

Accelerate your Cloud-Driven Transformation

Antonio Forzieri

EMEA Cyber Security Specialization and Advisory

splunk® > turn data into doing™







New companies

Greatwide Truckload

Next update: **8 Days 5 : 22 : 37**

CI Selecta SIA

Next update: **9 Days 4 : 54 : 38**

ALIZON

Next update: **8 Days 4 : 11 : 22**

Hamel Homes LLC

Next update: **8 Days 3 : 38 : 38**

MSPharma

Next update: **7 Days 18 : 01 : 32**

Cathar Games

Next update: **6 Days 18 : 44 : 21**

Active Business & Technology

Next update: **5 Days 18 : 48 : 58**

Grupo Pájar

Next update: **5 Days 18 : 36 : 37**

Cambridge Wright Plan Ltd

Next update: **5 Days 18 : 17 : 37**

Avaddon team collects and analyzes information about our clients and their companies. We specialize in customer privacy data, financial information, databases, credit card information and more.

Now we would like to talk about the cost of non-cooperation and self-service data recovery.

Encrypted files are not the main problem. Companies cannot understand the risk of information leakage, especially private information.

Such leaks of information lead to losses for the company, fines and lawsuits. And don't forget that information can fall into the hands of competitors!

As we know from the reports, the cost of company recovery services can be ten times more than our amount for the ransom.

When hiring third-party negotiators or recovery companies, listen to what they tell you, try to think, are they really interested in solving your problems or are they just thinking about their profit and ambitions?

Avaddon Locker cannot be decrypted without the help of the Avaddon general decryptor!

Greatwide Truckload

Company: Greatwide Truckload

Address: 2150 Cabot Blvd W, Langhorne, Pennsylvania, 19047, United States

Website: www.greatwide-trk.com

Phone: (215) 428-4800

800-283-9700

877-562-0837

Next update: **8 Days 5 : 22 : 37**

Greatwide Truckload, the company does not want to cooperate with us, so we give them **240 hours** to communicate and cooperate with us. If this does not happen before the time counter expires, we will leak valuable company documents.

We have a lot of valuable data, such as: classified information, confidential agreements and more, contracts, legal data, driver's documents, customer database as well as their personal data, tax

Full dumps

Steel Art Signs Corp

Published size: **517.74 MB**

Targetcom

Published size: **947.98 MB**

Banque Center for Applied Mathematics-BCAM

Published size: **134.1 MB**

Mikon Trading

Published size: **2.38 MB**

Schneider & Branch

Published size: **28.23 MB**

Dzhufo Languan Electronic Technology Co., Ltd

Published size: **118.85 MB**

AlphaADA

Published size: **1.4 MB**

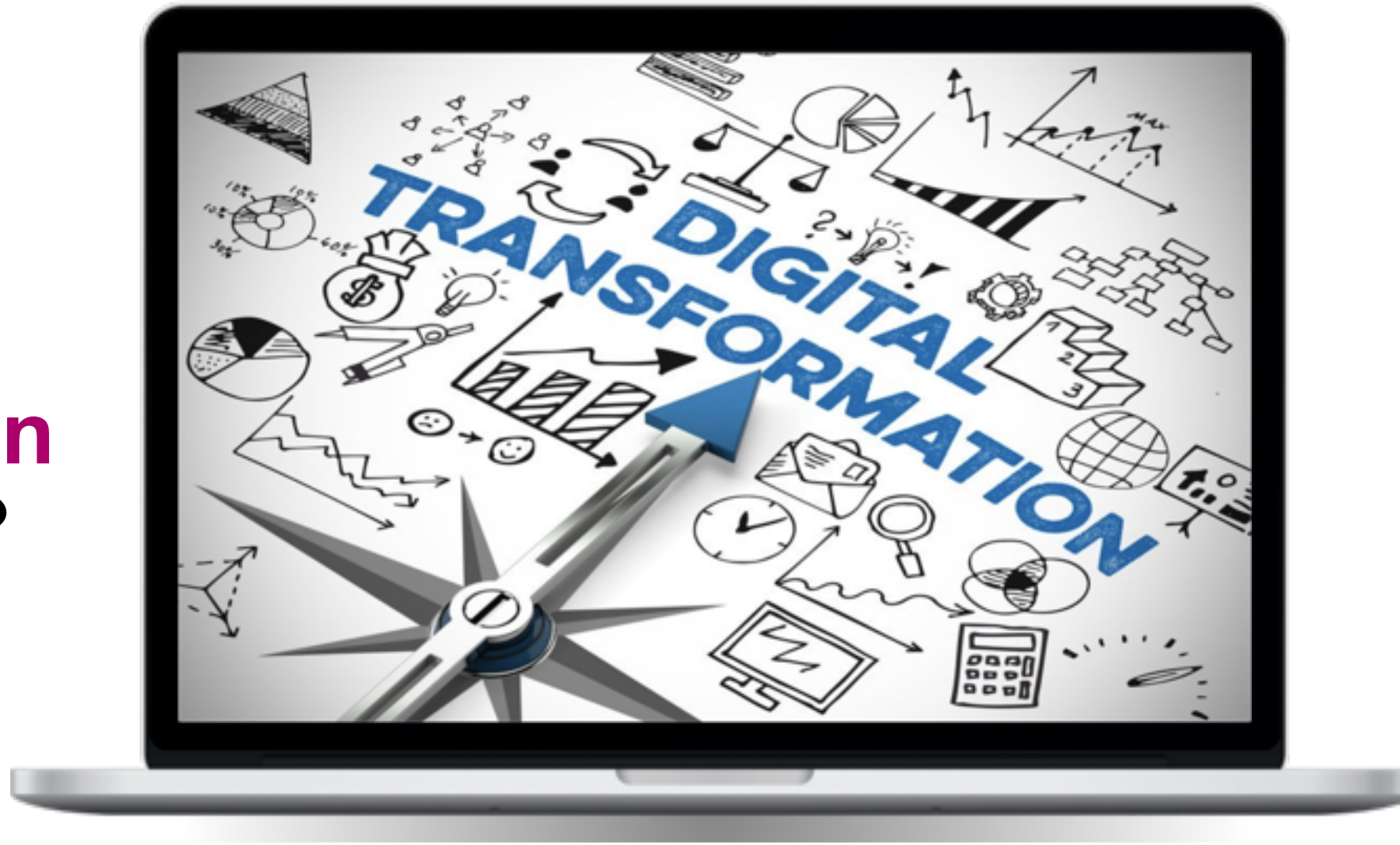
SISCONT

Published size: **483.98 MB**

La compagnie du SAV

Published size: **28.38 MB**

What does Digital Transformation Mean to YOU?



Cloud is here to stay

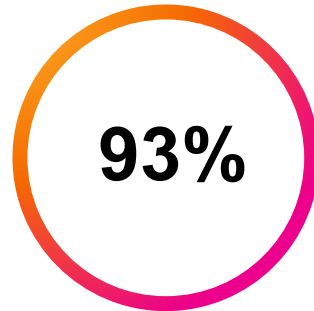
Enterprise Cloud Adoption Continues to Accelerate - Present & Projected

**Cloud
Market**



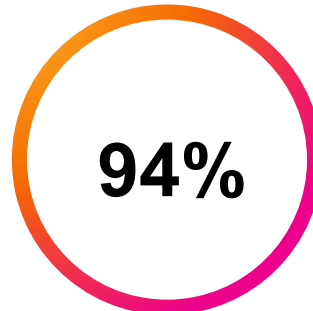
2023

**Multi-Cloud
Strategy**



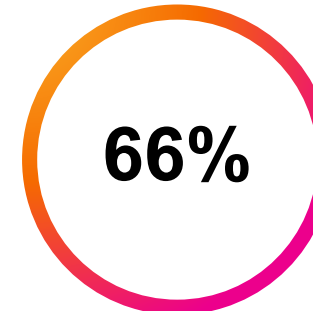
Present

**Cloud Services
& Security**



Present

**Cloud
Teams**



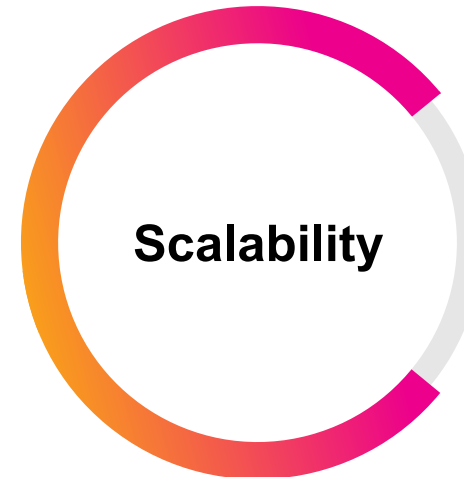
Present

**Cloud
Spend**

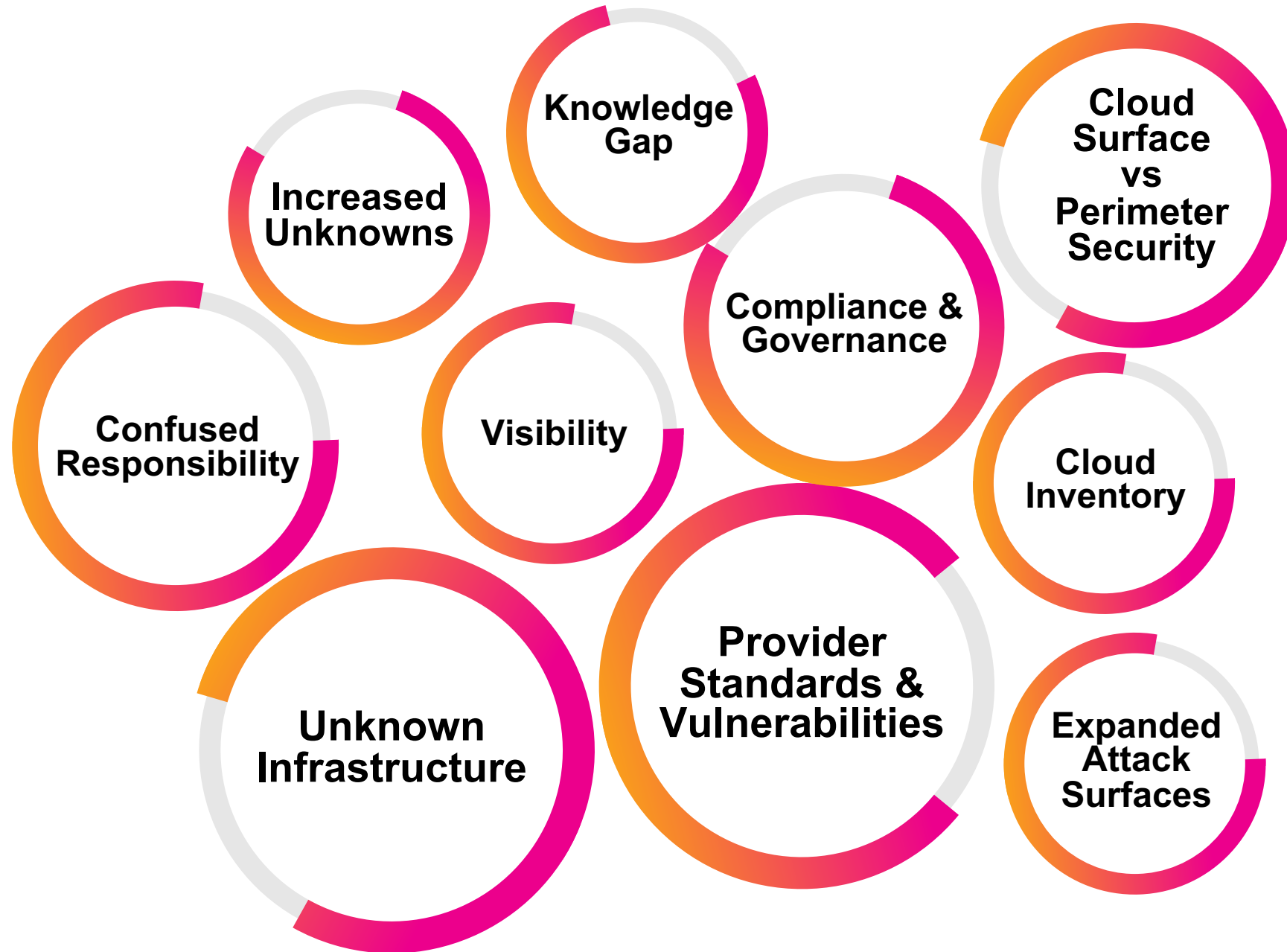


Present
50% of Enterprises

Benefits of Multi-Cloud Adoption



Challenges of Cloud Security & Operations



The Drive & Priorities

84%

Actively Pursuing
Digital Transformation

45%

Security is Top Priority

Top Challenges

27%

Integration Issues are
Top barriers.

26%

Security is Top
barriers.

The Human Touch

30%

Need to improve
Collaboration

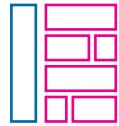
27%

Need to Transform
Culture

Cloud is a Critical Enabler of Transformation but **Increases Complexity**

Retain & Optimize

Tightly Coupled Apps,
Slow Deployment Cycles



Phase 1

Lift & Shift

Primarily Cloud IaaS



Phase 2

Re-Factor

More Modular, Dependent
App Components



Phase 3

Re-Architect

Loosely Coupled Microservices,
Serverless Functions



Phase 4



More data centers to
monitor and secure



More data across an
expanded attack surface



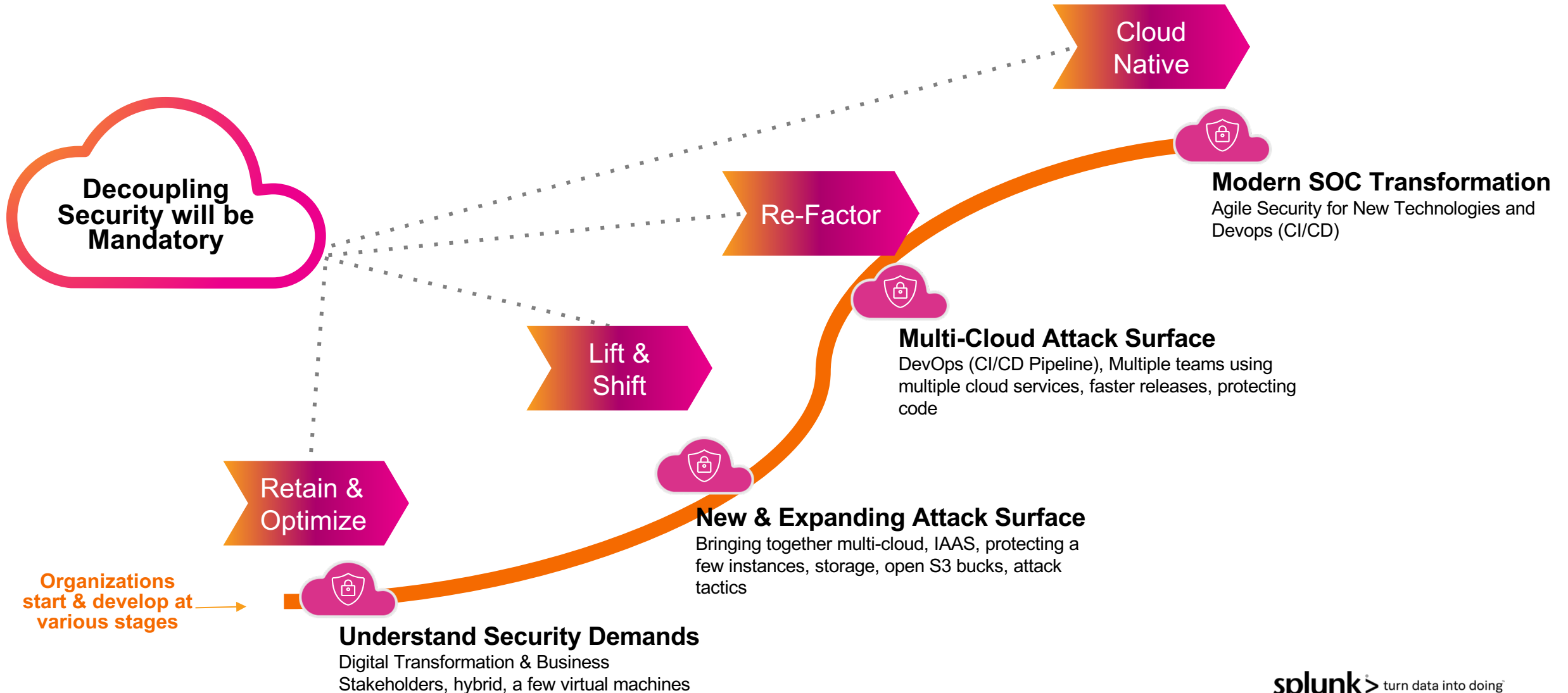
More complexity and
unpredictability



More frequent releases
and risk

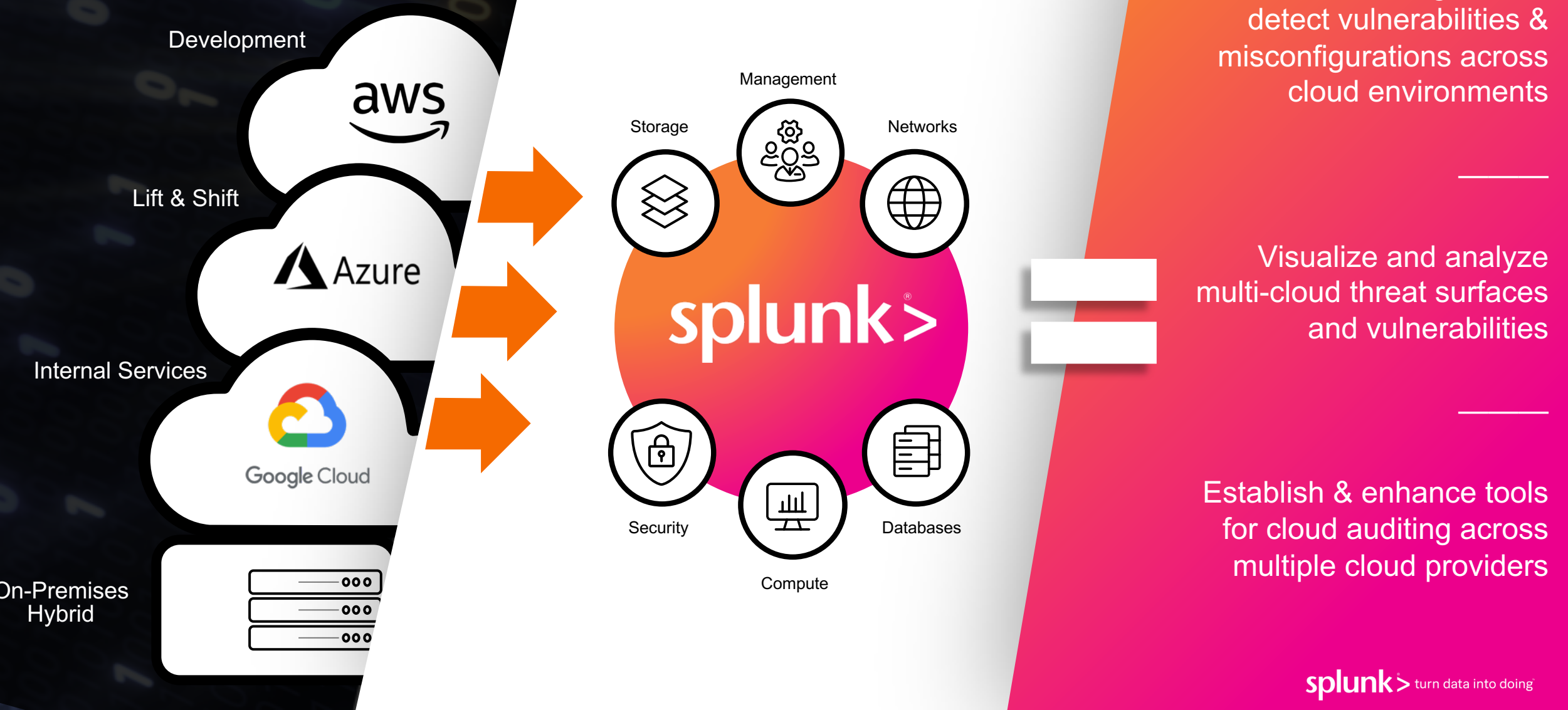
Parallelized Cloud Transformation

Cloud Security shifts at different speeds



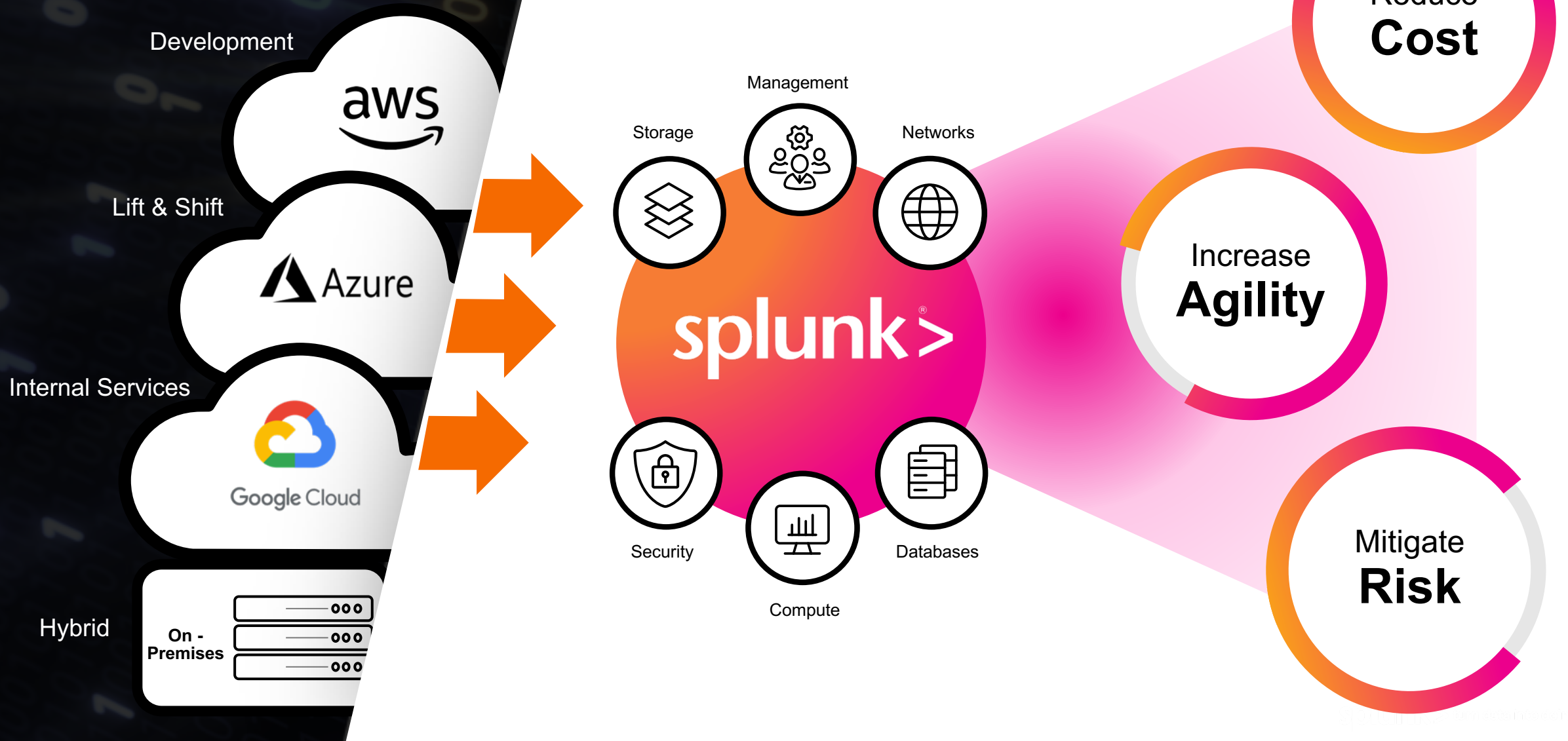
Operationalize Security

Value of seeing events across hybrid-cloud environments



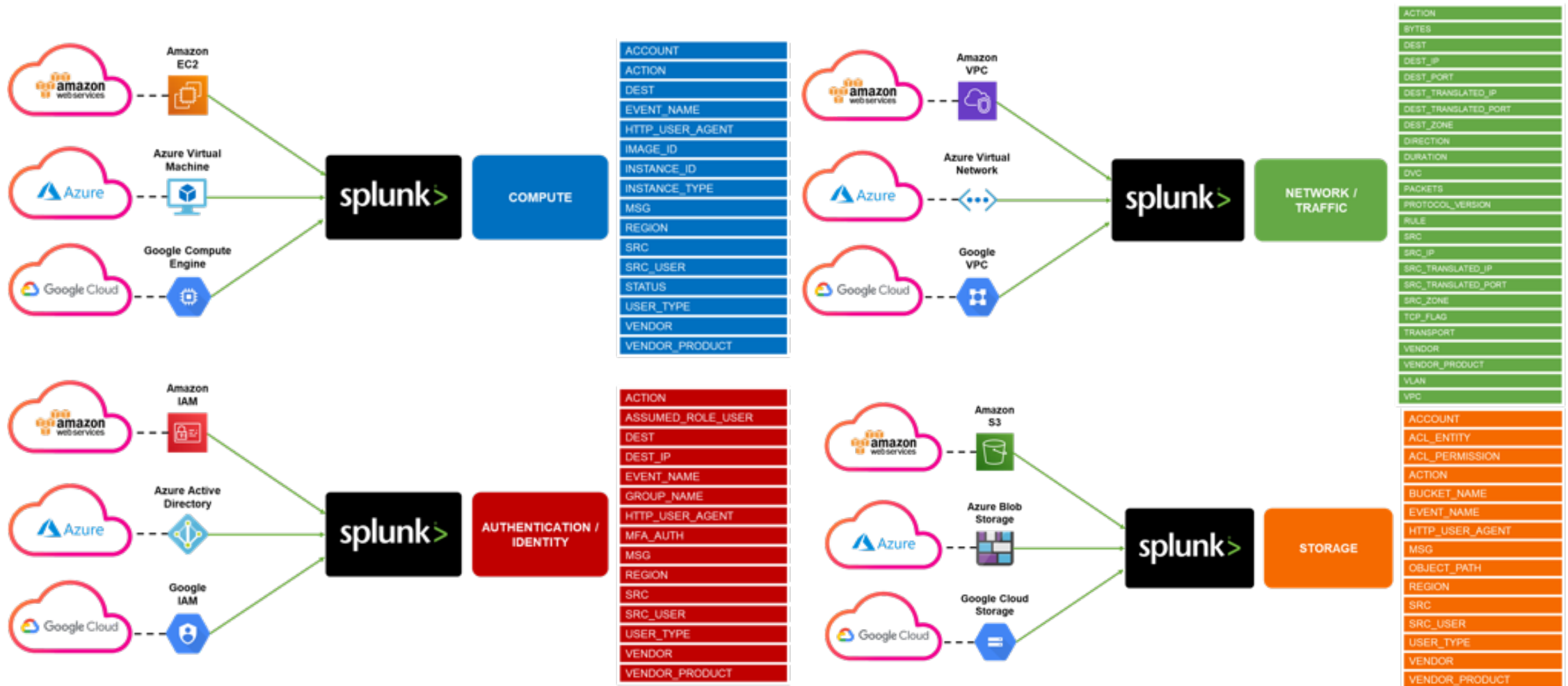
Splunk for Hybrid-Cloud

Value of seeing events across multi-cloud & hybrid environments



DeepDive for Multi-Cloud Security Monitoring

Splunk Expert-Led Session



Build and strengthen a unified cloud security posture

Operationalize data across multi-cloud environments

- Proactively monitor, investigate and detect threats and misconfigurations across cloud environments
- Bring cloud security data together for better visibility and faster response
- Comprehensive security with enhanced auditing, visualization and analytics



HOW DO I DO THAT?

A person with dark hair and glasses is shown from the nose up, looking upwards with a questioning expression. Their head is surrounded by a dense, swirling cloud of small, dark question marks. The background is a solid dark grey.

What we hear from customers

CONFUSION: I have no clear understanding where I should start.

PLANNING: I'm not sure I can build a roadmap to mature my SOC.

SPEED: Deploying a SIEM is very complex and takes a lot of time.

BUDGET: I don't have enough money to monitor my infrastructure.

VALUE: I'm not sure I can easily show value to my boss.

MITRE | ATT&CK™



All models are wrong, but some are
useful.

— *George E. P. Box* —

AZ QUOTES

MITRE ATT&CK: your friendly framework!

Exfiltration and Encryption are only the last stages



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 5 techniques	Execution 12 techniques	Persistence 10 techniques	Privilege Escalation 12 techniques	Defense Evasion 40 techniques	Credential Access 18 techniques	Discovery 28 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 8 techniques	Impact 10 techniques
Active Scanning [link]	Acquire Infrastructure [link]	Drive-by Compromise [link]	Command and Scripting Interpreter [link]	Account Manipulation [link]	Abuse Elevation Control Mechanism [link]	Abuse Elevation Control Mechanism [link]	Adversary in-the-Middle [link]	Account Discovery [link]	Exploitation of Remote Services [link]	Adversary in-the-Middle [link]	Application Layer Protocol [link]	Automated Exfiltration [link]	Account Access Removal [link]
Gather Victim Host Information [link]	Compromise Accounts [link]	Exploit Public-Facing Application [link]	Container Administration Command [link]	APIs, Jobs [link]	Access Token Manipulation [link]	Access Token Manipulation [link]	Brute Force [link]	Application Window Discovery [link]	Internal Spearphishing [link]	Active Collected Data [link]	Communication Through Removable Media [link]	Data Transfer Size Limits [link]	Data Destruction [link]
Gather Victim Identity Information [link]	Compromise Infrastructure [link]	External Remote Services [link]	Deploy Container [link]	Boot or Login Autostart Execution [link]	Boot or Login Autostart Execution [link]	Boot or Login Autostart Execution [link]	Credentials from Password Stores [link]	Browser Bookmark Discovery [link]	Lateral Tool Transfer [link]	Audio Capture [link]	Data Encoding [link]	Exfiltration Over Alternative Protocol [link]	Data Encrypted for Impact [link]
Gather Victim Network Information [link]	Develop Capabilities [link]	Hardware Additions [link]	Exploitation for Client Execution [link]	Boot or Login Initialization Scripts [link]	Boot or Login Initialization Scripts [link]	Boot or Login Initialization Scripts [link]	Exploitation for Credential Access [link]	Cloud Infrastructure Discovery [link]	Remote Service Session Hijacking [link]	Automated Collection [link]	Data Obfuscation [link]	Exfiltration Over CI Channel [link]	Data Manipulation [link]
Gather Victim Org Information [link]	Establish Accounts [link]	Phishing [link]	Inter-Process Communication [link]	Browser Extensions [link]	Create or Modify System Process [link]	Create or Modify System Process [link]	Forged Authentication [link]	Cloud Service Dashboard [link]	Remote Service Session Hijacking [link]	Browser Session Hijacking [link]	Dynamic Resolution [link]	Exfiltration Over Other Network Medium [link]	Defacement [link]
Phishing for Information [link]	Obtain Capabilities [link]	Realization Through Removable Media [link]	Native API [link]	Compromise Client Software Binary [link]	Create or Modify System Process [link]	Create or Modify System Process [link]	Forge Web Credentials [link]	Cloud Service Discovery [link]	Remote Services [link]	Clipboard Data [link]	Encrypted Channel [link]	Exfiltration Over Physical Medium [link]	Disk Wipe [link]
Search Cloud Sources [link]	Image Capabilities [link]	Supply Chain Compromise [link]	Scheduled Task/Job [link]	Domain Policy Modification [link]	Domain Policy Modification [link]	Domain Policy Modification [link]	Host Capture [link]	Container and Resource Discovery [link]	Replication Through Removable Media [link]	Data from Cloud Storage Object [link]	Exfiltration Over Other Network Medium [link]	Exfiltration Over Physical Medium [link]	Endpoint Denial of Service [link]
Search Open Technical Databases [link]	Malware Capabilities [link]	Trusted Relationship [link]	Shared Modules [link]	Event Triggered Execution [link]	Event Triggered Execution [link]	Event Triggered Execution [link]	Modify Authentication Process [link]	Domain Trust Discovery [link]	Software Deployment Tools [link]	Data from Configuration Repository [link]	Exfiltration Over Web Service [link]	Exfiltration Over Web Service [link]	Hardware Corruption [link]
Search Open Malware Databases [link]		Valid Accounts [link]	Software Deployment Tools [link]	Event Triggered Execution [link]	Event Triggered Execution [link]	Event Triggered Execution [link]	Network Sniffing [link]	File and Directory Discovery [link]	Test Shared Content [link]	Data from Information Repository [link]	Multi-Stage Channels [link]	Scheduled Transfer [link]	Initial System Recovery [link]
Search Victim-Owned Websites [link]			System Services [link]	External Remote Services [link]	Exploitation for Privilege Escalation [link]	Exploitation for Privilege Escalation [link]	OS Credential Dumping [link]	Group Policy Discovery [link]	Use Alternate Authentication Material [link]	Data from Local System [link]	Non-Application Layer Protocol [link]	Transfer Data to Cloud Account [link]	Network Denial of Service [link]
			User Execution [link]	Host Execution Flow [link]	Host Execution Flow [link]	Host Execution Flow [link]	Local Application Access Token [link]	Network Service Scanning [link]		Data from Network Shared Drive [link]	Protected Tunneling [link]		Resource Hijacking [link]
			Windows Management Instrumentation [link]	Implant Internal Image [link]	Process Injection [link]	Process Injection [link]	Local or Forge Kerberos Tickets [link]	Network Share Discovery [link]		Data from Removable Media [link]	Proxy [link]		Service Stop [link]
				Modify Authentication Process [link]	Scheduled Task/Job [link]	Scheduled Task/Job [link]	Local Web Session Cookies [link]	Network Sniffing [link]		Data from Local System [link]	Remote Access Software [link]		System Shutdown/Reboot [link]
				Office Application Malware [link]	Valid Accounts [link]	Valid Accounts [link]	Two-Factor Authentication Interception [link]	Peripheral Device Discovery [link]		Email Collection [link]	Traffic Signaling [link]		
				Pre-OS Boot [link]			Unsecured Credentials [link]	Repository Group Discovery [link]		Input Capture [link]	Web Service [link]		
				Scheduled Task/Job [link]				Process Discovery [link]		Screen Capture [link]			
				Server Software Component [link]				Query Registry [link]		Video Capture [link]			
				Traffic Signaling [link]				Remote System Discovery [link]					
								Software Discovery [link]					

MITRE
ATT&CK™

The de-facto gold standard Cyber Security Framework

about

Ransomware

domain

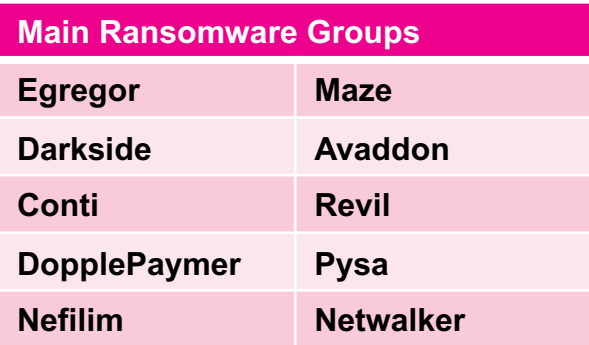
Enterprise
ATT&CK v10

platforms

Linux, macOS, Windows,
Azure AD, Office 365, SaaS,
IaaS, Google Workspace,
PRE, Network, Containers

legend

1.0 2.8 4.6 6.4 8.2 10



How can Splunk help me with this?



How can Splunk ES help me?

Security Content [What's New in 3.3.4?](#)

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

Search
enter search here... [Examples](#)

Filters
[Edit](#) **818 Total | 383 Filtered**

Journey
All selected (5) ▾

Security Use Case
All ▾

Category
All ▾

Data Sources
All ▾

Data Model
All ▾

ATT&CK Technique
All selected ▾

ATT&CK Software
All ▾

Originating App
Enterprise Security Co...

☒ All

☐ (0 matches)

☐ AWS (29 matches)

☐ Anti-Virus or Anti-Malware (5 matches)

☐ Any Splunk Logs (0 matches)

☐ App Server (0 matches)

☐ Application Data (0 matches)

☐ Audit Trail (34 matches)

☐ Authentication (12 matches)

☐ Azure (0 matches)

☐ Backup (0 matches)

☐ Cloud Infrastructure Data (1 matches)

☐ Configuration Management (0 matches)

☐ DLP (0 matches)

☐ DNS (7 matches)

☐ Email (3 matches)

☐ Endpoint Detection and Response (206 matches)

☐ GCP (4 matches)

☐ Host-based IDS (0 matches)

☐ IDS or IPS (2 matches)

☐ IP Address Assignment (0 matches)

☐ Kubernetes (0 matches)

☐ Malware Analysis (1 matches)

☐ Network Communication (11 matches)

☐ Okta (4 matches)

☐ Patch Management (0 matches)

☐ Physical Security (0 matches)

☐ Ticket Management (0 matches)

☐ User Activity Audit (4 matches)

☐ Vulnerability Detection (0 matches)

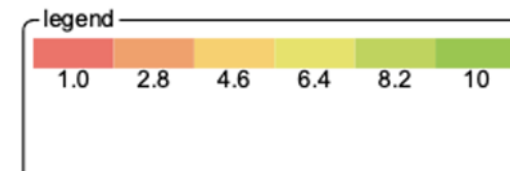
☐ Web Proxy (4 matches)

☐ Web Server (4 matches)

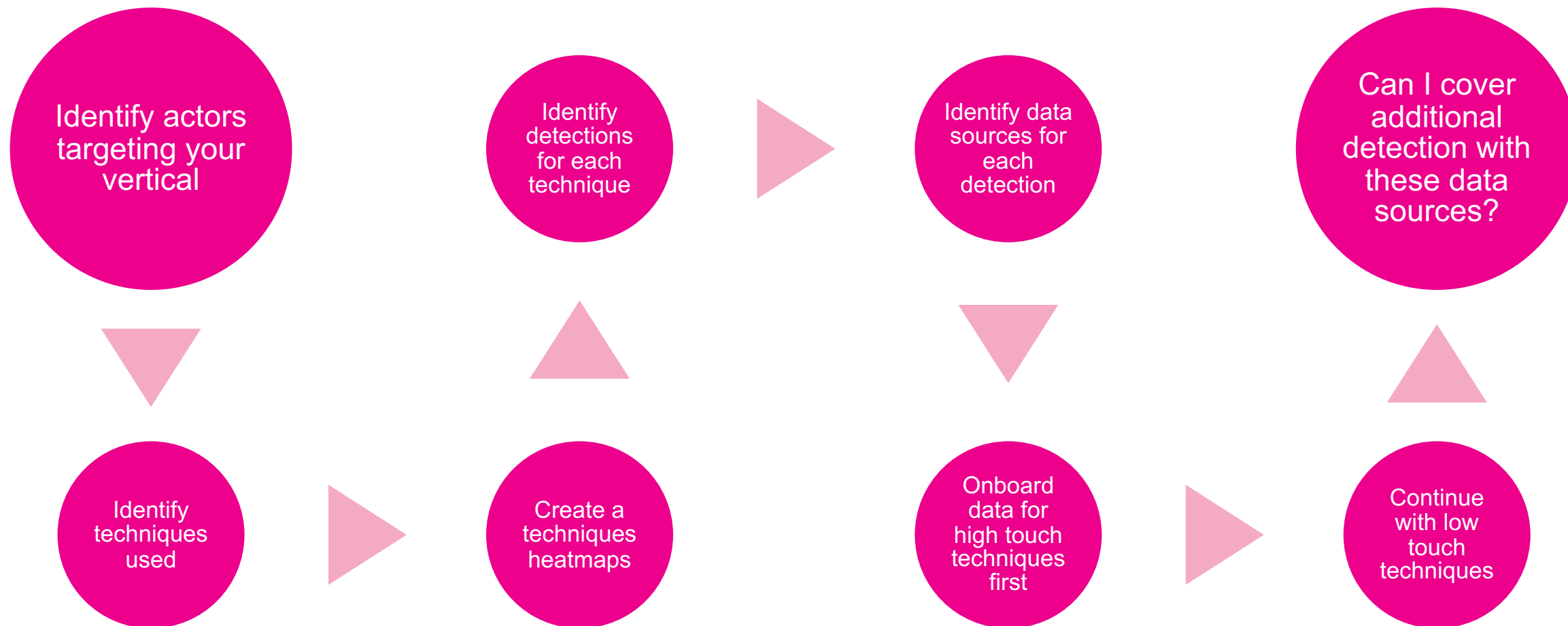
☐ Windows Security (26 matches)

In order to enable these out-of-the-box rules these data sources are required:

- Endpoint Detection and Response (CrowdStrike/Sysmon/Osquery...)
- Windows Workstation and Server logs (Windows Event Security, Audit Trail, User Activity)
- Network devices (Firewalls and IDS)
- DNS
- EMAIL
- Cloud



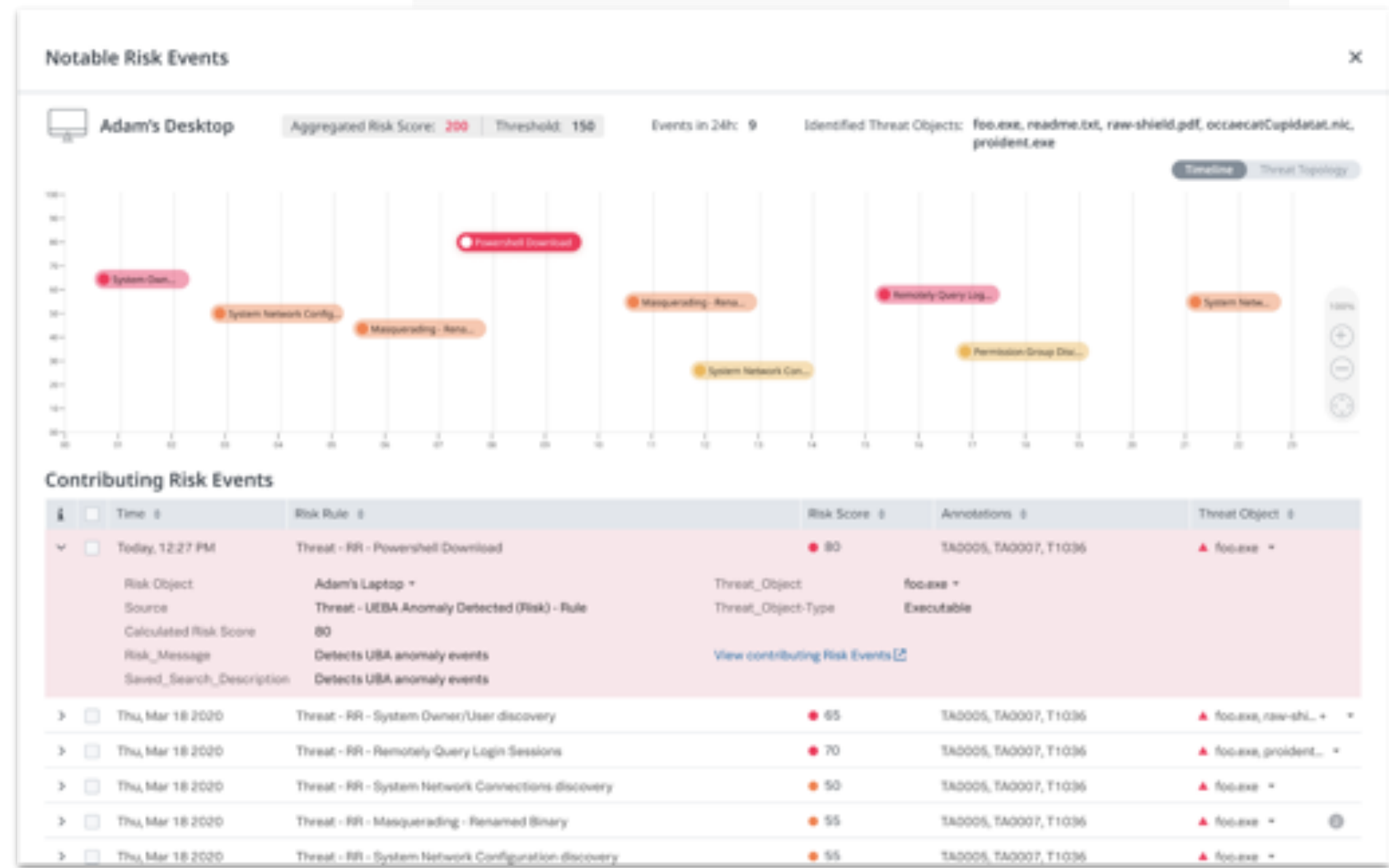
Which process can we embrace ?



Risk-Based Alerting Event Timeline

Splunk Enterprise Security 6.6

- Quickly identify timelines around contributing Risk Events
- Comprehensive view of overall threat activity combined into a single risk-based event.
- Improved visibility between risk objects, risk attributions, threat objects and the timeline of detection
- Reduce MTTD and shorten MTTR SOC metrics



Thank you

