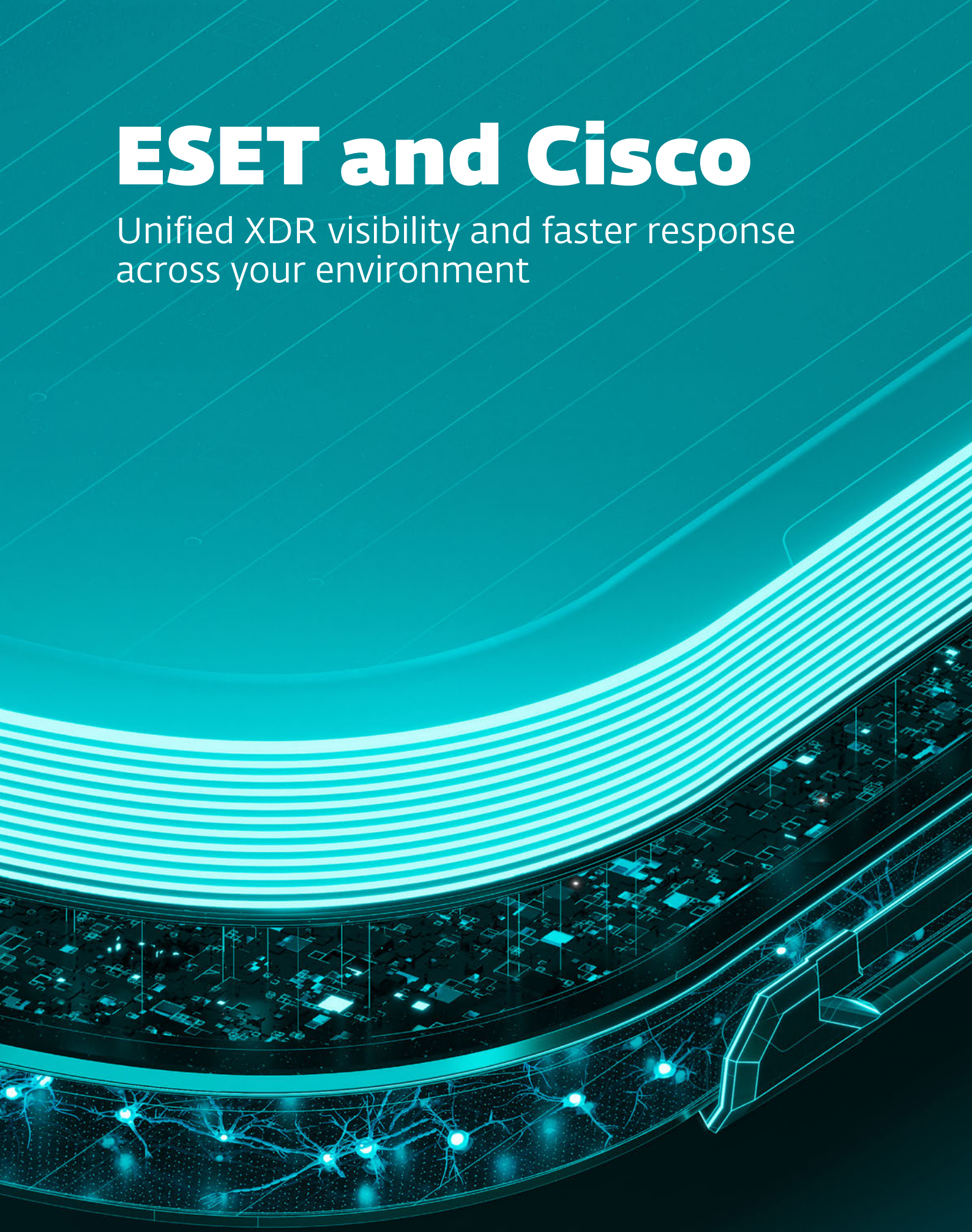
ESET and Cisco

Unified XDR visibility and faster response across your environment



eset Cybersecurity
Progress. Protected.

SOLUTION BRIEF

Consolidated endpoint and network intelligence for faster, more confident decisions

Security teams often struggle while juggling multiple consoles, data sources, and tools. When endpoint detections live in one place and network telemetry in another, investigations slow down, and threats can slip through the cracks. Organizations need a way to bring these worlds together, without adding complexity.

ESET's integration with Cisco XDR brings these worlds together seamlessly. The integration sends ESET PROTECT endpoint indicators into Cisco XDR, giving your SOC a unified view of endpoint, network, and cloud activity so analysts can respond faster and with more confidence.

KEY BENEFITS

BETTER RETURN ON EXISTING INVESTMENTS

Increase the value of both ESET and Cisco by connecting them, not replacing them. The integration enables you to build upon your current tools and processes, rather than starting from scratch.

FEWER SILOS, SIMPLER OPERATIONS

Bridge the gap between endpoint and XDR workflows with automated data flows, consistent context, and shared views for more efficient investigations.

UNIFIED VISIBILITY

View ESET endpoint indicators side by side with Cisco XDR network, cloud, and identity telemetry so that analysts can see the full story of an attack in one place.

ACCELERATED DETECTION AND RESPONSE

Automated ingestion and correlation reduce manual effort and help your SOC move from detection to containment in less time.

KEY FEATURES

NATIVE CISCO CTIM MAPPING

ESET events are transformed into Cisco's CTIM "Sightings" and "Judgments," ensuring data arrives in a format Cisco XDR understands, correlates, and can act on immediately.

CONSISTENT END-TO-END VISIBILITY

By aligning ESET endpoint intelligence with Cisco's network and cloud telemetry, analysts get a clear view of attacker behavior across the environment.

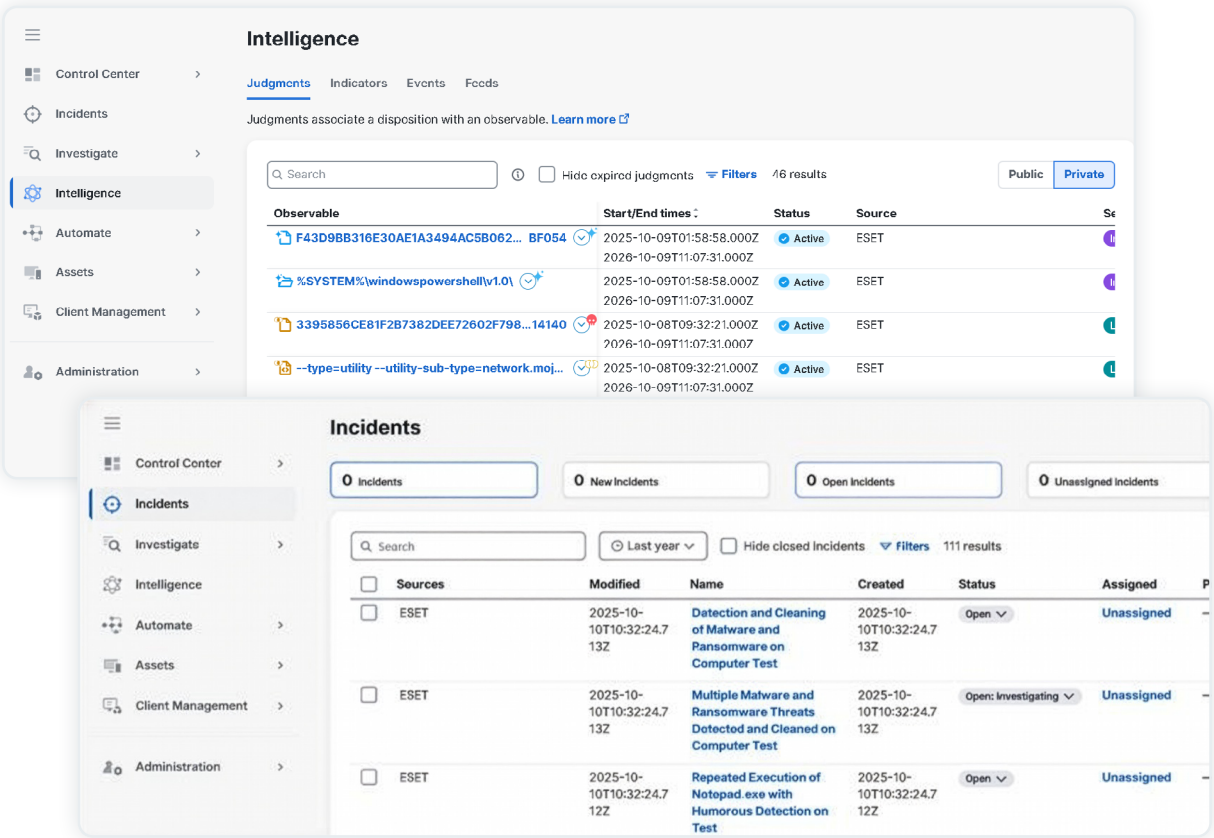
AUTOMATED ENDPOINT-TO-XDR DATA FLOW

The integration continuously pulls detections and incident data from ESET PROTECT via ESET Connect and pushes them into Cisco XDR. No more manual exports or ad hoc data sharing.

HOW IT WORKS

The ESET-Cisco integration uses the ESET Connect API to pull relevant detection and incident data from ESET PROTECT. This data is normalized and converted into Cisco's CTIM format as "Sightings" and "Judgments". A Docker-based app, deployed in your environment, regularly polls ESET and forwards these transformed events into Cisco XDR.

Inside Cisco XDR, this endpoint intelligence is automatically correlated with network, firewall, identity, and cloud telemetry. Analysts gain a single, consolidated timeline of events that spans both ESET-protected endpoints and Cisco-observed infrastructure, making root-cause analysis and response orchestration faster and more reliable.

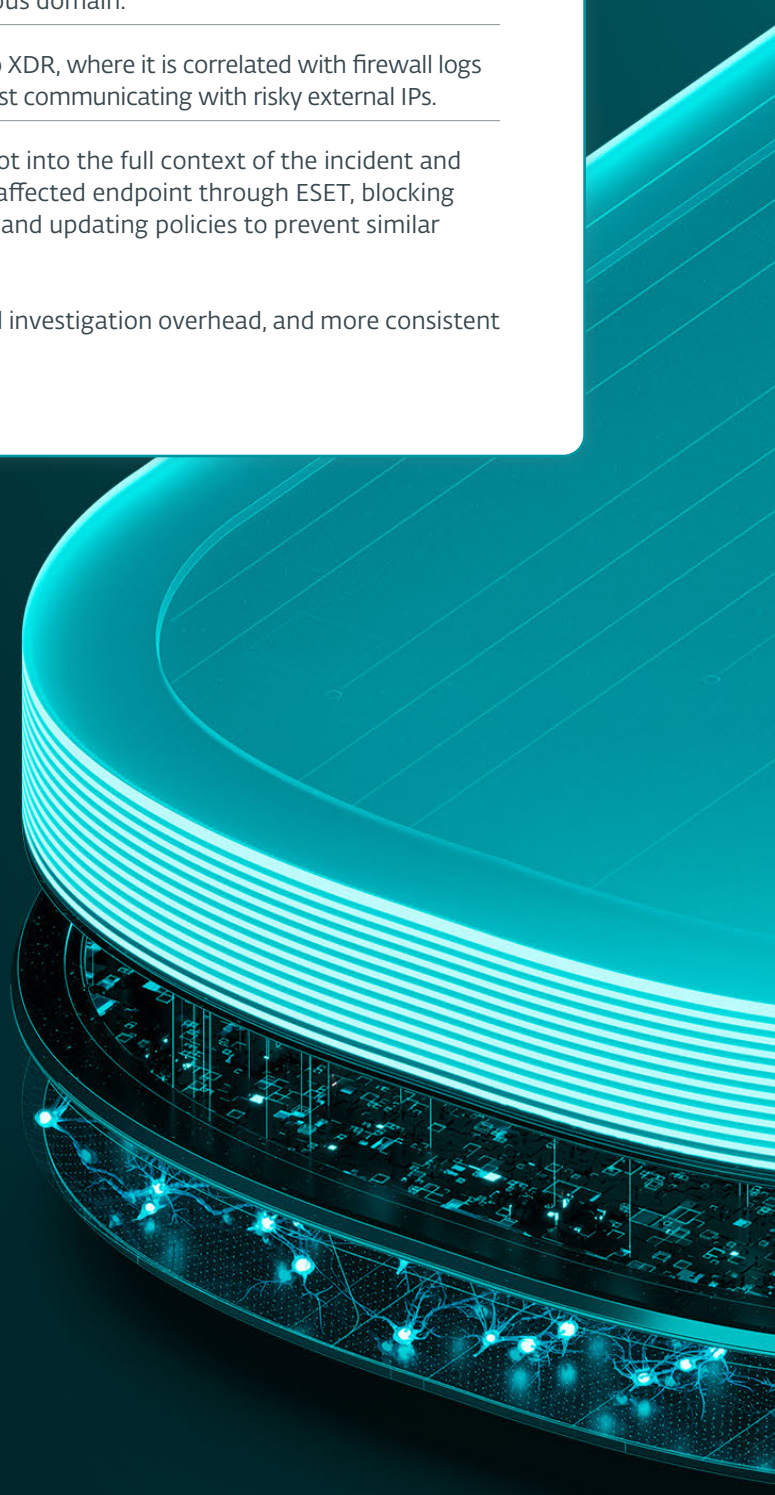


Cybersecurity
Progress. Protected.

Example Use Case

1. ESET detects a suspicious process on an endpoint—such as a process spawning from an unusual parent or contacting a known malicious domain.
2. The integration forwards this detection to Cisco XDR, where it is correlated with firewall logs and network anomalies that show the same host communicating with risky external IPs.
3. From the Cisco XDR console, the SOC can pivot into the full context of the incident and trigger an automated response: isolating the affected endpoint through ESET, blocking malicious domains on Cisco security controls, and updating policies to prevent similar behavior in the future.

The result is faster containment, reduced manual investigation overhead, and more consistent enforcement across the environment.



About ESET

PROACTIVE DEFENSE. MINIMIZE RISKS WITH PREVENTION.

Experience best-in-class protection thanks to ESET's in-house global cyber threat intelligence, compiled and examined for over 30 years, which drives our extensive R&D network led by industry-acclaimed researchers. ESET PROTECT, our cloud-first XDR cybersecurity platform, combines next-gen prevention, detection, and proactive threat-hunting capabilities. ESET protects your business so you can unlock the full potential of technology.

About Cisco

Cisco is the worldwide technology leader that is revolutionizing the way organizations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry-leading AI-powered solutions and services, Cisco enables its customers, partners, and communities to unlock innovation, enhance productivity, and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all.