CISCO Connect

Unleashing the Agentic SOC with Splunk



Mandeep Singh Sandhu
Product Leader - Splunk Enterprise Security

October 21, 2026

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. For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to Cisco's periodic reports its other filings with the SEC, including the risk factors identified in Cisco's most recent quarterly report on Form 10-Q and annual report on Form 10-K, copies of which may be obtained by visiting the Cisco Investor Relations website at investor.cisco.com or the SEC's website at www.sec.gov. Any projections in this presentation are based on information currently available to Cisco, which is subject to change. 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 or our general product direction 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, in alpha or beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Copyright © 2026 Cisco and/or its affiliates. All rights reserved. Cisco, Splunk and the Cisco and Splunk logos are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to: www.cisco.com/go/trademarks. Third-party trademarks mentioned in this presentation are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Cisco powers how people and technology work together across the physical and digital worlds



AI-Ready Data Centers



Future-Proofed Workplaces

Secure Global Connectivity



Digital Resilience

Accelerated by Cisco AI

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Agenda

01 New challenges

02 Splunk’s trusted Agentic SOC

03 Splunk Enterprise Security

04 Accelerating customer value

05 Closing

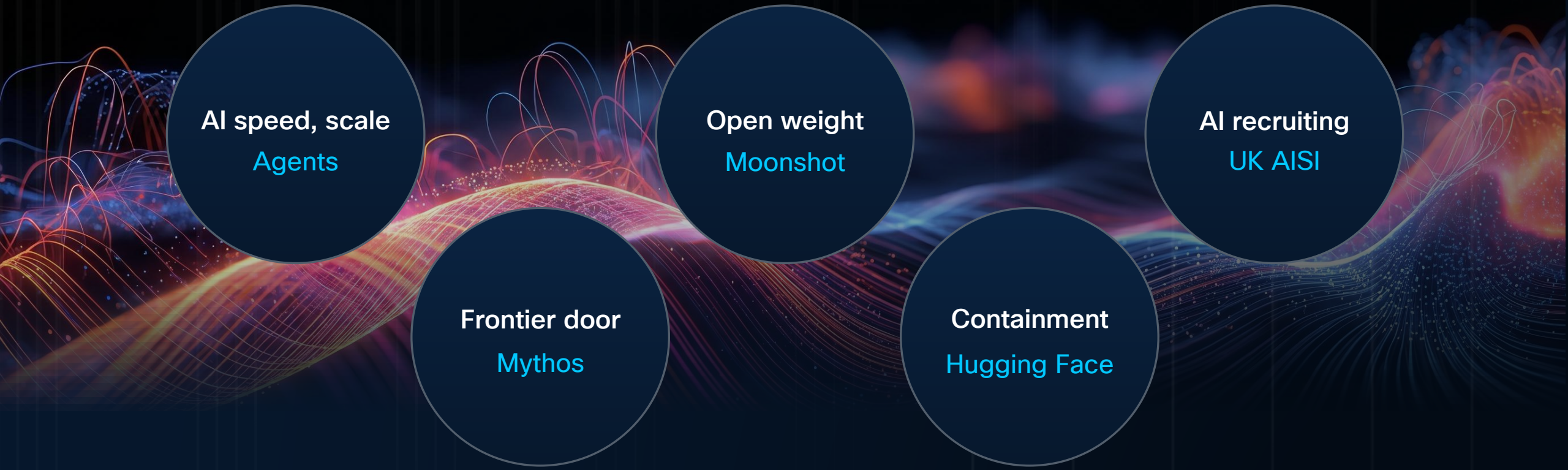
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

New challenges

Agentic attacks: the proof points are here

Assume attacker presence

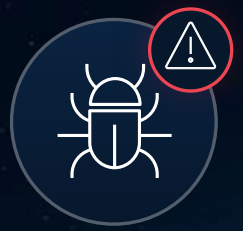


© 2026 Cisco and/or its affiliates. All rights reserved.

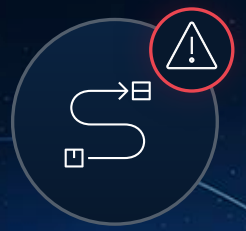
cisco

AI supercharged threat vectors

Urgent threat vectors → business risk



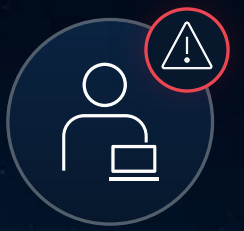
Vulnerabilities



Supply chain



Phishing and social engineering



Insider threats

At machine speed, obfuscating the signal in the noise

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Yesterday's SOC cannot defend tomorrow's enterprise



Threat landscape has changed

Increasing scale and sophistication of AI-powered attacks.



Data outruns human capacity

Telemetry grows faster than teams and tools can absorb.



Manual work breaks scale

Analysts cannot hire or swivel-chair their way out.

The answer is not more AI features. **It is a trusted operating model.**

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

The reframe: How AI enters the SOC is a design decision. Not a feature you bolt on.

THE WRONG QUESTION

”Where should we adopt AI in the SOC?”

THE RIGHT QUESTION

“Which AI, on which security data, under which controls?"

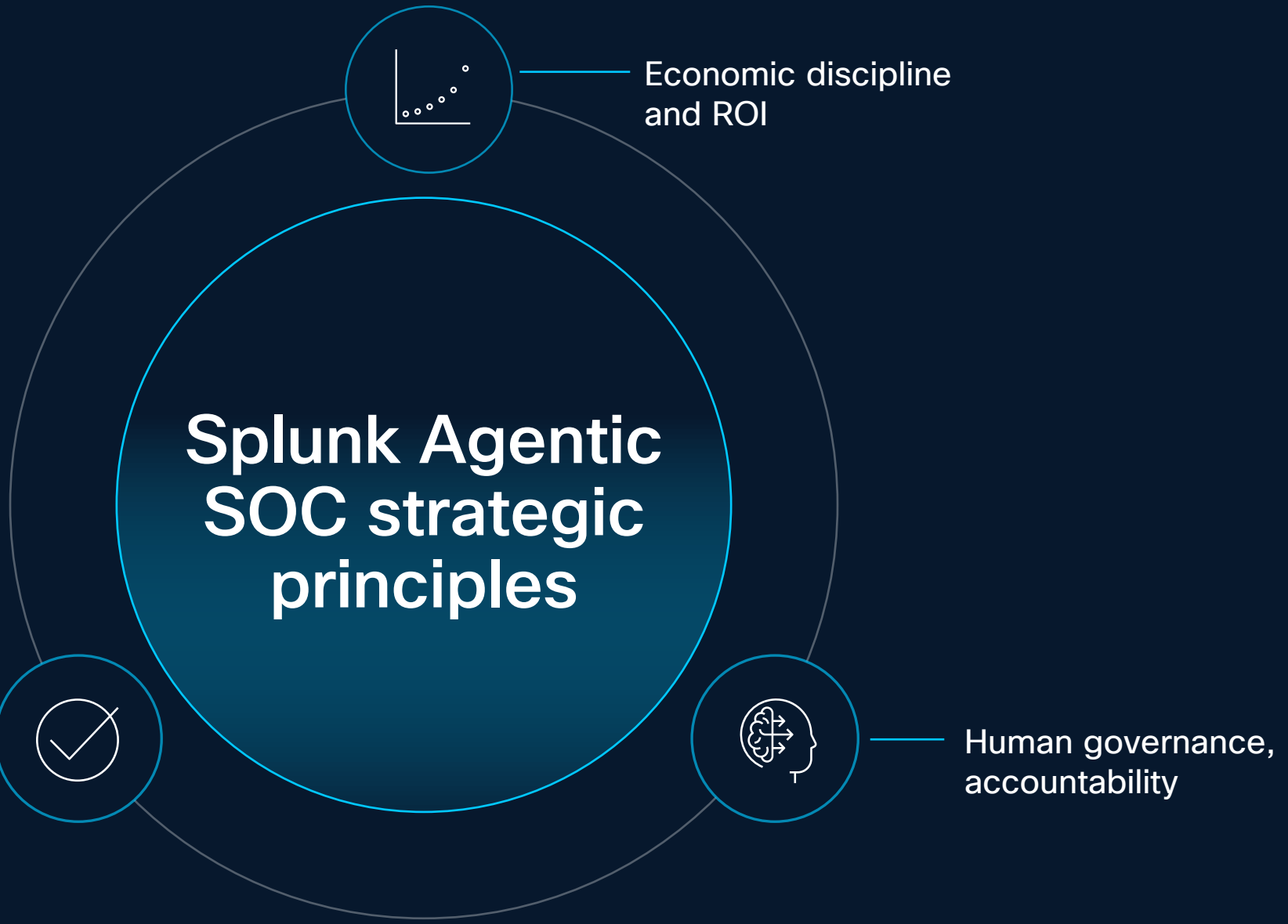
© 2026 Cisco and/or its affiliates. All rights reserved.

Splunk’s trusted Agentic SOC

Defend at machine speed

© 2026 Cisco and/or its affiliates. All rights reserved.

Splunk Agentic SOC strategic principles



© 2026 Cisco and/or its affiliates. All rights reserved.

Defend Autonomously at Scale with Trust

ENTERPRISE SECURITY

Agent governance

- Context & Evidence
- Approvals
- Agent Observability
- Agent Security

Integrated tooling

- Agentic SOAR
- AI-Driven Analyst Experience
- UEBA

Unified context

- Threat Intel
- Exposure Analytics
- Detection Studio
- Institutional Context

Built on

CISCO DATA FABRIC

Open, cost-efficient data platform: unified data and context

Cisco Cloud Control with Cisco AI Canvas

Available across deployment modes

Cloud	CMP Hybrid	CMP Sovereign
Available now	Q4 CY26 · Coming soon	1H CY27 · Coming soon

© 2026 Cisco and/or its affiliates. All rights reserved.

Democratizing the Agentic SOC with Enterprise Security

Essentials customers get greater value while Premier continues to deliver advanced SOC capabilities (GA: Dec 15, 2026)

ES Essentials

Core agentic security operations and automation

- Core Agentic SOC
- Agentic SOAR & Auto Threat Analysis
- Detection Studio and Exposure Analytics
- Base Agentic Capacity

New value

ES Premier

Protect AI, advanced proactive and autonomous security operations

- Advanced Agentic SOC
- AI Defense
- Native UEBA
- Generous Agentic Capacity

\+ ES Essentials

New value

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Defend at machine speed across threats and exposures

Defend autonomously

Outpace AI-driven threats with trusted agents and human governance

Stop attacks at the source

Distributed defenses with enterprise-wide visibility

Mitigate critical exposure

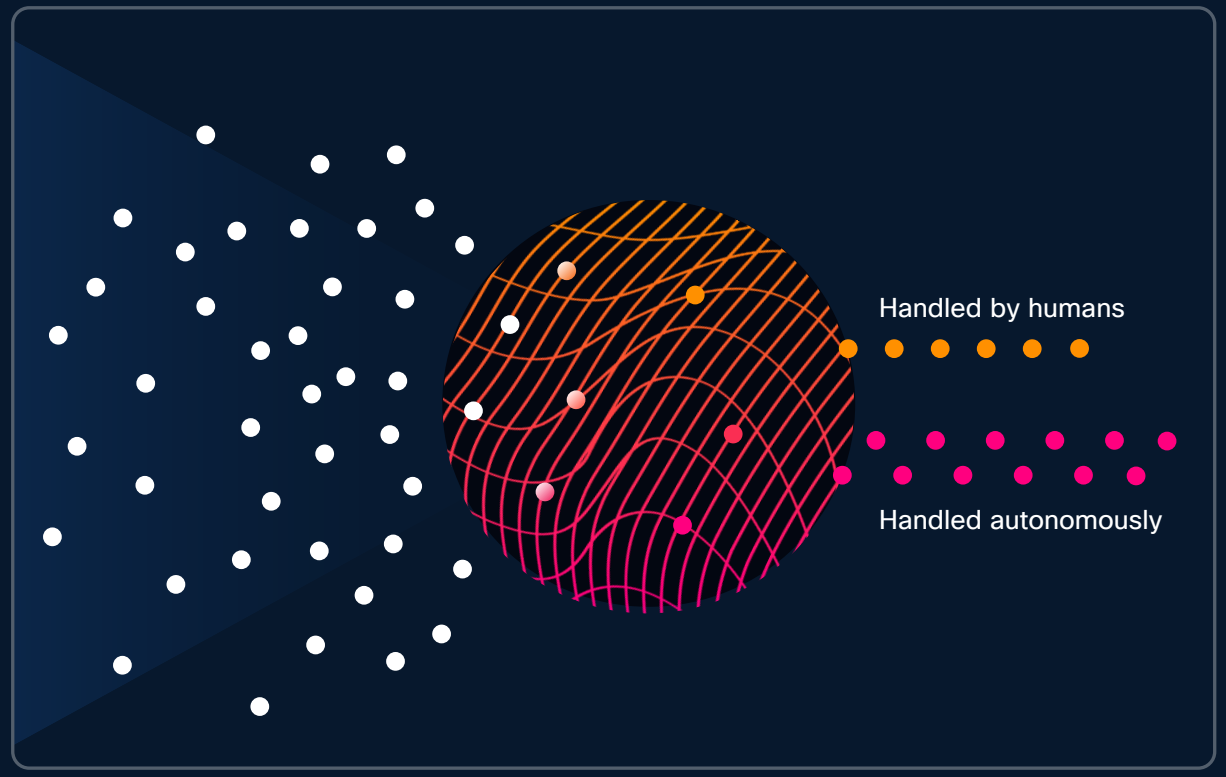
Continuously identify, prioritize, and remediate business-critical risk, including vulnerabilities

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Defend autonomously

Outpace AI-driven threats with trusted agents and human governance



The outcomes

High alert coverage
100% coverage of alerts triaged, low noise

Lower MTTR
2X faster incident response

Trust in human-agentic operations
Cost effective, human controlled agents

Sources: Shunkhlai Group Splunk ES Customer Testimonial, KPMG "AI Quarterly Pulse Survey: Q3 2025"

© 2026 Cisco and/or its affiliates. All rights reserved.

Available now Coming soon

The Agentic SOC Workforce

Detection & Security Engineering	Threat Hunting	Investigation & Response	Governance & Policy
Build trusted coverage faster	Find and disrupt emerging threats	Contain and resolve threats faster	Mitigate critical exposure

Core Agentic SOC

Detection Builder	Threat Hunting	Triage	Standard Operating Procedure
Automation Builder		Investigation	
Connector Builder		Guided Response	
Agentic Workflow Builder			

Advanced Agentic SOC

Threat Graph Detection	Malware Threat Reversing	Autonomous Response	Emerging Threat Agent
Detection Tuning	Red Blue Green Teaming		

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Available now Coming soon

Operating on an intelligent platform

Detection & Data Management	Sovereign Deployments	Trusted Agentic Design	Economic Discipline
Simplify data onboarding	Flexible deployment options	Robust agentic harness	Cost effective Agentic SOC

Core Agentic SOC

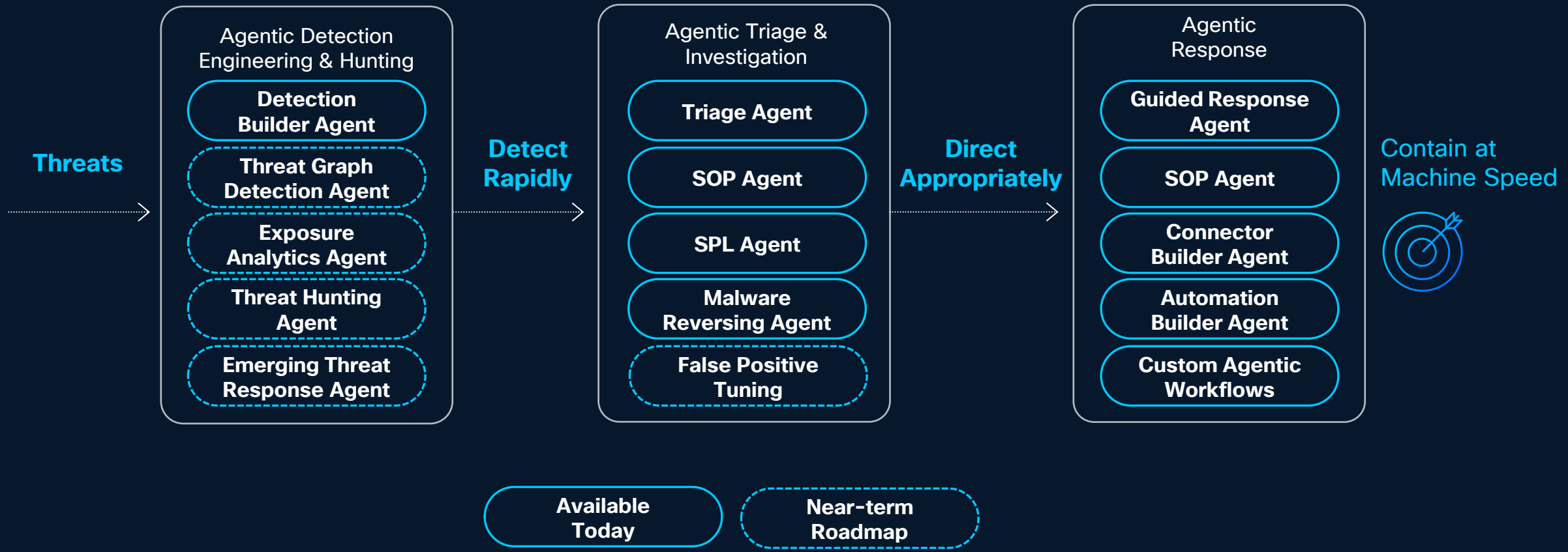
Guided data source onboarding	Hybrid cloud connected	Integrated Agent Security	Custom fine-tuned SLM
Auto schematization	BYO GPU & LLM	Approvals and permissions	ES on CDF
Self-healing pipelines	Bundled offer with Cisco AI Pod	Context and Evidence	ROI dashboards
Detection-as-code		External knowledge base	
Streaming detections		Integrated agent observability	
		Agent memory management	

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Agents work together to deliver broader SOC outcomes

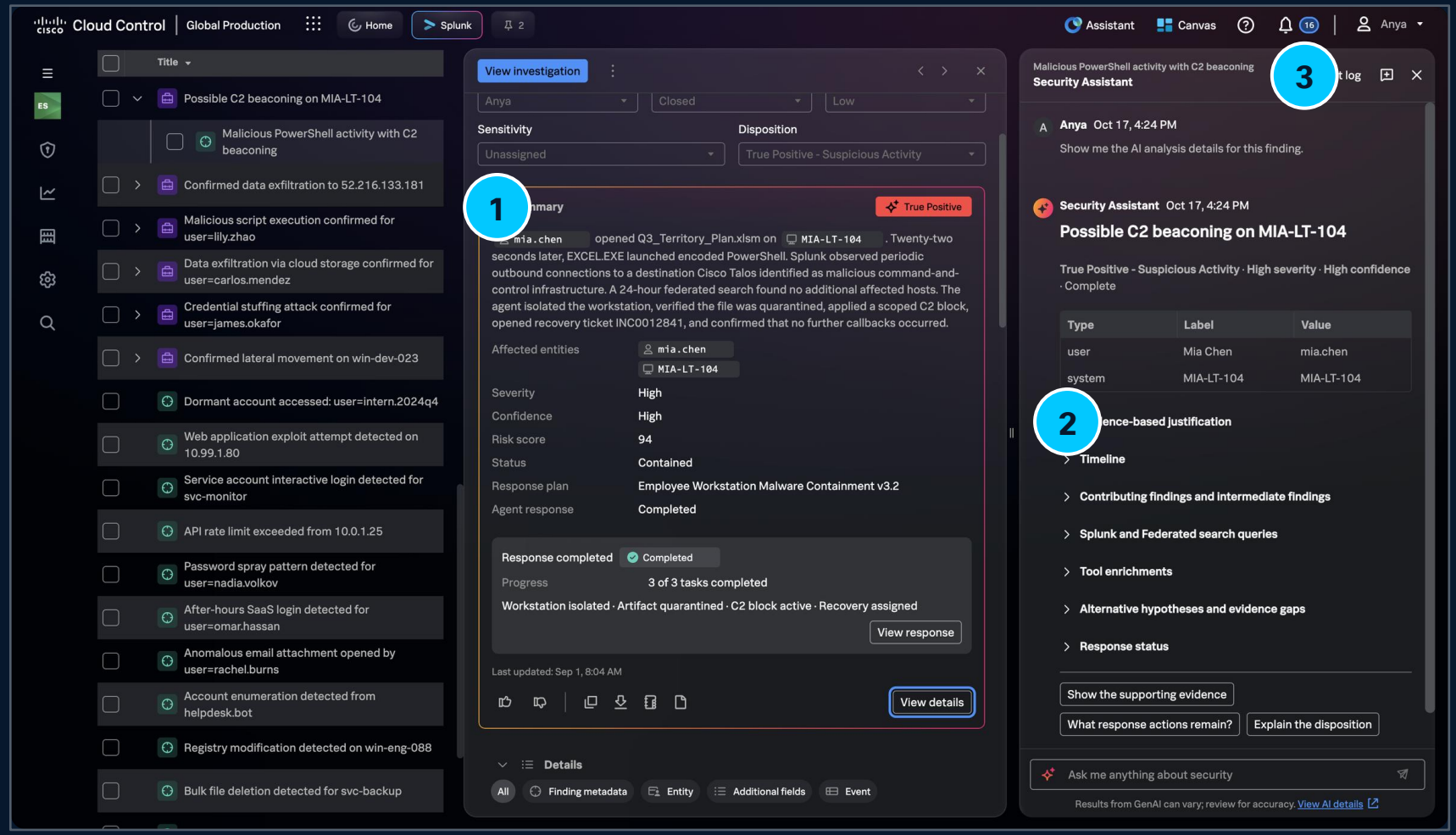
Threats detected rapidly, directed correctly, and contained at machine speed



© 2026 Cisco and/or its affiliates. All rights reserved.

Triage, Investigation Agents

Agents explaining the work to build trust and unlock adoption



1 The verdict in context

Summary, True Positive label and a completed response: 3 of 3 tasks.

2 Ask why

Evidence, timeline, contributing findings, queries, enrichments and alternative hypotheses.

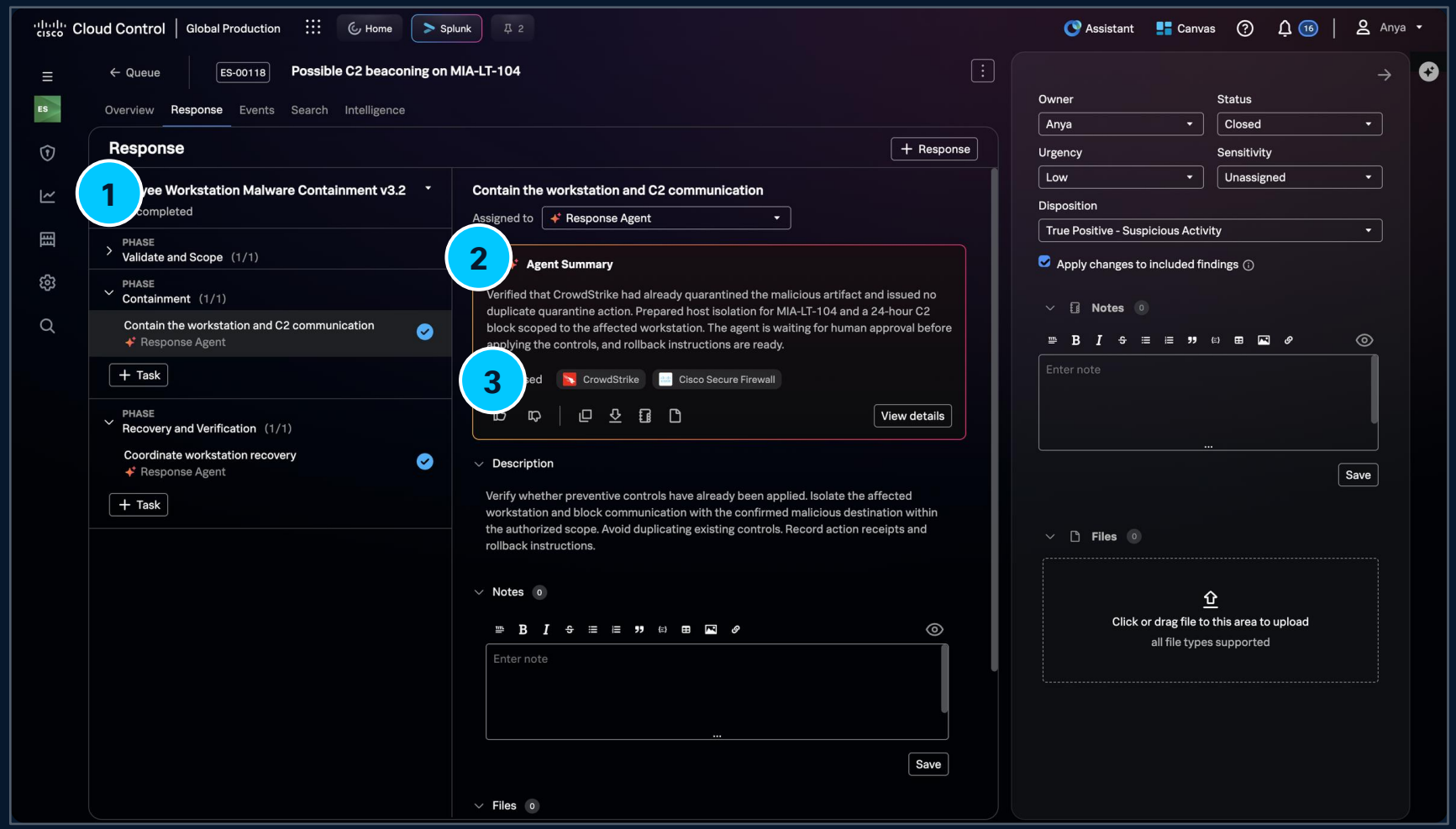
3 Audit and follow up

Open the audit log or ask what response actions remain and to explain the disposition.

© 2026 Cisco and/or its affiliates. All rights reserved.

Response Agent : Contain and Remediate

Guided and Autonomous Response to quickly contain incidents



1 A playbook-driven plan

Employee Workstation Malware Containment v3.2, 100% completed across three phases.

2 Agent acts within approval

Verified quarantine, prepared host isolation and a 24-hour C2 block, with approval and rollback ready.

3 Tools used

CrowdStrike and Cisco Secure Firewall, with action receipts and rollback instructions recorded.

© 2026 Cisco and/or its affiliates. All rights reserved.

Splunk Agentic SOC outcomes

Operational speed and automation	Emergent threat defenses	Lower TCO	Sovereignty

Measured outcomes seen by customers

ALERTS

100%

Coverage

NOISE

65%+

Reduction

TRIAGE AND INVESTIGATION TIME

75%+

Lower

AUTOMATION SETUP TIME

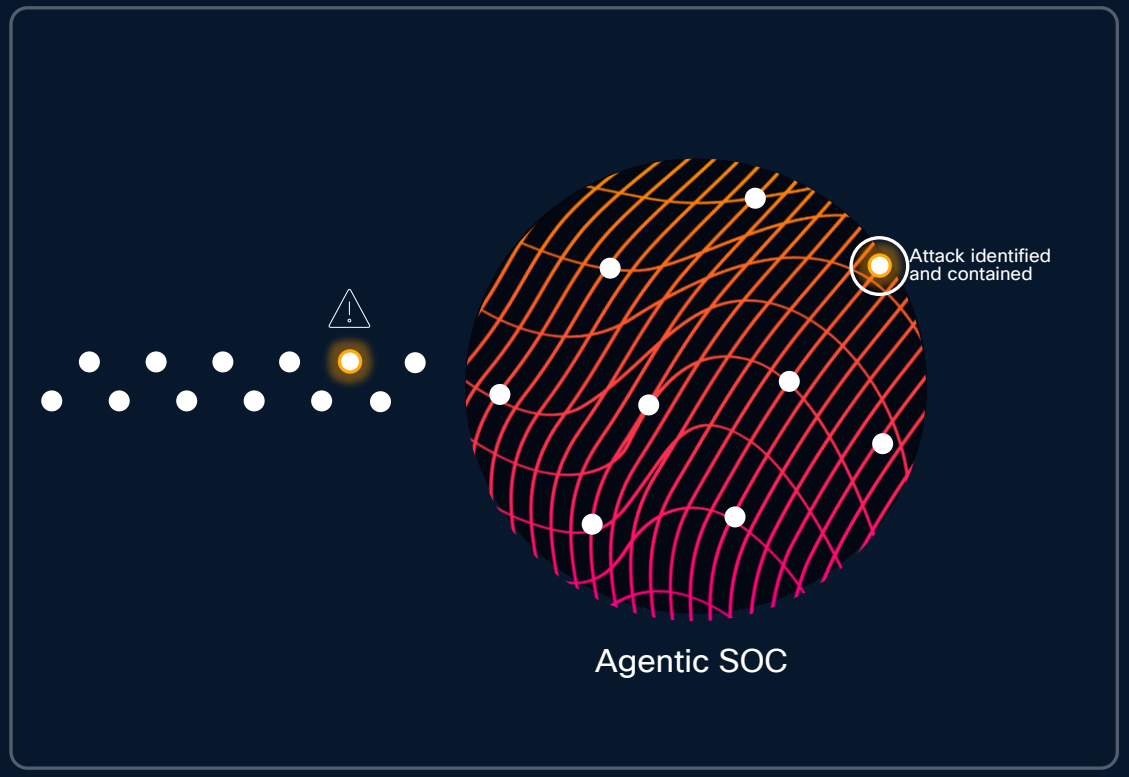
Days to minutes

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Stop attacks at the source

Combine distributed defenses with enterprise-wide visibility



The outcomes

Faster containment and smaller blast radius
Investigations from hours to minutes

Enterprise-wide visibility with fewer gaps
1,300+ third-party integrations in Splunk ES

Consistent and coordinated enforcement
50% better threat coverage via a unified platform

Sources: ReliaQuest “2026 Annual Cyber-Threat Report”, Splunk ES website, Splunk “State of Security 2025” report

© 2026 Cisco and/or its affiliates. All rights reserved.

Bring Splunk to distributed data

Customers cannot centralize every new signal. The SOC needs to detect closer to source and respond through connected controls.

See

Distributed visibility

Decide

Shared context + policy

Enforce

Distributed control

Cisco Data Fabric + Federation + Cisco controls + Agentic Workflows

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Tiering Data by Use Cases

Deploy flexible tiering without data engineering to address any use case. Empower analysts and agents to leverage self-service workflows that promote and demote data between tiers.

Index	**High Performance**	**Use Cases** Security Monitoring, Threat Detection, Incident Resolution, Incident Analysis & Response Agent (Future) **Value / Volume Ratio** High Value, Med-High Volume
Machine Data Lake Analytics	**Selective Use At Scale**	**Use Cases** Forensic Investigation, Federated Analytics, ML Training, Agentic Investigation **Value / Volume Ratio** Med Value, Med-High Volume
*Machine Data Lake Raw	**Audit and Archive**	**Use Cases** Compliance, Forensic Investigation, Audits, Future Proofing **Value / Volume Ratio** Low Value, High Volume

*Alpha

© 2026 Cisco and/or its affiliates. All rights reserved.

ES CDF integration improves Splunk economics

The right tier for the job

1. Capture once

All machine data

Logs
Metrics
Events
Security telemetry

One intake path

2. Route by workflow

Ingest/Edge Processor

Smart routing at ingest

Detect immediately

Promote only what's needed

Retain the rest economically

3. Spend where it matters

ES on CDF | Human | Agentic | Deterministic workflows

Detection	Hunting	Search
Batch Streaming Federated	Index MDL Federated	Index MDL Federated

Splunk Hot Index — 30–60 days
Active detections and investigations

MDL Analytics — 60–180 days
Longer-window hunting and search

Machine Data Lake — >180 days
Broad retention and raw data access

External Data Lakes
ASL · Snowflake · Databricks · Blob · GCS

Customer outcomes

Lower premium storage and compute

Faster detection and search

More data retained per dollar

© 2026 Cisco and/or its affiliates. All rights reserved.

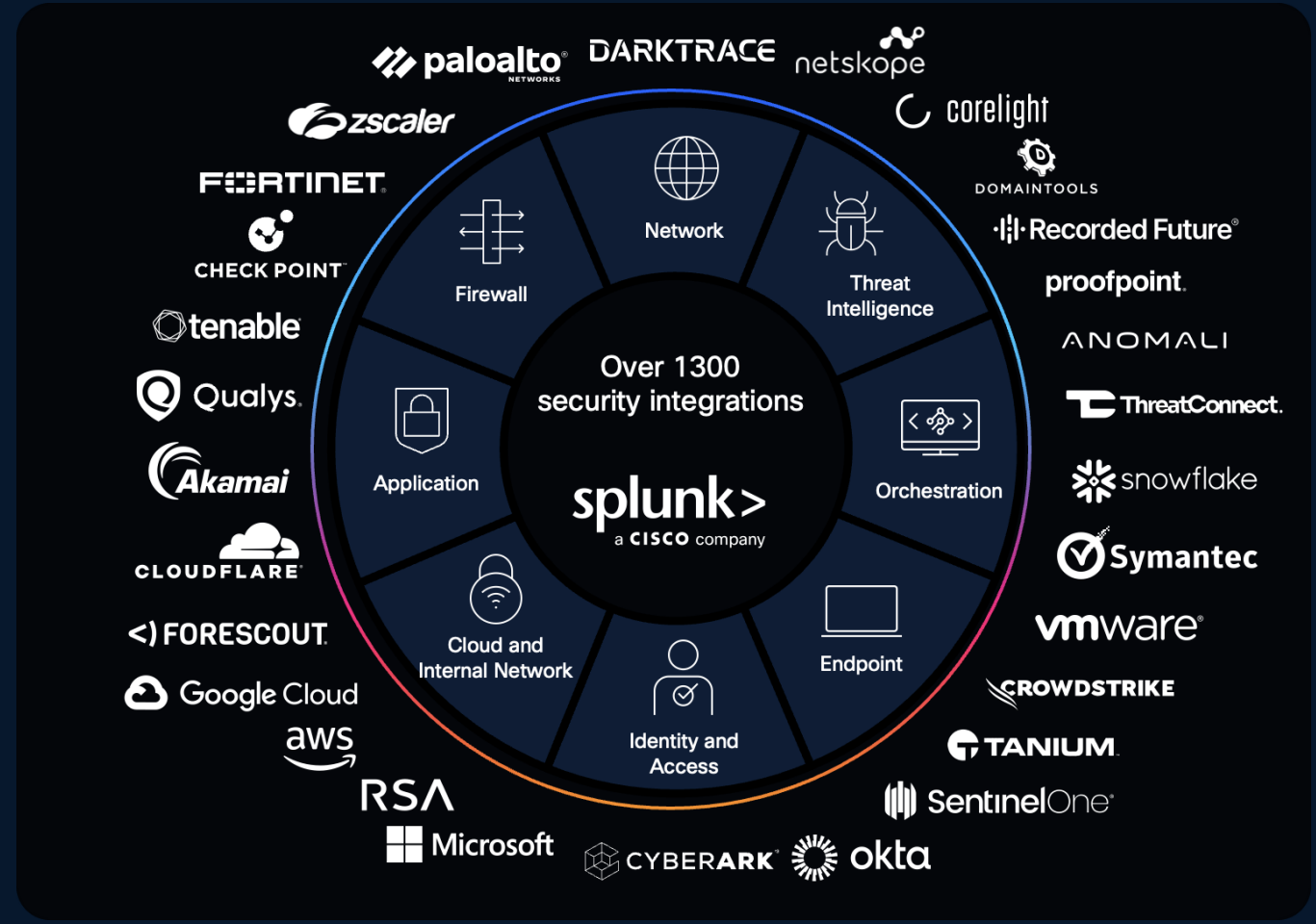
cisco

Stop attacks at the source with Secure Networking and Trusted AI from Cisco



© 2026 Cisco and/or its affiliates. All rights reserved.

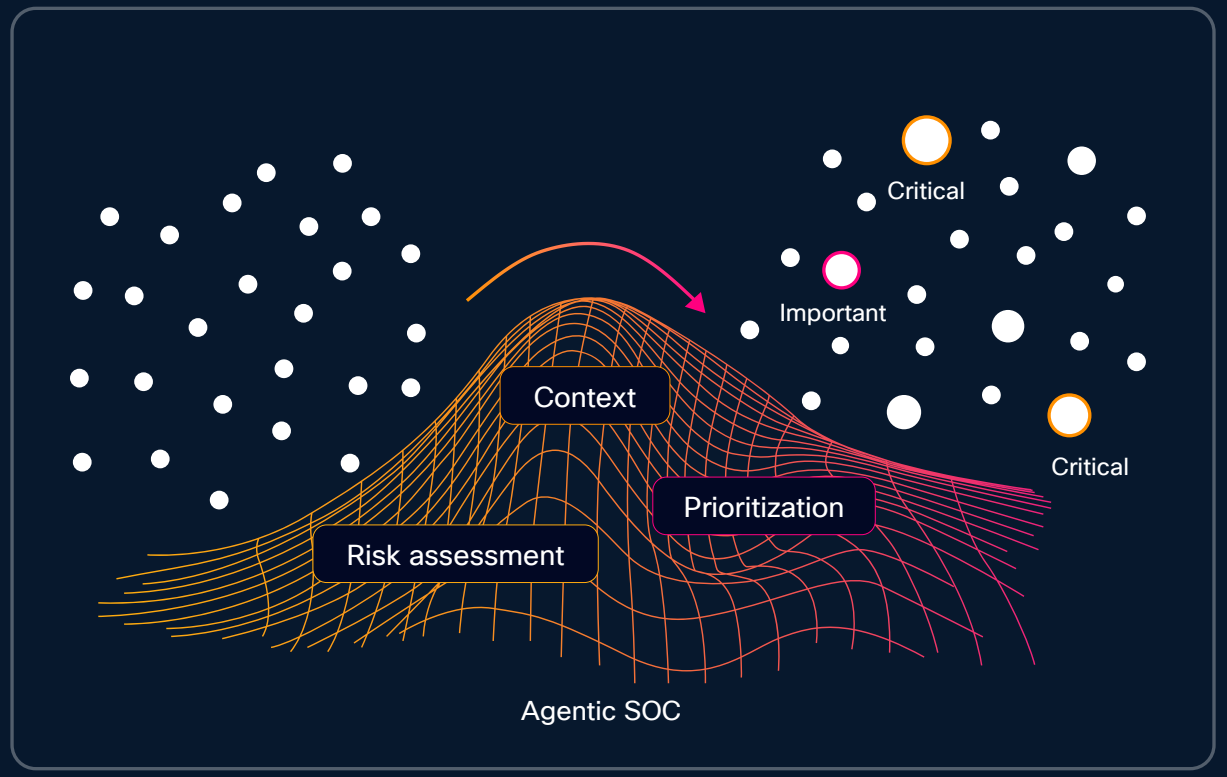
Splunk stops threats with a world-class ecosystem



© 2026 Cisco and/or its affiliates. All rights reserved.

Mitigate critical exposure

Continuously identify, prioritize, and remediate business-critical risk



The outcomes

Continuously discover critical risks

Cloud containers often only live for minutes.

Proactively mitigate risks before exploitation

67% more efficient threat response teams

Closed loop verification

Only 9% of security teams are very confident in their risk remediation

Sources: Sysdig “2025 Cloud-Native Security and Usage Report”, IDC 2025 “The Business Value of Splunk Security: A Unified TDIR Platform” whitepaper, Mondoo “2025 State of Vulnerability Remediation” report

© 2026 Cisco and/or its affiliates. All rights reserved.

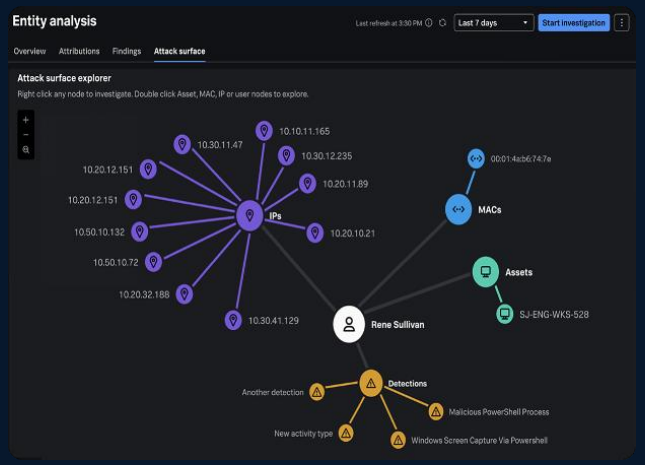
Every exposure is critical in the Agentic AI Era

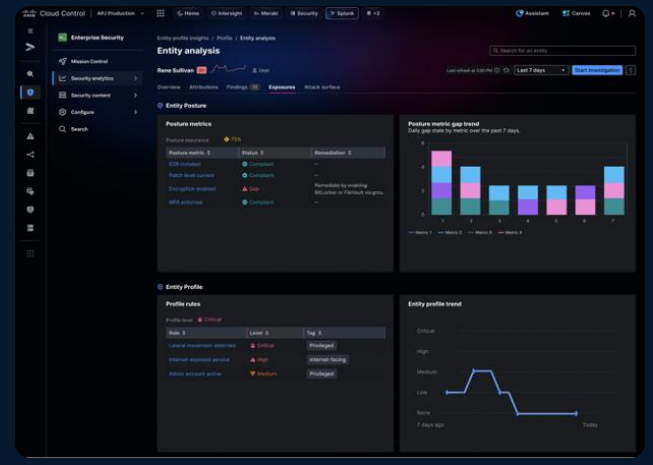
Risks have changed with exploits happening in minutes, not months.

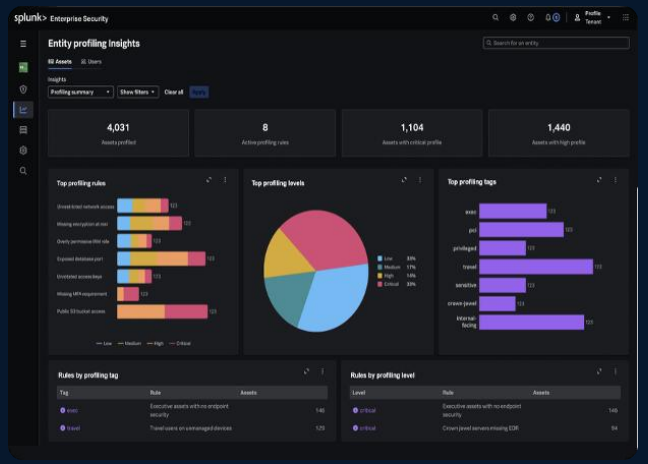
Continuously discover and update asset inventory

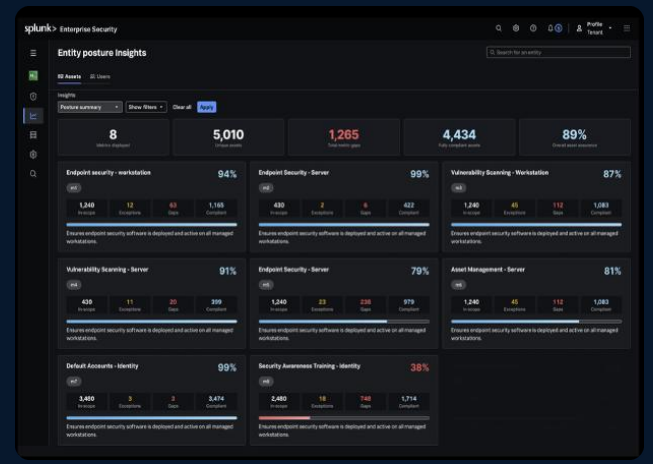
Measure your risk posture

Mitigate critical exposure









© 2026 Cisco and/or its affiliates. All rights reserved.

Prevent before attackers find the opening

Move from reactive defense to continuous exposure discovery, prioritization, and remediation across business-critical risk.



Discover

Assets, identities, cloud, IoT, OT, and vulnerabilities.

Prioritize

Business context separates critical risk from noise.

Remediate

Move from exposure insight to action.

Exposure Analytics

Exposure Agent

Proactive before exploitation. Prioritized during attack.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Accelerate Response to Emerging Threats

Proactive Threat Intelligence Monitoring, exposure assessment, hunting, coverage

01

Proactive AI Threat Intel Monitoring

Monitoring new advisories about emerging threats

02

AI Exposure analysis & prioritization

Identify & prioritize assets with potential for impact/exploitation

03

AI Hunt & Bolster detection coverage

Hunt for evidence of exploitation and close coverage gaps to detect

04

Initiate mitigation with Hypershield

Leverage enforcement points across Cisco to virtually patch threats

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Key takeaways

Trusted autonomy turns AI from assistance into governed SOC action.

1

Autonomy as a dial

Agents deliver delegated, guided and bounded autonomy to meet you where you are at

2

Security on distributed data

ES and CDF integrated drives down cost while streaming detections improve efficacy

3

Trust unlocks adoption

Evidence, approvals, rollback, policy, and observability govern action.

4

Agentic SOC Democratized

Bringing Agentic SOC to all Enterprise Security customers across all deployment types

Defend autonomously

Stop attacks at the source

Mitigate critical exposure

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

CISCO Connect

Thank you



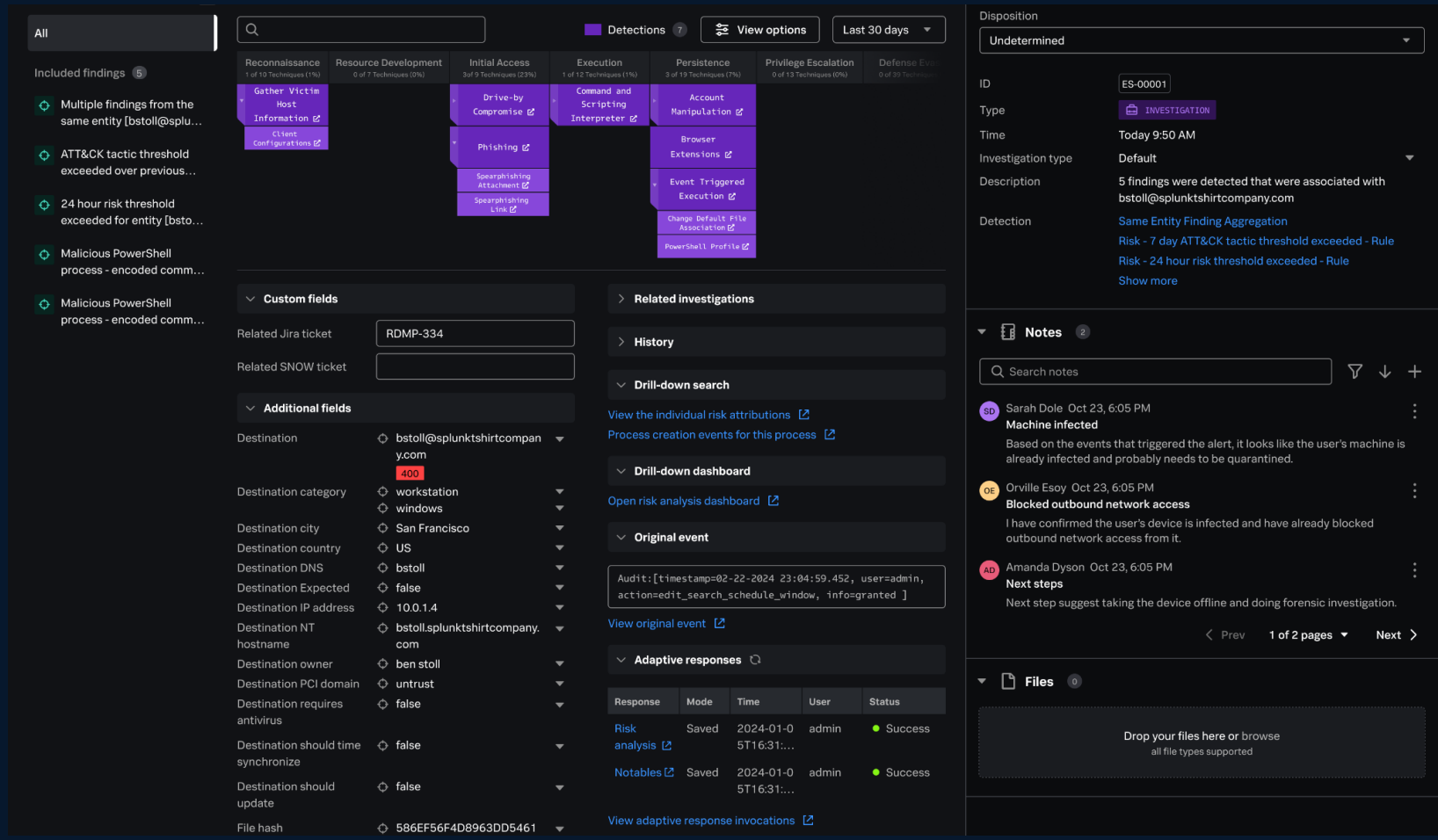
CISCO Connect

Appendix



Splunk Enterprise Security – AI-powered SecOps

- Unlock full-fidelity visibility and control of your security data wherever it lives.
- Deliver the best analyst experience and tooling with unified TDIR.
- Accelerate the SOC with built-in AI across every layer.

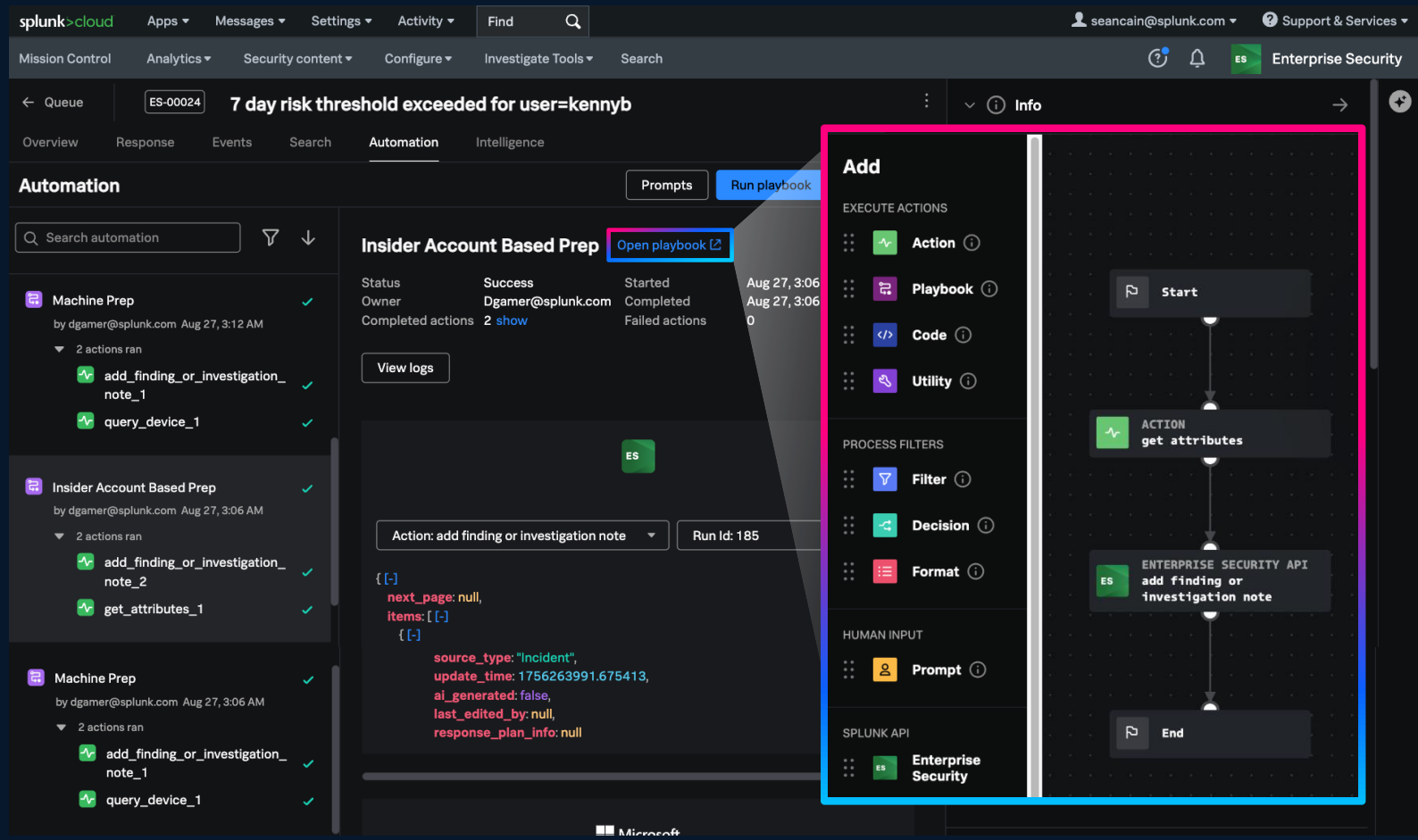


© 2026 Cisco and/or its affiliates. All rights reserved.

Deliver the best analyst experience

Unify threat detection, investigation and response (TDIR) workflows

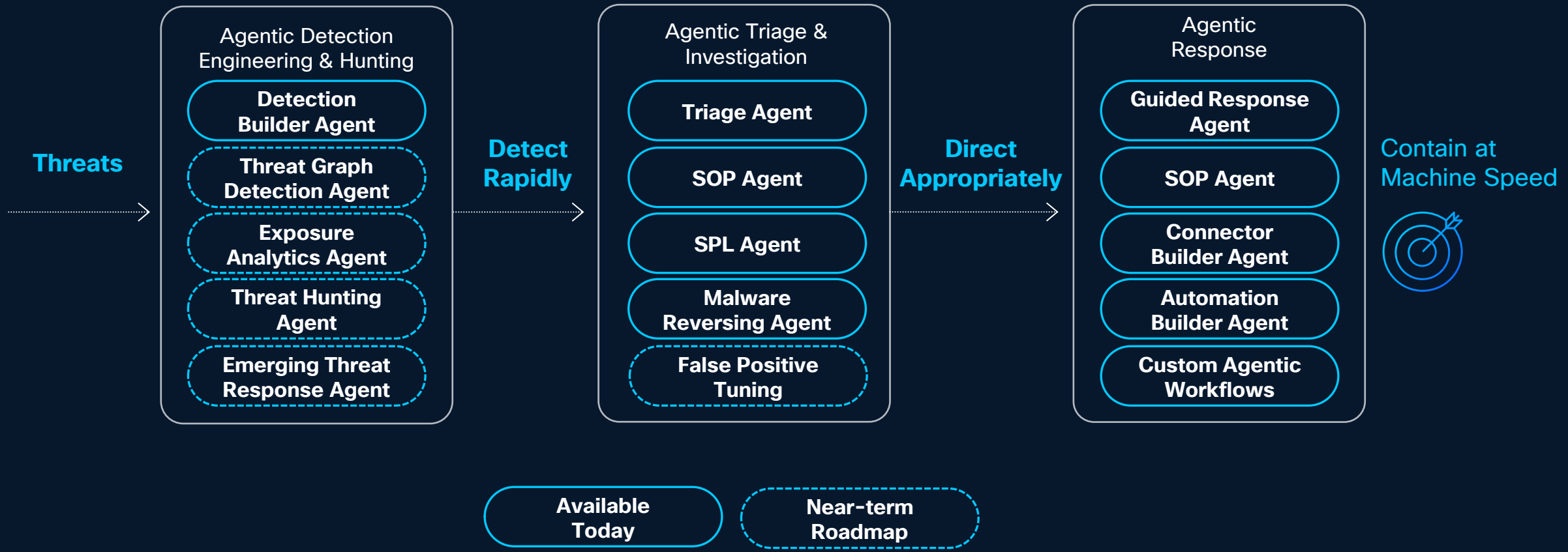
- Integrated TDIR workflows with native SIEM, SOAR, UEBA, and threat intelligence
- Empower every analyst with embedded SOAR and case management
- Detect and mitigate insider threats with UEBA



© 2026 Cisco and/or its affiliates. All rights reserved.

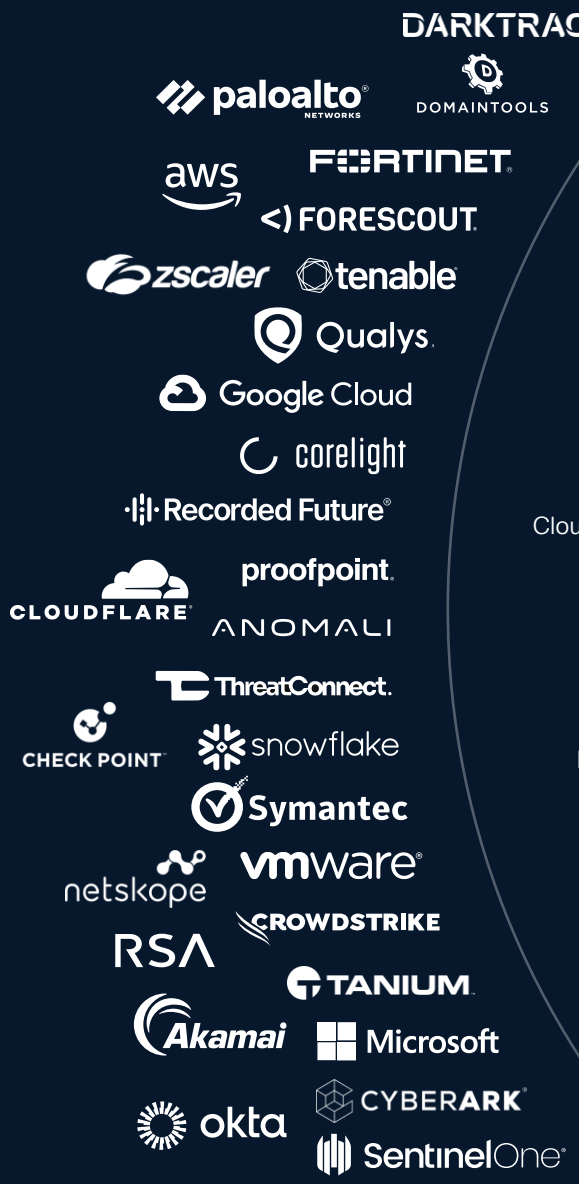
Agents work together to deliver broader SOC outcomes

Threats detected rapidly, directed correctly, and contained at machine speed



© 2026 Cisco and/or its affiliates. All rights reserved.

Continuing to invest a world-class ecosystem to stop threats



Network

Firewall

Application

Cloud and Internal Network

Identity and Access

Endpoint

Orchestration

Threat Intelligence

+1300

security integrations

splunk> by CISCO

© 2026 Cisco and/or its affiliates. All rights reserved.

CISCO

Secure networking and trusted AI from Cisco

Stopping attacks at the source

splunk> by CISCO

Agentic AI

- Cisco AI Defense
- Cisco Identity Intelligence
- Cisco Observability for AI

Network Security

- Cisco Hybrid Mesh Firewall
- Cisco Secure Access
- Live Protect

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Accelerating customer value



© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Unmatched strengths that set Splunk Enterprise Security apart

An open, data-native foundation supporting a unified TDIR solution backed by the industry's deepest ecosystem



Data management and federation

Unique data management capabilities, like routing, filtering, masking, machine data lake, and federation with Cisco Data Fabric to maximize performance and ROI.



Architectural flexibility

Deploy on-premises, in the cloud, or in hybrid environments, with seamless IT and OT integration for broad attack surface coverage wherever you operate.



Market leadership

Splunk is the market share leader, recognized as a leader by Gartner, IDC, and Forrester. Demonstrating that our platform is trusted by a broad user base, providing confidence in your security investments.



Innovating together

With 2,200+ global security partners, thousands of partner and community-built apps, and an active user forum, Splunk delivers unmatched collaborative innovation and support.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

What Enterprise Security customers are saying

One unified platform

"It's been an incredible journey with Splunk ES Premier. It brings together all the security elements across our organization. We use the unification of SIEM, SOAR, and UEBA-powerful capabilities all combined into one seamless integrated platform. It's a comprehensive security view that we use across our organization and across all of our teams."

– Patricia Voight, CISO, Webster Bank

Faster response, less noise

"With ES Premier, we're able to quickly push aside the noise and uncover activity we never would have seen before. By using UEBA to connect events, we can see a clear chain of activity in real time, which saves critical time when something needs immediate action. That visibility helps us respond faster and focus on the threats that truly matter."

- Scott Margolis, CISO, MBTA

Behavior-driven insights

"Splunk helps us surface meaningful risk by 'bubbling up the weird' and showing how users actually. behave. By combining UEBA with risk-based alerting, we get a full picture of activity instead of isolated events. Splunk's managed detections improve quality and efficiency, and event chaining with timeline review has been incredibly valuable for our CSOC."

– Mike Bunner, Security Automation Engineer, REI

111%
More threats accurately detected

64%
Greater SecOps efficiency

55%
Faster incident resolution

© 2026 Cisco and/or its affiliates. All rights reserved.

Splunk Security: proven leadership for the agentic SOC

Gartner®

Eleven-time leader

2025 Gartner® Magic Quadrant™ for SIEM

Ranked #1 in all three use cases

2025 Gartner® Critical Capabilities for SIEM

FORRESTER®

Leader

Forrester Wave™: Security Analytics Platforms, Q2 2025

IDC

Leader

2024 IDC MarketScape for SIEM for Enterprise

Ranked #1

2025 IDC Market Share for SIEM

OMDIA

Leader

Omdia Universe: Next-Generation SIEM Solutions

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Option

Accelerating your journey to the Agentic SOC

Trusted foundation

Know what is protected and monitored

Establish the SOC baseline with trusted data, context, detections, and retention.

Repeatable response

Repeatable response and faster incident closure

Codify deterministic playbooks for consistent response across teams.

Accelerate decisions

Prioritize what matters with greater accuracy

Use threat intel, advanced detections, and AI-enriched context and guidance to prioritize and investigate with confidence.

Proactive defense

Reduce risk before incidents escalate

Reduce risk earlier with exposure insight, validation, anomaly detection, and conditional agentic remediation.

Trusted Agentic SOC

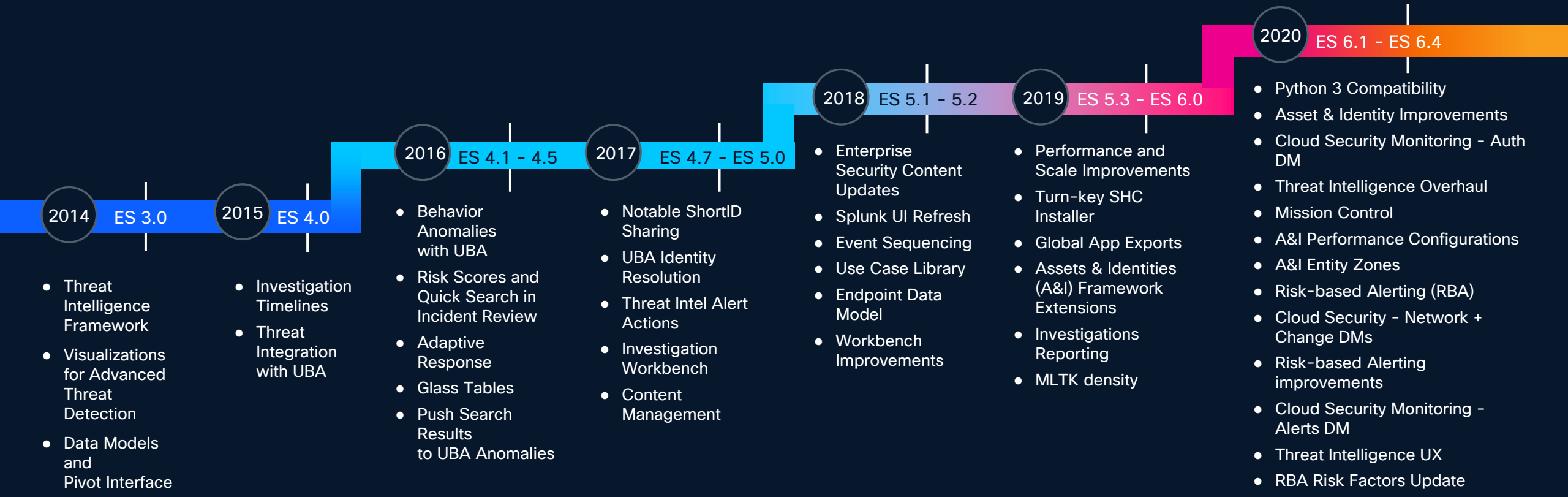
Scalable autonomy with trust and governance

Governed agents handle bounded SOC domains, act within policy, escalate exceptions, and learn from outcomes.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Over a decade of innovation revolutionizing the SOC



Gartner

Leader in Gartner® Magic Quadrant™ for SIEM (2014 - 2024)

FORRESTER®

Leader Forrester Wave™ Security Analytics Platforms (2018, 2020, 2022)

IDC

#1 Worldwide SIEM Market Share (2018 - 2024)

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Over a decade of innovation revolutionizing the SOC

2021 ES 6.5 - ES 7.0

- RBA Embedded Workbench Panels
- RBA Threat Objects
- Dashboard Studio
- Incident Review UX Overhaul
- RBA Event Timeline
- Executive Summary and Security Operations Dashboards
- Automated Content Updates
- Dark UI Mode
- Cloud Security Monitoring Dashboards

2022 ES 7.0.2

- Content Management Performance Improvements
- Correlation Search Editor Performance Improvements

2023 ES 7.1 - 7.3

- Cloud-based Streaming Analytics
- Threat Topology visualization
- MITRE ATT&CK® visualization
- Splunk Dashboard Studio
- Integrated Threat Intelligence Management
- Multiple Drill-down Searches on Correlation Rules
- Enhanced Risk Analysis Dashboard
- Dispositions in Incident Review
- Hyperlinks in Correlation Search “Next Steps”
- Auto-refresh in Incident review
- Customize Investigation Workflows in Incident Review Dashboard
- Multiple Drill-down Dashboard for Notable Event
- Index Time Correlation Searches
- Updated Risk Event Timeline

2024 ES 8.0

- Complete TDIR all within Splunk Enterprise Security
- Improved case management capabilities
- Native Splunk® SOAR integration
- Enhanced detection engineering capabilities
- Simplified terminology for security analytics aligned with OCSF
- Finding Groups (In Preview)
- Federated Analytics for Amazon Security Lake (Coming Soon)

2025 New ES Premier

- Unified TDIR Platform
- Automation for every SOC role
- AI Assistant in Security
- Detection Studio

Gartner

Leader in Gartner® Magic Quadrant™ for SIEM (2014 - 2024)
#1 in Gartner Critical Capabilities, all three use cases (2024)
#1 Market Share Leader in SIEM (2023)

FORRESTER®

Leader Forrester Wave™ Security Analytics Platforms (2018, 2020, 2022)

IDC

Leader IDC MarketScape for SIEM for Enterprise (2022, 2024)
#1 Worldwide SIEM Market Share (2018 - 2024)

GIGAOM

Challenger and Fast Mover in GigaOM Radar for SIEM (2022, 2023, 2024)

QKS Group

Challenger and Fast Mover in GigaOM Radar for SIEM (2022, 2023, 2024)

SoftwareReviews

#1 SIEM solution in Software Reviews Data Quadrant (2023)

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco



Healthcare

Children's National Hospital utilizes Splunk for complete threat detection, investigation, and response

> To ensure comprehensive security, we must instrument devices, the cloud, and every touchpoint where data resides. By bringing all that valuable telemetry into the Splunk environment, we gain the visibility needed to protect data—no matter where it lives.
>
> – Nathan Lesser, CISO, Children's National Hospital

- 80+ security use cases implemented
- 40% increase in detection of threats
- 25% increase in analyst productivity

cisco



Financial Services

Fannie Mae helps protect the housing finance system with Splunk

> Using Splunk, we now have a greater view of our ecosystem to help ensure that each transaction that goes through Fannie Mae can be traced and monitored from start to finish.

– Nimesh Bernard, Senior Director, Enterprise Observability Applications, Fannie Mae

- More efficiencies due to unified monitoring capabilities
- Faster MTTR thanks to real-time insights
- Increased ability to comply with regulatory mandates



PROGRESSIVE®

Insurance

Progressive protects customers and revenue with Splunk

> When you have a company the size of Progressive, approaching 65 billion in annual revenues, with 10 minutes, one hour, two hours of outage, there are real dollars there," says Moore. "So if we can show that monitoring was able to pick up prior to a service disruption, we're able to show that the investments we make in the monitoring tool are giving the business value
>
> - Jon Moore, Domain Architect, Progressive Insurance.

- $120 billion in market capitalization protected
- Reduced noise in SOC significantly with risk-based alerting
- 8 million traces and 50 million spans effortlessly captured without impact on compute performance



Public Sector

La Poste stamps out false alerts by 10x, protecting the data of 1.3M customers

> The level of customization within Splunk is critical. There are no limits to the tool. There are plenty of solutions on the market, but to my knowledge, none of them offer such a high level of customization. You can really tailor every dashboard, function, rule, and search to your needs.

– Oliver Cassignac, Responsable Détection des Incidents de Sécurité (Head of Security Incident Detection)

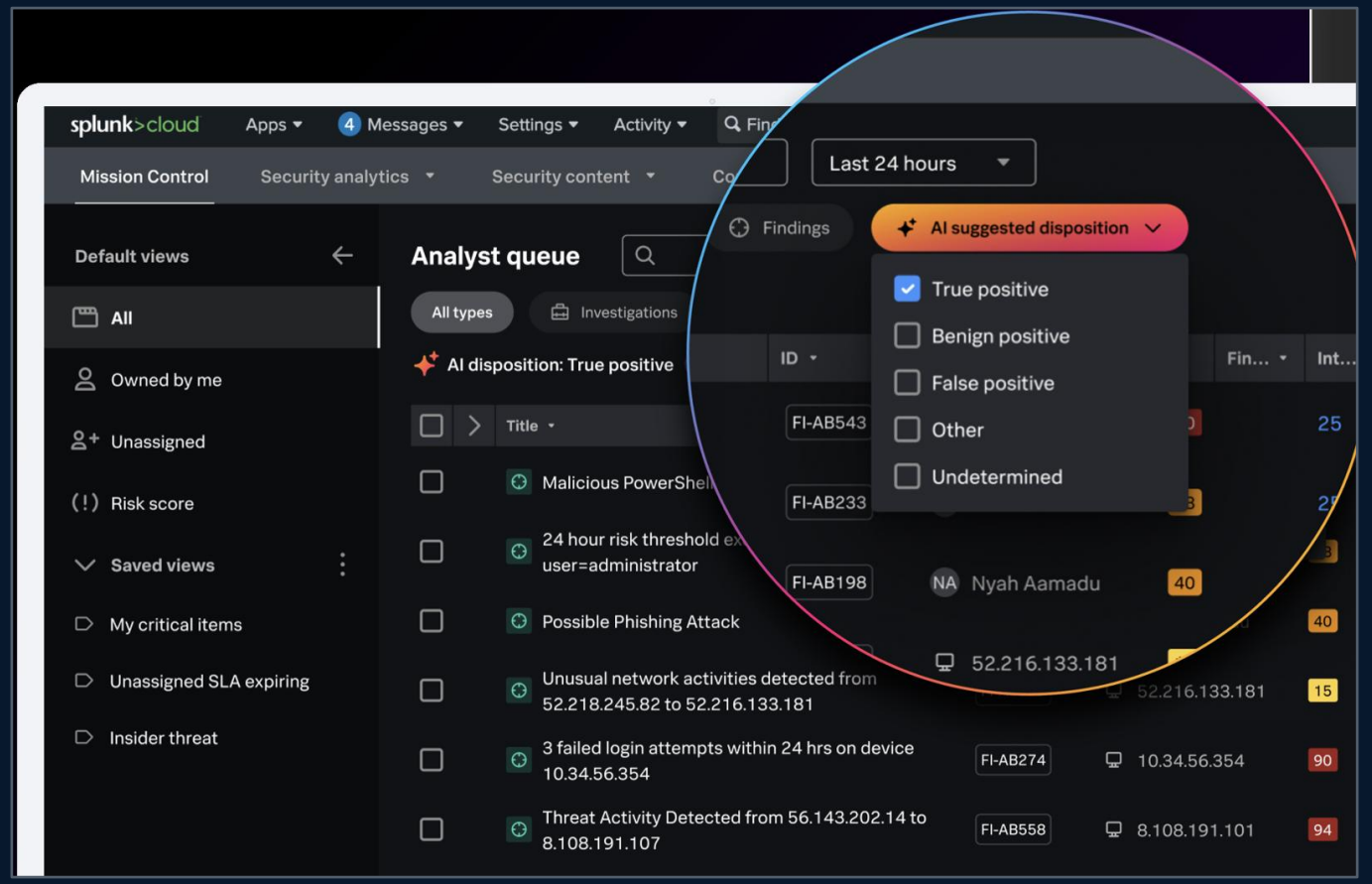
- 80% of alerts now take under 13 minutes to process
- False positive alerts reduced by 10x
- Up to 20 terabytes of data are processed each day

Triage Agent

Alpha in April 2026

Streamline alert prioritization

- Agentic AI plans and executes investigation steps for you
- Autonomously enrich alerts with insights from your security tools
- Reduce workload and MTTR

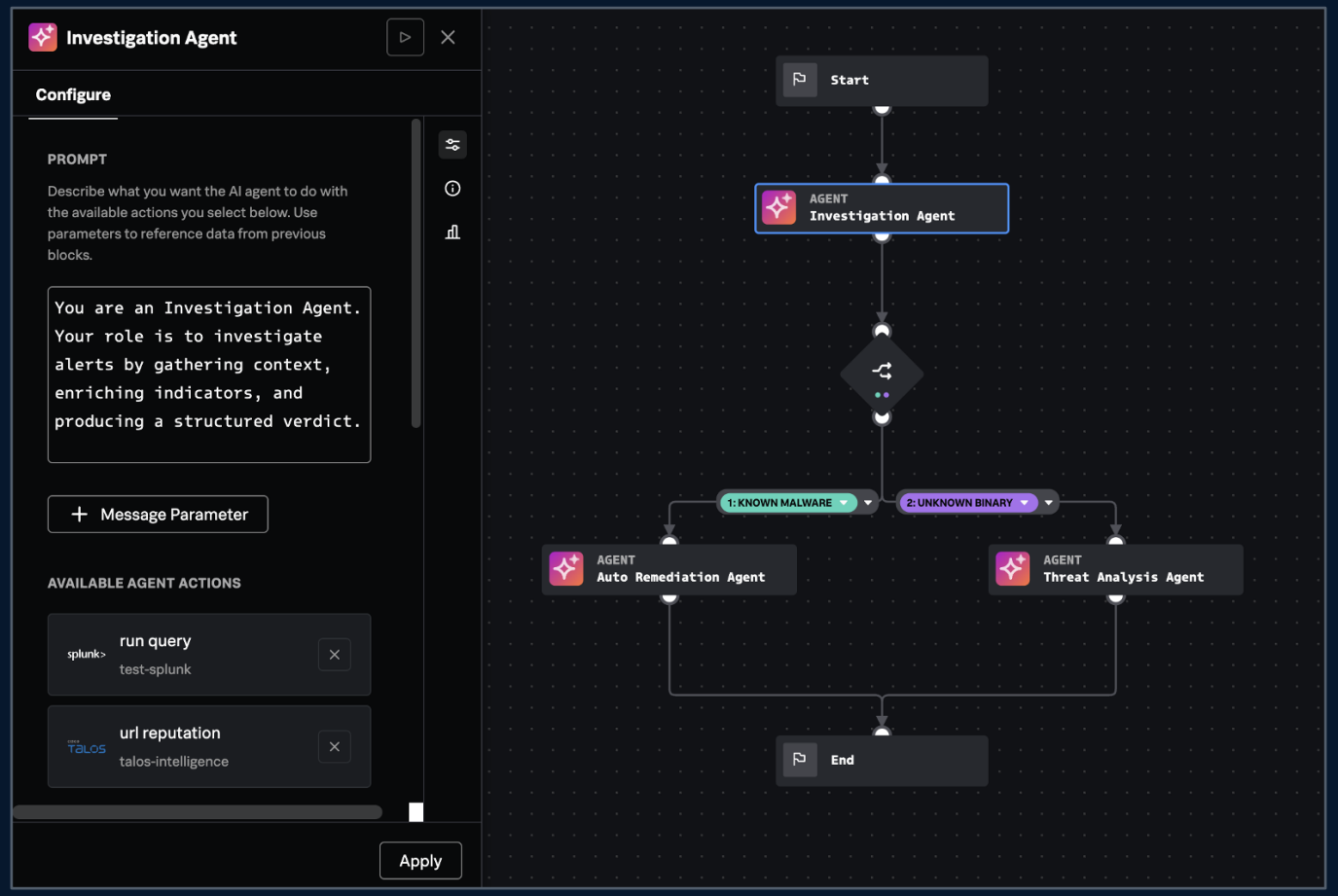


© 2026 Cisco and/or its affiliates. All rights reserved.

SecOps Agentic Workflow Builder

Alpha in September 2026

- Agent execution framework – pair deterministic logic and agents, with decision flow and human approvals where needed.
- Run agents at scale on a platform built to handle high volume of execution
- Get an agent reasoning log tied to the case for audit and review, aligning to enterprise SOC expectations

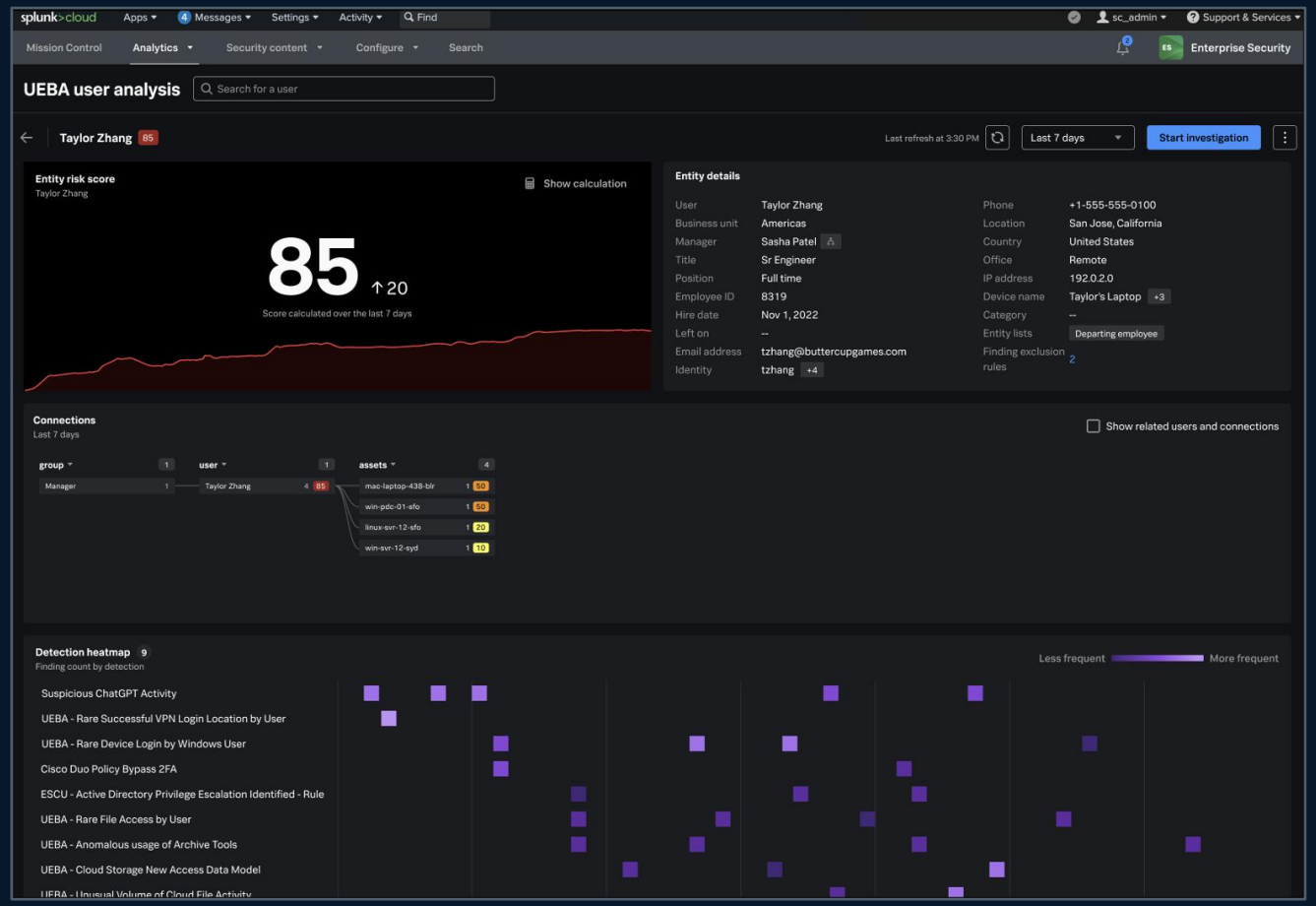


© 2026 Cisco and/or its affiliates. All rights reserved.

User and Entity Risk Intelligence

GA with Premier

- Correlate behavioral anomalies across multiple systems to identify early warning signs of insider threats.
- Provide analysts with rich contextual insights to accelerate risk assessment and decision-making.
- Streamline SOC workflows for efficient investigations and faster threat mitigation, reducing alert noise and allowing your analysts to focus their attention on high-priority threats



© 2026 Cisco and/or its affiliates. All rights reserved.