CISCO Engage | Tech Day Miami

Transforming Security Operations to Punch Above Your Weight Class

Stronger Together: Elevate Your Security Game with Cisco and Splunk Integration

Jake Ruddy
Solutions Engineer, Security

Eric Meadows
Cybersecurity Leader - XDR

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

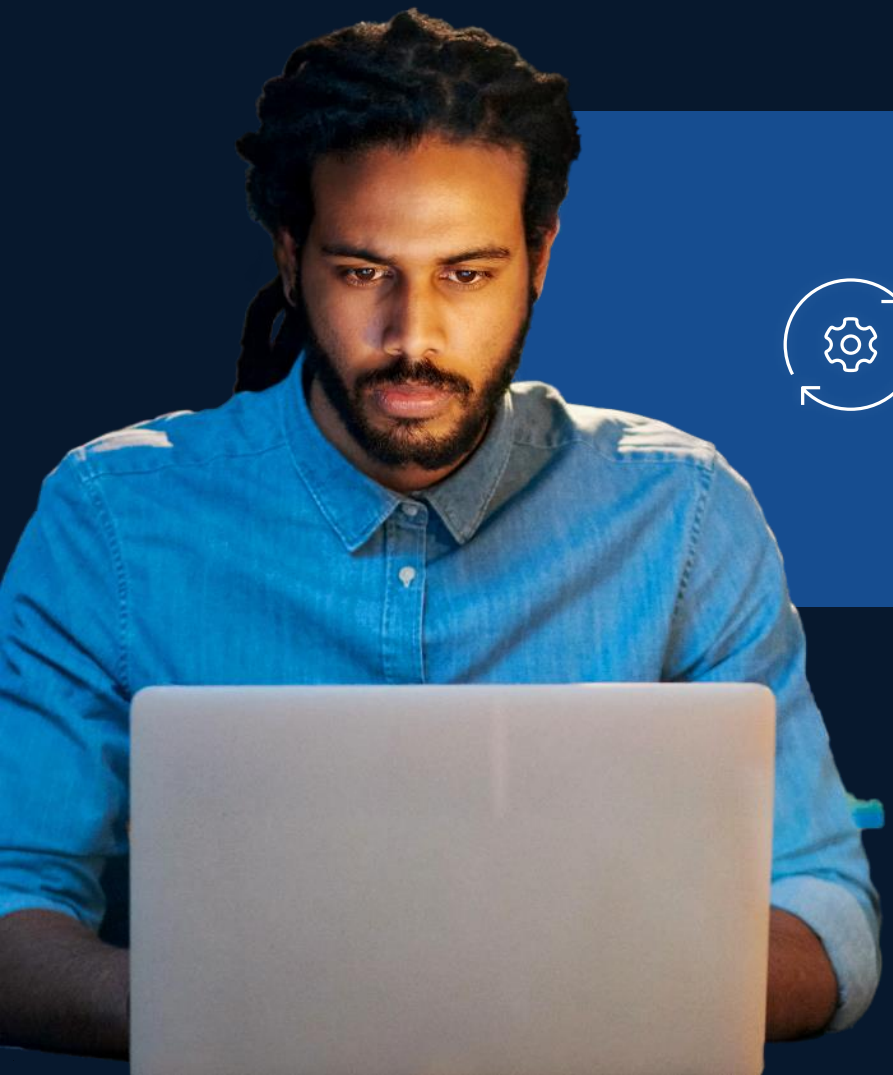
Organizations are doubling down on cyber resilience as it is critical to achieve digital resilience

“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

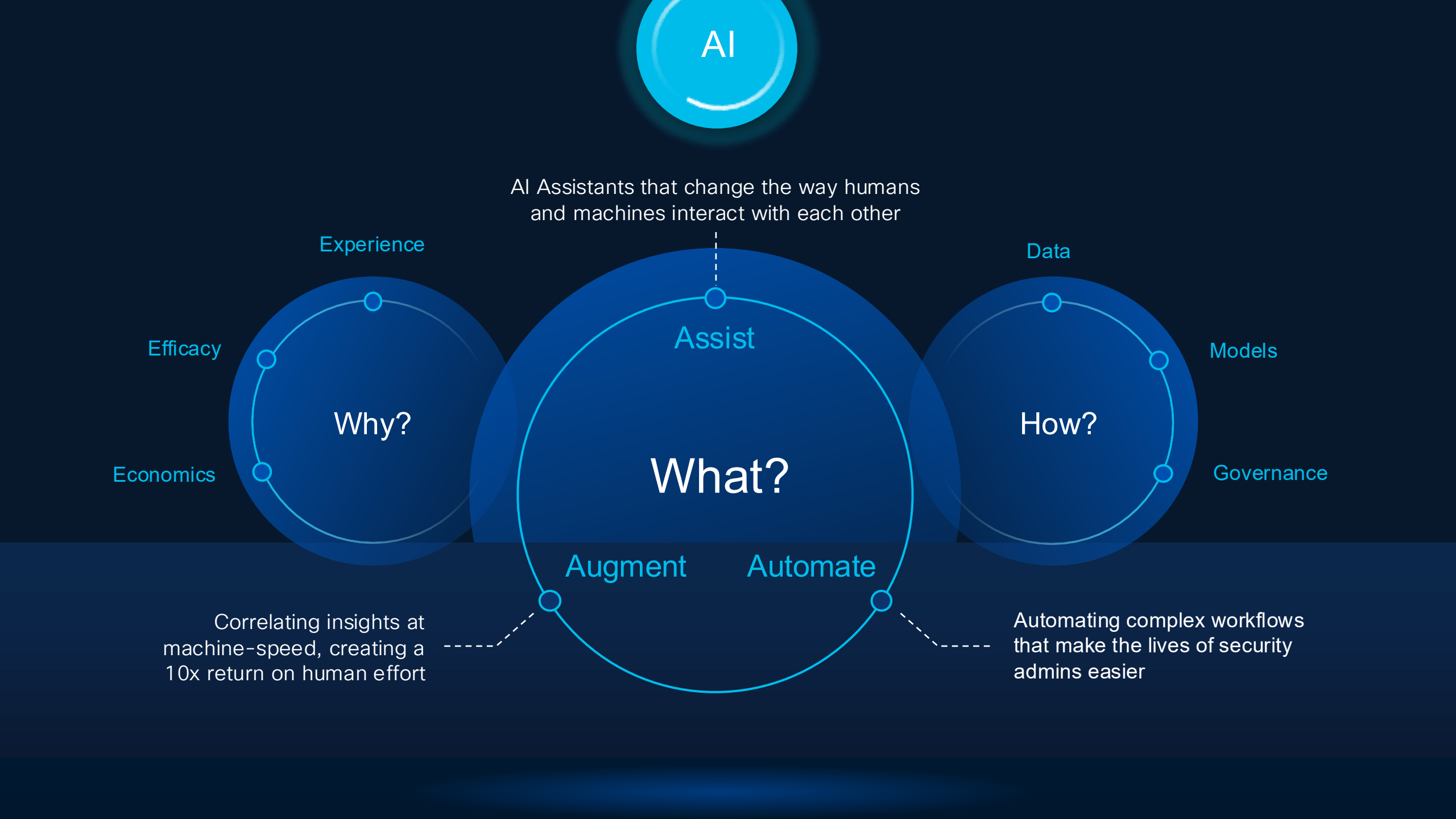
Engineering team

Shaping the SOC of the future

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.

XDR: Instincts and Fundamentals in the Ring

Our open XDR integrates with other security tools

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

Cloud Telemetry

Amazon Web Services, Google Cloud Platform, Microsoft Azure, Oracle Cloud Infrastructure

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

Endpoint Telemetry

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

Identifies tactics, techniques, and procedures (TTPs) used

Firewall Telemetry

Cisco Secure Firewall Threat Defense, Cisco Meraki MX, Check Point, Fortinet, Palo Alto Networks

Network Telemetry

Cisco Secure Network Analytics, Darktrace, ExtraHop

Apps/Email Telemetry

Cisco Email Threat Defense, Microsoft 365, Proofpoint

Prioritizing threats based on impact to the business

Telemetry data source importance

The top six data sources that customers believe are essential for XDR are:
Endpoint, Network, Firewall, Identity, Email, and DNS

Essential

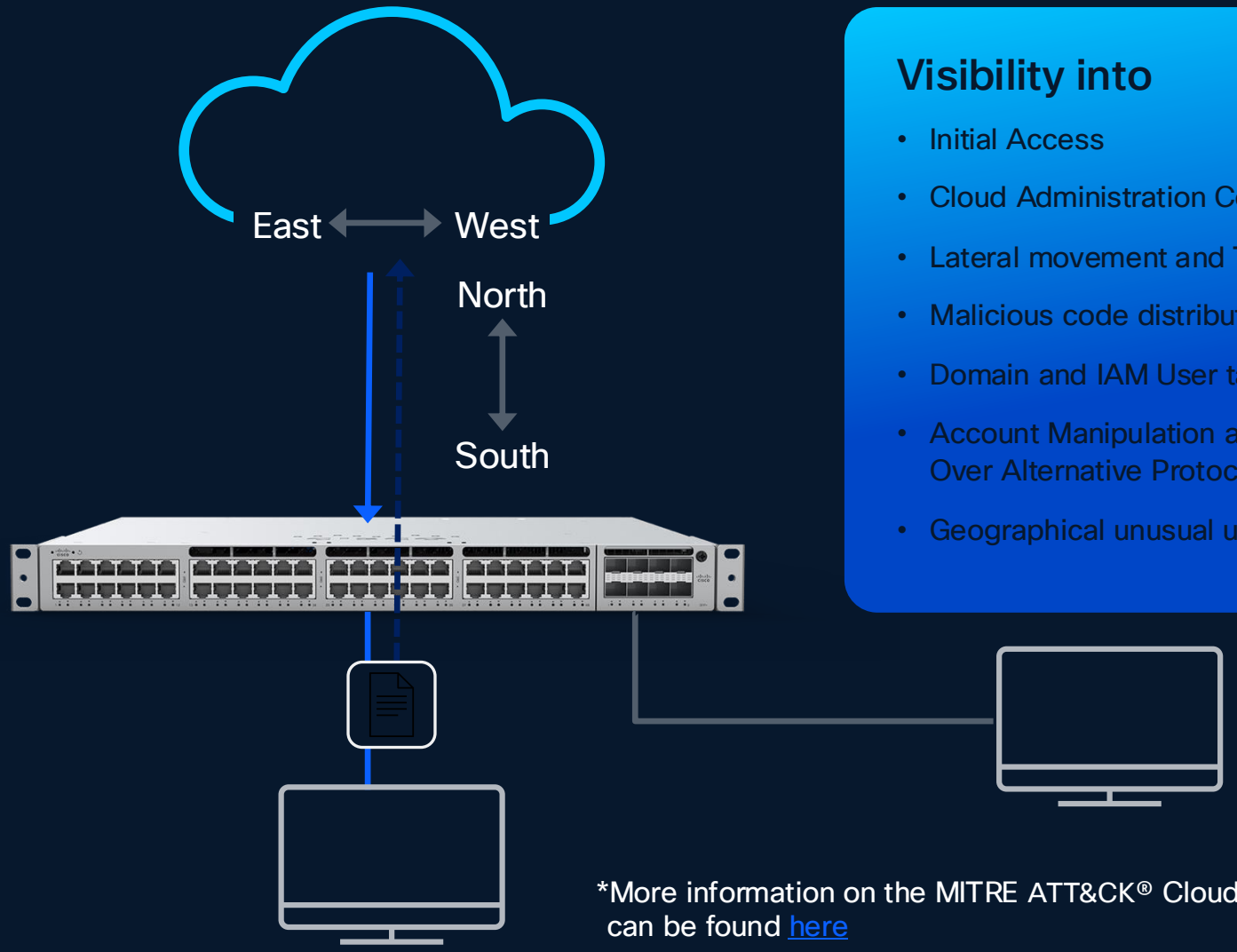
	Count	Share
Endpoint	255	85.0%
Network	226	75.3%
Firewall	207	69.0%
Identity	191	63.7%
Email	179	59.7%
DNS	140	46.7%
Public Cloud	137	45.7%
Non-Security Sources	36	12.0%

Cisco SOC of the future

The value with built-in cloud native NDR

Visibility into

- Indicators of compromise
- Malicious outbound/inbound behavior
- Command and control / heartbeat tracking
- More and more traffic is northbound due to cloud services like SaaS, PaaS, IaaS, Kubernetes, etc.



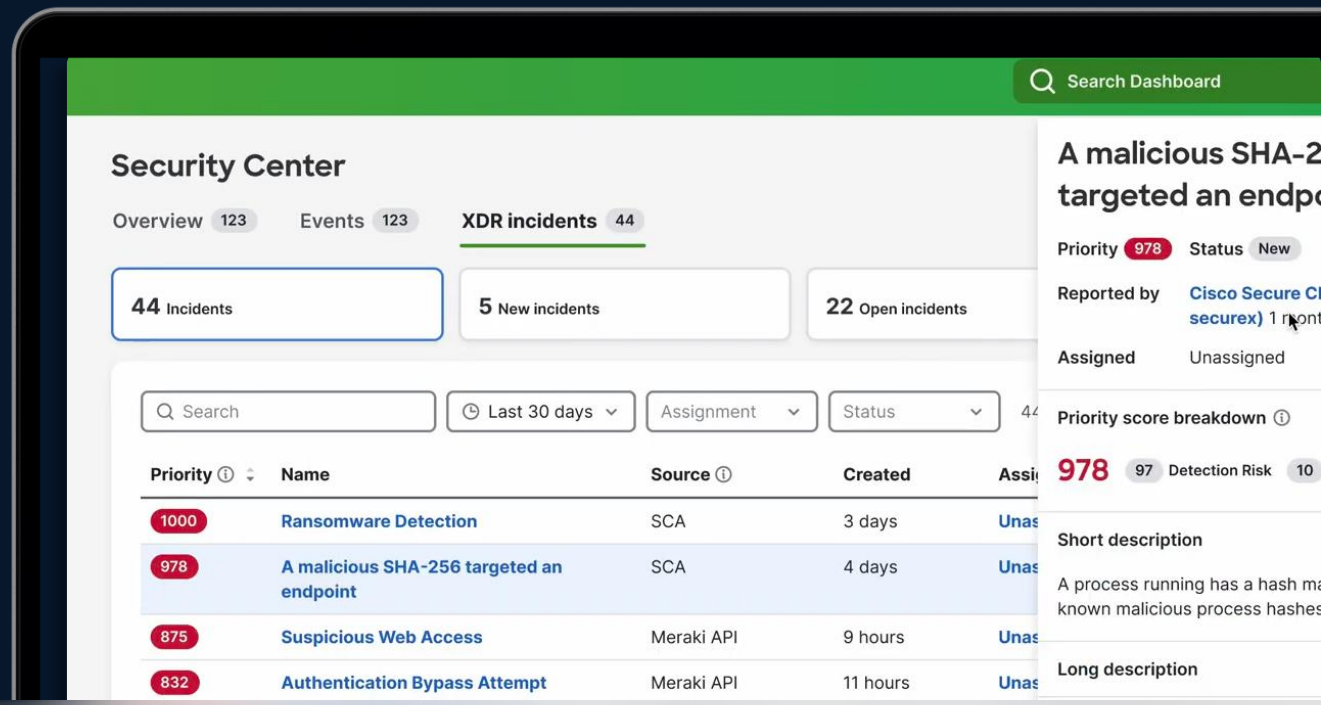
Visibility into

- Initial Access
- Cloud Administration Command
- Lateral movement and Transfer data
- Malicious code distribution and execution
- Domain and IAM User takeover
- Account Manipulation and Exfiltration Over Alternative Protocol
- Geographical unusual usage

*More information on the MITRE ATT&CK® Cloud Coverage can be found here

Cisco XDR

Innovating to detect and stop common attacks



Optimized for lean teams

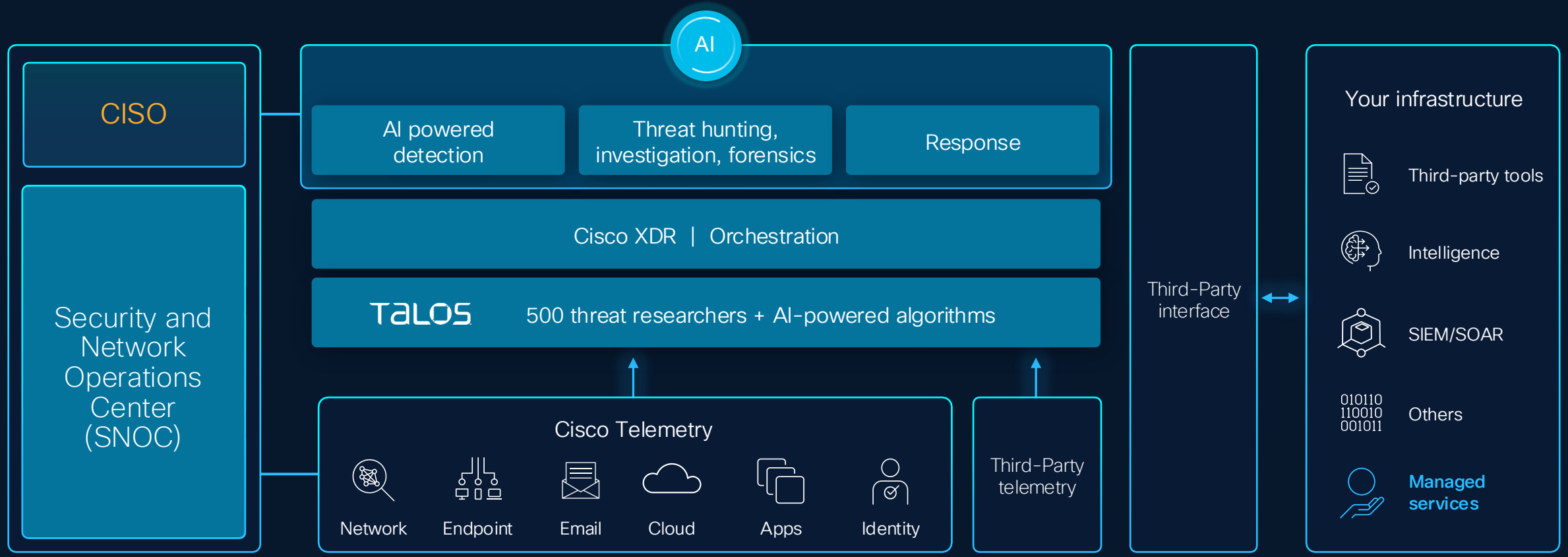
Speed to value

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

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.

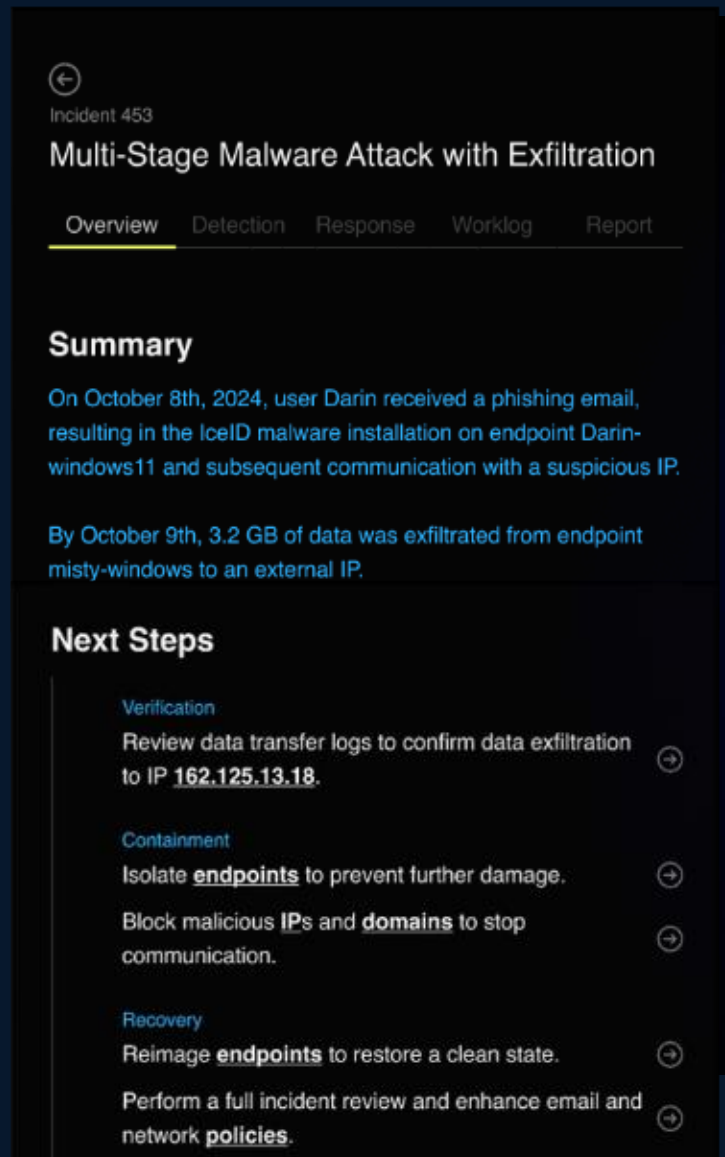
Instant Attack Verification with a Clear Verdict

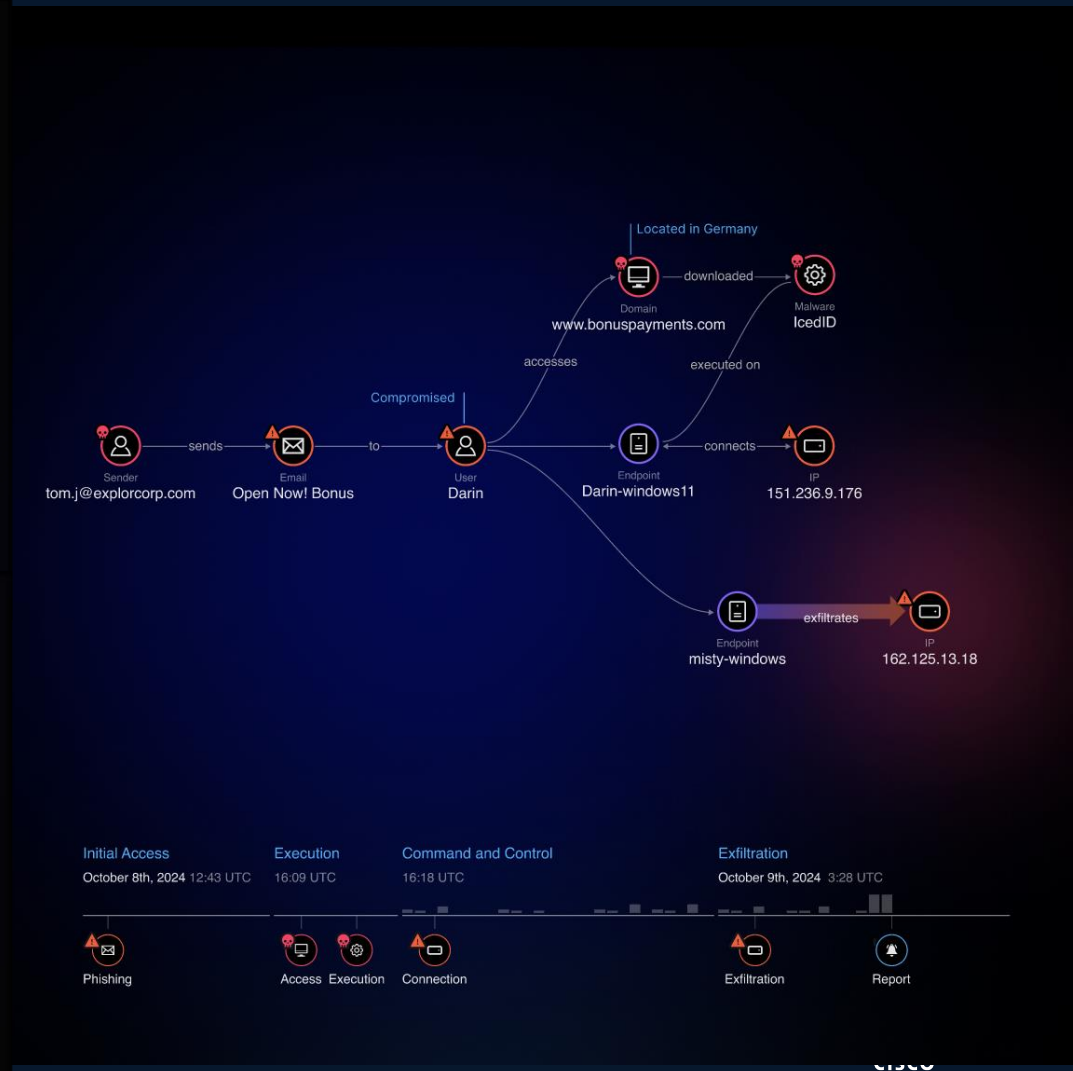
Clear verdict. Decisive action. AI speed.

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

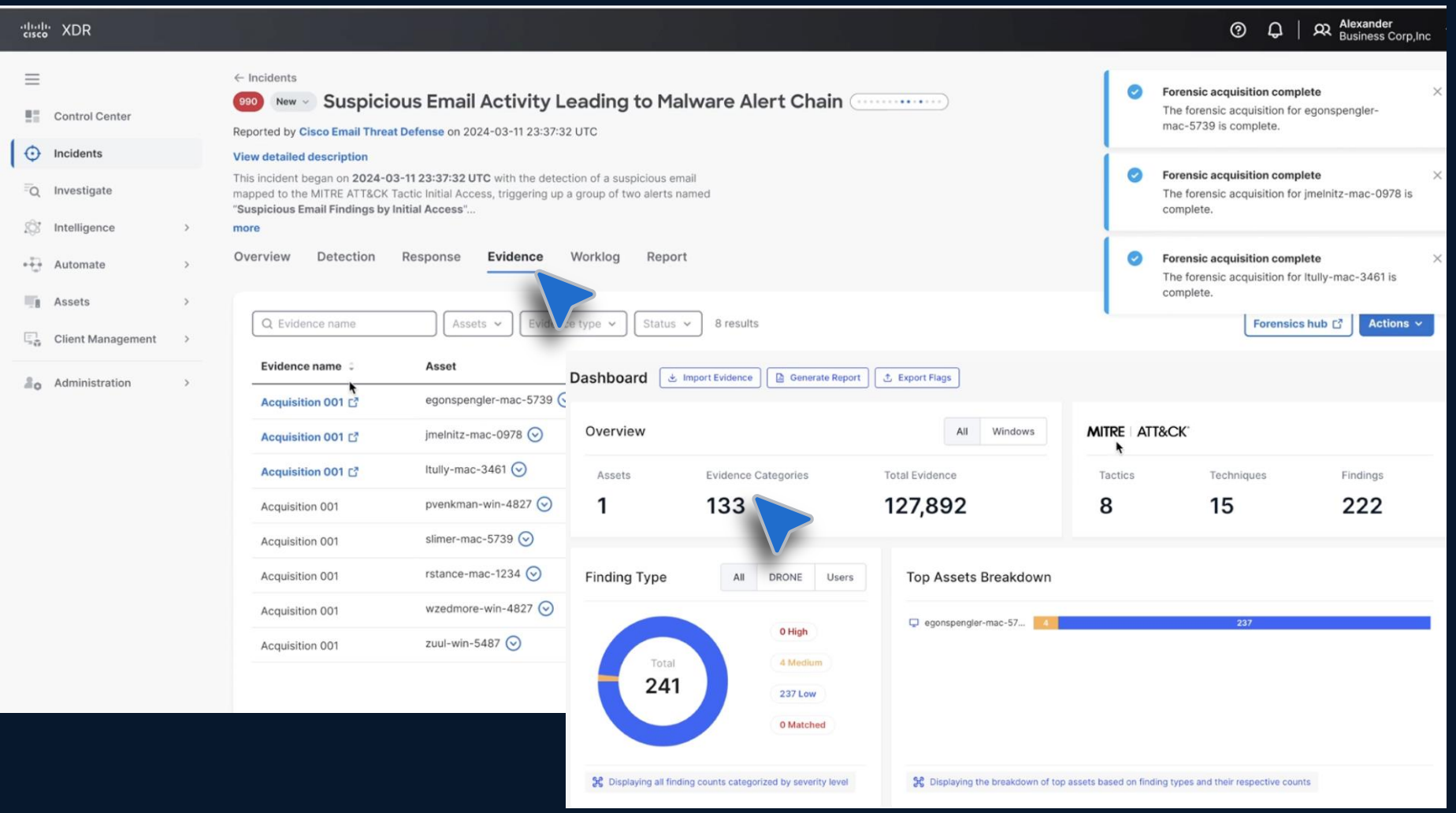
Trigger a decisive response through playbooks in XDR/ SOAR





Automated Forensics to Gather Evidence Instantly

Clear verdict. Decisive action. AI speed.



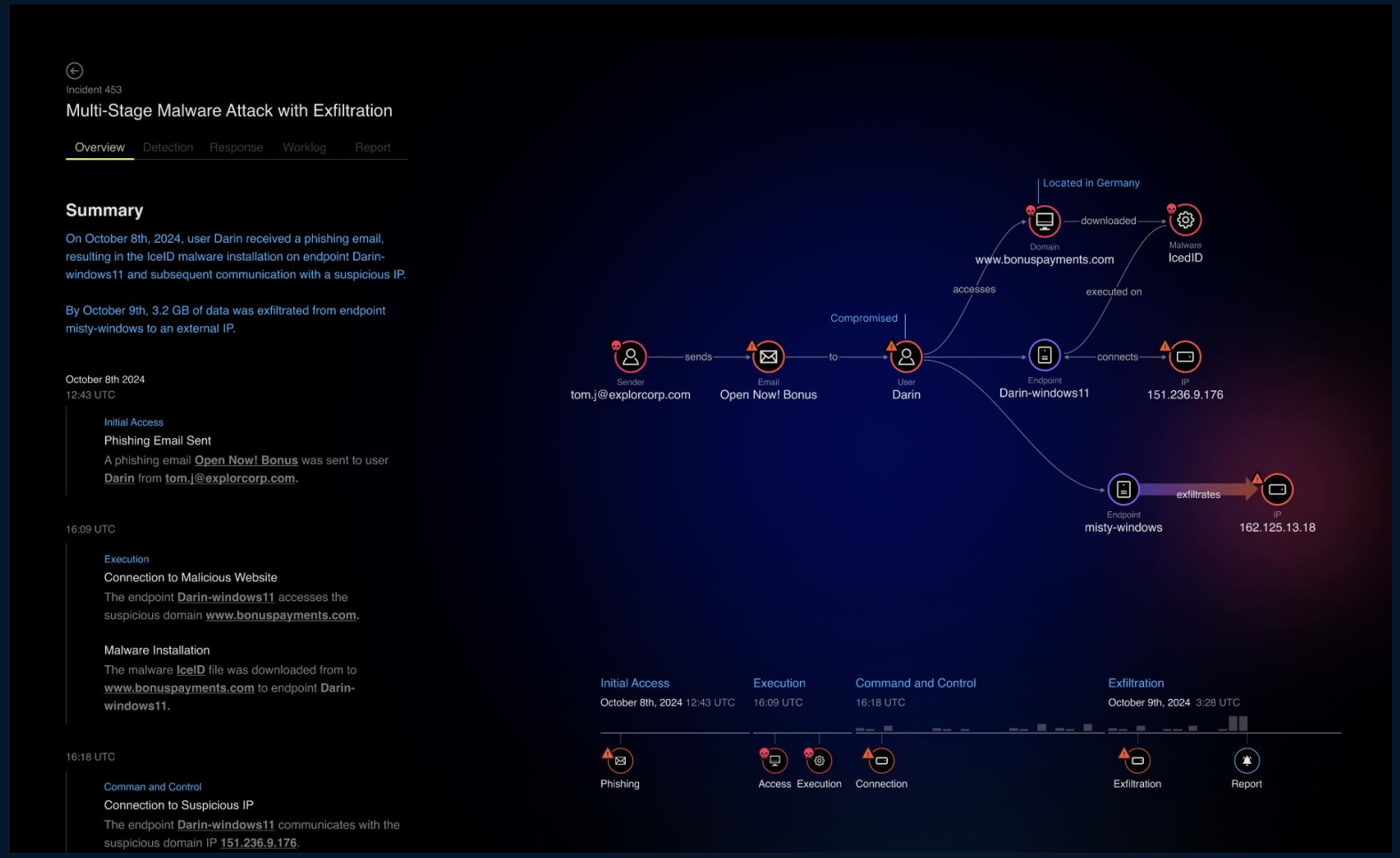
Trigger forensics before you know that you need it

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

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

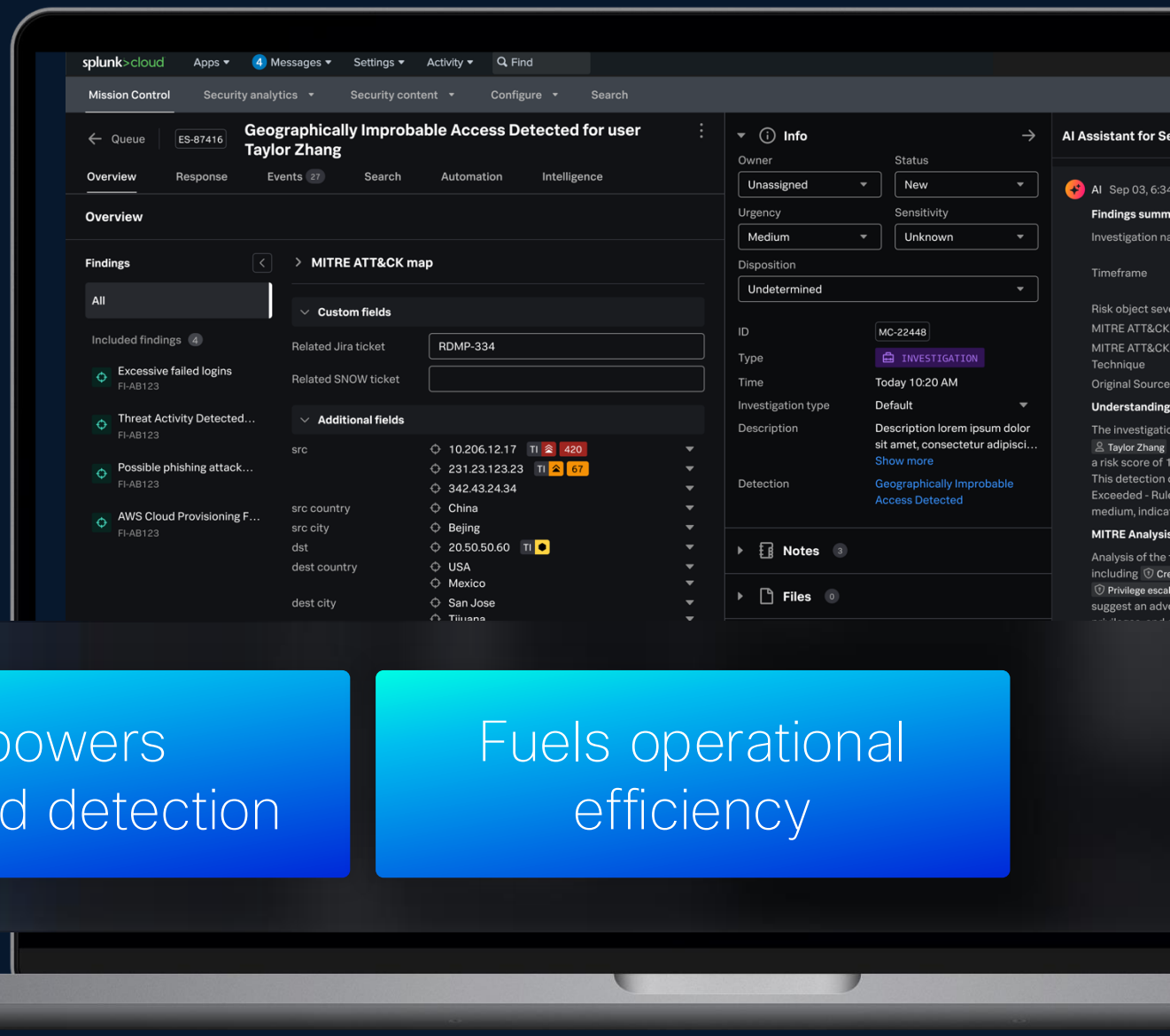
Speed up investigations

Accelerate response

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

+

Knowledge

Knowing what to look for

Threat Intel, Indicators, Detections, Context

+

Action

Ability to take Action

Policies, Blocking, Patching, Remediating

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

Cisco Talos: 2,000 new samples analyzed every minute

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

cisco

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 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

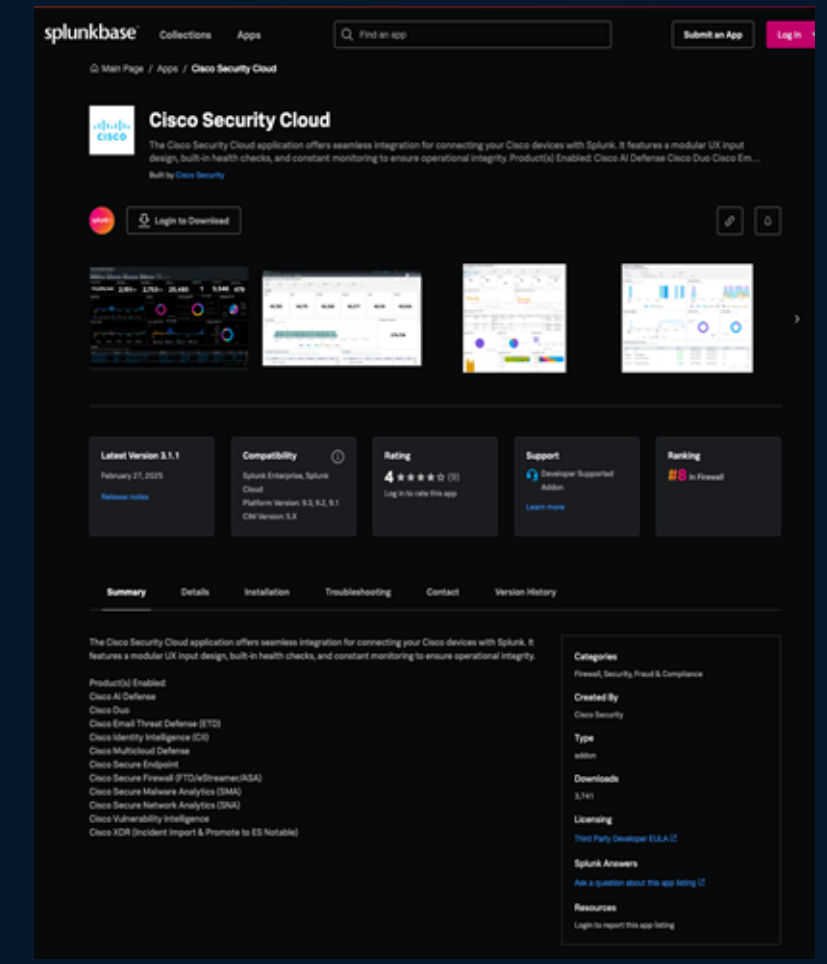
Replaces the older individual Cisco TA's and Apps that are now archived

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®)

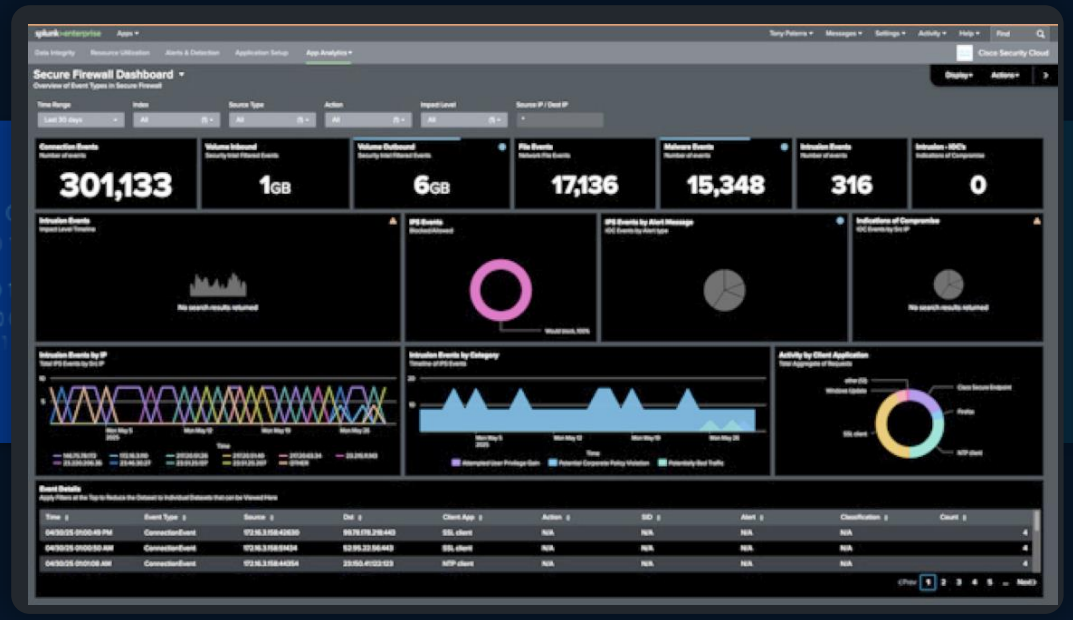
Detection authoring and management
(Automatic Detection Versioning, Open-Source Tools)

NEW

Security Insight, on Us

Free Cisco firewall logs to Splunk*

AVAILABLE since August 2025



New detections | Automated response

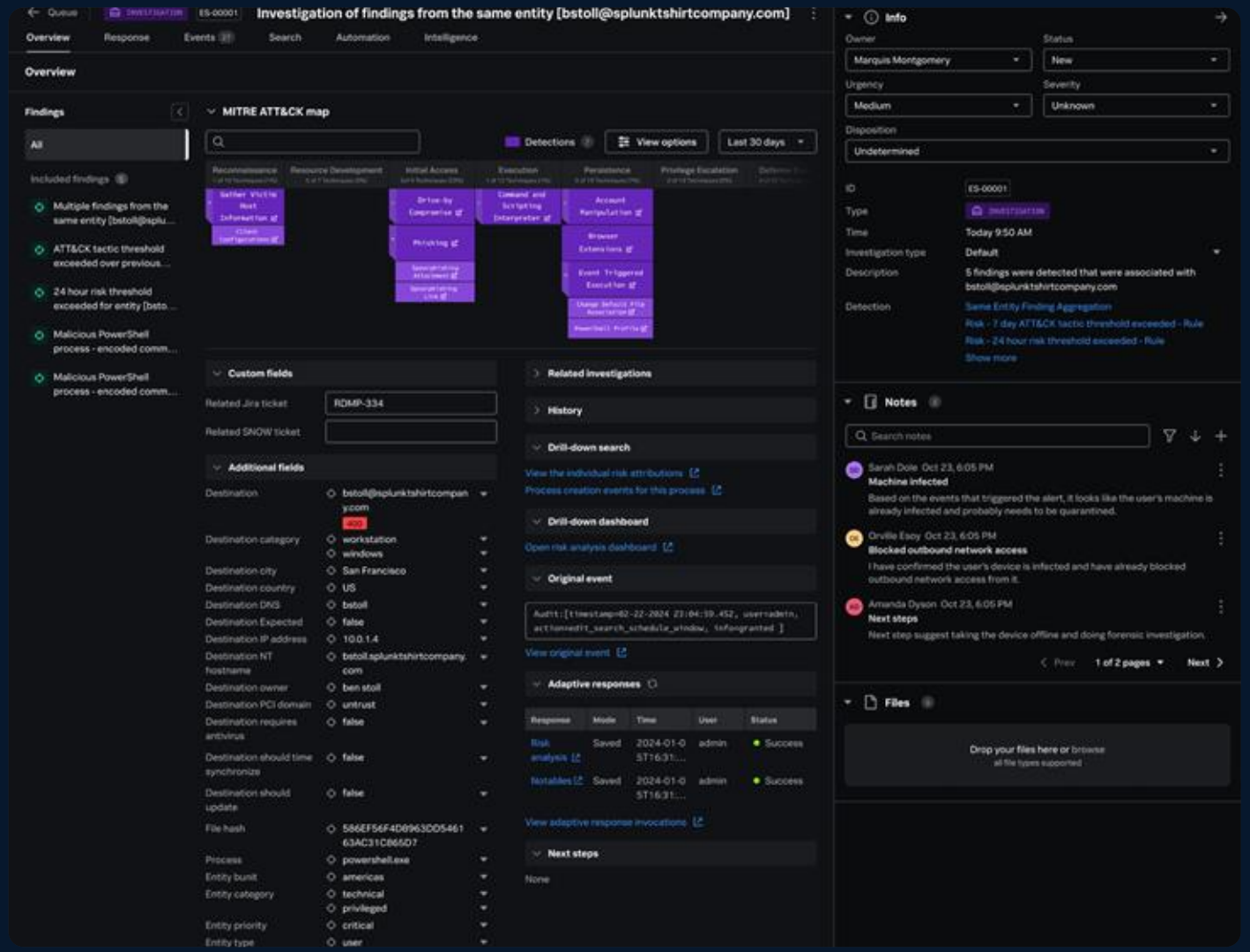
*Ingest up to 5GB/device/day requires Firewall Threat Defense subscription and Splunk license

cisco

Enterprise Security 8.0

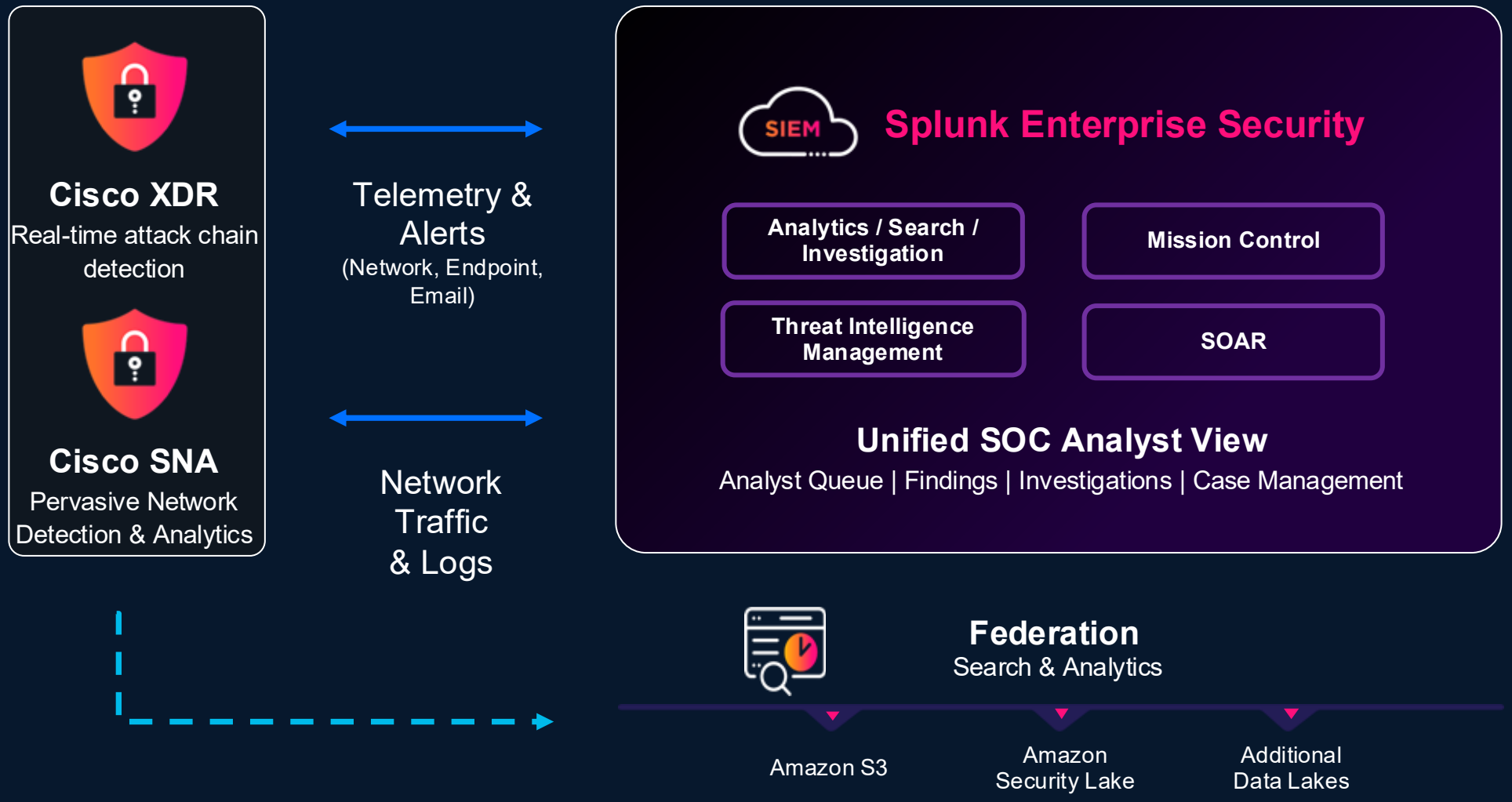
The Market-Leading SIEM to Power the SOC of the Future

- 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

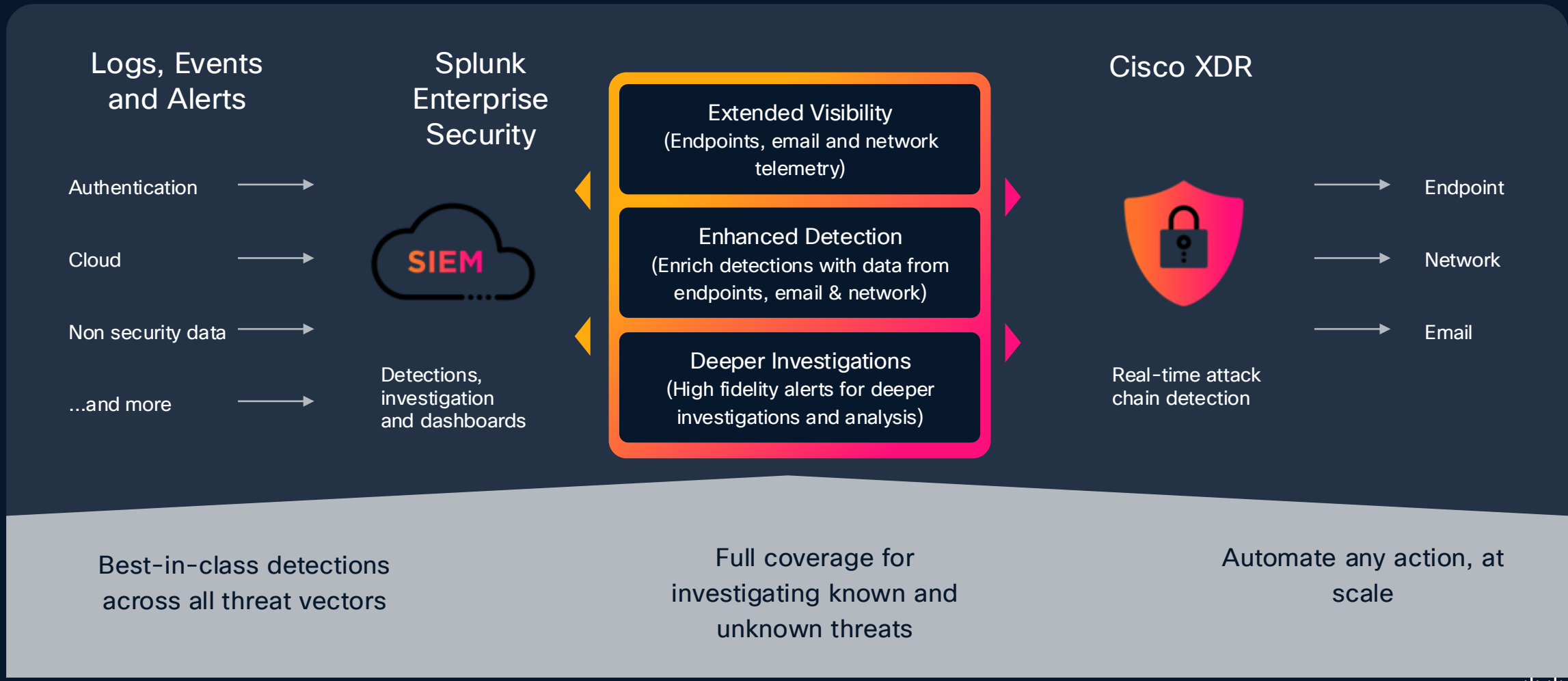
Ensure resilient networks and applications

But what does this mean in practice?

cisco

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

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

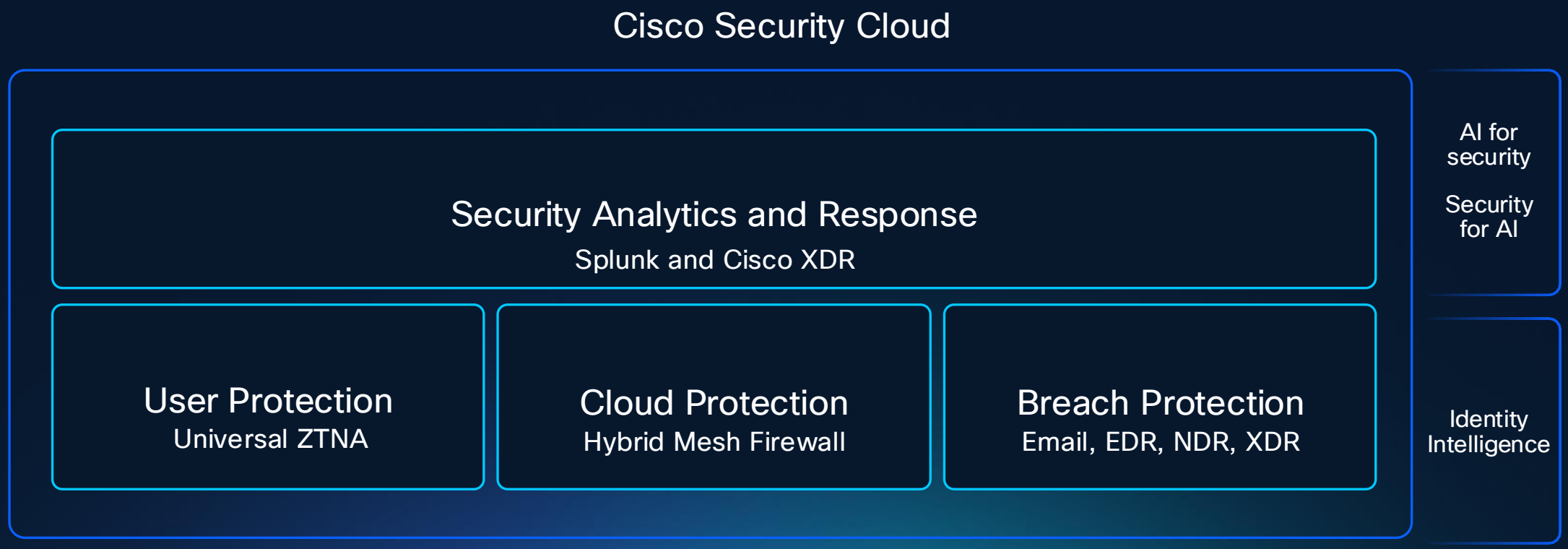

Devices


Data centers


Applications

cisco

What Cisco brings to the security problem



Thank you