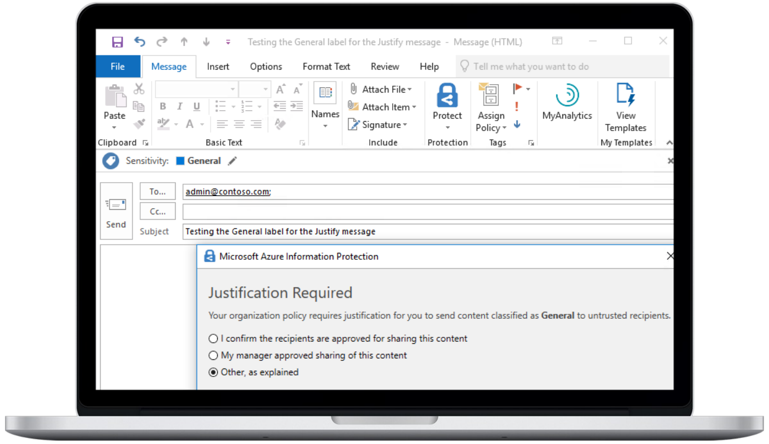
DevOps/ DevSecOps

Protections are built to the level of risk

Employee Vacation Schedules

compan
y
Budget

Sensitive Messages



Sensitivity: General

To... admin@contoso.com;

Subject: Testing the General label for the Justify message

Microsoft Azure Information Protection

Justification Required

Your organization policy requires justification for you to send content classified as **General** to untrusted recipients.

○ I confirm the recipients are approved for sharing this content

○ My manager approved sharing of this content

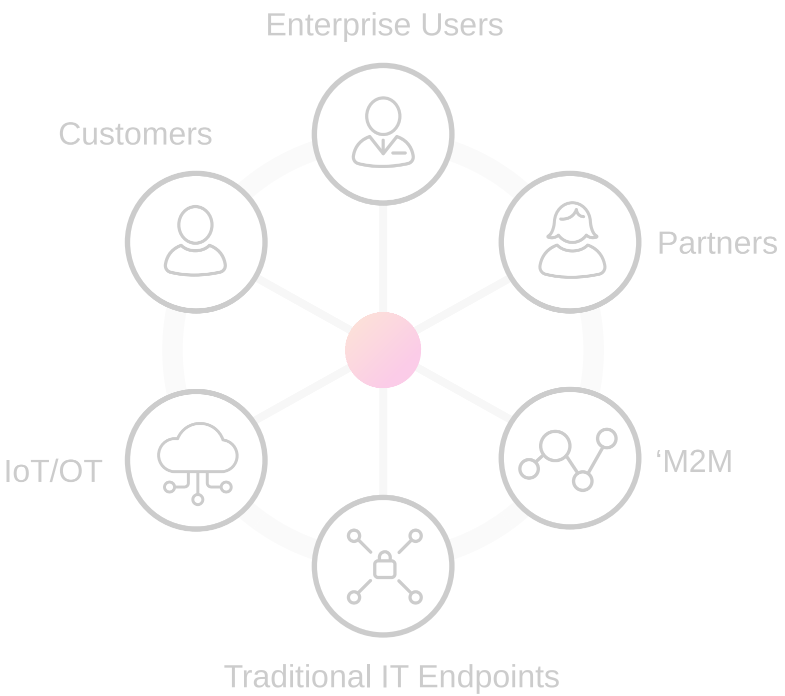
● Other, as explained

Data Sensitivity

Lower Sensitivity/Less Restrictions 🟨🟧🟧🟥🟪 Higher Sensitivity/More Restrictions

Instrumentation Case In Point: “Zero Trust”

Who seeks access?



Under *what* conditions?

Examples

Decision-Making: AI/ML-Enabled

- User Credentials
- Device Type
- Device Health
- Device Location
- Patch Levels
- Time
- User Risk Score
- System Logs

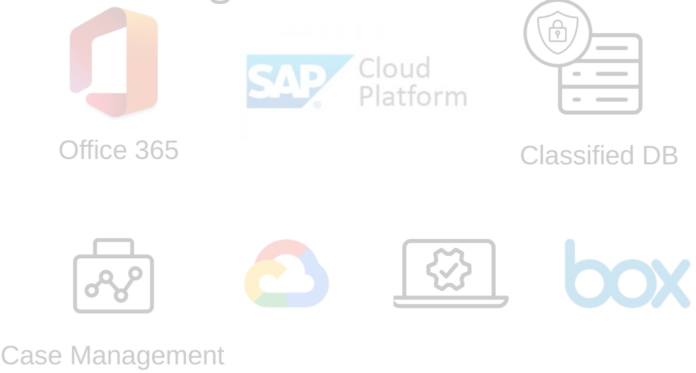
Policy Engine

'Continuous’ validation

To *which* targets?

Fine-Grained Authorization and Access Control

Applications

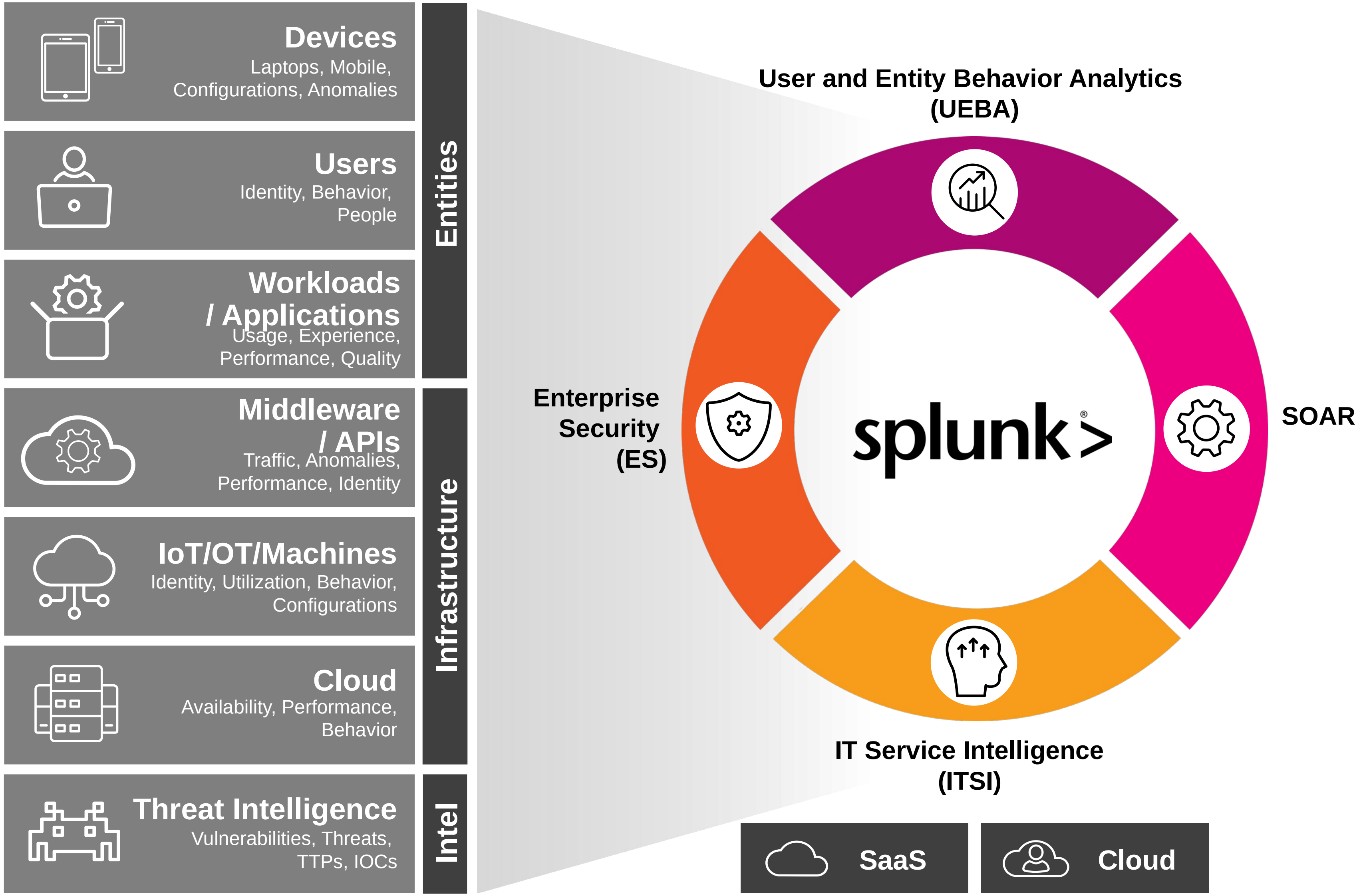


WITH SECURITY FOR DATA THROUGHOUT

The above graphic example was approved for use by 451 Research, a part of S&P Global Market Intelligence.

Your Data is the Foundation for Zero Trust

Splunk is the platform for continuous monitoring, visibility, analytics and automation



Entities

Devices
Laptops, Mobile, Configurations, Anomalies

Users
Identity, Behavior, People

Workloads / Applications
Usage, Experience, Performance, Quality

Infrastructure

Middleware / APIs
Traffic, Anomalies, Performance, Identity

IoT/OT/Machines
Identity, Utilization, Behavior, Configurations

Cloud
Availability, Performance, Behavior

Intel

Threat Intelligence
Vulnerabilities, Threats, TTPs, IOCs

User and Entity Behavior Analytics (UEBA)

Enterprise Security (ES)

splunk>

SOAR

IT Service Intelligence (ITSI)

SaaS

Cloud

- Continuous Monitoring
- Real-Time Visibility
- Behavior Analytics
- Continuous Risk Scoring
- Automation/Orchestration
- Compliance
- Service Insights

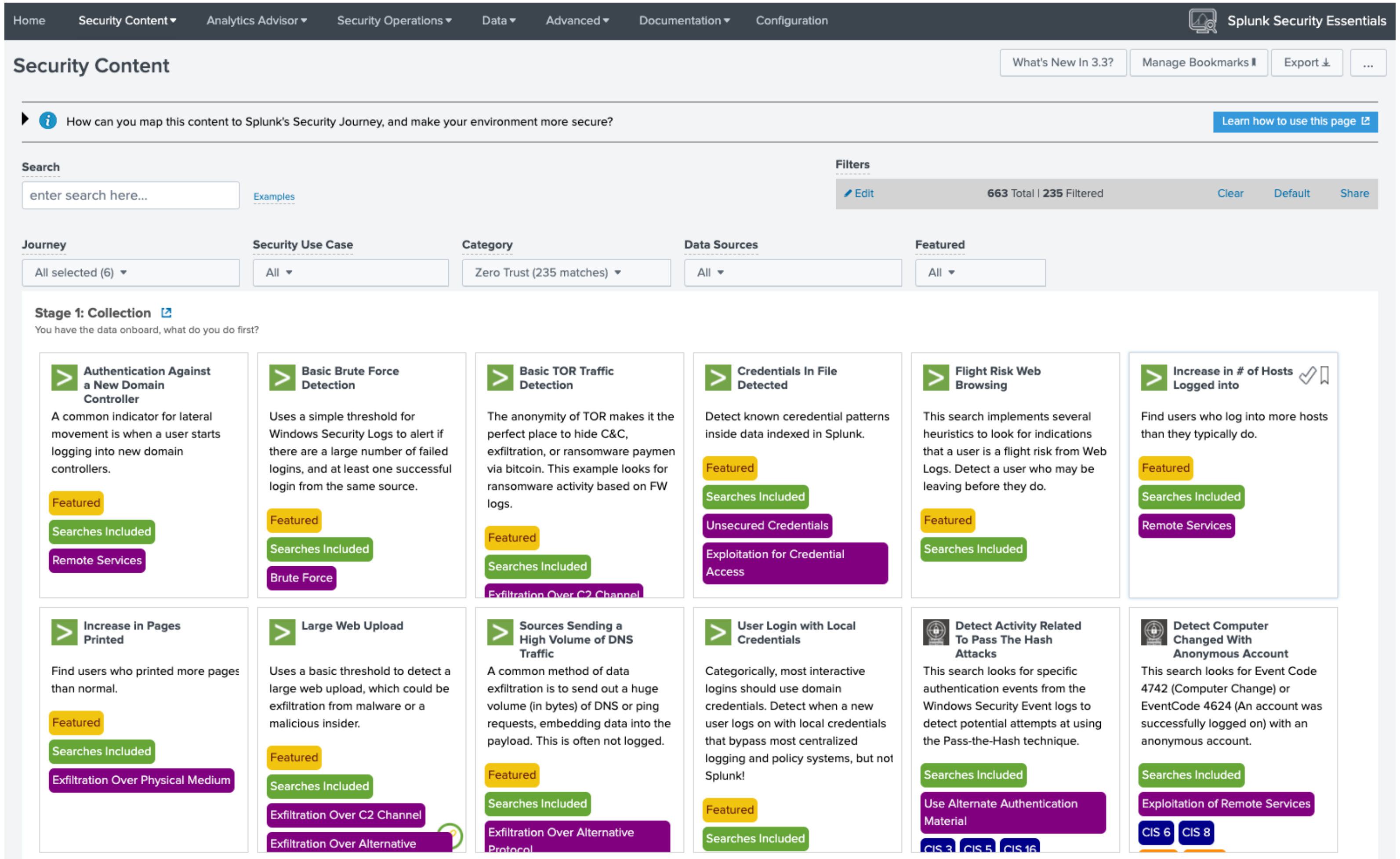
Getting Started

With Splunk & Zero Trust

splunk> turn data into doing™

Splunk Zero Trust Use Cases

Getting Started with Splunk Security Essentials for Zero Trust



Security Content

How can you map this content to Splunk's Security Journey, and make your environment more secure?

Search: enter search here...

Filters: 663 Total | 235 Filtered

Journey: All selected (6)

Security Use Case: All

Category: Zero Trust (235 matches)

Data Sources: All

Featured: All

Stage 1: Collection

You have the data onboard, what do you do first?

Authentication Against a New Domain Controller

A common indicator for lateral movement is when a user starts logging into new domain controllers.

Featured | Searches Included | Remote Services

Basic Brute Force Detection

Uses a simple threshold for Windows Security Logs to alert if there are a large number of failed logins, and at least one successful login from the same source.

Featured | Searches Included | Brute Force

Basic TOR Traffic Detection

The anonymity of TOR makes it the perfect place to hide C&C, exfiltration, or ransomware paymen via bitcoin. This example looks for ransomware activity based on FW logs.

Featured | Searches Included | Exfiltration Over C2 Channel

Credentials In File Detected

Detect known ceredential patterns inside data indexed in Splunk.

Featured | Searches Included | Unsecured Credentials | Exploitation for Credential Access

Flight Risk Web Browsing

This search implements several heuristics to look for indications that a user is a flight risk from Web Logs. Detect a user who may be leaving before they do.

Featured | Searches Included

Increase in # of Hosts Logged into

Find users who log into more hosts than they typically do.

Featured | Searches Included | Remote Services

Increase in Pages Printed

Find users who printed more pages than normal.

Featured | Searches Included | Exfiltration Over Physical Medium

Large Web Upload

Uses a basic threshold to detect a large web upload, which could be exfiltration from malware or a malicious insider.

Featured | Searches Included | Exfiltration Over C2 Channel | Exfiltration Over Alternative

Sources Sending a High Volume of DNS Traffic

A common method of data exfiltration is to send out a huge volume (in bytes) of DNS or ping requests, embedding data into the payload. This is often not logged.

Featured | Searches Included | Exfiltration Over Alternative Protocol

User Login with Local Credentials

Categorically, most interactive logins should use domain credentials. Detect when a new user logs on with local credentials that bypass most centralized logging and policy systems, but not Splunk!

Featured | Searches Included

Detect Activity Related To Pass The Hash Attacks

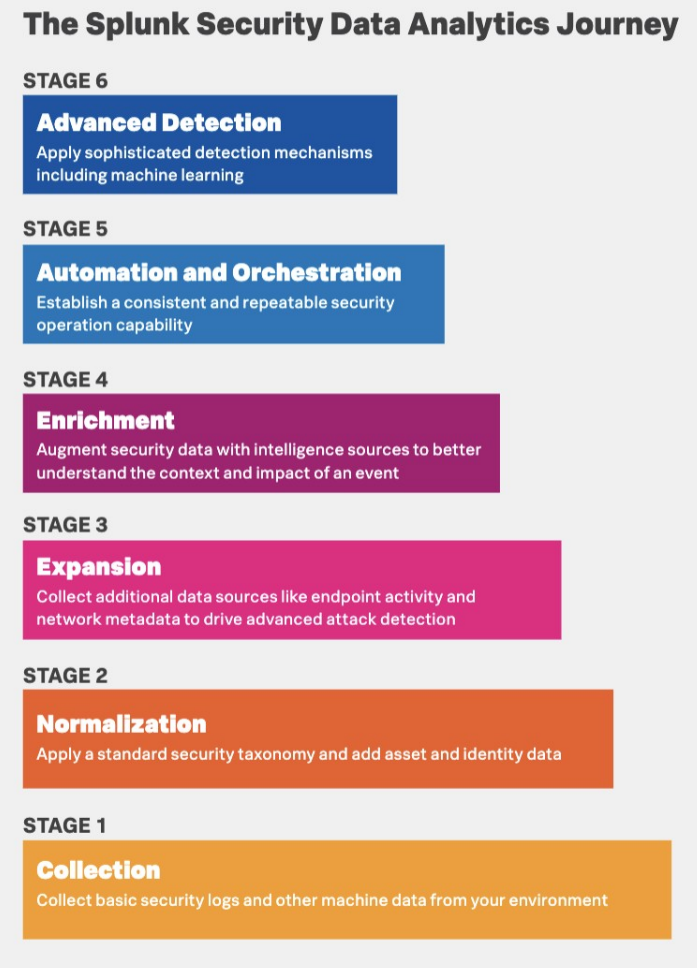
This search looks for specific authentication events from the Windows Security Event logs to detect potential attempts at using the Pass-the-Hash technique.

Searches Included | Use Alternate Authentication Material | CIS 3 | CIS 5 | CIS 16

Detect Computer Changed With Anonymous Account

This search looks for Event Code 4742 (Computer Change) or EventCode 4624 (An account was successfully logged on) with an anonymous account.

Searches Included | Exploitation of Remote Services | CIS 6 | CIS 8



The Splunk Security Data Analytics Journey

STAGE 6

Advanced Detection

Apply sophisticated detection mechanisms including machine learning

STAGE 5

Automation and Orchestration

Establish a consistent and repeatable security operation capability

STAGE 4

Enrichment

Augment security data with intelligence sources to better understand the context and impact of an event

STAGE 3

Expansion

Collect additional data sources like endpoint activity and network metadata to drive advanced attack detection

STAGE 2

Normalization

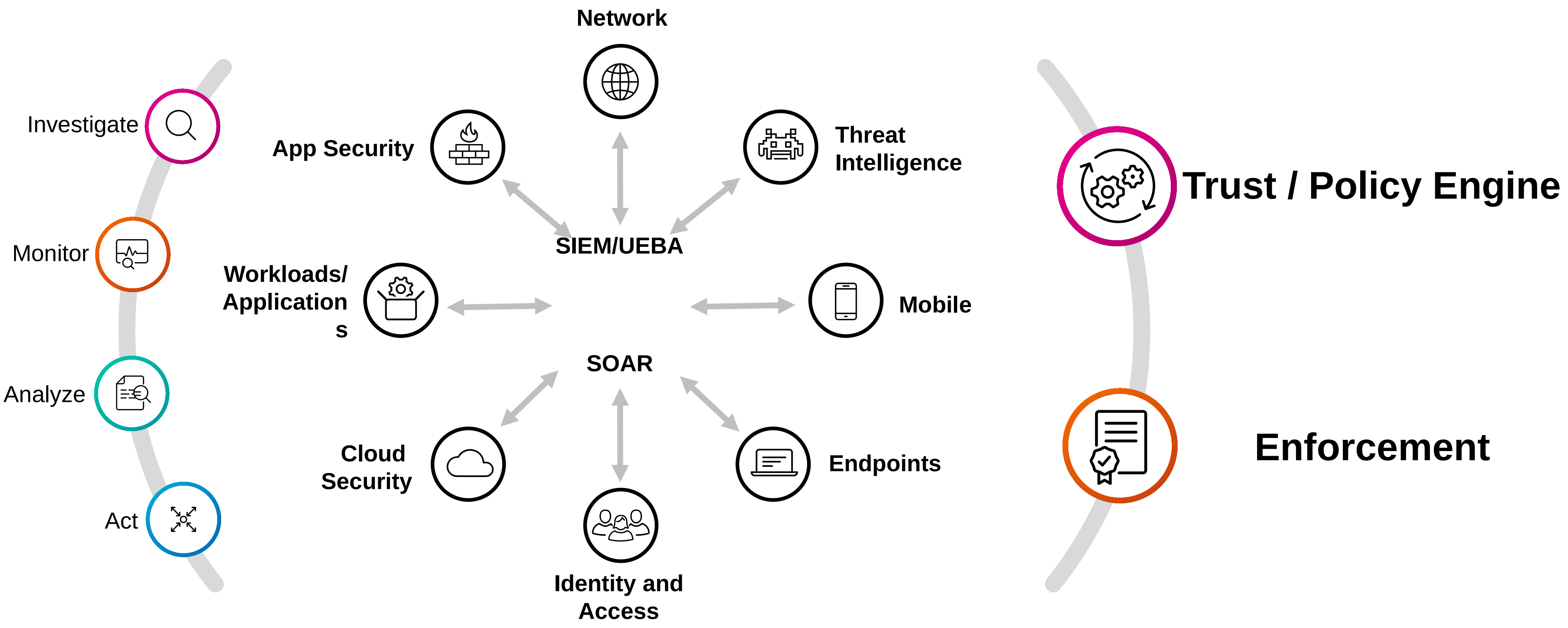
Apply a standard security taxonomy and add asset and identity data

STAGE 1

Collection

Collect basic security logs and other machine data from your environment

Zero Trust Decision Making with Splunk



Confidence and Trust in Decisions

Increases confidence and trust in access decisions to enterprise resources

Visibility

- Continuous monitoring
- Help validate user, asset and service for confidence in their trustworthiness

Analytics

- Rich, contextual details
- Correlation and analytics for fast insights and holistic decisions

Risk Scoring

- Real-time risk scoring
- Automation, security & behavior analytics augmented by ML for a proactive defense

Optimize and Improve Effectiveness

Real-time policy adherence, performance and availability of components across the entire ecosystem

Full-Stack Visibility

- View the health and status of Services, infrastructure, and component relationships
- Predict issues before they happen with machine learning

Compliance

- Real-time granular visibility across the network, endpoints and application stack
- Orchestrate any remediations of configuration drifts

Policy Adherence

- Continuously monitor policy compliance – including the zero-trust infrastructure
- Conduct quick, yet detailed assessments and audits

Reduce Fatigue and Costs

Enforce Zero Trust policies by automating tasks and orchestrating workflows

Automation & Orchestration

- Automate repetitive tasks and orchestrate workflows to reduce manual efforts
- Free up resources

Nerve Center

- Connect disparate security systems to provide a single pane of glass
- Focus on what matters

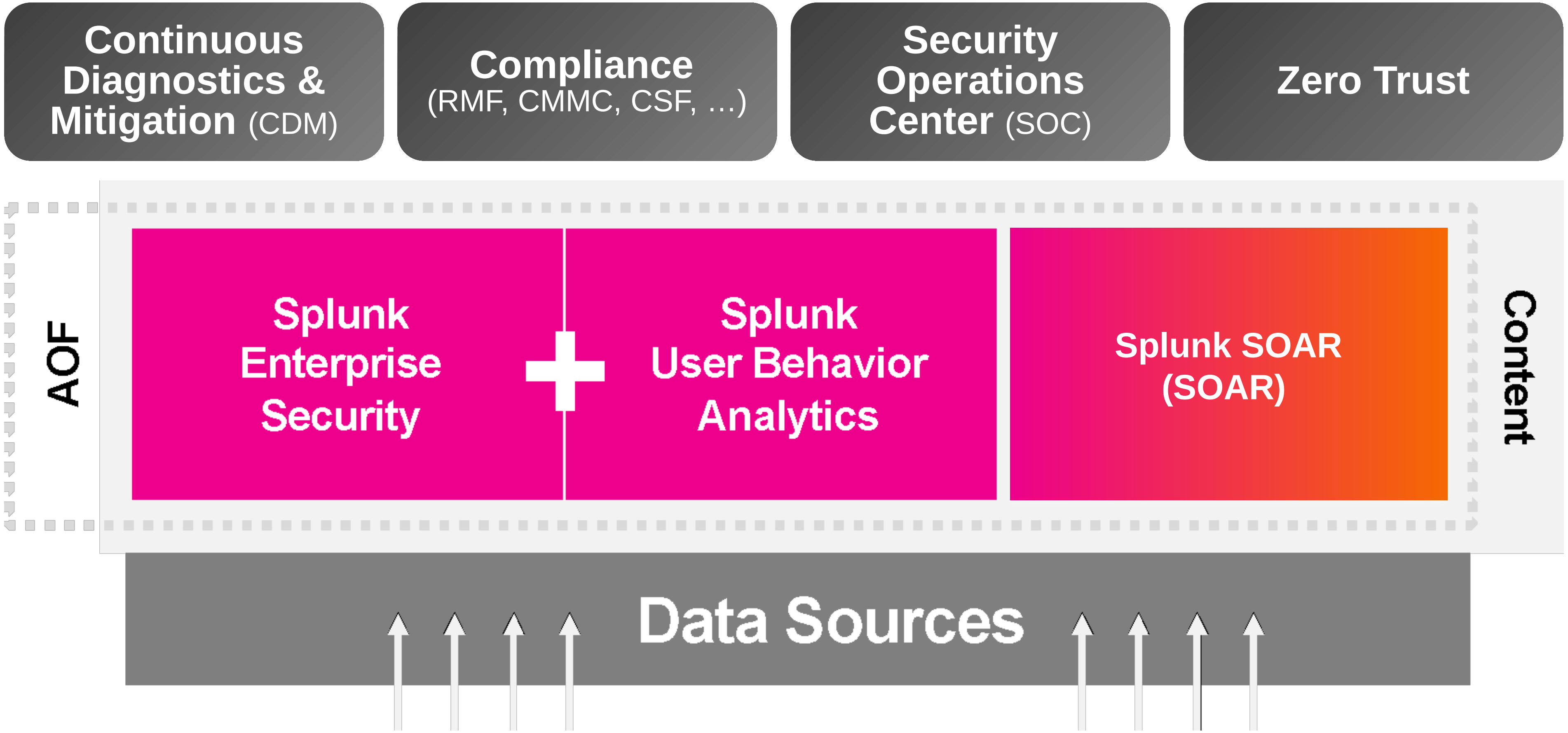
Playbooks

- Reusable template approach speeds action and improves consistency
- Guide fast remediation

Splunk Security Operations Suite

Data is the foundation for all your compliance and security initiatives

__AOF__ = Adaptive Operations Framework - our ecosystem of apps and security partner integrations.



Continuous Diagnostics & Mitigation (CDM)

Compliance (RMF, CMMC, CSF, …)

Security Operations Center (SOC)

Zero Trust

AOF

Splunk Enterprise Security

Splunk User Behavior Analytics

Splunk SOAR (SOAR)

Content

Data Sources

__Content__ = Pre-packaged security content (searches, detection models, automation playbooks) from the Splunk Research Team. Stay current with latest threat intelligence

Any Format, Any Scale, Any Structure

Analytics-Driven Security: Portfolio

- Search and Investigate
- Dashboards and Reports
- Incident & Breach Response
- Monitoring & Alerting
- Threat Detection
- Security Operations
- Automation & Orchestration
- Discover Anomalous Behavior
- Detect Unknown Threats

3rd Party Apps & Add-ons (700+)

cisco
ForeScout
proofpoint
NetFlow LOGIC
f5
OSSEC

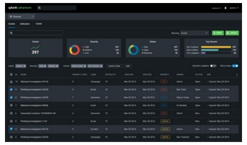
Splunk Security Apps & Add-ons

- Security Essentials
- RDBMS (any) data
- ES Content Update
- ML Toolkit
- Network data
- Windows host data
- Windows Infrastructure
- Exchange data
- PCI Compliance
- App for AWS
- Google Cloud
- Microsoft Cloud

Premium Solutions

Enterprise Security

User Behavior Analytics



SOAR

splunk> Platform for Security – SOC Operations, Compliance & Zero Trust

Thank You

splunk> turn data into doing™