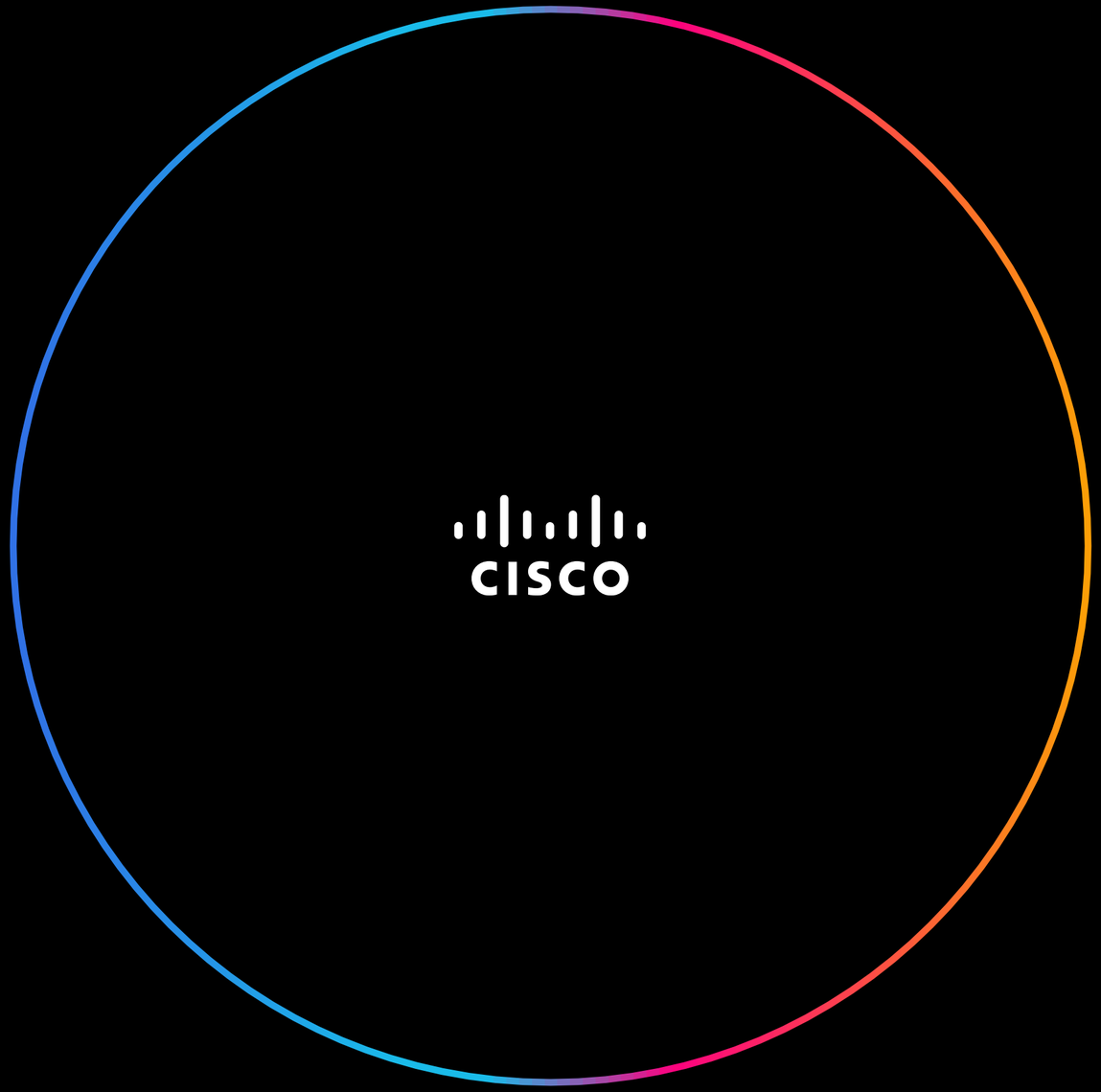
CISCO Engage | Tech Day

Power of Your Data

From Unobserved Systems to Adaptive Defense



Chris Perkins
Solutions Architect | Splunk

December 17, 2025

From Unobserved Systems to Adaptive Defense

A New Story for a New Era

Chris Perkins
Solutions Architect
Splunk Public Sector

splunk> a CISCO company

Chris Perkins

- ➔ Staff Solutions Architect @ Splunk, a Cisco company
- ➔ ~19 years in cybersecurity
- ➔ ~5 of which in fraud while at Splunk
- ➔ Based in New Mexico (ABQ -> LC)

I work on a security overlay team that covers the country's state, local, and tribal governments as well as K-20 and high ed.

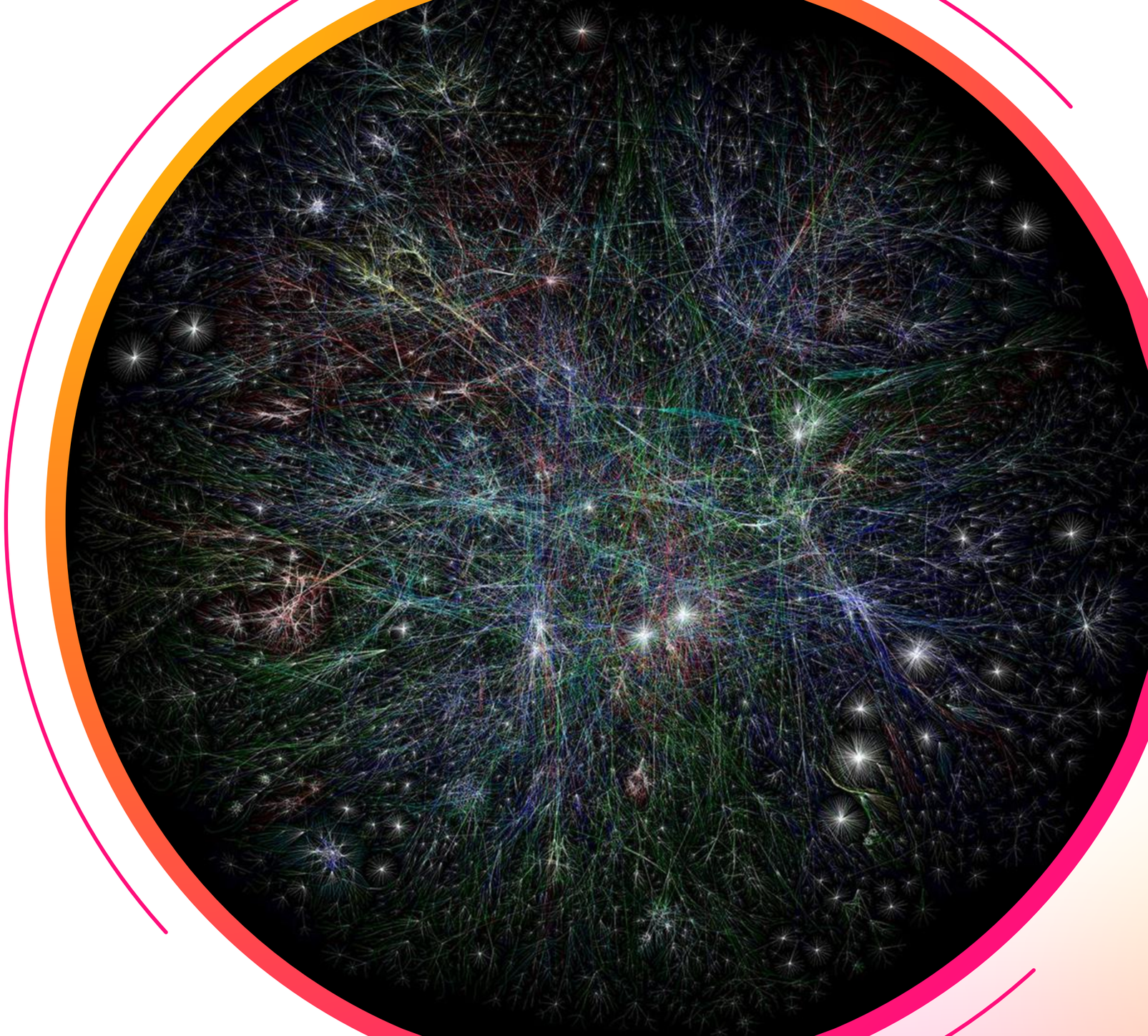
Agenda

1. Threat Paradigm Shift
    a. Agentic AI
    b. We need a new metric
2. Attack Sequences and Cascades
3. Speeding up Time-to-Good-Decision (TTGD)
4. Toolkit for Leading the Narrative
    a. Data Compass
    b. 5 Cs
5. Storytelling
6. Deep Dive
7. Q & A

The End of the Old Story

AI Agent	Agentic AI
Executes predefined tasks.	Sets its own sub-goals to achieve objectives.
Follows programmed workflows.	Adapts strategy based on environment.
Single-purpose tool.	Multi-capability problem solver.
Requires human oversight.	Operates autonomously for extended periods.
Stops when blocked.	Finds alternative paths.
Example: Chatbot answering FAQs.	Example: System autonomously infiltrating a network.

Now What?!



Storytelling is the Substrate of Effective Cybersecurity

1. Who or what is on the network?

1. How, where, and what are they accessing?

1. What is their experience, as measured/monitored by application and network visibility?

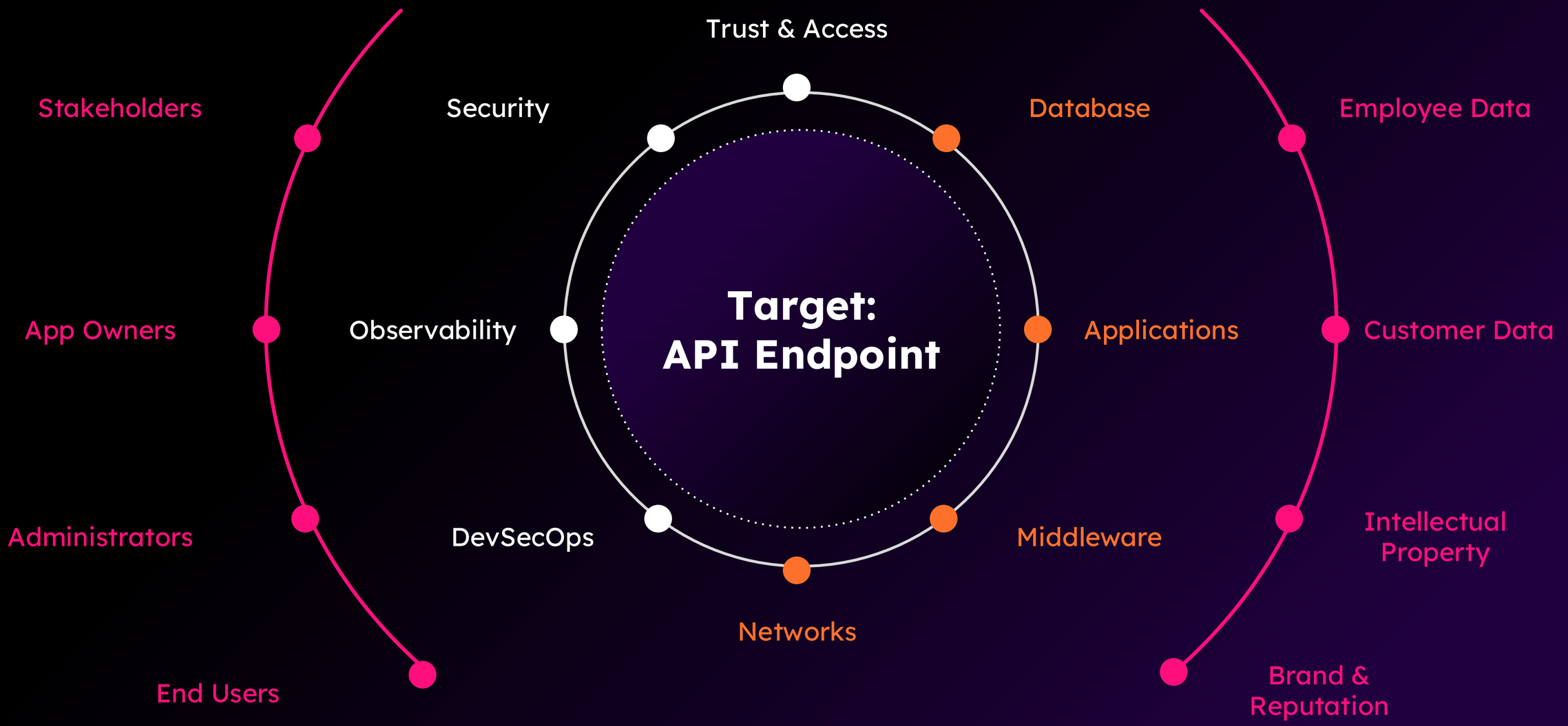
1. How do we monitor and protect the users, systems, and data that run their business?

1. How do we respond when something happens?

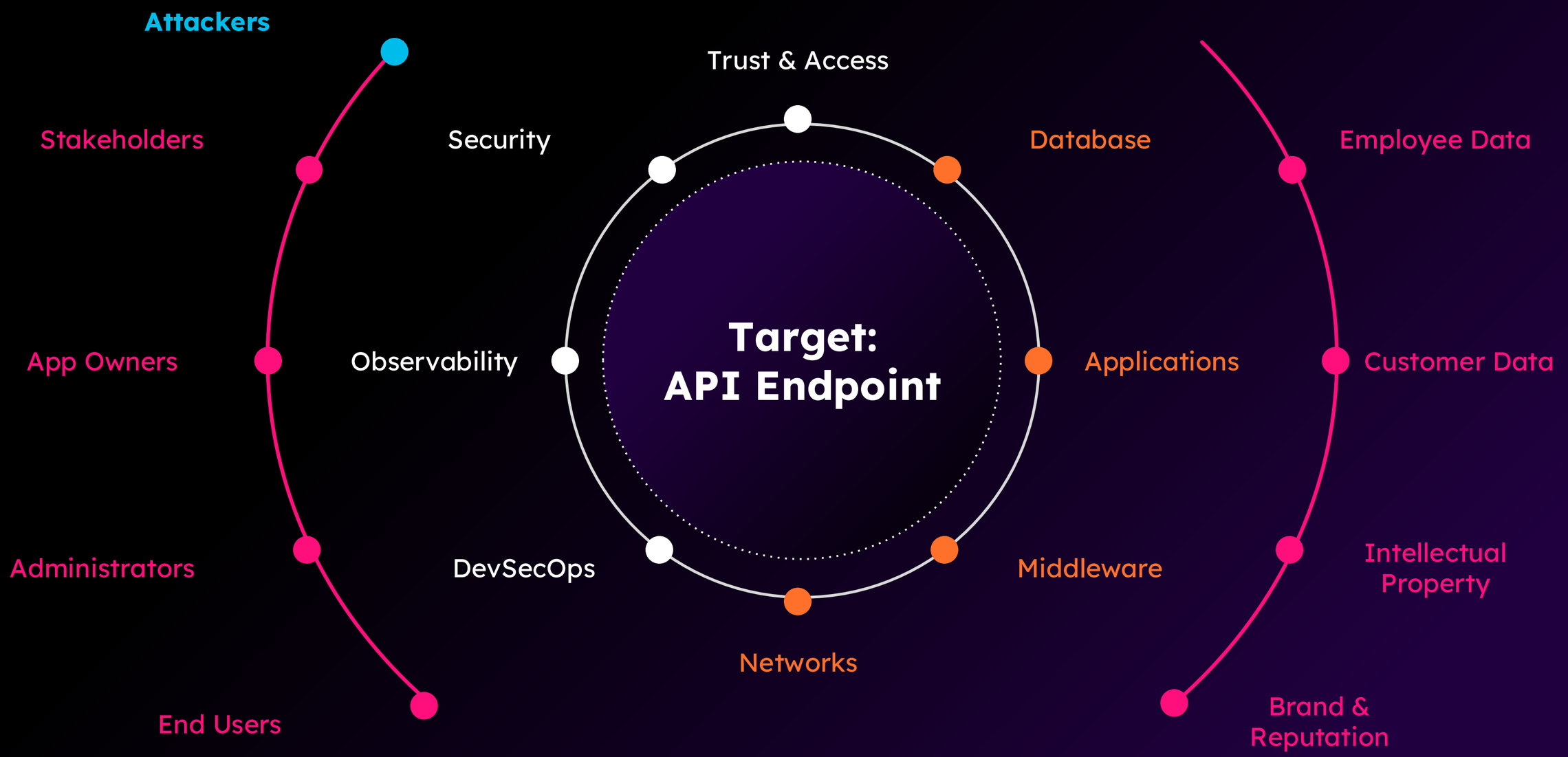
Time

~~MTTD~~
~~MTTR~~
TTGD

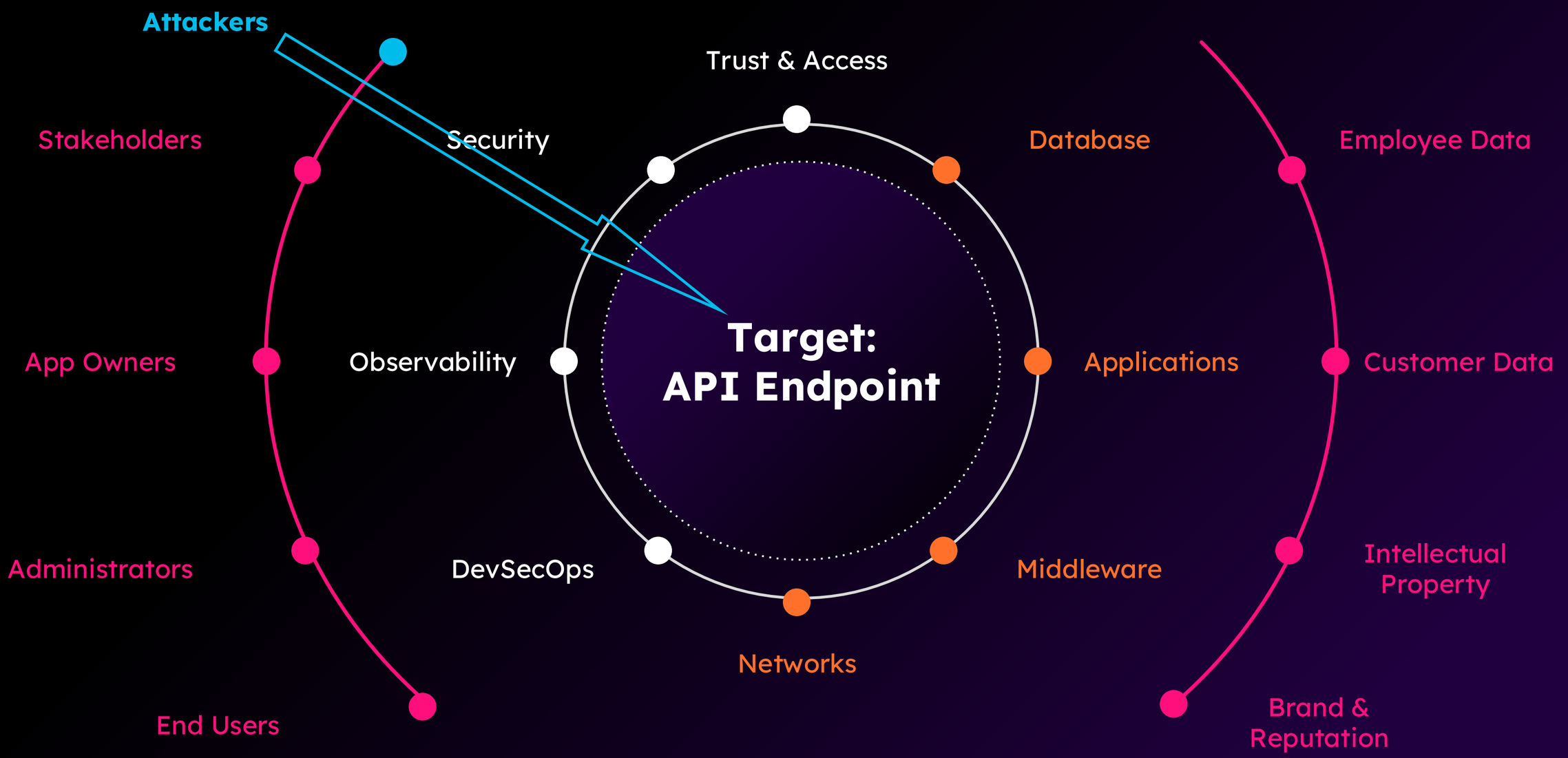
Cascades (Spatial)



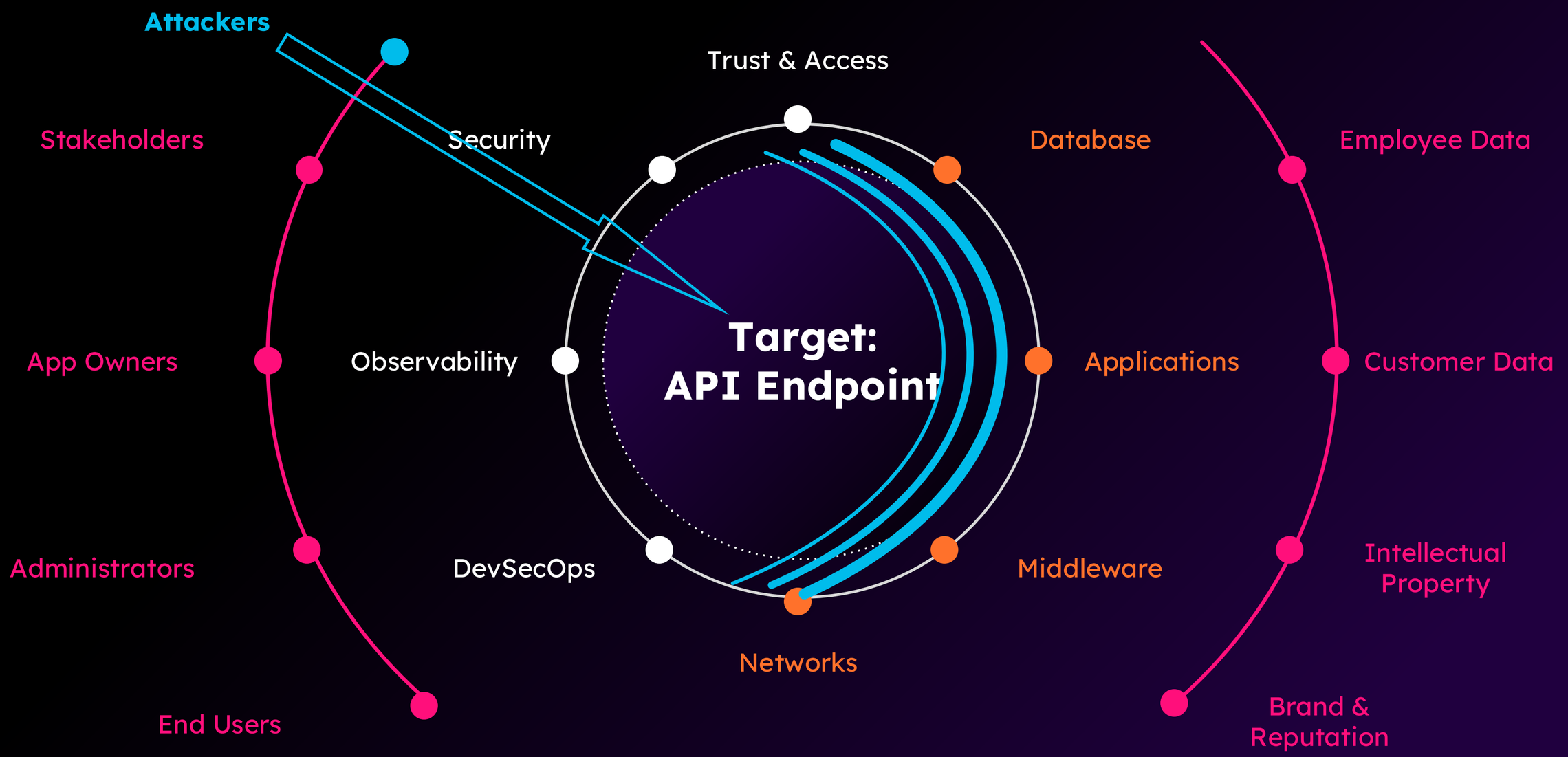
Cascades (Spatial)



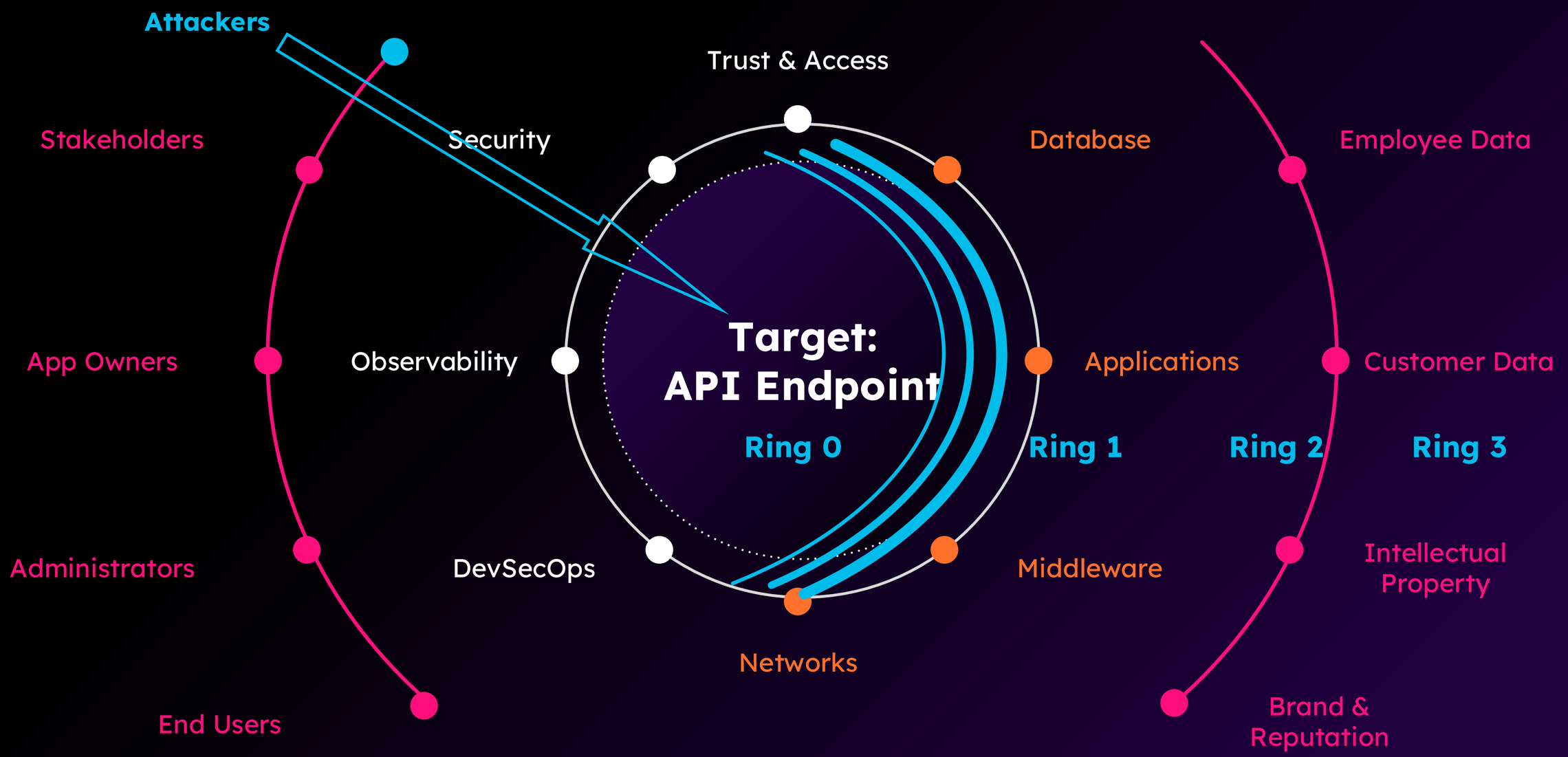
Cascades (Spatial)



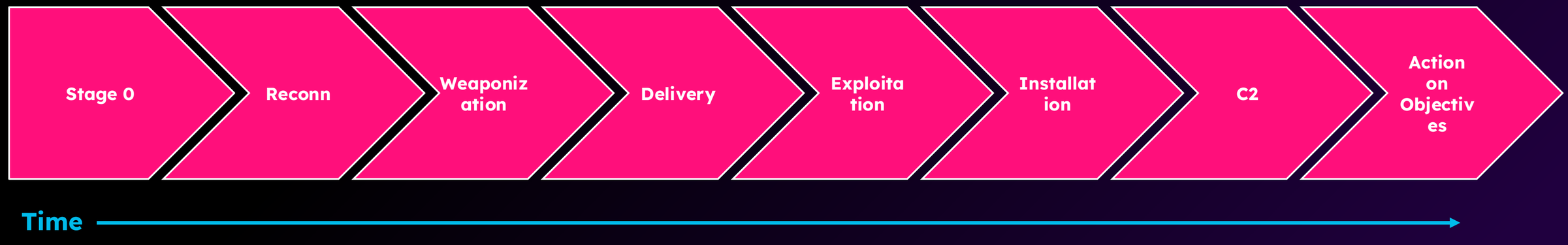
Cascades (Spatial)



Cascades (Spatial)



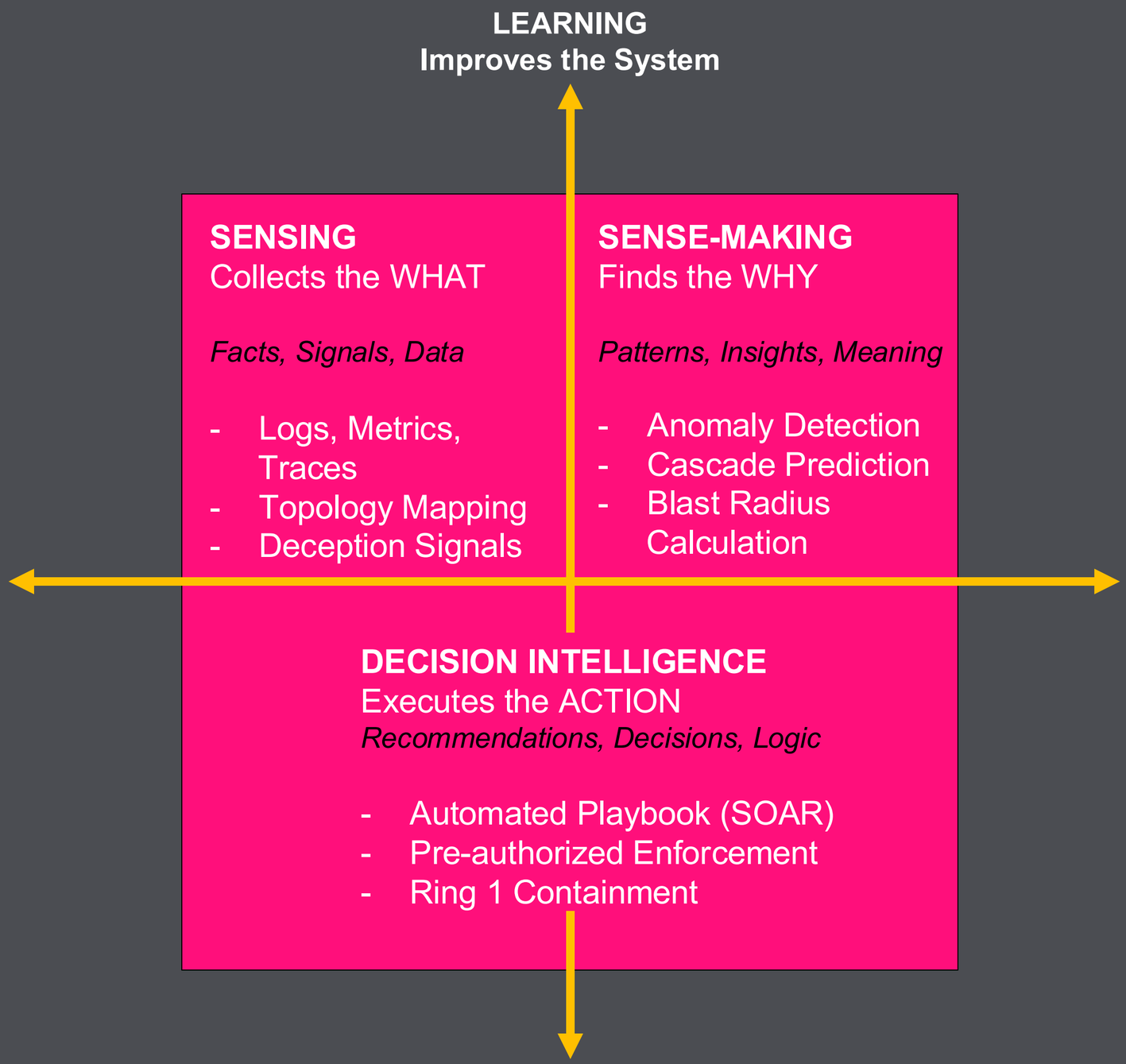
Attack Sequences (Temporal)



Attack Sequences (Temporal)

How do we speed up decision-making?

Authentication Clues	How you prove you're you.	Login from residential IP when user always connects from corporate VPN.
Device & Endpoint Clues	What you're using.	Browser fingerprint changes mid-session.
Network Clues	Where you're coming from and going.	East-west traffic to systems never accessed before.
Geographic Clues	Where in the world you are.	Singapore login 10 minutes after New York activity.
Resource Access Clues	What data and systems you're touching.	Accessing 100 customer records when typical is 5.
Temporal Clues	When you're working.	3 AM activity for a 9-5 employee.
Privilege Escalation Clues	How you're moving through the system.	Service account suddenly requesting admin rights.
Communication Clues	How you sound.	How Agentic AI systems sound differently.



Data Compass

Using the Data Compass, organizations can navigate their complex cyber terrain

	What	Why	Action
Signals	Facts	Patterns, Trends, Anomalies	Alerts
Meaning (Semantics)	Context	Insights	Recommendations
Wisdom (Logic)	Principles	Strategies	Decisions (Manual or Automated)

Moving from Current State to the Desired State

	Descriptive (What's Happening?)	Diagnostic (Why's It Happening?)	Prescriptive (What Should We Do?)
Signals	Gather raw data	Identify patterns underlying patterns	Propose immediate responses
Semantics	Clarify meaning and context	Understand relationships and drivers	Outline steps toward desired outcomes
Logic	Map system structure	Model reasons and behaviors	Optimize strategy for future state

Data Compass: Compromised Endpoint on Campus

Managed endpoint used by a mid-level manager, exhibiting command and control (C2) traffic at a sports facility.

	What	Why	Action
Signals	**Facts** • Endpoint generates anomalous network traffic (C2) detected in **XDR**. • Endpoint compromised indicator observed in **XDR**.	**Patterns, Trends, Anomalies** • Network traffic is anomalous and indicative of C2 activity. • The "compromised indicator" is a direct anomaly from expected endpoint behavior.	**Alerts** • An instant alert is generated in **XDR**. • An automated workflow is initiated by **XDR**.
Meaning	**Context** • The endpoint's asset details, and associated user context are identified and correlated in **Splunk**.	**Insights** • The immediate risk of the compromised endpoint is evaluated. • Potential for lateral movement within the network is understood based on the endpoint's role and user's access.	**Recommendations** • Enrich incident with additional data in **Splunk**. • Escalate to the appropriate security team. • Create a ServiceNow ticket.
Wisdom	**Principles** • The full attack chain is clearly mapped and confirmed through **XDR** and Splunk. • The confirmed compromise establishes a clear understanding of the threat.	**Strategies** • A broader risk assessment is performed to identify other potentially affected systems or users. • Immediate containment is recommended.	**Decisions (Manual or Automatic)** • Automated endpoint isolation is executed via **XDR**. • Detailed forensic logs are retained in **Splunk**.

The 5 Cs

Brené Brown's work: *Strong Ground: The Lessons of Daring Leadership, the Tenacity of Paradox, and the Wisdom of the Human Spirit*

1. **CONTEXT:** Why does this matter now?
2. **COLOR:** What does success look like?
3. **CONNECTIVE TISSUE:** Who do we need?
4. **COST:** What's the investment?
5. **CONSEQUENCE:** What's at stake?

Storytelling / Scenarios

Storytelling Blueprints

1. Campus to Cloud Experience | Security
2. SOC Outcome Acceleration
3. Data Cost Control with Visibility
4. Zero Trust Access Modernization
5. Application / Workload SLO Assurance
6. Create Your Own

Storytelling Blueprint Setup

1. Persona & Problem
2. Desired Outcome
3. Solution
4. Evidence
5. Next Steps

Deep Dive

Prevent issues before they affect customers, remediate rapidly, and adapt to new opportunities

Digital Resilience

Security

Gain comprehensive threat prevention, detection, investigation, and response for organizations of any size and security maturity

Observability

Prevent downtime and optimize experiences with visibility and insights across end-to-end services, including owned and unowned environments

Assurance

Enable seamless end-to-end connectivity across cloud, internet and enterprise networks to assure the delivery of applications and services

How Cisco and Splunk advance digital resilience

Catalyst Center ISE

Catalyst SDWAN

Meraki

ThousandEyes

UCS

Nexus, ACI

Network Monitoring

Distributed Enforcement Automated Repair

splunk> a CISCO company

Right Data, Right Analytics, Right Actions

Network Performance

How do network events impact user experience, application performance, and business metrics?

Application and Infrastructure

How can I improve performance of my hybrid, three-tier and cloud-native applications?

Security

How do seemingly independent alerts correspond to a threat? And how can I enforce at the source?

External data sources

Threat Detection

Distributed Enforcement Automated Remediation

Secure Firewall

Duo

Secure Network Analytics

Secure Email WSA

Multicloud Defense ASA

Secure Malware Analytics

Secure Access Umbrella

AI Defense

Talos

XDR

Workloads

- Security
- Observability
- Network Ops
- Custom Applications

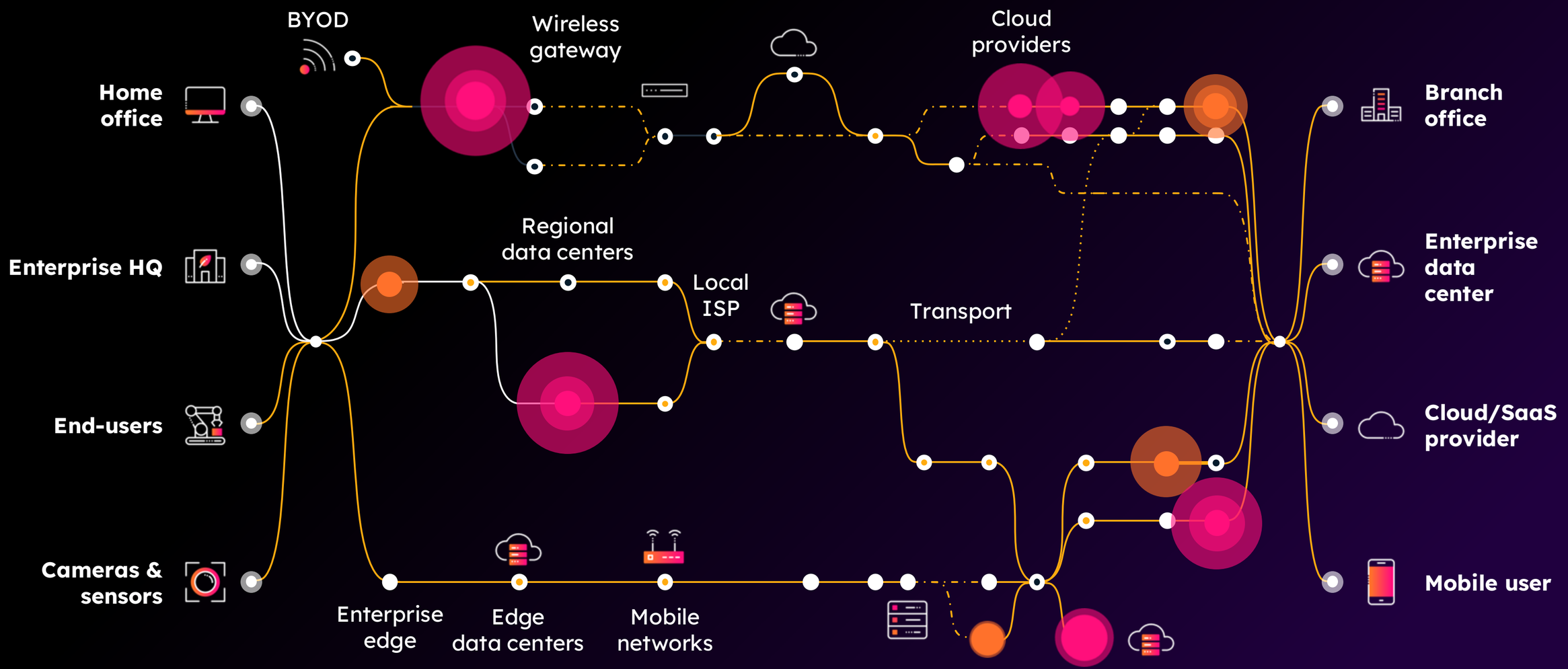
Cisco Data Fabric

- AI-powered data management
- Federated Search and Analytics
- AI-Native Experiences and Platform for AI
- Machine Data Lake

Sources

- Infrastructure
- Applications
- Security
- Users & Devices

Complexity Creates Risk



Cisco Sources

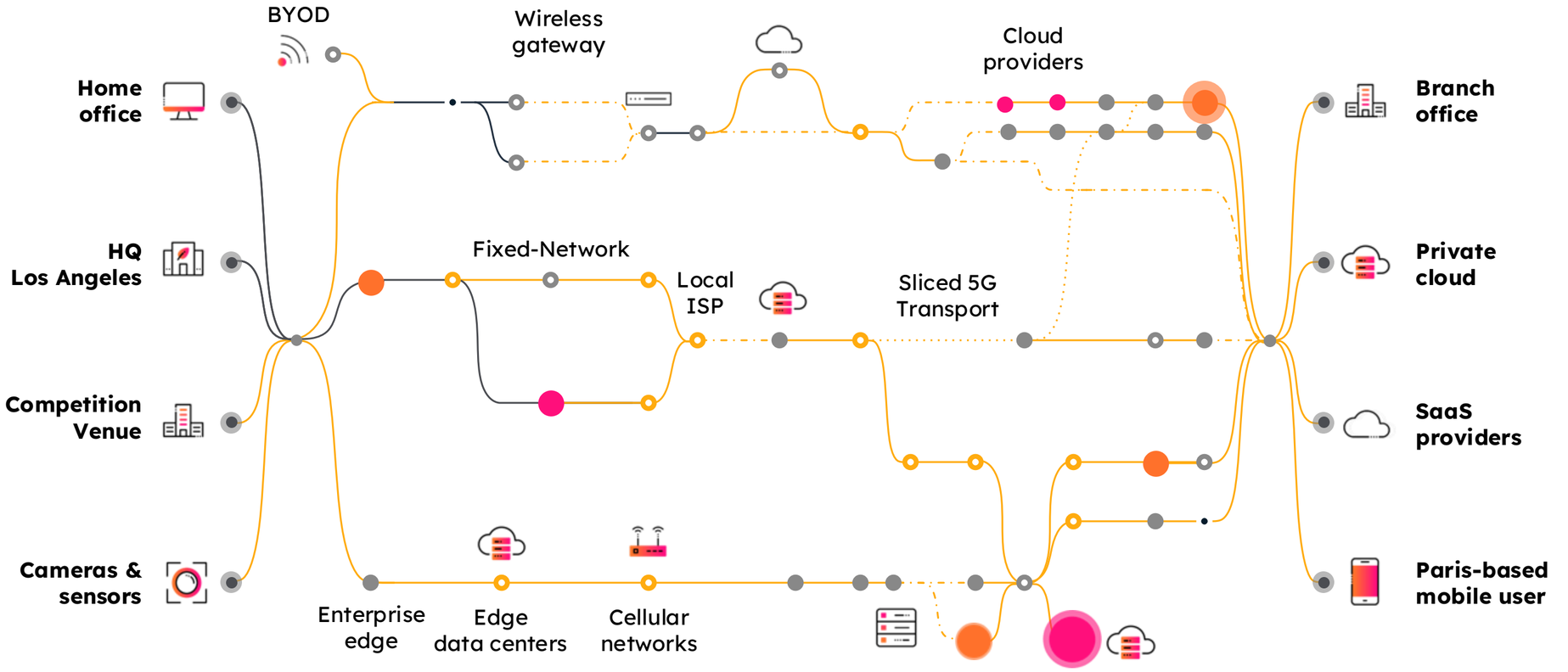
Cloud

Physical Infra

Apps

SaaS

Traditional Workloads



Security

Apps

Network

Custom Apps

Endpoints & Users

Unified AI Agent Orchestration

End-to-End Unified Observability

UF, HEC, OTel

Metrics

Traces

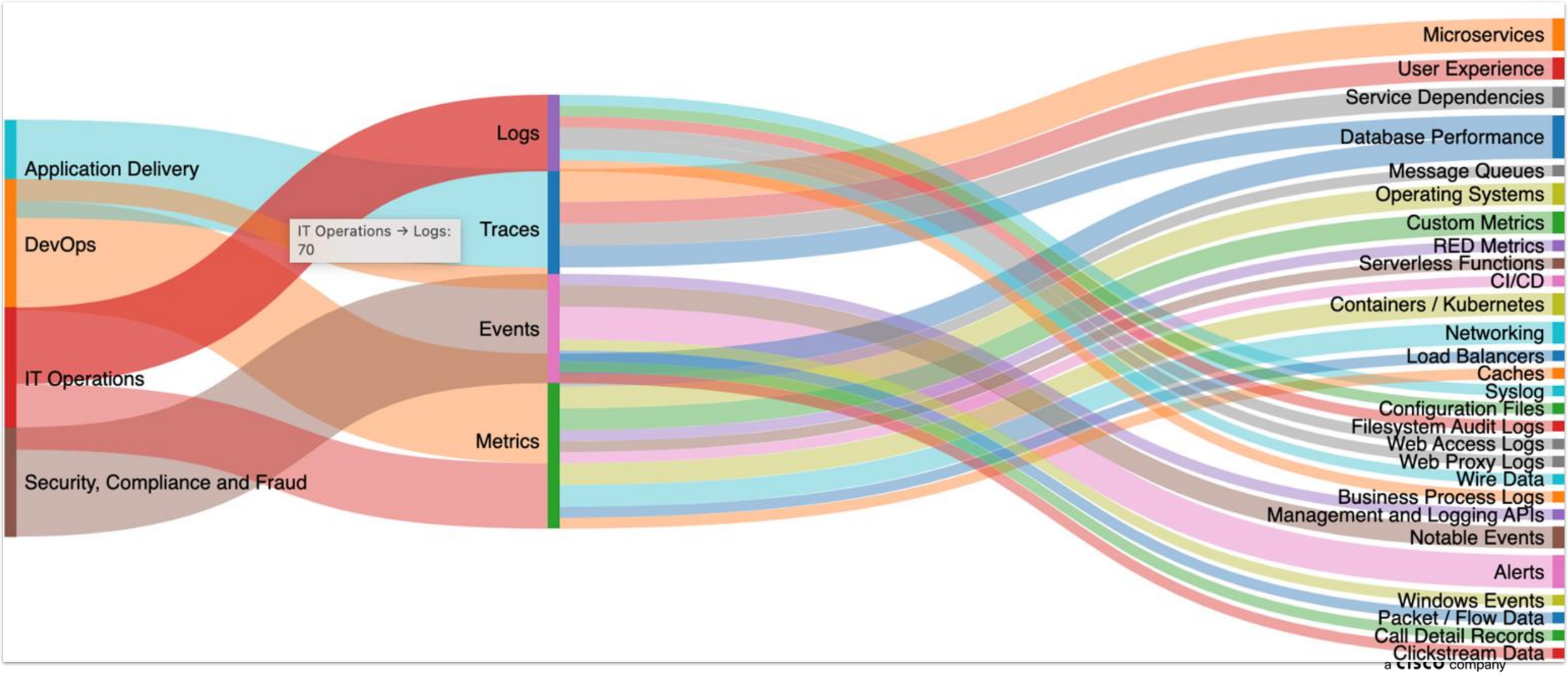
Events

Logs

Monitor	Federated Search & Analytics | Log Observer | Visualization | Reporting | Alerting
Store	Scalable Data Index | Full Fidelity No-Sample Metrics Store | Data Lakes
Collect	Universal Collection | Stream Processing | Filter | Normalize | Aggregate | Enrich | Formatting | Routing | Labeling | Mask

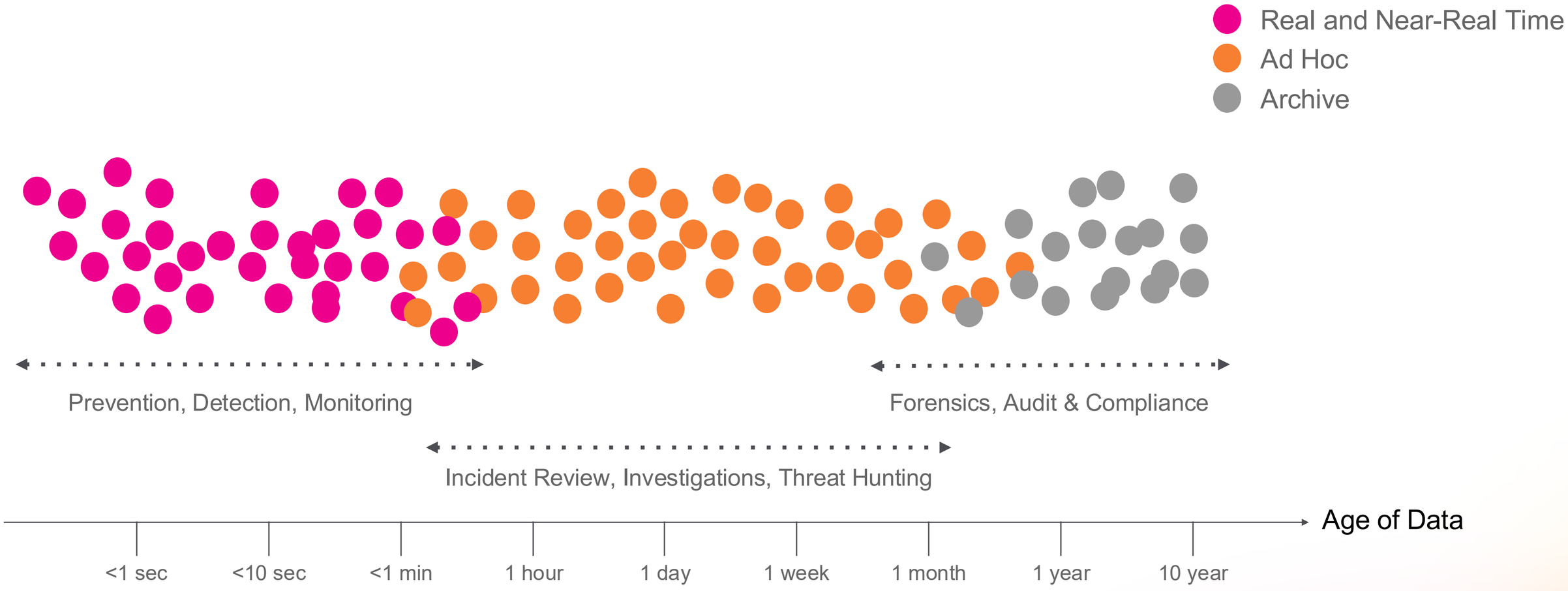
Data Visualization / Prescriptive, Actionable Analytics

Splunk Data Analytics Platform



a cisco company

Optimize Data for Your Use Cases



Chargeback / Showback

splunkbase Collections Apps Find an app Submit an app Log In

Main Page / Apps / Splunk App for Chargeback

Splunk App for Chargeback

The Splunk App for Chargeback aids customers in both Splunk Enterprise and Splunk Cloud Platform to better understand their license usage by categorizing it usage by business units and departments.

Built by Splunk LLC

Log in to Download

Latest Version 2.0.58
October 27, 2025

Compatibility
Splunk Enterprise, Splunk Cloud
Platform Version: 10.0, 9.4, 9.3, 9.2, 9.1, 9.0
CIM Version: 6.X, 5.X

Rating
4 ★★★★☆ (9)
Log in to rate this app

Support
Splunk Supported App
Learn more

Ranking
#19 In Business Analytics

1. Input Filters

2.1 Business Units Usage in the last : -1d@d

	Business Unit	SVC Usage	Ingestion (GB)	DDAS Usage (GB)	DDAA Usage (GB)	Business Description	Business Owner	Business Email
1	Global Information Security	70.56 SVCs	34.82 GB	1,264.18 GB	856.60 GB	Threat Defense and Response	SVP, Chief Information Security Officer	support@splunk.show
2	Global IT Operations	29.82 SVCs	16.47 GB	193.75 GB	475.57 GB	Network infrastructure	SVP, IT Operations	support@splunk.show
3	Global Marketing	11.24 SVCs	33.08 GB	538.86 GB	998.60 GB	Growth Marketing	SVP, GTM Operations	support@splunk.show
4	Global Support	9.25 SVCs	56.52 GB	804.40 GB	634.49 GB	Education Ecosystem Development	SVP, Chief Customer Officer	support@splunk.show
5	Global Sales	7.40 SVCs	16.20 GB	757.06 GB	765.46 GB	Sales Engineering	SVP, Chief Revenue Officer	support@splunk.show

Organization SVC Usage

128.3 SVCs

Organization Ingestion

157.08 GB

Organization DDAS Usage

3,558.25 GB

Organization DDAA Usage

3,730.71 GB

Click on any Business Unit to see Department Details --> Selected Business Unit: Global Information Security

2.3 Departmental Breakdown for Business Unit: Global Information Security

Note: This is a static table and updates daily (The above time selector does not apply here)

	Business Unit	Department	SVC Usage	Ingestion (GB)	DDAS Usage (GB)	DDAA Usage (GB)	Start Period	End Period
1	Global Information Security	Security Engineering and Architecture	37.94 SVCs	0.16 GB	118.16 GB	138.58 GB	Sun Aug 13 2023 00:00	Sun Aug 13 2023 00:00
2	Global Information Security	Threat Defense and Response	16.28 SVCs	29.30 GB	1,034.43 GB	254.15 GB	Sun Aug 13 2023 00:00	Sun Aug 13 2023 00:00
3	Global Information Security	Identity and Access Management	8.42 SVCs	0.01 GB	0.52 GB	145.54 GB	Sun Aug 13 2023 00:00	Sun Aug 13 2023 00:00
4	Global Information Security	Risk and Compliance	7.15 SVCs	5.35 GB	111.06 GB	318.34 GB	Sun Aug 13 2023 00:00	Sun Aug 13 2023 00:00

CLOUD STORAGE HOME

1. Ingestion | 2. Ingestion Forecasting | 3. Splunk Cloud Storage (DDAS) | 4. Splunk Cloud Archiving (DDAA)

1. Daily Ingestion Inputs

2.1 Daily Ingestion By Index, B-Unit & Department

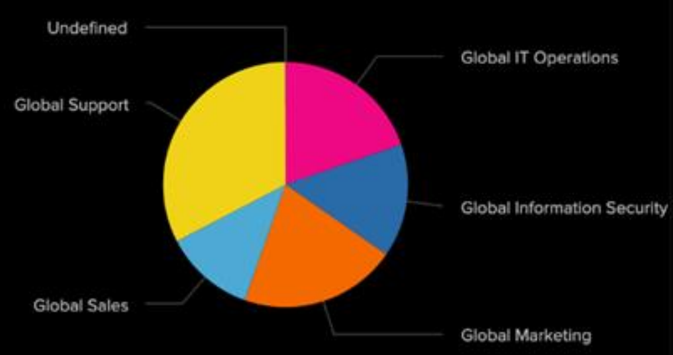
	B-Unit	Department	Time_Period	Index	Sourcetype	% Ownership	Ingestion Index GB	In
1	Global Support	Education Ecosystem Development	Sat Aug 19 2023	epnet	juniperfw_srx	100 %	30.06 GB	
2	Global Support	Education Ecosystem Development	Thu Aug 17 2023	epnet	juniperfw_srx	100 %	30.06 GB	
3	Global Support	Education Ecosystem Development	Fri Aug 18 2023	epnet	juniperfw_srx	100 %	30.06 GB	
4	Global Support	Education Ecosystem Development	Sun Aug 20 2023	epnet	juniperfw_srx	100 %	29.66 GB	
5	Global Support	Education Ecosystem Development	Mon Aug 21 2023	epnet	juniperfw_srx	100 %	29.66 GB	
6	Global Support	Education Ecosystem Development	Tue Aug 22 2023	epnet	juniperfw_srx	100 %	29.65 GB	
7	Global Support	Education Ecosystem Development	Wed Aug 23 2023	epnet	juniperfw_srx	100 %	29.63 GB	
8	Global Marketing	Growth Marketing	Thu Aug 17 2023	netvpn	vpn.ciscosa	100 %	24.02 GB	
9	Global Marketing	Growth Marketing	Fri Aug 18 2023	netvpn	vpn.ciscosa	100 %	24.02 GB	
10	Global Marketing	Growth Marketing	Sat Aug 19 2023	netvpn	vpn.ciscosa	100 %	24.02 GB	

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Avg Daily Ingestion in GB	Unit Cost / GB	Avg Daily Cost	Avg Yearly Cost
151.61 GB	0.11 USD	17 USD	6,087 USD

2.2 Total Ingestion By biz_unit

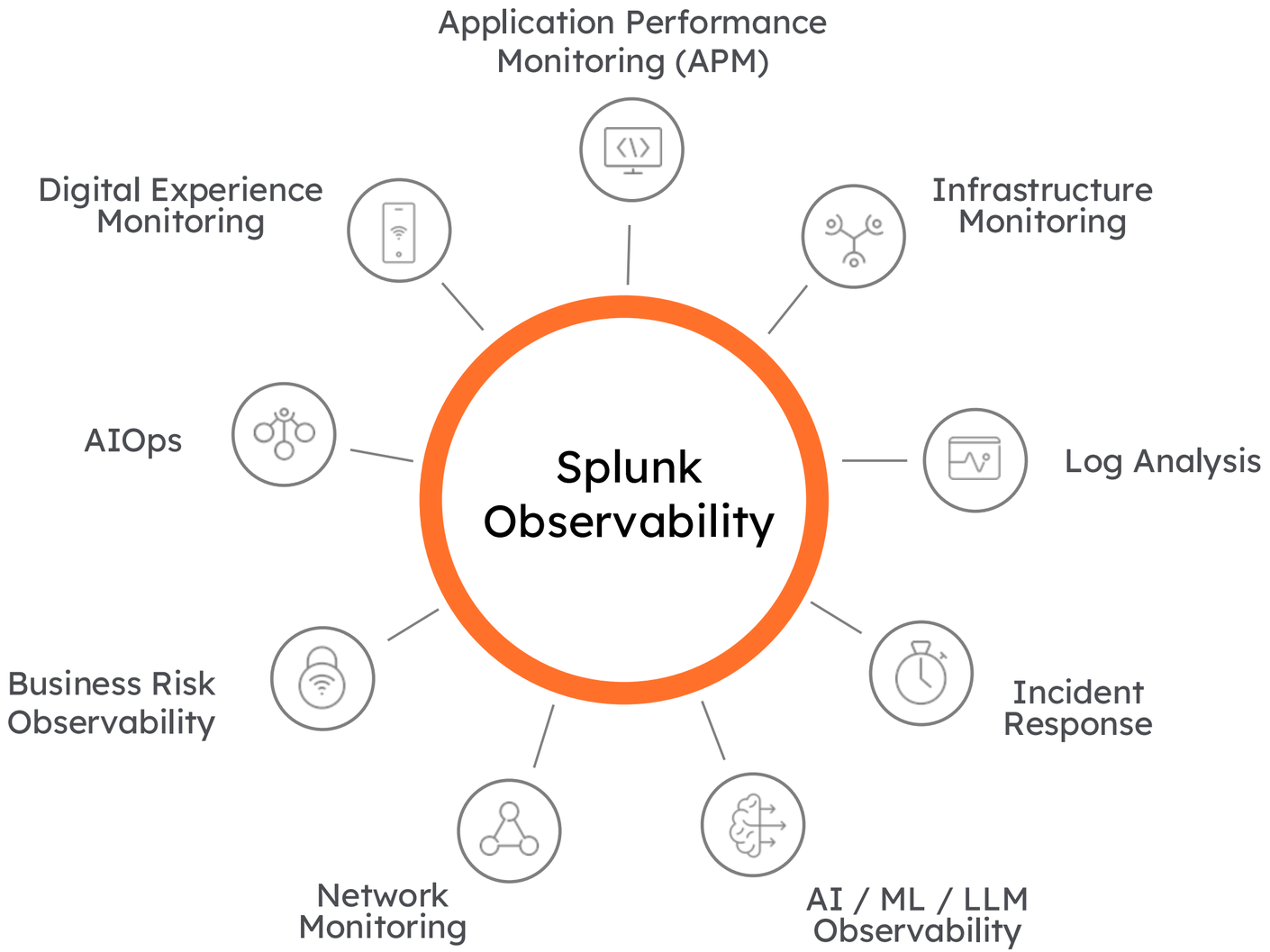
1. Split By: B-Unit



ORG INGEST Entitlement	ORG INGEST Yearly Cost
500.00 GB	20,075 USD

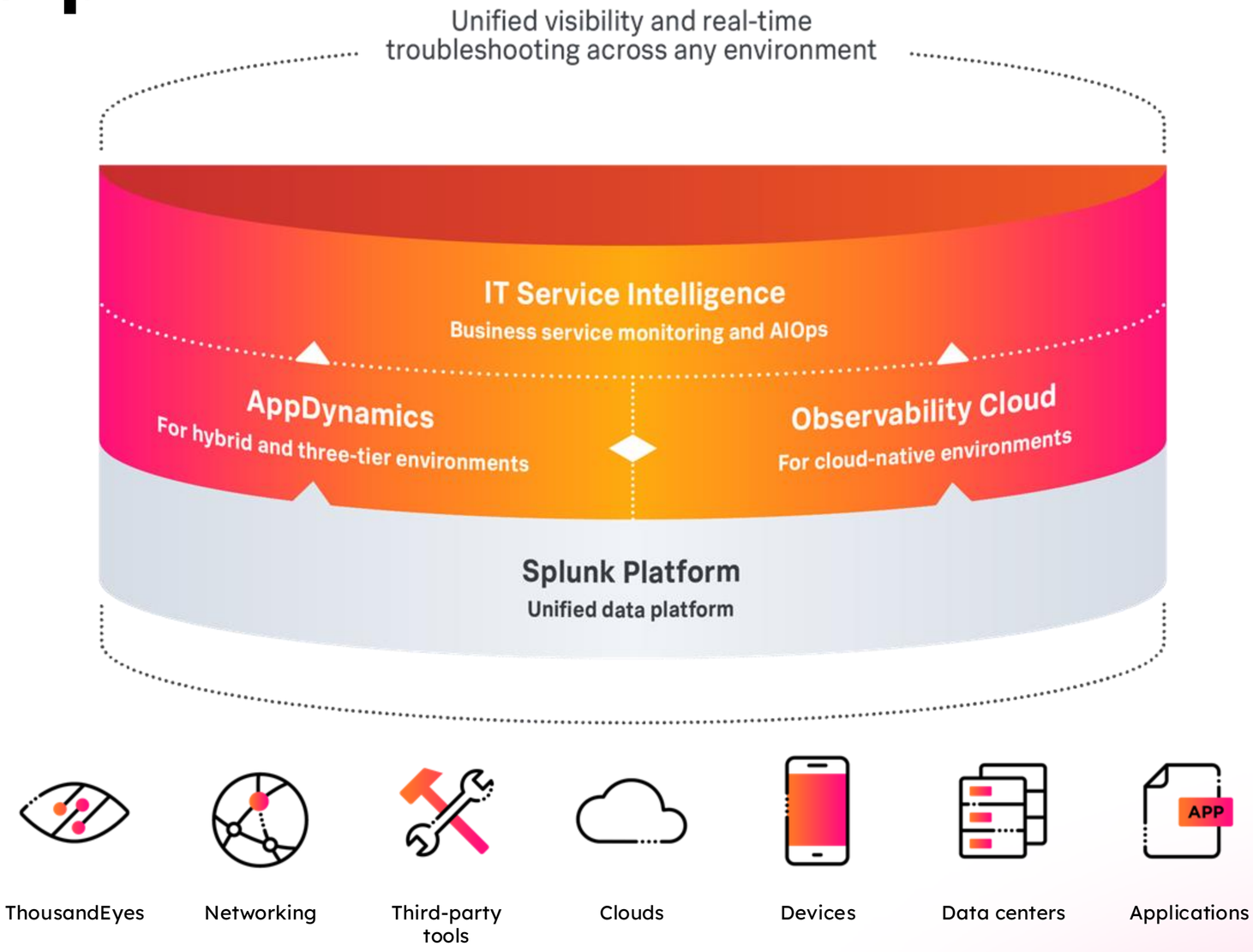
Observability

Splunk Observability



- Real-Time Insights
- AI Powered
- Enterprise Grade
- Open Telemetry Native
- Extensible
- Cross MELT
- Business Context

Complete visibility across your entire digital footprint



The path to greater digital resilience.

Foundational Visibility

See across environments

Security
SecOps

Search, monitor and investigate for real-time security monitoring

Observability
ITOps and Engineering

Troubleshoot mission-critical apps and infrastructure

Guided Insights

Detect threats and investigate issues with context

Reduce noise, detect more threats and identify risk with AI/ML powered detections

Prioritize issues based on business impact

Proactive Response

Get ahead of issues

Accelerate incident investigations and response using automation

Prevent outages & accelerate MTTR with guided root cause analysis

Unified Workflows

Increase operational efficiency

Maximize SOC productivity with integrated threat detection, investigation and response

Standardize observability practices across teams

Enabled by data
Accelerated by Splunk AI

Efficiency in Government

Use Case Domains

Splunk Is More Than Just a Security Solution; Splunk Solves Your Data Problems

Cost Efficiency

Detecting duplicate software licenses, unused cloud resources, and unnecessary spending.

Fraud, Waste, Abuse Prevention

Real-time detection of procurement fraud, misuse of resources, and financial irregularities.

Employee & Office Management

Securing remote workers, managing return-to-office logistics, and maintaining productivity.

Operational Resilience

Ensuring critical services remain available and reliable.

Use Cases

1. Finding Unused or Duplicate Software Licenses
2. Reducing Cloud & IT Infrastructure Waste
3. Detecting and Preventing Fraud & Financial Abuse
4. Automating Compliance Audits & Reporting
5. Improving Citizen-facing Digital Services (Websites, Portals)
6. Enhancing Remote Workforce Productivity & Security
7. Optimizing Campus and Workplace Resource Use (Rooms, Labs, Equipment)
8. Proactively Preventing Downtime of Critical Systems
9. Simplifying IT Modernization & Legacy System Management
10. Tracking and Improving Employee Productivity (e.g., easily monitor key productivity tools)
11. Reducing Energy and Utility Costs (real-time monitoring to identify unnecessary energy consumption)
12. Identifying Unused or Underused Hardware and Devices (quickly spot equipment sitting idle)
13. Simplifying Helpdesk & IT Ticket Management (reduce service desk workload through proactive alerts)
14. Real-time Visibility into Application Performance (ensure critical applications run smoothly, saving on downtime costs)
15. Streamlining Compliance Reporting (automatically prepare audit-ready reports)
16. Detecting Shadow IT Spending and Unauthorized Apps (control rogue IT spend immediately)

Data Sources per Domain

Domain	Use Case	Tier 1 Signals (IT System Logs & Unstructured Data)	Tier 2 Signals (Structured Business Data)	Key Metrics / KPIs
Fraud, Waste, Abuse, Inefficiency	**Finding Unused or Duplicate Software Licenses**	Software inventory logs, License server logs, Endpoint logs	Software license purchases, contracts, license allocations	Number of duplicate licenses, Cost savings from license consolidation
	Reducing Cloud & IT Infrastructure Waste	Cloud infrastructure logs (AWS, Azure, GCP), Server usage logs	Cloud billing and financial data, Infrastructure inventory records	Unused resources identified, Cost reduction percentage
	Detecting and Preventing Fraud & Financial Abuse	Financial transaction logs, Network logs, System access logs, Identity, Web, behavior	Financial transaction databases, Payroll and procurement data	Fraud incidents prevented, Value of fraud prevented
	Automating Compliance Audits & Reporting	Security event logs, Access logs, Compliance system logs	Compliance audit records, Regulatory reporting data	Time/cost reduction in audits, Compliance violation reduction
	Detecting Shadow IT Spending and Unauthorized Apps	Firewall/proxy logs, DNS logs, Network access logs	Procurement records, Credit card transactions, Expense reports	Shadow IT incidents detected, Unauthorized spend avoided
Employee & Office Management	**Enhancing Remote Workforce Productivity & Security**	VPN logs, Endpoint security logs, User authentication logs	Employee productivity data (O365, G Suite), HR system records	Productivity improvement %, Remote security incident reduction
	UberAgent Utilization (Citrix Environments)	Citrix session logs, Endpoint performance logs	Employee remote session data, User experience surveys	User experience improvement, System latency reduction
	Optimizing Campus and Workplace Resource Use	Access control system logs, Room utilization sensors/logs, Wi-Fi logs	Room booking system data, Facility management records	Facility usage efficiency, Resource cost savings

Data Sources per Domain

Domain	Use Case	Tier 1 Signals (IT System Logs & Unstructured Data)	Tier 2 Signals (Structured Business Data)	Key Metrics / KPIs
Operational Resilience	**Improving Citizen-facing Digital Services**	Website logs, API logs, Application error logs	Citizen engagement metrics, Service availability records	Reduced downtime incidents, Improved user satisfaction
	Proactively Preventing Downtime of Critical Systems	System/application performance logs, Infrastructure logs, Event logs	Incident management system data, Service-level agreement (SLA) records	Reduced outage frequency, Downtime duration reduction
	Simplifying Helpdesk & IT Ticket Management	Helpdesk logs, System alerts/logs, Endpoint logs	ITSM (IT Service Management) data, Ticketing records	Ticket resolution time reduction, Ticket volume decrease
	Real-time Visibility into Application Performance	Application performance monitoring (APM) logs, Transaction logs	User experience data, Application SLA data	Reduced application latency, Higher availability %
Cost Efficiency	**Simplifying IT Modernization & Legacy System Management**	Legacy system logs, Application logs, Migration logs	Asset management data, Project management records	Reduced legacy system costs, Accelerated modernization timelines
	Tracking and Improving Employee Productivity	Endpoint usage logs, Application access logs	Productivity tool usage data (O365 analytics), HR data	Productivity tool adoption rates, Employee output metrics
	Reducing Energy and Utility Costs	Facility management sensor logs (IoT), HVAC system logs, Lighting control logs	Utility billing data, Facility operational costs	Energy usage reduction %, Operational cost savings
	Identifying Unused or Underused Hardware and Devices	Network device logs, Endpoint inventory scans, Asset tracking logs	Hardware inventory databases, Asset purchase records	Asset utilization improvement, Hardware cost avoidance

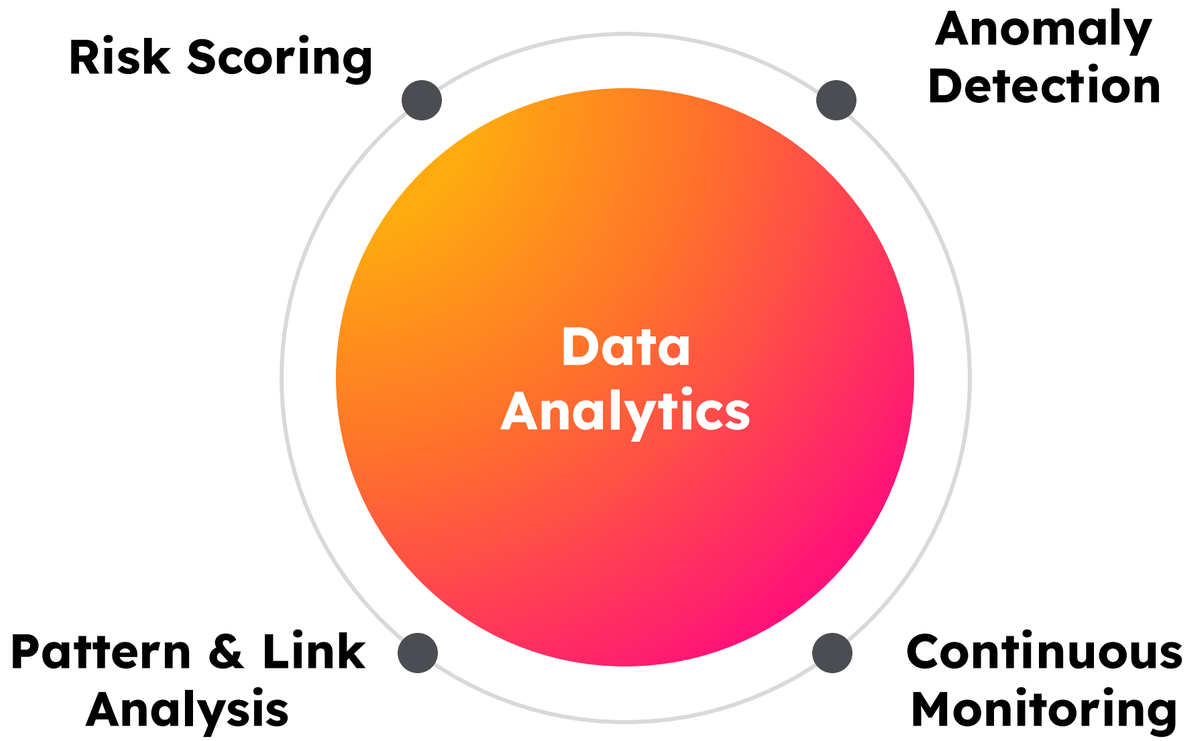
Splunk's Approach to Fraud Analytics

splunk> a CISCO company

Anti-Fraud Triad

- Build for the future.
- Unstructured and structured data analytics.
- Data is key.

Methodologies and Approaches

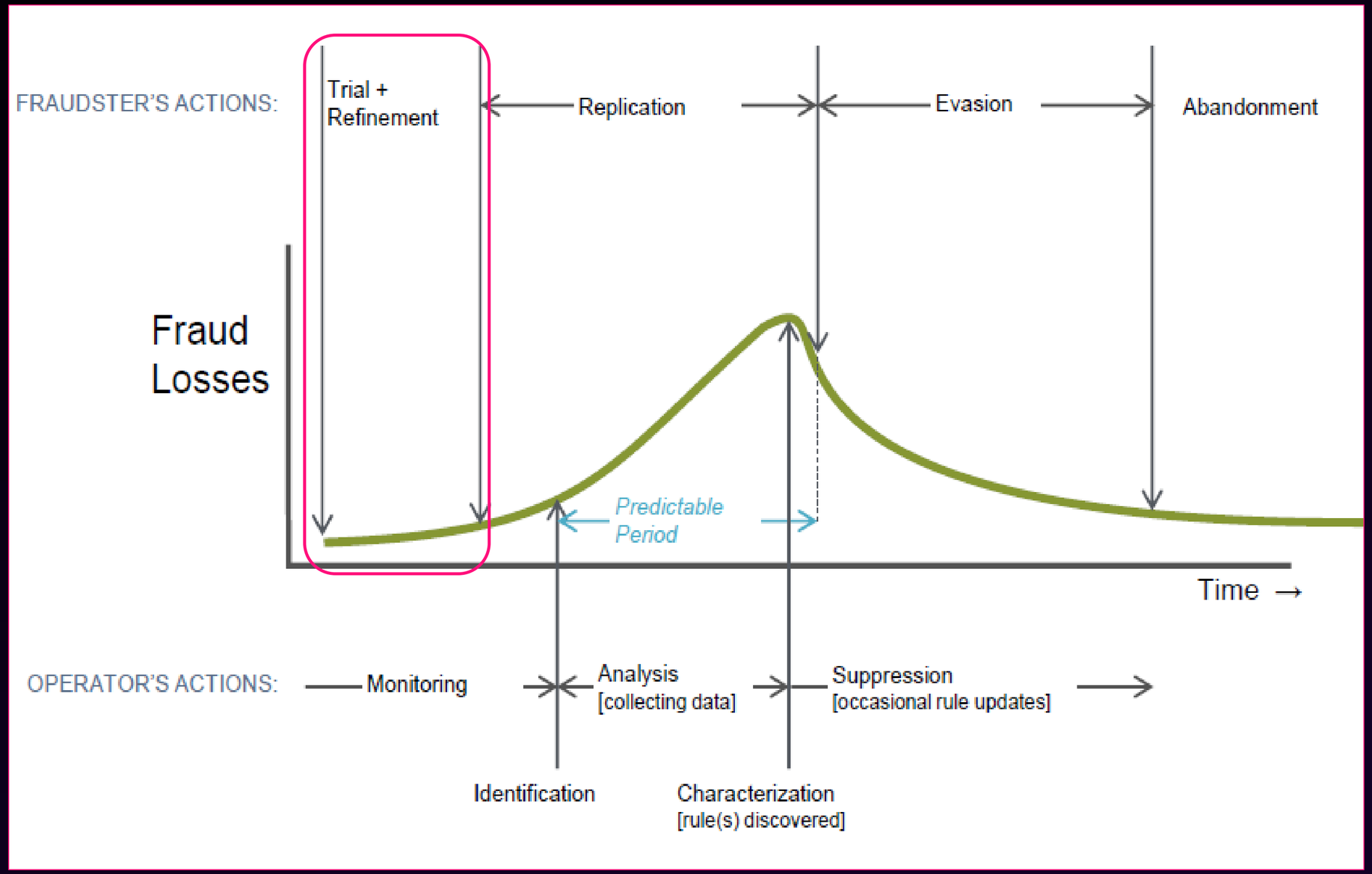


Monitor activity in the Trial + Refinement phase.

1. **Monitor user identity.**
2. **Monitor endpoint identity.**

3. **Monitor user behavior.**
4. **Monitor endpoint behavior.**

Find anomalies and risks.



splunk> a CISCO company

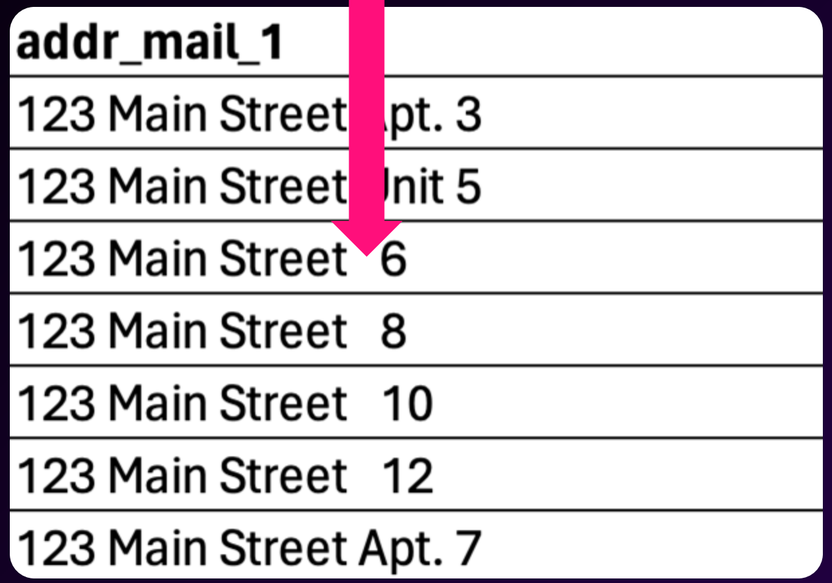
Risk Indicator Found

Claim records contained two spaces in the physical address field

Two spaces (%20 or 0x20) in `mail_street_address` field.

StreetXAddress **StreetXXAddress**

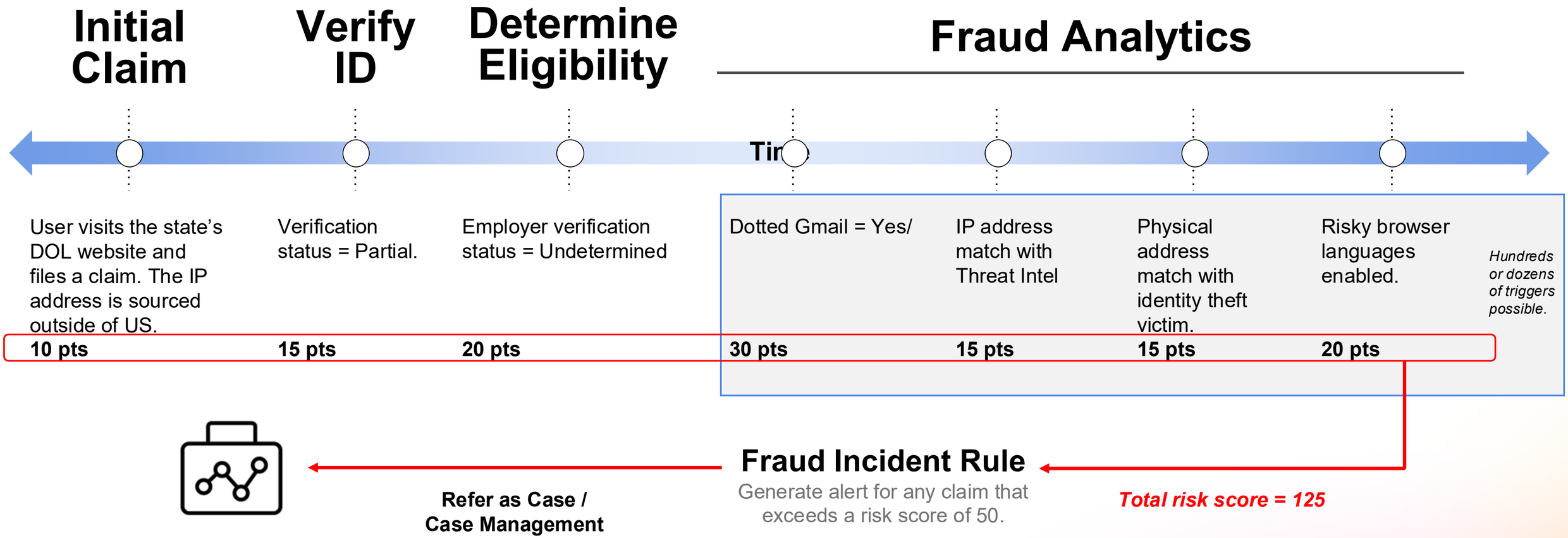
Two Spaces



addr_mail_1
123 Main Street pt. 3
123 Main Street Unit 5
123 Main Street 6
123 Main Street 8
123 Main Street 10
123 Main Street 12
123 Main Street Apt. 7

Risk-Based Claims Analysis

Accumulating risk per claim, account, or application over a period of time.

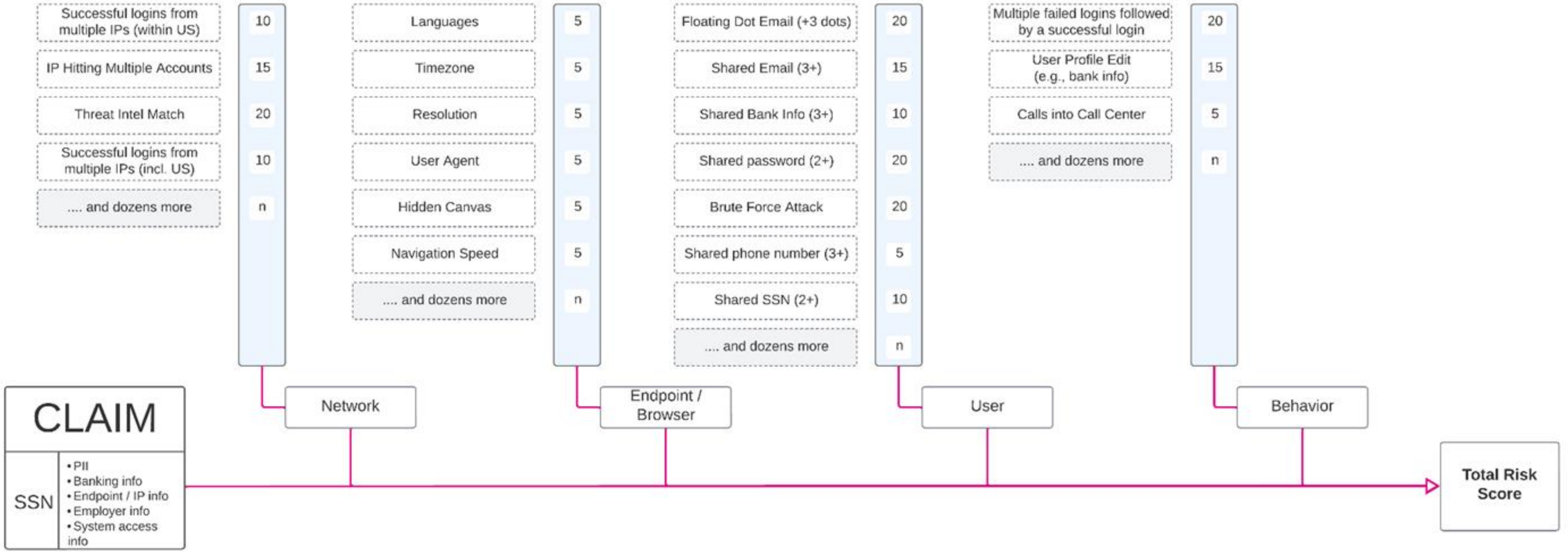


Fraud Detection and Prevention

Updated: December 20th, 2022

Updated/Reviewed by: Chris Perkins (SA)

Fraud Detection Mechanisms

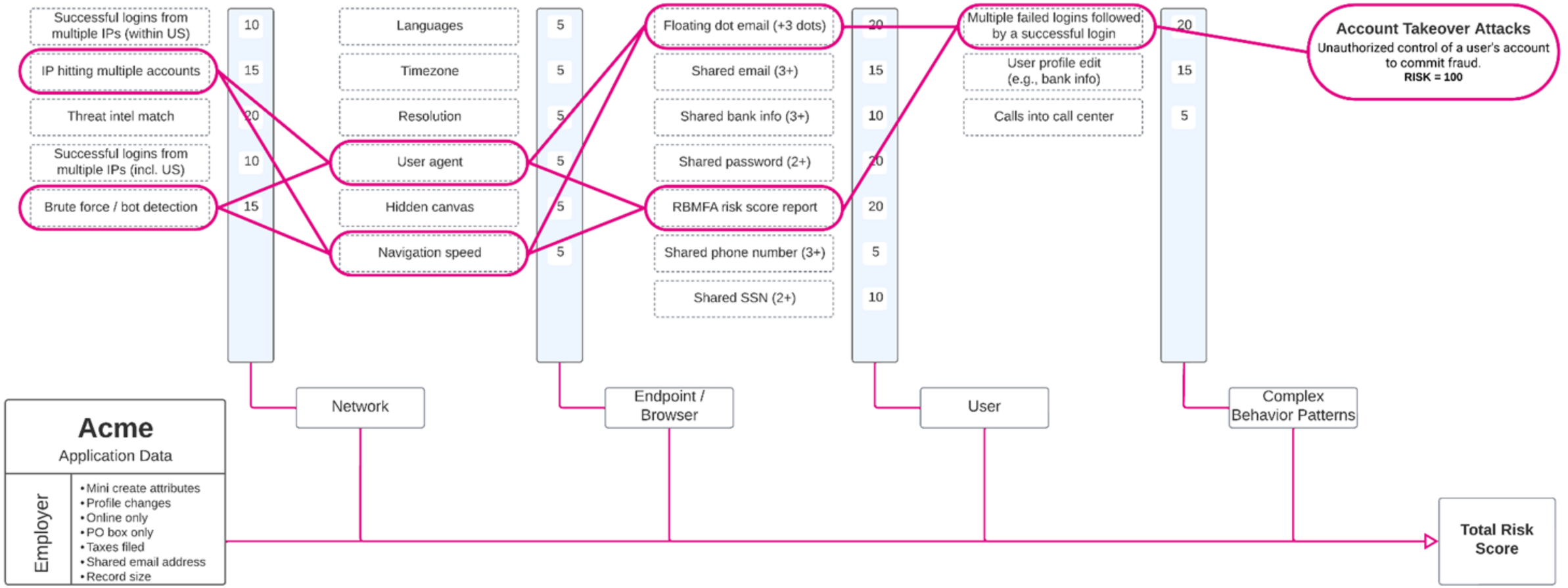


Applied Analytics for Anomaly Detection and Fraud Prevention

Updated: November 6th, 2023

Updated/Reviewed by: Chris Perkins (Splunk)

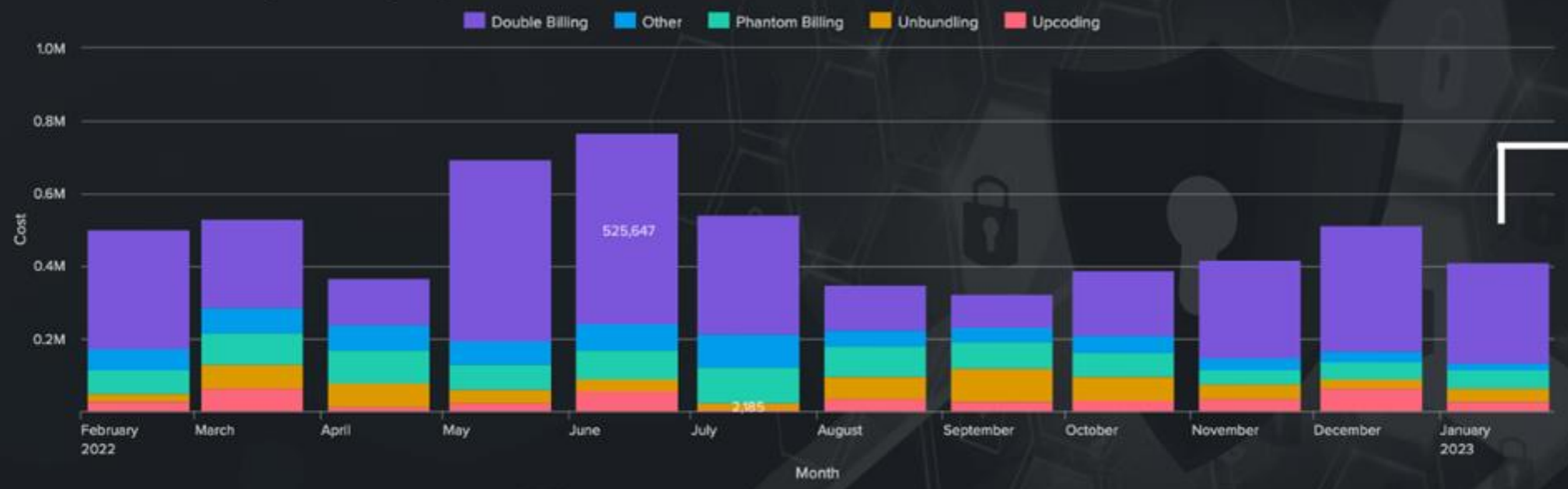
Account Takeover Attacks and Bot Detection Use Case



Medical Billing Fraud

Medical billing fraud is the number one most targeted by criminals today due to the high volume of money exchanged. Medicare, Falsified/Double Billing (Phantom), Unbundling and Upcoding Forgery are some of the many types of fraud committed today.

Cost Of Fraud By Category For Last 12 Months



Current Month Summary Of Fraud

Percentage of overall cost of medical fraud by each prominent category.

Double Billing

This is when a provider bills multiple times for the same medical services. Sometimes providers bill the same party (e.g., the government) multiple times for the same services. To avoid detection, they can alter the date of the service, its description, or the name of the patient or provider.

$3,328,571 Total Cost Over 12 Months

$665,714 Savings Mitigated By Splunk

57% % Of Total Cost

Upcoding

Upcoding occurs when a healthcare provider submits codes for more severe and expensive diagnoses or procedures than the provider diagnosed or performed.

$420,474 Total Cost Over 12 Months

$243,875 Savings Mitigated By Splunk

7% % Of Total Cost

Other

Using bogus marketing ploys to convince individuals to disclose their health insurance, identity theft or impersonations.

$632,930 Total Cost Over 12 Months

$259,501 Savings Mitigated By Splunk

10% % Of Total Cost

Phantom Billing

In the phantom billing scam, patients are billed for services never performed and sent an explanation of benefits that are usually discarded. Without notice from patients, insurers may be unaware they are being defrauded.

$846,628 Total Cost Over 12 Months

$135,460 Savings Mitigated By Splunk

15% % Of Total Cost

Unbundling

"Unbundling" is a form of medical billing fraud that is similar to upcoding. In unbundling, medical providers bill complex, multi-step procedures separately, instead of as one coded procedure. Billing the steps individually allows the provider to recover more reimbursement for the same services.

$572,883 Total Cost Over 12 Months

$234,882 Savings Mitigated By Splunk

10% % Of Total Cost

Total Fraud Cost For Period

$5,801,486

Total Savings Mitigated By Splunk

$1,536,432

splunk>

Splunk Adoption & Professional Services

Immediate Acceleration and Increased Accuracy

Rapidly deploy Splunk to enhance speed and accuracy, driving immediate operational improvements.

Capability Expansion

Leverage Splunk's advanced functionalities to extend capabilities and derive deeper insights from your data.

Sustainable Growth

Embed data analytics into your organization's strategic planning to ensure long-term sustainability and continuous innovation

Scale and Elevate Data Analytics' Impact Organization-Wide

Amplify Splunk's benefits by scaling its deployment and fostering a data-driven culture throughout the organization.

Continuous Optimization and Governance

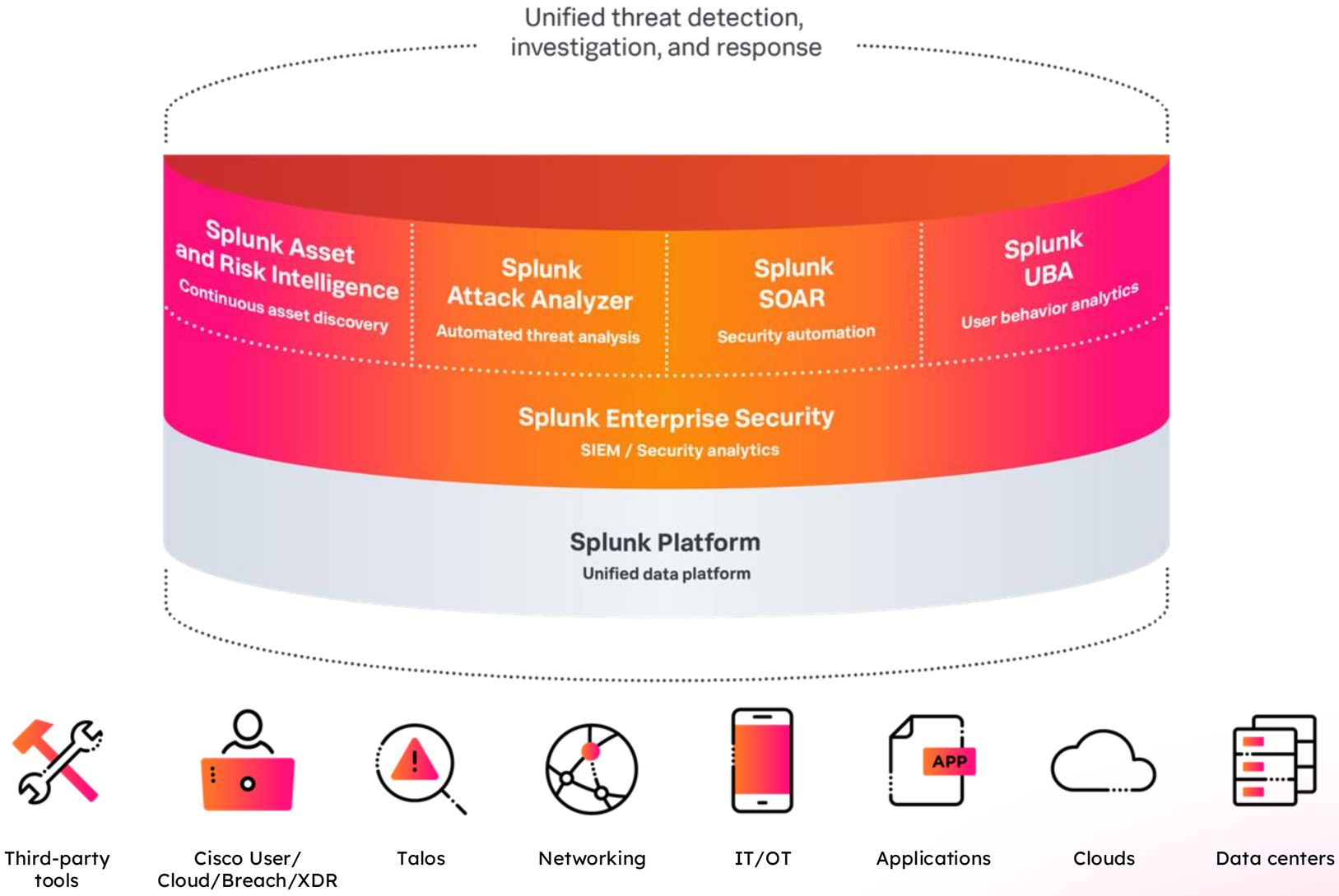
Establish robust management and governance practices to maintain program effectiveness and ensure long-term success.

1st Project (4 weeks to 12 months)

Adoption (Iteration)

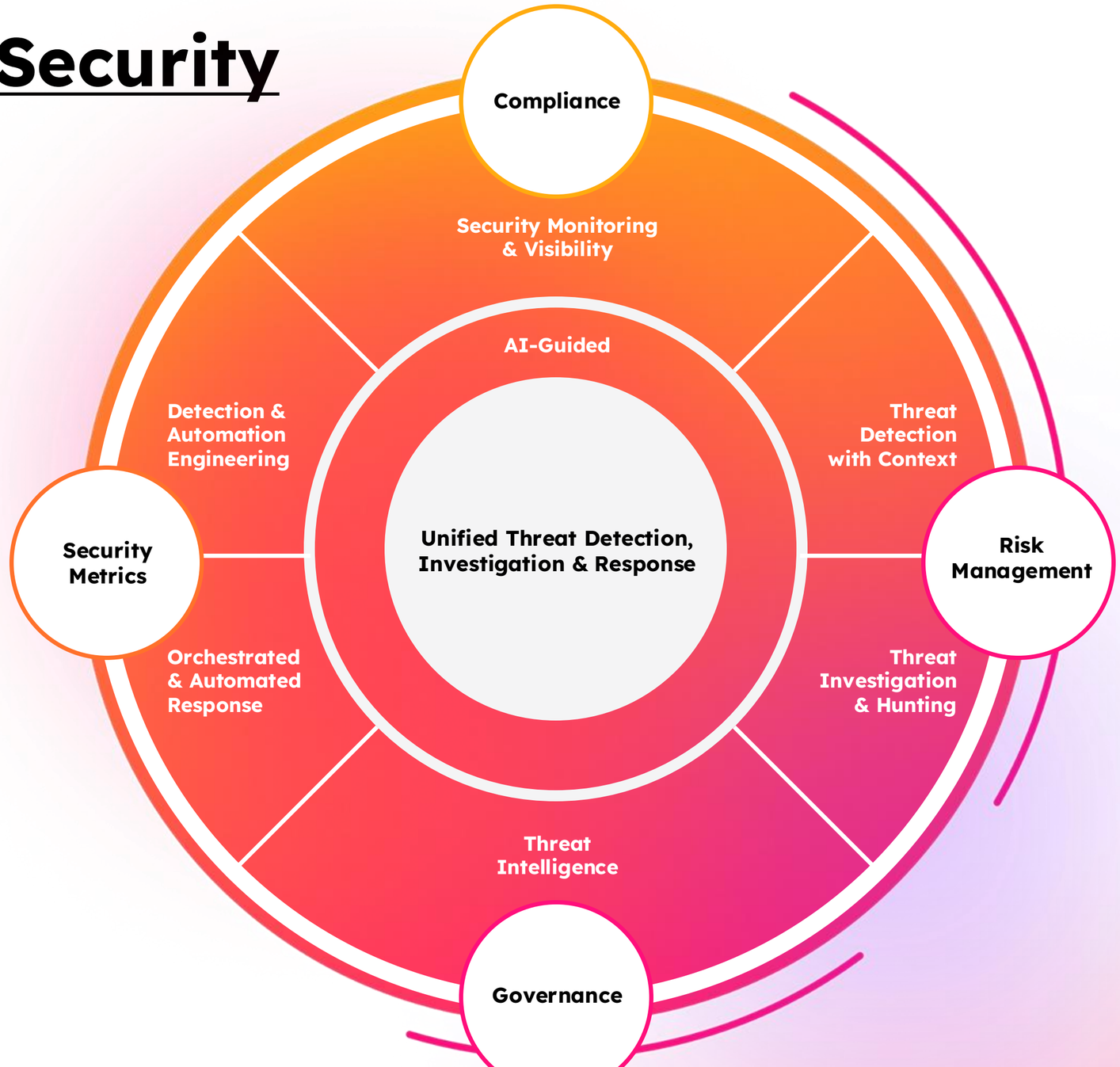
Security

Powering the SOC of the future with the leading TDIR solution



Splunk Enterprise Security

- Detect What Matters
- Investigate Holistically
- Respond Rapidly



Delivering the essential elements of a Unified TDIR Platform

The foundation for the SOC of the future

Flexible Deployment Models

Unified Analyst Experience
Workflows | Case Management | Collaboration

Threat Detection
Static | Dynamic (ML) | Pre-Built | Custom | Authoring

Investigation
Risk-Based Alerting | Threat Hunting | Integrated Analytics

Response
Enrichment | Automation | Orchestration | Playbooks

GenAI for SecOps
Summarization | Natural Language Search | Reporting

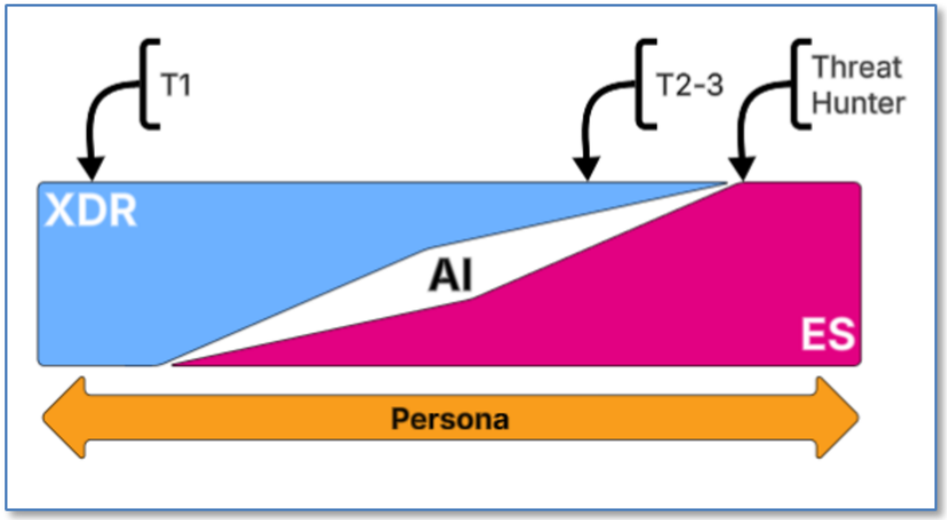
Common Services
Threat Intelligence | Assets & Identities | Risk Intelligence

Data Management & Federation
Filter | Mask | Route | Access

True Multi-Vendor

Logs **Events** **Alerts** **Telemetry**

Future of Security Operations



Persona	Console	Why
Tier 1 Analyst	Cisco XDR	Curated incidents with AI-generated summaries; fastest containment
Tier 2-3 & Threat Hunter	Splunk ES	Full historical data access; advanced correlation and search
Incident Response Lead	Cisco XDR (live), Splunk ES (retrospective)	Coordinates immediate containment, then assembles comprehensive evidence
Compliance Officer / Auditor	Splunk ES	Runs regulatory reports and attestation
SOC Engineer	Both (Admin)	Tunes detections, monitors data feeds and APIs

What Each Platform is Really For

Console choice is a policy decision, not an architecture constraint. SOC teams leverage the right tool at the right time.

Focus Area	Cisco XDR	Splunk Enterprise Security (ES)
Primary Mission	Real-time detection and rapid, automated response.	Comprehensive SIEM: collect all data, search thoroughly, retain for compliance audits.
Data Model	Curated incidents: correlated events single incident records	Raw logs ingested "as-is," normalized via Common Information Model (CIM).
Retention	Short-term hot storage (90/180/365 days), optimized for rapid response.	Multi-year retention for extensive audits, compliance, and deep hunting (typically 1-7 years).
Response Actions	Immediate, one-click containment on integrated enforcement points, Cisco and 3rd party	Comprehensive SOAR playbooks integrated across IT, cloud, and security stacks.
AI / ML Assistance	Cisco AI Assistant auto-summarizes incidents, recommends next actions.	Splunk AI Assistants enable natural language queries (SPL), correlation search tuning. AI Toolkit (AITK) supports advanced analytics. Triage Agent.
Data Visualizations	Storyboard with kill-chain timelines, entity graphs, real-time dashboards.	Glass Tables, drill-down dashboards, risk timelines combining security and business metrics, all customizable.

Cisco XDR Data Examples

Immediate Detection and Containment

1. **Real-Time Ransomware Response:**

   Endpoint detection events showing active ransomware encryption behavior require instant host isolation to limit business disruption.

2. **Phishing Attack Mitigation:**

   Email security gateway alerts detecting credential theft attempts trigger immediate, automated email quarantine and recipient alerts.

3. **Command-and-Control (C2) Traffic:**

   Network traffic anomalies indicating malicious external communications activate instant containment actions to prevent lateral movement.

4. **Privilege Escalation on Critical Servers:**

   High-risk behaviors on critical infrastructure detected in real-time trigger automated access revocation and alerts.

5. **Malware Activity on Managed Devices:**

   Immediate containment and remediation are executed when malicious executables are detected on corporate endpoints.

6. **IoT Device Security:**

   Real-time monitoring alerts of compromised IoT devices prompt immediate isolation to protect critical infrastructure and operational continuity.

Splunk Enterprise Security Data Examples

Long-term Investigation and Compliance

1. **Insider Threat Detection:**

   Historical analysis of VPN and remote access logs enables detection of abnormal long-term employee behavior patterns.

2. **Cloud Infrastructure Compliance:**

   Detailed cloud provider logs (AWS, Azure, GCP) retained long-term for regulatory compliance, audit trails, and investigations into unauthorized configurations or access.

3. **Identity Management Audits:**

   Authentication logs stored for years to validate compliance with access management policies and assist in fraud investigations.

4. **Advanced Threat Hunting:**

   Detailed, retained event data facilitates retrospective threat hunting, analyzing indicators that emerged well before active detection.

5. **Data Exfiltration Investigations:**

   Historical network and application logs enable comprehensive forensic investigations into data loss or compromise incidents.

6. **Regulatory Audit and Reporting:**

   Multi-year retention of security and event data fulfills complex regulatory reporting requirements (e.g., GDPR, HIPAA, PCI DSS), providing clear and consistent evidence trails.

7. **Vulnerability Management:**

   Historical tracking and analysis of vulnerabilities, patch management effectiveness, and exposure risks to support compliance reporting, risk mitigation, and proactive remediation strategies.

8. **Supply Chain Security:**

   Analysis of historical vendor access logs and transaction data to detect and investigate risks from third-party integrations and dependencies, ensuring the integrity of the supply chain.

9. **Compliance Violation Investigations:**

   Long-term retention and analysis of policy and access control violations to meet regulatory reporting requirements and support internal governance.

10. **Zero Trust Policy Enforcement Audits:**

    Persistent logging and analysis of network, user, and system access data to validate adherence to zero trust policies, enabling regular auditing and continuous improvement of access control practices.

Data Management

By intentionally and intelligently routing data to the platform where it provides the greatest operational impact and value per dollar, organizations can achieve:

- **Faster Mean Time to Containment (MTTC)**: Immediate, confident response at the first sign of a threat, minimizing business disruption.
- **Reduction in Duplicate Data Storage Costs**: Efficiently storing and processing only the data needed for immediate response and long-term compliance, without sacrificing visibility or depth.
- **Fewer Clicks from Alert to Containment**: Intuitive, integrated workflows featuring seamless, right-click pivots and deep links between Cisco XDR and Splunk Enterprise Security consoles, eliminating unnecessary context switching.
- **Unified Incident Lifecycle Management**: A coherent, continuous workflow from initial threat detection through comprehensive investigation to final compliance reporting—streamlined into a single operational flow.

The End