CISCO Connect

Transforming Security Operations to Punch Above Your Weight Class

Mike McPhee – Principal Solutions Engineer, Security

October 30, 2025

Agenda

Organizations today face the challenge of combating sophisticated cyber threats with limited security resources, making it difficult to efficiently manage risks across multiple tools and vendors. To address this, there is a critical need for integrated, AI-driven solutions that unify threat detection, investigation, and response. By leveraging the combined capabilities of Cisco XDR and Splunk, organizations can achieve enhanced visibility, reduce alert fatigue, and accelerate threat remediation through automation and advanced analytics, empowering security teams to prioritize critical threats, streamline investigations, and "punch above their weight class" in defending against evolving cyber risks.

The Problem

Digital resilience is a $400B problem

Total direct cost of downtime:

$200M

Per year per company

Hidden cost of downtime:

94%

Report slowed innovation

The Hidden Costs of Downtime, Splunk sponsored Oxford Economics research

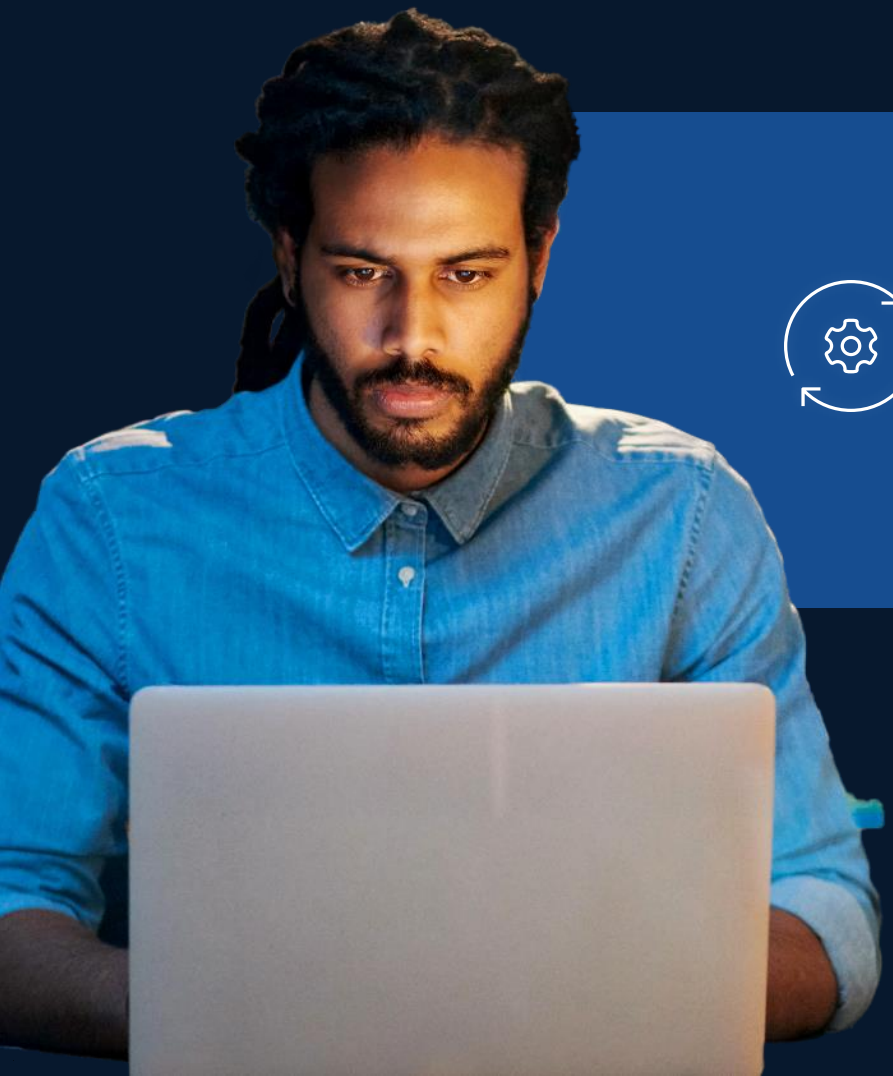
Organizations are doubling down on cyber resilience as it is critical to achieve digital resilience

“The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.”

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

cisco

Your Challenges



Limited Staff vs 24/7 threats

Network blind spots

Alert Fatigue Tool Crawl

Manual investigation delays

Security is a problem of plenty

Detect, investigate, & respond in real time to build resilience

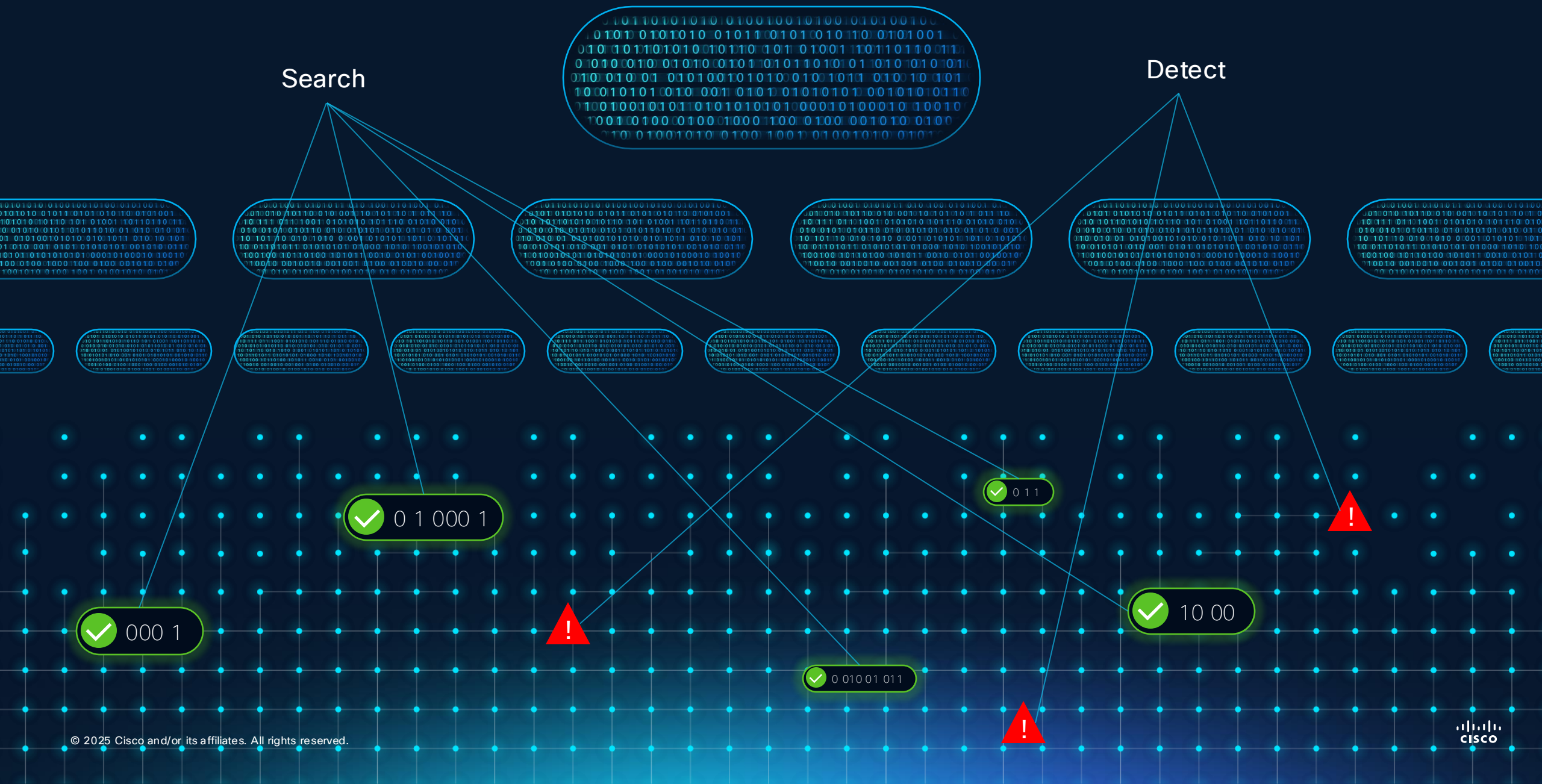
Network team

IT team

Security team

Engineering team

FUTURE



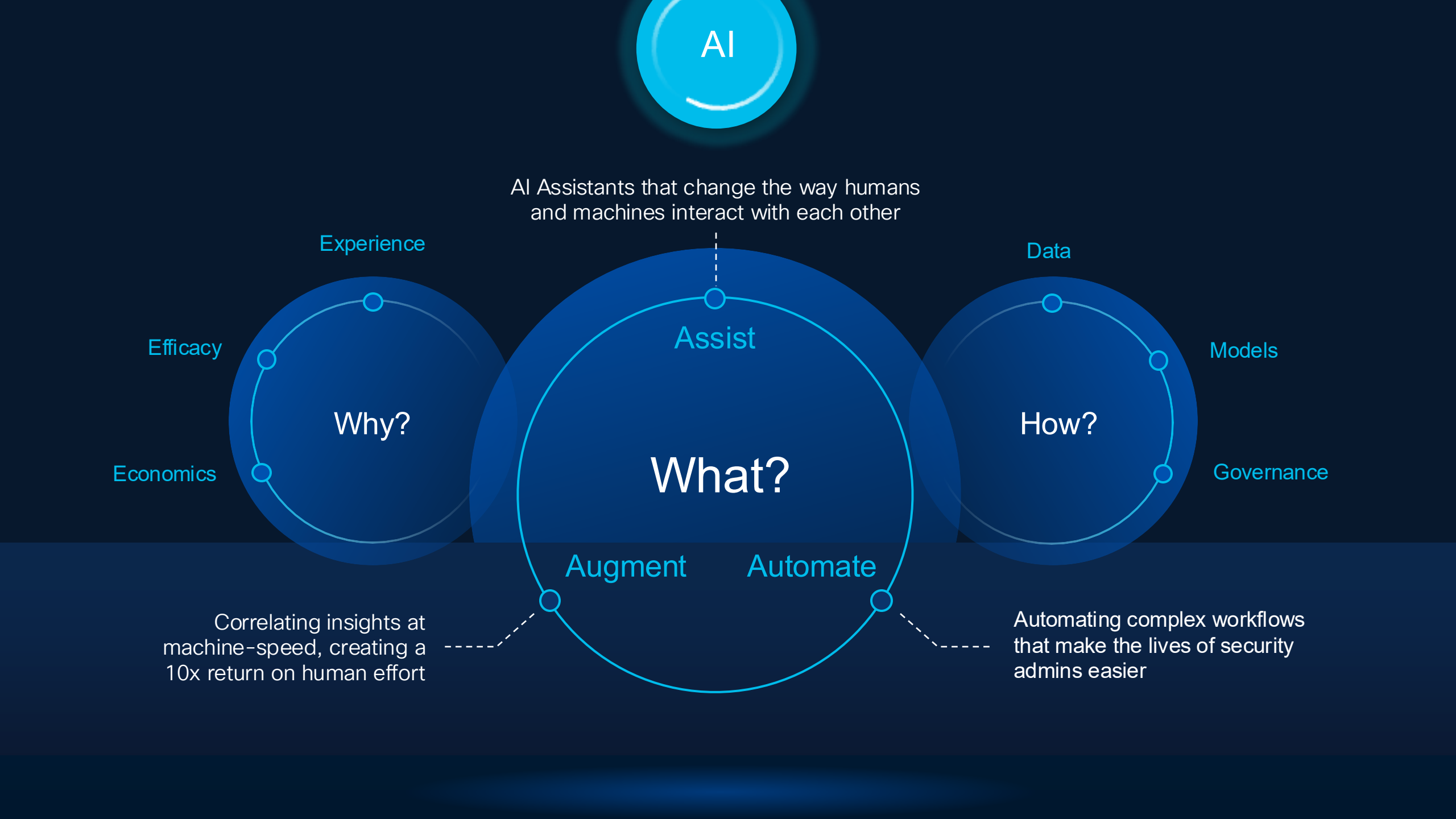
Shaping the SOC of the future

CENTRALIZED

Centralization with a unified SOC platform

Using AI: Fighting for an Unfair Advantage

Shaping the SOC of the future


AI
AI Assistants that change the way humans and machines interact with each other
Experience
Efficacy
Economics
Why?
Assist
What?
Augment
Automate
Data
Models
Governance
How?
Correlating insights at machine-speed, creating a 10x return on human effort
Automating complex workflows that make the lives of security admins easier

We Are Leveraging AI Across The Portfolio

Assist

Augment

Automate

AI Assistant Experience

Give your admins superpowers.
Simplify management, improve outcomes.

AI Powered Detection

Correlate 550B security events at machine-speed.

Autonomous Actions

Learn from human-to-machine interactions to automate complex playbooks.

Cisco Security Cloud

Breach Protection

User Protection

Cloud Protection

Firewall Foundation

cisco

AI-driven Security Operations

Unified Threat Detection, Investigation & Response (TDIR)

Journey to the self-driving SOC

Foundational AI

AI used to detect & prioritize incidents

AI Assists

AI provides insights & recommendations, but humans make all decisions.

AI flags a suspicious login pattern and recommends an investigation path.

AI Augments

Human in the loop, AI automates actions

AI automatically escalates high-fidelity threats and drafts response actions for human review

Autonomous SOC

AI detects, investigates, and mitigates threats end-to-end

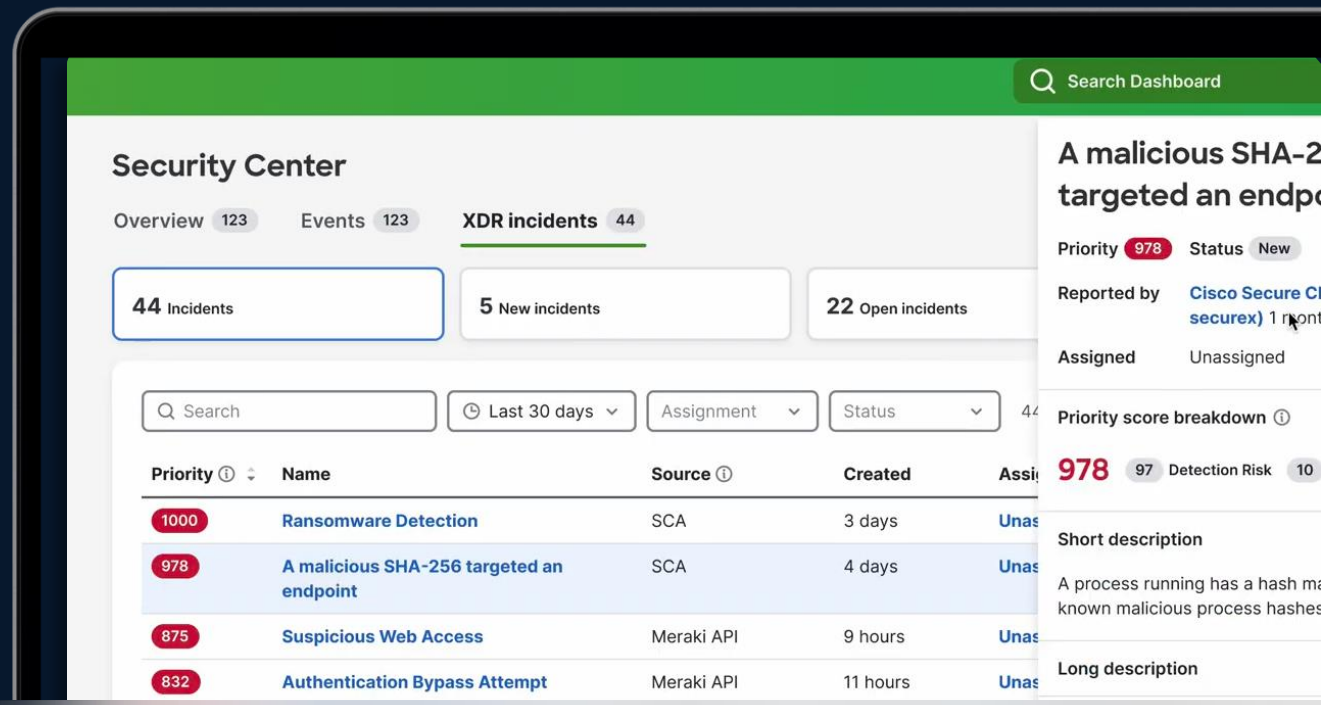
AI acts without human involvement, except in edge cases.

cisco

XDR: Instincts and Fundamentals in the Ring

Cisco XDR

Innovating to detect and stop common attacks



Optimized for lean teams

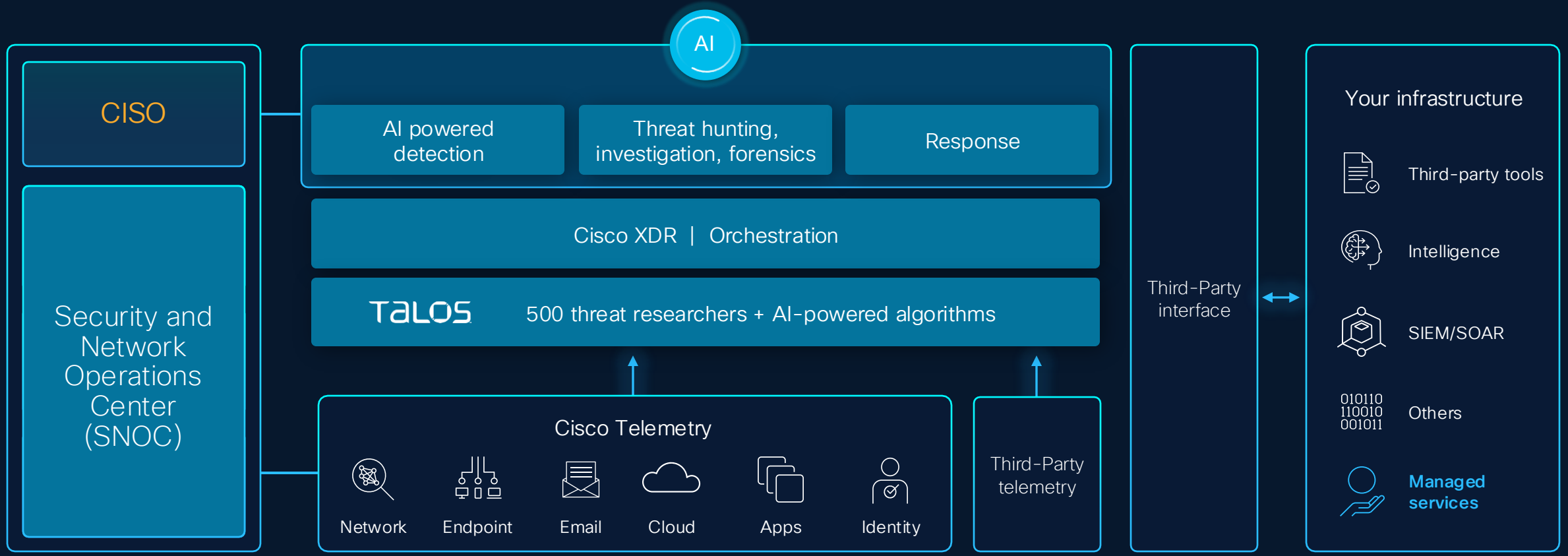
Speed to value

Deeply integrated with the network

Every Meraki MX becomes a sensor

In under 60 seconds

Simplify security operations with AI-driven Cisco XDR



Real-time attack chain detection for the most common attacks with curated integration and response guidance

Our open XDR integrates with competitive EDR tools

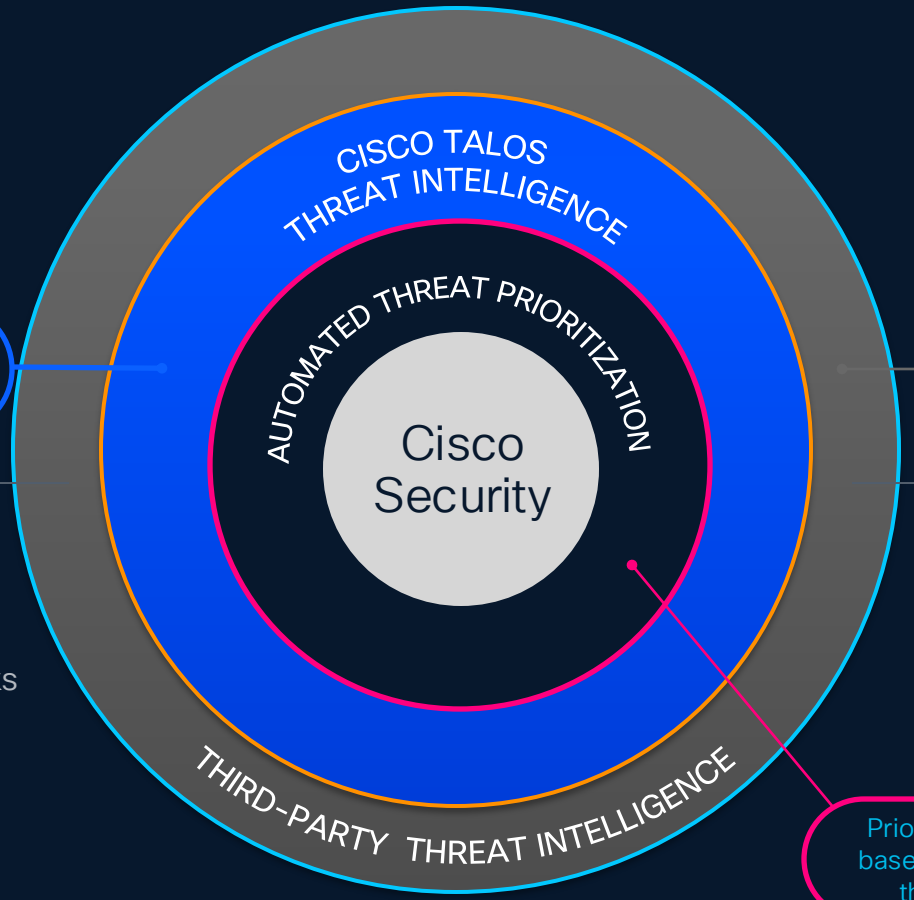
Cisco XDR has curated integrations with the top best-of breed security vendors

Cloud Telemetry supported:

Cisco, AWS, Google, Microsoft Azure

Endpoint Telemetry supported:

Cisco, CrowdStrike, Cybereason, Microsoft Defender for Endpoint, Palo Alto Networks, SentinelOne, Trend Micro



Cisco Talos: Unrivaled collection of actionable intelligence for known and emerging threats

Identifies tactics, techniques, and procedures (TTPs) used

Prioritizing threats based on impact to the business

Firewall Telemetry supported:

Cisco, Check Point, Fortinet, Palo Alto Networks

NDR Telemetry supported:

Cisco, Darktrace, ExtraHop

Email Telemetry supported:

Cisco, Microsoft 365, Proofpoint

Introducing Cisco XDR 2.0

Clear verdict. Decisive action. AI speed.

Instant Attack Verification

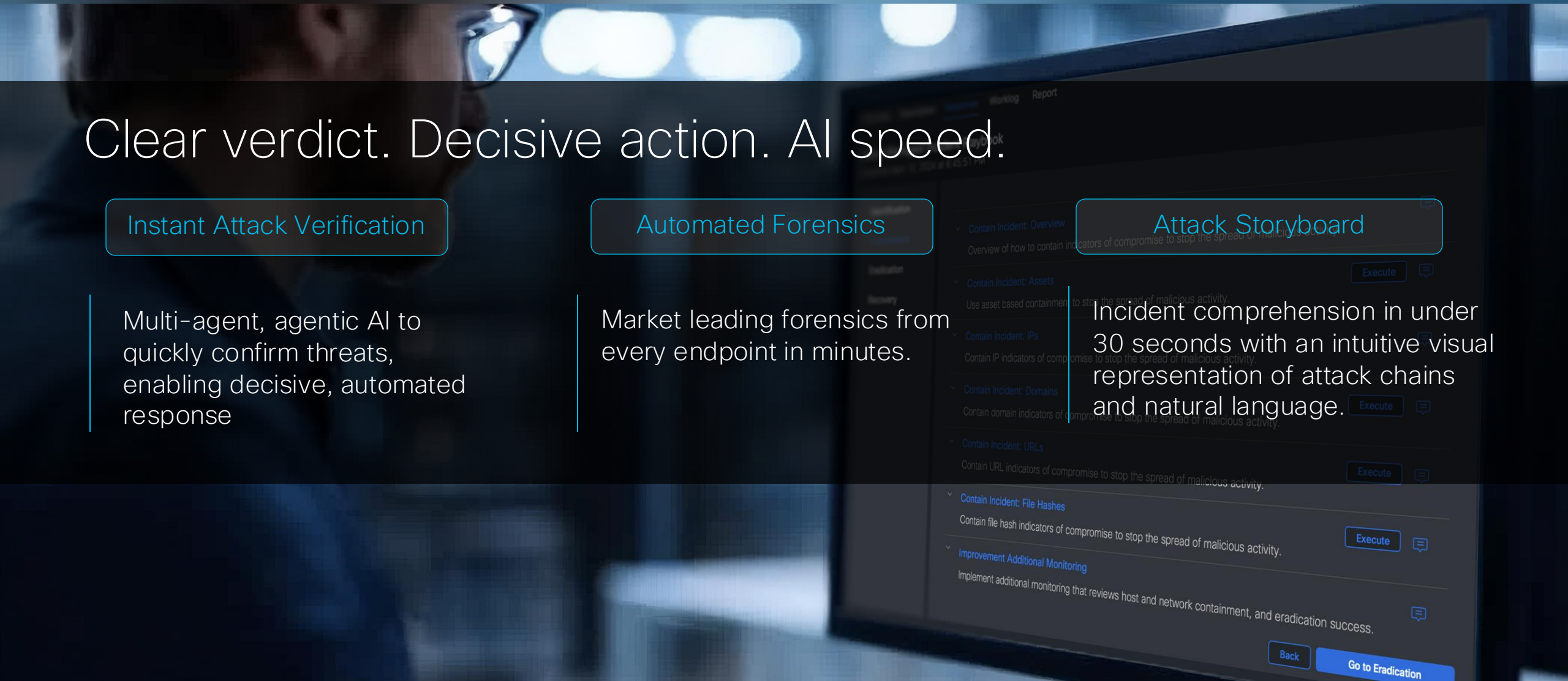
Multi-agent, agentic AI to quickly confirm threats, enabling decisive, automated response

Automated Forensics

Market leading forensics from every endpoint in minutes.

Attack Storyboard

Incident comprehension in under 30 seconds with an intuitive visual representation of attack chains and natural language.



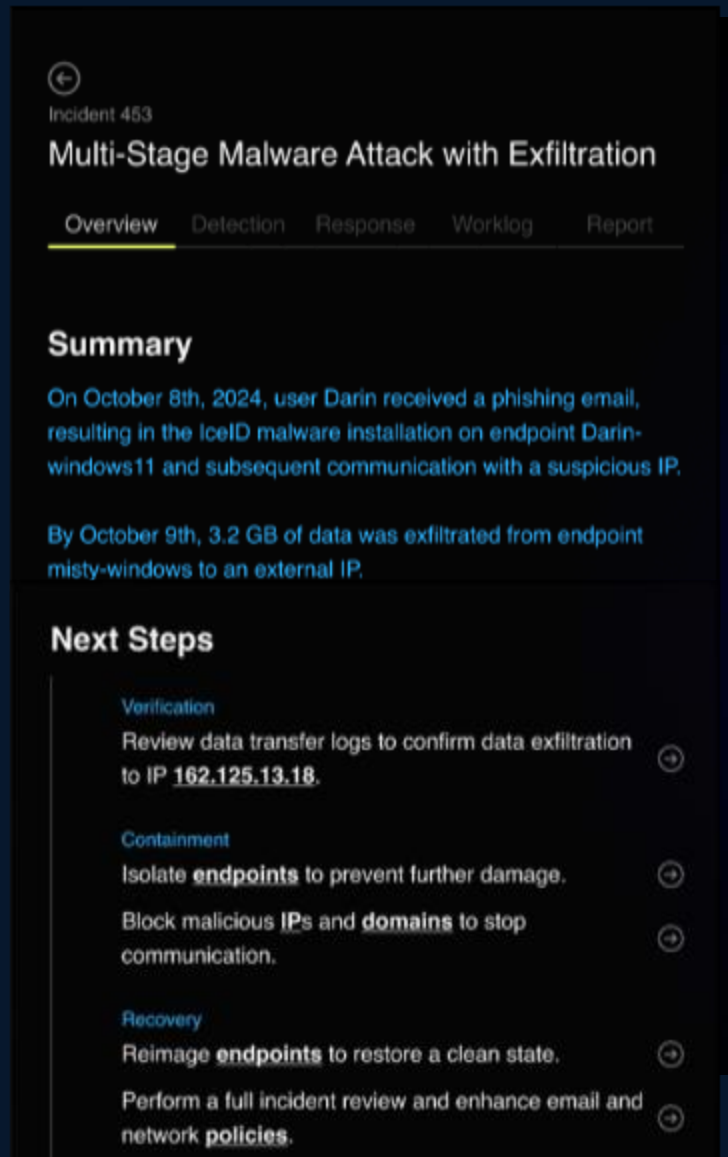
Instant Attack Verification with a Clear Verdict

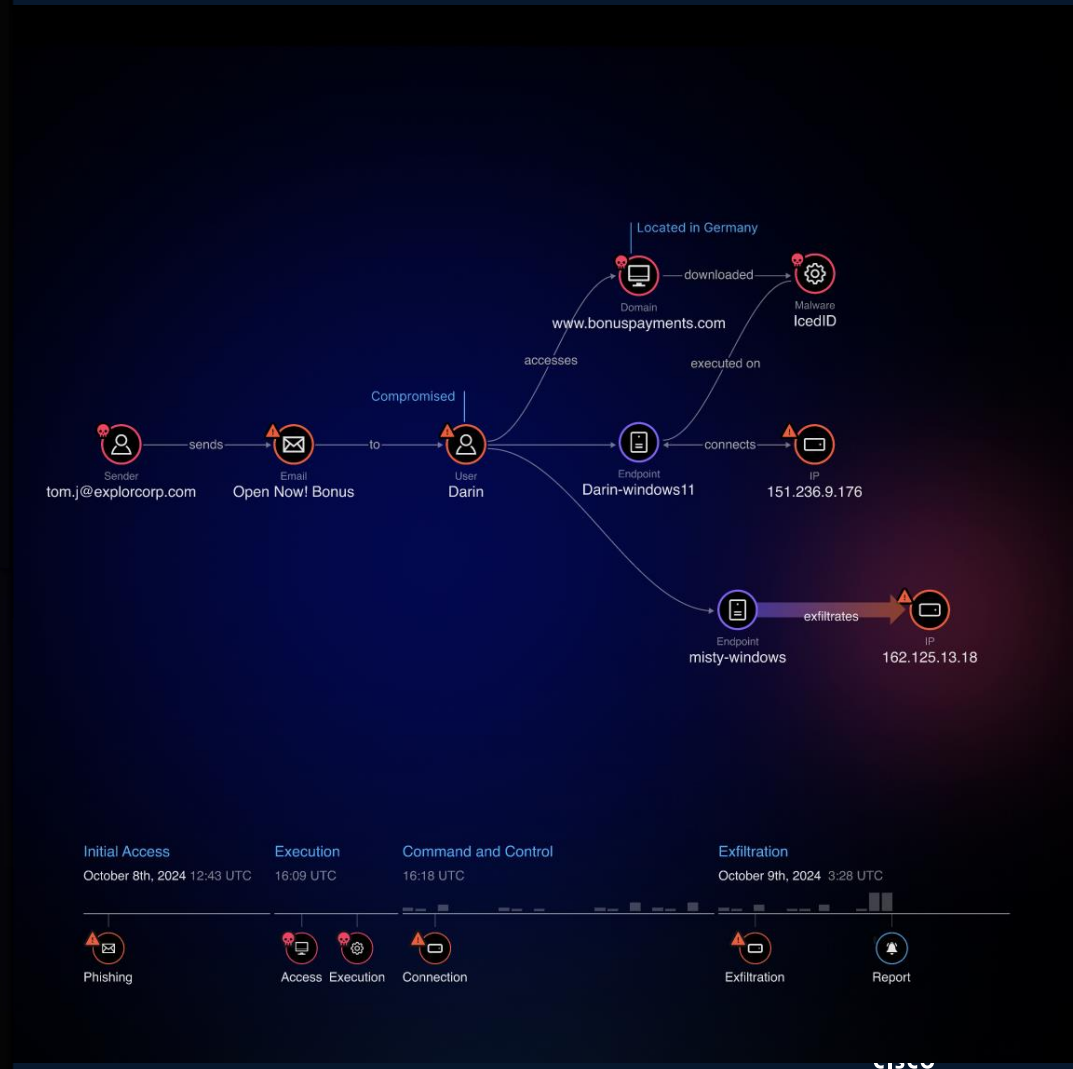
Clear verdict. Decisive action. AI speed.

Each alert is analyzed by AI agents to eliminate false positives

Multiple AI agents launch investigation plan to verify real attack with a clear verdict

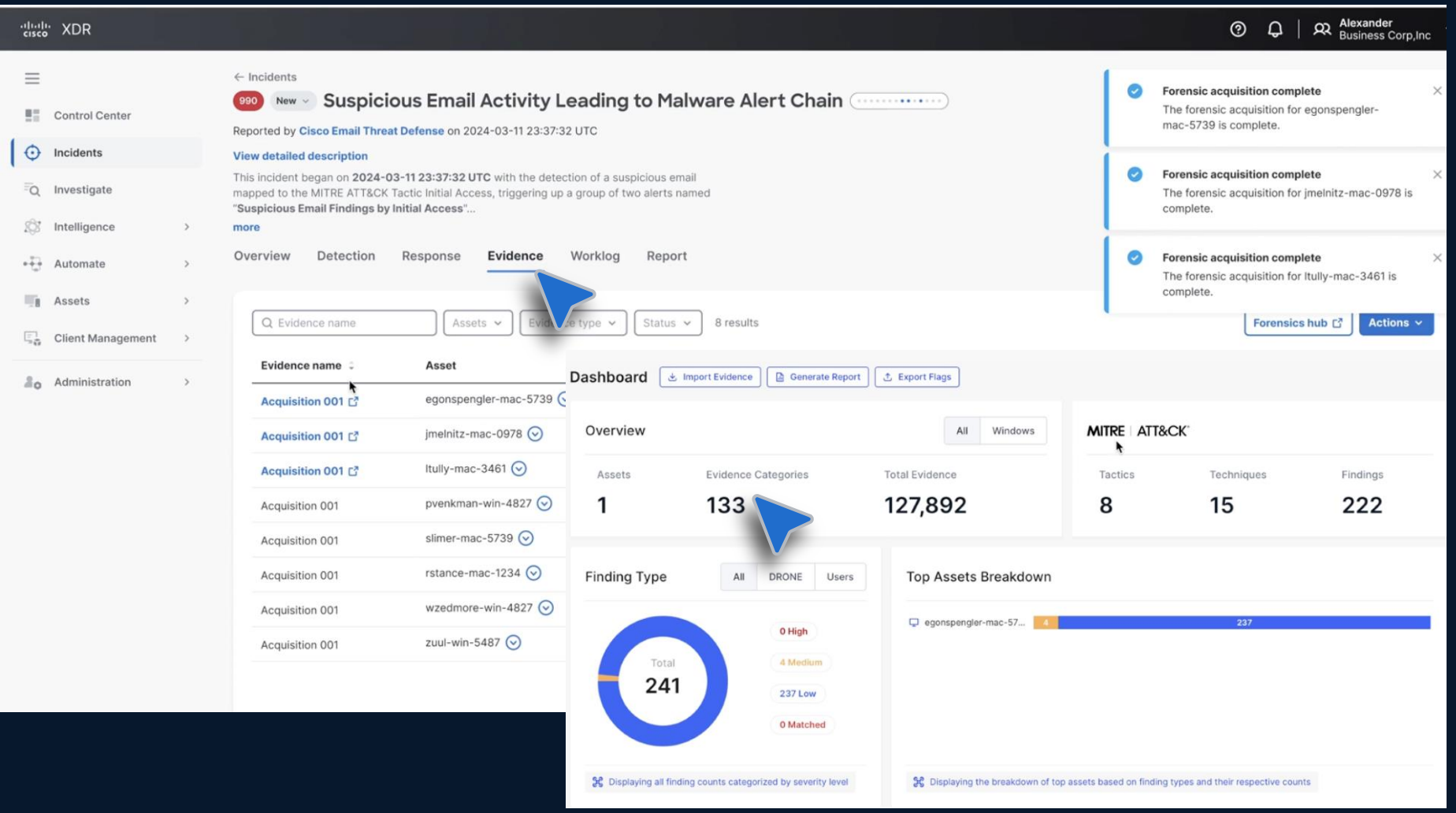
Trigger a decisive response through playbooks in XDR/ SOAR





Automated Forensics to Gather Evidence Instantly

Clear verdict. Decisive action. AI speed.



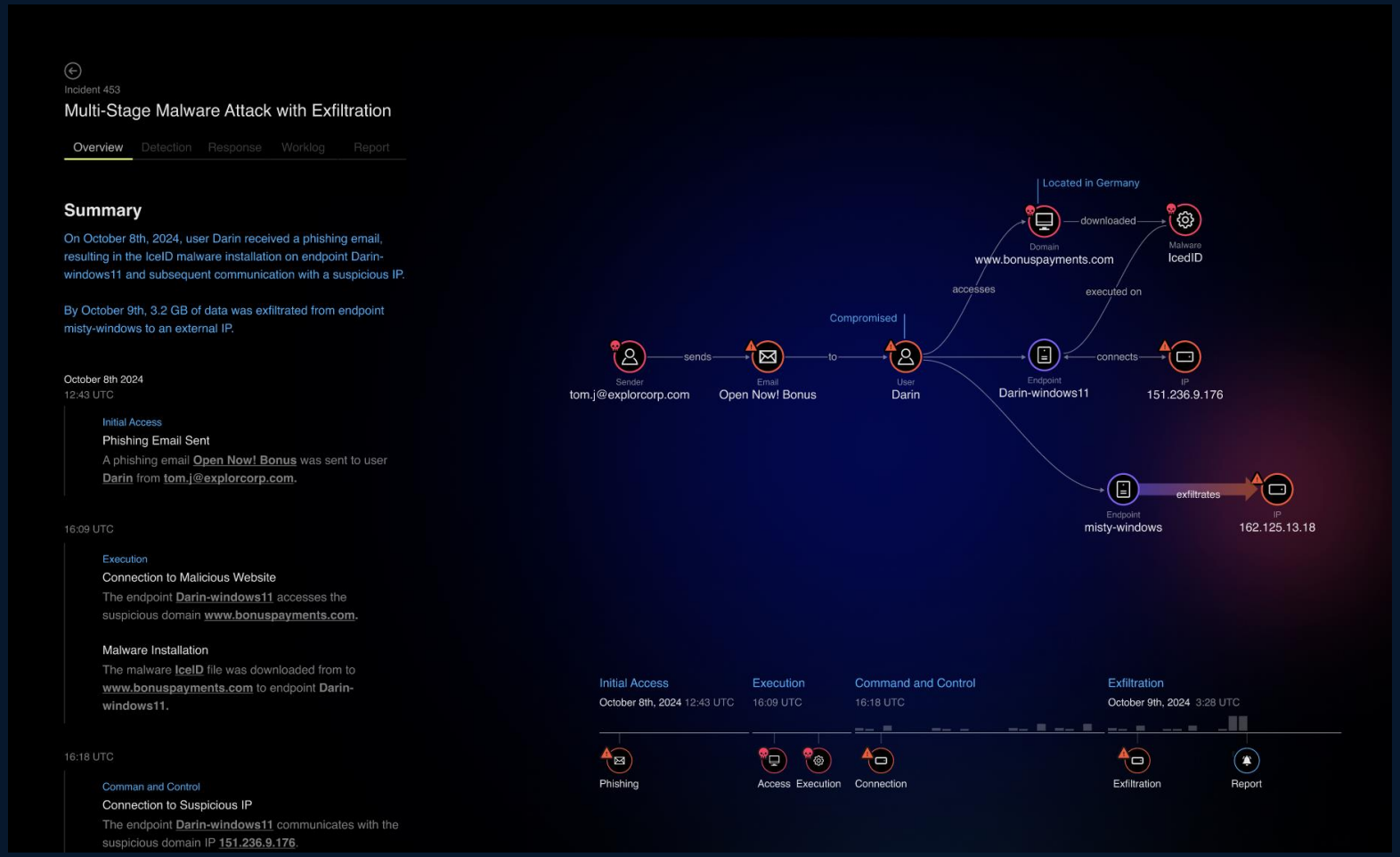
Trigger forensics before you know that you need it

100s of evidence components are captured even from compromised device

Evidence builds confidence to take decisive next steps

Attack Storyboard to Comprehend an Incident in 30 Sec

Clear verdict. Decisive action. AI speed.



Turn complex attacks into visual narratives with explanation summary

Attack graph mapped MITRE tactics

Unified workflow from investigation to remediation with no context switching

Cisco SOC of the future

Advanced threat detections

90
PERCENT

Faster to identify root cause of threats

- Real-time attack chain detection
- Curated and custom detections
- Automated threat enrichment with Cisco Talos

Cisco SOC of the future

AI-accelerated investigations

83
PERCENT

Reduction in case management time

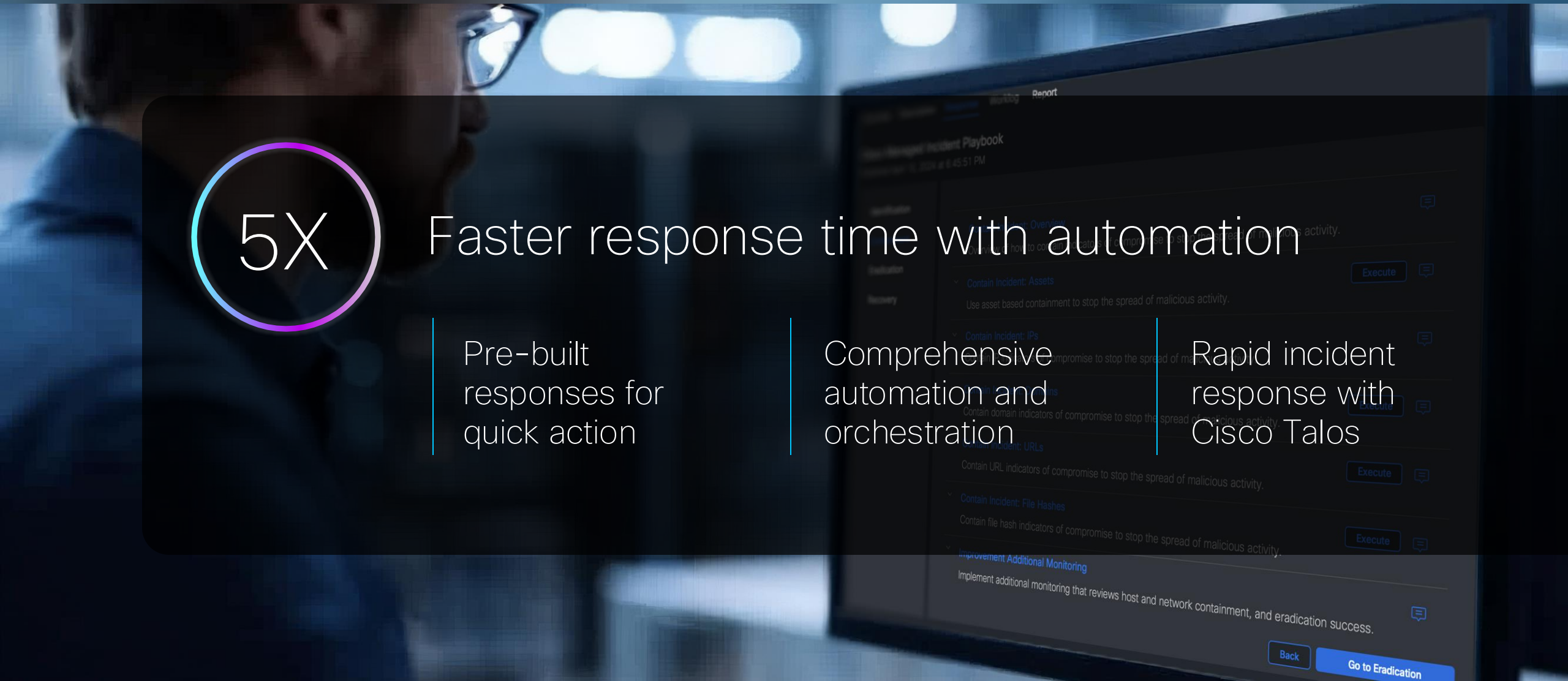
AI-guided investigations

Unified investigations and threat hunting

Fully automate threat analysis

Cisco SOC of the future

Automated response



5X

Faster response time with automation

Pre-built responses for quick action

Comprehensive automation and orchestration

Rapid incident response with Cisco Talos

The Cisco XDR difference

Clear verdict. Decisive action. AI speed.

Agentic AI paired with human intelligence

Create clarity and increase confidence in every decision with Agentic AI

Network + Endpoint at the core

Detect the most advanced attacks since Cisco XDR is powered by network insights

Open and unified approach to XDR

Get unified visibility via broad integrations with Cisco security solutions and third-party tools

Security Operations Simplified

Detect sooner

Prioritize by impact

Speed up investigations

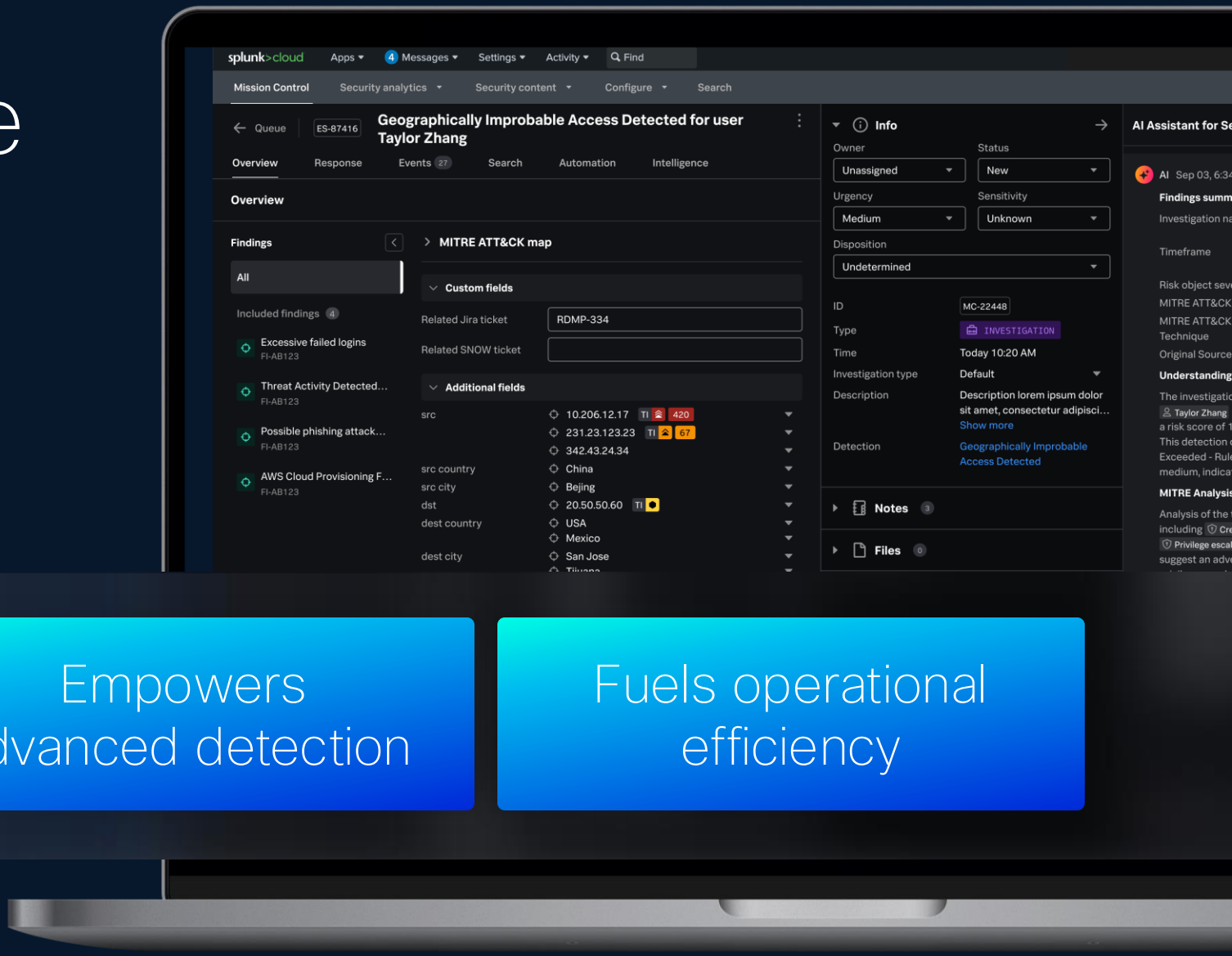
Accelerate response

cisco

Splunk ES: Using Insights to Exploit Every Advantage

Splunk Enterprise Security

Market-leading SIEM with AI-powered capabilities



Unmatched visibility

Empowers advanced detection

Fuels operational efficiency

Effective security operations require

Visibility

Of the Attack Surface

Telemetry & Logs

Cisco Security Cloud Technical Add-on: +25K downloads

+

Knowledge

Knowing what to look for

Threat Intel, Indicators, Detections, Context

Cisco Talos: 2,000 new samples analyzed every minute

+

Action

Ability to take Action

Policies, Blocking, Patching, Remediating

SOAR ecosystem: +300 connectors with +2,800 automated actions

cisco

Cisco SOC of the future

Federated data management

Reduction in event size for more efficient SecOps

Shape, store and access data your way

Optimize costs and enhance decision making

Data pipeline management to filter, mask, enrich, route data pre-ingest

Power the SOC of the future

Data Management and Federation

Search, Analyze and Manage Data Wherever it Resides

Effectively manage complex data management needs. Seamlessly access data stored across different data stores for search and analytics.

Transform Threat Detection

Tackle an Expanding Threat Landscape

Author and engineer detections to support a range of detection methodologies and effectively implement detection as code.

Reduce Risk Exposure

Reduce Your Exposure to Risk and Compliance Gaps

Unleash continuous asset discovery to enhance compliance posture and close gaps in security controls.

Simplify SecOps with AI

Simplify the Analyst Experience with AI

Augment your SOC team with AI to help analysts with routine yet error-prone tasks such as writing investigative summaries.

Unify TDIR

Unify TDIR with Automated Workflows

Coordinate and collaborate across the TDIR lifecycle with automated workflows using custom SOAR playbooks.

cisco

Cisco integrations made seamless

The Cisco Security Cloud app enables easier integration of your Cisco data sources within Splunk

Single application that packages all Cisco Security integrations in a single offering based on “gold standard” best practices

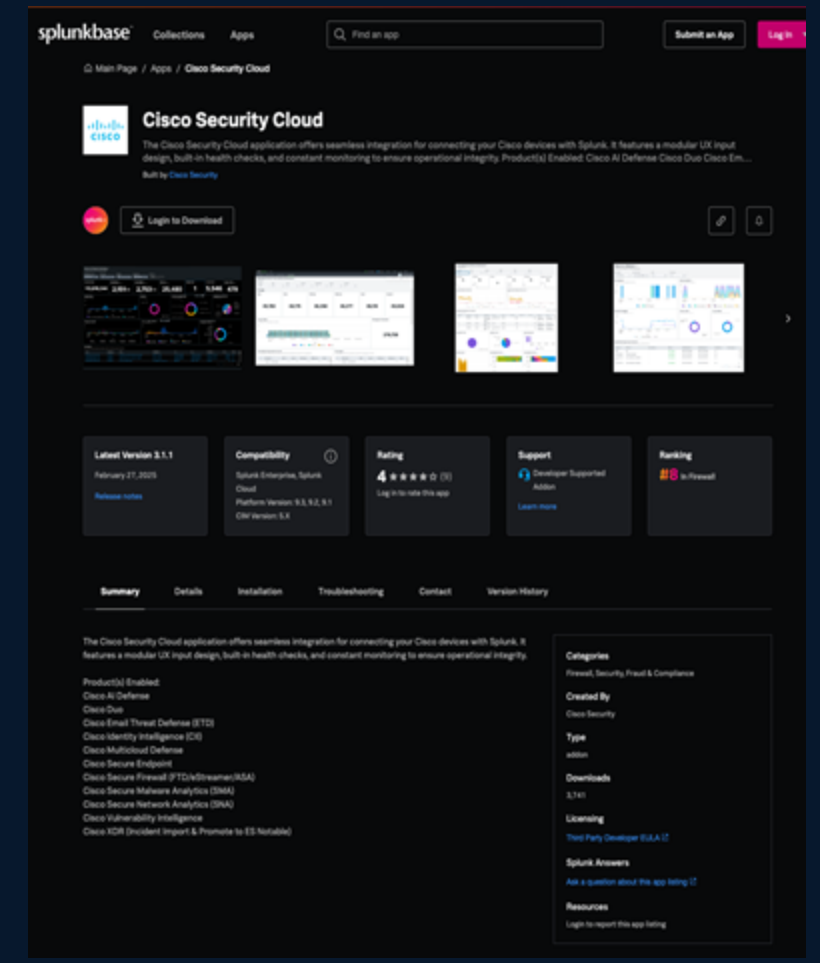
Replaces the older individual Cisco TA's and Apps that are now archived

Available Today:

- AI Defense
- Secure Network analytics
- XDR (Incident Reporting)
- Email Threat Defense
- Multi Cloud Defense
- Secure Firewall (FTD, Estreamer, ASA)
- Malware Analytics
- Secure Endpoint
- Kenna Vulnerability Intelligence
- Identity Intelligence
- Duo

Next Up:

- Secure Workload
- Isovalent (Hypershield)
- Crosswork Cloud



Splunk Security delivering a comprehensive approach

World class detection approach for the SOC of the future

Pre-built detections
- 1,700+ Curated Detections by Splunk Threat Research
- 225+ Analytic Stories
- 75+ Automation Playbooks

Rule-based detections
- Event-based Detections
- Findings-based Detections
- Adaptive Response Actions
- Automation Rules and SOAR Playbooks

Dynamic detections
- ML-based Detections
- Real-time Behavioral Analytics
- Risk-Based Alerting

Custom detections
- Fully customizable built-in detections
- Full flexibility to create custom detections
- Machine Learning Toolkit

Automatic threat intelligence enrichment

(Threat Intelligence Management, Talos Threat Intelligence, 3rd Party)

Integration with cybersecurity frameworks

(Threat Topology Visualization, MITRE ATT&CK, NIST CSF 2.0, Cyber Kill Chain®)

Detection authoring and management

(Automatic Detection Versioning, Open-Source Tools)

NEW

Security Insight, on Us

Free Cisco firewall logs to Splunk*

AVAILABLE since August 2025

New detections | Automated response

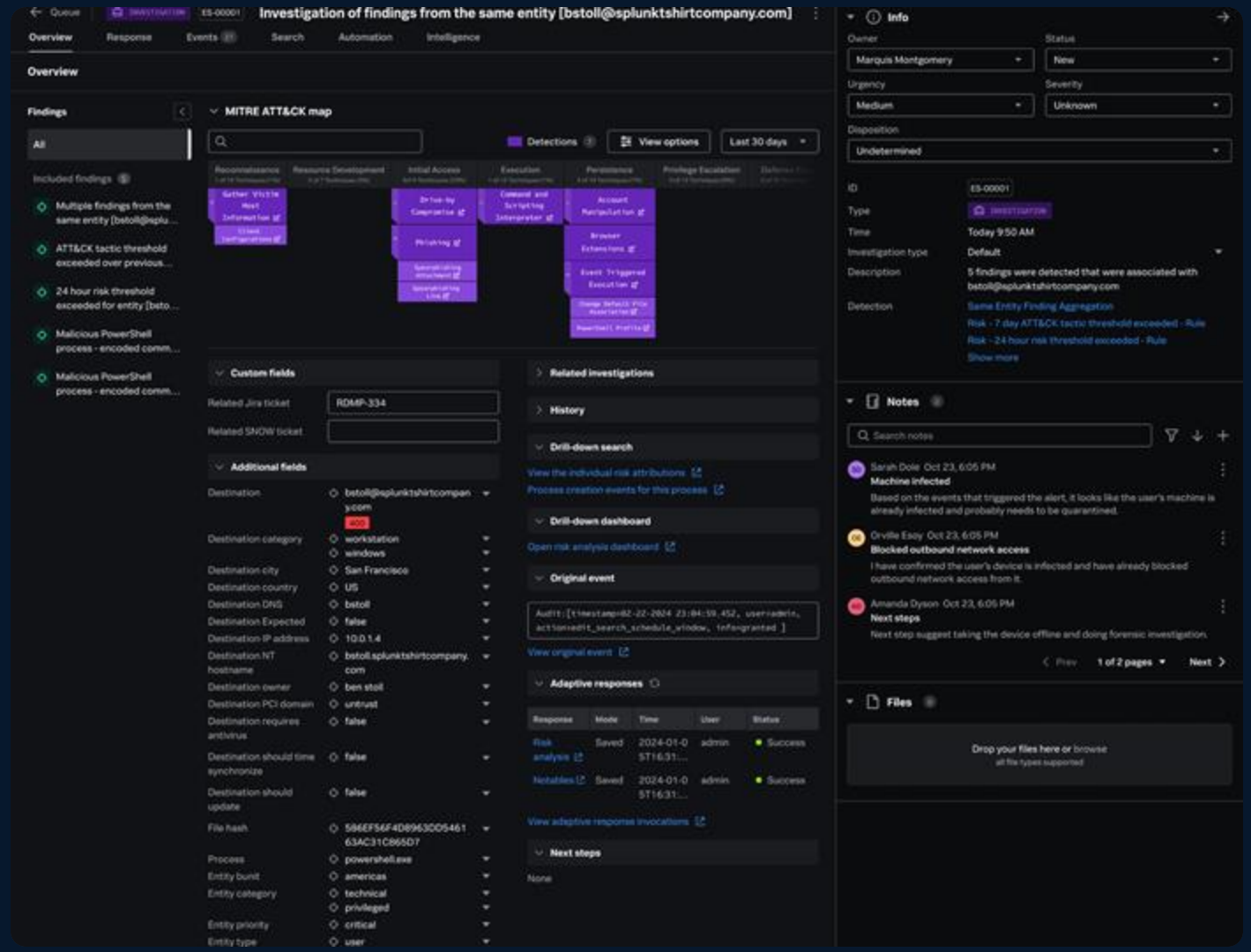
*Ingest up to 5GB/device/day requires Firewall Threat Defense subscription and Splunk license

cisco

Enterprise Security 8.0

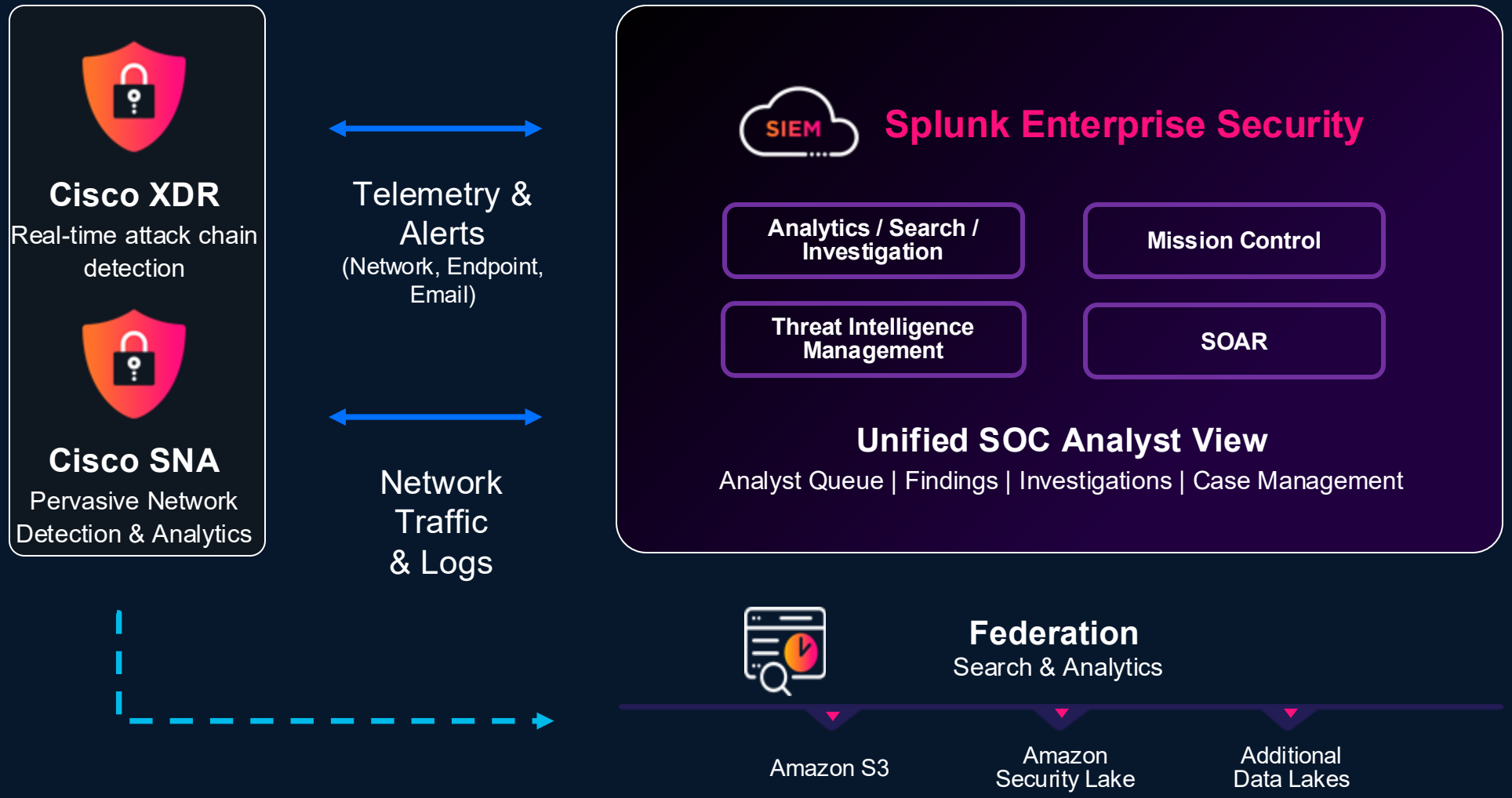
The Market-Leading SIEM to Power the SOC of the Future

- Improved case management capabilities
- Native Splunk® SOAR integration
- Enhanced detection engineering capabilities
- Simplified terminology for security analytics



Unifying Threat Detection, Investigation and Response

Splunk Enterprise Security: The Core of the Unified TDIR Experience



The SOC: Float Like a Butterfly, Sting Like a Bee

Splunk and Cisco drive actionable insights

Splunk + Cisco = Unmatched outcomes

4PB+ data ingested daily

800B+ Security events daily

1B Endpoints

625B Web requests analyzed daily

Stop billions of attacks

Ensure resilient networks and applications

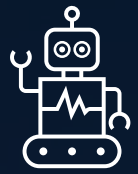
But what does this mean in practice?

cisco

Strategy Guiding Principles

Integration

- Combine the best fit of the Cisco + Splunk portfolios to deliver a custom-fit solution unique to Customers needs.
- Allow for all personas to work within a similar set of views/platforms to reduce switching costs and tool sprawl.



Automation

- Make hyper-automation a priority in all aspects of the design and execution of this solution.
- Innovate wherever possible to reduce manual work and total cost of ownership.
- Increase Customers potential for future success and scalability.

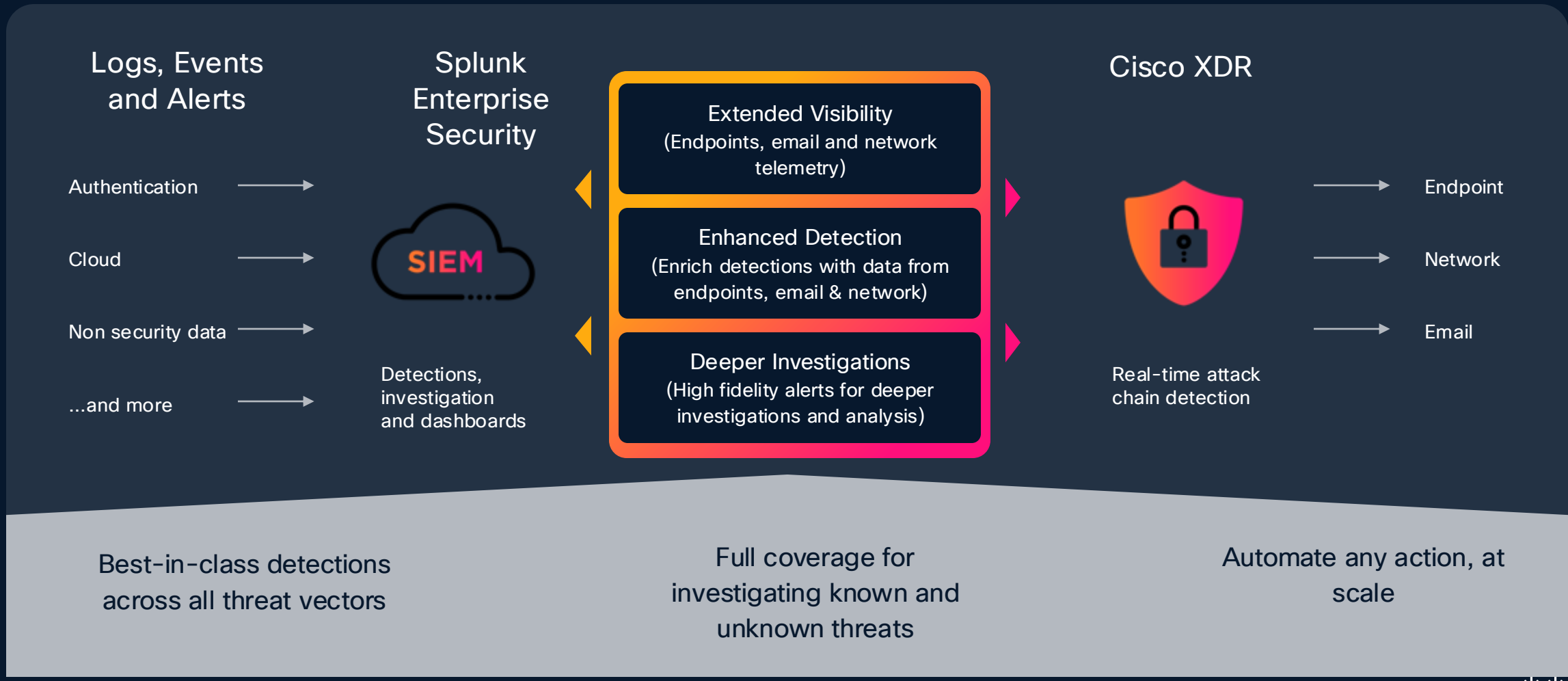
Simplicity

- Define guidelines around data hygiene and intake processes to reduce technical debt and complexity.
- Implement processes around continuous monitoring and improvement of data sources, reports, and detections.

cisco

Expand detection surface and context

Cisco XDR integration with Splunk ES



Best-in-class detections across all threat vectors

Full coverage for investigating known and unknown threats

Automate any action, at scale

Unified TDIR: XDR w/Splunk dashboards, federated search and long-term log storage

Easy Button

XDR

- Easy button
- Foundational TDIR
- Out of box workflows and basic investigation
- Integrated SOAR
- Fewer 3rd Party integrations than Splunk
- Complete Forensics
- Agentic AI Investigations
- <1 year storage

Increasing Maturity & Sophistication

XDR w/ Splunk Core Platform (Splunk Enterprise)

- Everything in XDR
  - Unlimited integrations
  - Splunk Dashboards
  - Investigation (SPL)
  - Federated Search
  - Cloud Only Deployments (AWS)

Splunk Enterprise Security (ES)

- On-prem support
- PCI /SOX HIPAA compliance requirements
- FedGov Certification requirements (FIPS/CC/IL5+)

Splunk Enterprise Security (Ess/Adv) w/ XDR Detections

- Ad-hoc investigations
- Deep Threat Hunting
- Bespoke workflows
- Unlimited Automation
- Detection engineering
- XDR pre-built detections
- Cisco XDR Forensics
- Agentic AI Investigations

Mature SOC

Splunk ES Premier w/ XDR Detections

- Everything in ES & XDR plus:
  - Custom detections
  - Insider Threat / UBA
  - Asset Risk Intelligence
  - SnapAttack detections

XDR UI	**XDR UI w/ Splunk dashboards**	**Splunk UI**	**Enterprise Security UI w/ XDR Pivots**
XDR Storage	**XDR & Splunk Storage**	**Splunk Storage**	**Splunk & XDR Storage**

Additive features & functionality starting with XDR, adding Splunk Core then layering in Enterprise Security advanced security use cases

Customer Product Integrations - Security

Foundational	Transformative	Maximized

Efficient User and Workload Pricing

Breach Protection Suite
Cisco XDR

Premier – Managed XDR
Advantage – Third-Party Integrations
Essentials – Cisco Only

Cisco XDR + Splunk Cloud / Enterprise

Splunk Enterprise Security

Essentials	Premier	Add-ons
Cisco XDR	SOAR, TIM Cisco XDR, UEBA	Asset Risk Intelligence, Attack Analyzer

Breach Protection Suite
Secure Network Analytics, Secure Endpoint, Email Threat Defense, Identity Intelligence, Malware Analytics

Customer Provided Integrations
Email, Proxy/Secure Access Service Edge, Firewall, Netflow, Zeek, Packet Capture, Endpoint Protection, SOAR, Identity, Cloud, and others security tools.

Delivering critical capabilities for a foundational TDIR solution

	Cisco XDR	Splunk Security	Cisco + Splunk
Threat Detection:	Built-in detections focused on email, network & endpoint	Supports custom detections across any data source	Best-in-class detections across all threat vectors
Investigation:	Built-in workflows for common investigations	Flexible investigations including ad-hoc threat hunting	Full coverage for investigating known and unknown threats
Response:	Built-in responses for quick actions	Rich automations with custom playbooks	Automate any action, at scale.
	Easy-to-Use	**Flexible**	**Complete Solution**

Better together: SOC of the Future

Market leading SIEM + Innovative XDR

- Federated data management
- Advanced threat detections
- AI-accelerated investigations
- Automated response

EMBEDDED AI

CONTENT AND THREAT RESEARCH


User/Cloud/ Breach/


Networking


Third-party tools


Talos


Clouds


Devices


Data centers


Applications

cisco

What Cisco brings to the security problem

Thank you