cisco SECURE

Threat Hunting with SecureX

Stop Cyberthreats Before They Start

cisco SECURE

Threat Hunting: The Next Evolution in Cybersecurity

With cyberattacks increasing, organizations must continue to invest in protecting against threats. Cybercriminals have become more intelligent and focused, leaving companies blindsided.

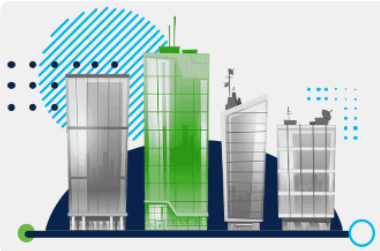
As a leading cybersecurity company, Cisco has integrated threat hunting into its offering, which can help to disrupt attacks before they materialize. By engaging Cisco to employ threat hunting, companies can proactively pursue, discover, and stop cyberthreats in their tracks.

Threat Hunting is Critical to Cybersecurity

Traditional cybersecurity tactics are reactive, waiting for malicious activity to begin.

While Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) are more effective than no cybersecurity at all, once cyberattacks are detected, it can be too late to stop them. That's why solely relying on protective measures to thwart attacks is no longer a sustainable strategy.

Threat hunting changes the way companies protect themselves by pursuing cybercriminals before they can create harm.



1 in 4 Companies risk a major breach in the next 24 months

206 days Industry average detection time for a breach

73 days Industry average time to contain a breach

$3.9M Average cost of a data breach

say threat hunting found previously undetected threats

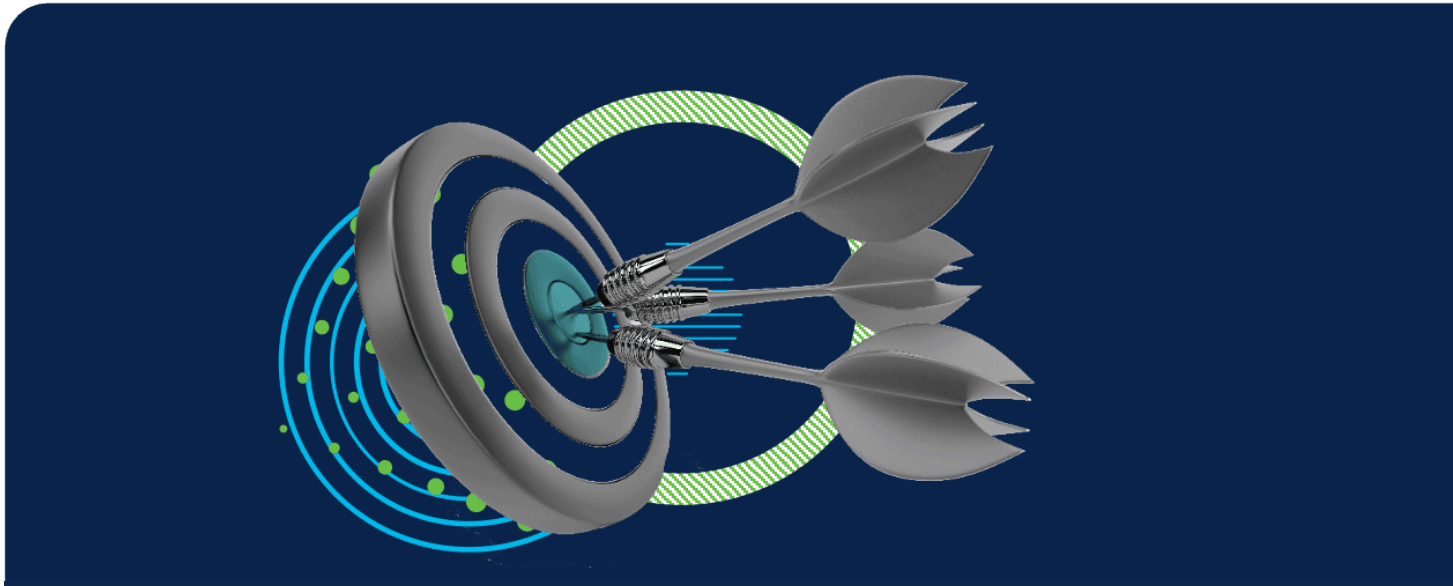
of those implementing threat hunting have reduced attack surfaces

enhanced speed and accuracy of response by using threat hunting

What is Threat Hunting

Threat hunters formulate hypotheses from a variety of input variables and apply them to a repeatable process utilizing previously catalogued information to find signs of compromise that have evaded detection.

Developed to enhance, not replace legacy cybersecurity tactics, threat hunting augments security measures already in place.



Traditional Cybersecurity vs. Threat Hunting

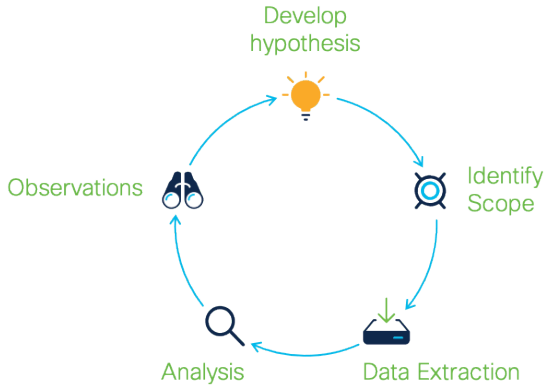
- Legacy security tools fail to stop advanced threats
- Sophisticated attackers make detection extremely difficult
- Even artificial intelligence and machine learning techniques may fall short in stopping all attacks

How It Works

Threat hunting analysts use a hypothesis driven methodology.

First, they identify techniques that may come from MITRE, incident response observations, or research. Next, they formulate a plan and scope. Analysts then execute the action plan and obtain data. With that data, they perform automated analysis and analytics. Finally, they adjust or accept the hypothesis, and repeat the process.

Unusual behavior or malicious activity is reported to an internal security team, so they can take measures to stop it.



Threat Hunting Categories:

Advanced analytics and machine learning investigations:

Combining powerful data analysis and machine learning to sift through a massive amount of information, threat hunters can detect irregularities pointing toward possible attacks.

Investigation based on known IOCs or IOAs:

Leveraging tactical threat intelligence to catalog known Indicators of Compromise (IOCs) and Indicators of Attack (IOAs) associated with new threats, threat hunters use these catalogs, such as MITRE ATT&CK™, to uncover malicious attacks or hidden activity.

Hypothesis-driven investigation:

Triggered by a new threat that's been identified through a large pool of crowdsourced attack data, threat hunters will look to discover if the attacker's specific behaviors are found in their own environment.

MITRE ATT&CK™ – The Backbone of Threat Hunting

Effective threat hunting doesn't happen just once or in a vacuum.

It's continual, proactive, and powered by strong intelligence built through analytic detection capabilities, which can be complex and time-consuming. That's why MITRE has been gathering information since 2013, to provide threat hunters with actionable information for an organization's cybersecurity program. MITRE developed ATT&CK™ (Adversarial Tactics, Techniques & Common Knowledge), an empirically-driven framework which facilitates gathering, interpreting and sharing information on cybercriminals.

ATT&CK provides clear, structured ways to understand how attackers work. By accessing this information on groups of adversaries, threat hunters can analyze intelligence to detect and mitigate attacks and create a threat-centric understanding of a company's vulnerabilities to customize defenses.

Threat Hunting Delivers Significant Improvement

Data shows that threat hunting is a must have for any organization looking to secure against cyberthreats. Most companies who had already implemented threat hunting tactics reported improvement across a number of measurable goals.

Measurable improvements as a result of threat hunting efforts	Some Improvement	Significant Improvement
Amount of breaches based on the number of incidents detected	54.2%	28.3%
Attack surface exposure/hardened network and endpoints	48.3%	47.5%
Breakout time (initial compromise to lateral movement)	44.2%	30.8%
Dwell time (infection to detection)	45.0%	40.0%
Exfiltration detection (data detected leaving your organization)	45.0%	31.7%
Frequency/number of malware infections	45.8%	37.5%
Resources (E.g., staff house, expenses) spent on remediation	49.2%	25.8%
Time to containment (detect/prevent spread or lateral movement)	55.8%	32.5%

Top 5 Barriers Keeping Companies from Adopting Threat Hunting

Limited Resources

Organizations are struggling in sourcing talented threat hunters. They are also challenged with their limited capability, legacy infrastructure and architecture.

Alert Prioritization

There are floods of alerts daily and it is difficult to prioritize investigations, compounded by the fact that it is difficult to identify the source of the threat.

Effective Intel Usage

It is difficult to operationalize threat intelligence and many sources are often unreliable and out-of-date.

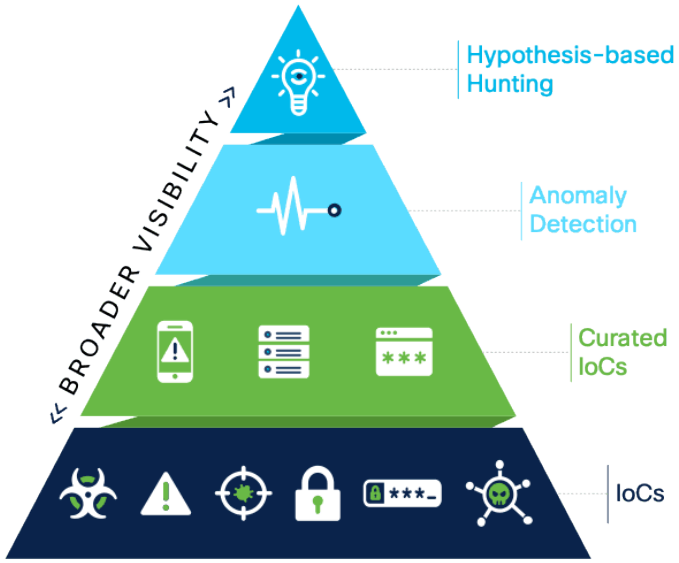
Internet-wide Threat Visibility

Organizations struggle with how to identify where attackers stage attacks and how domains, IPs, ASNs, and malware are connected.

Threat Hunting Has a Maturation Journey

When organizations begin a threat hunting practice, they typically start with only the low-level IOCs hunts and have to advance to higher levels, which takes time.

Threat Hunting Maturity Pyramid



cisco SECURE

Cisco Secure Endpoint Premier with SecureX Threat Hunting

Comprehensive Threat Hunting Made Accessible to Everyone

Cisco is Democratizing Threat Hunting

Through Cisco Secure Endpoint Premier with SecureX Threat Hunting, organizations of any size can now apply an established, mature threat hunting practice to their environment at a fraction of the cost and time of doing it themselves.

The average dollar cost of just personnel for an initial stand up team is $1.25M in human capital and $900k investment for a midsized organization to deploy architecture and storage and that's before investing in data stacking or machine learning.

Companies who already have their own threat hunting practices can also benefit. Cisco has methodologies that will overlap, compliment or supplement an organization's capabilities, but also has a global visibility of the threat landscape, as well as for a variety of verticals.

Explore

- Learn more about Cisco Secure Endpoint (formerly Cisco AMP for Endpoints)
- Cisco + MITRE, see how the two are working together to bring the best in cyber hunting
- Have questions? Check out the SecureX Threat Hunting FAQs
- Cisco Security and the Pyramid of Pain

Cisco Secure Endpoint Premier with SecureX Threat Hunting Deep Dive

Analytics Methodology

SecureX Threat Hunting takes and applies a level of subject matter expertise coupled with data science mechanisms to take seemingly benign or normal activity and easily identify areas that may be cause for concern.

Automated Methodology

Through the SecureX Threat Hunting feature, Cisco automates this process. It is a simple, effective mechanism to introduce a level of atomic indicators to search back as intelligence is introduced. Hunts that have sourced intelligence automatically add new information into the product in future releases.

True Threat Hunting

Threat hunting revolves around points of research and knowledge of the domain. Cisco applies subject matter expertise to backfill both the automated and analytics methods, and conduct contextual hunts, research possibilities, and dive deeper into problems which may have bypassed traditional means of detection.

Benefits of Cisco Threat Hunting

Threat Hunting Expertise
SME's with 20 years of industry experience continuously analyze customer environments to identify unknown threats.

Uncover Hidden Threats Faster Across the Attack Surface
Using MITRE ATT&CK™ and other industry best practices combined with our Orbital Advanced Search feature with expertise from elite threat hunters to proactively find more sophisticated threats.

Improve Security Posture Instantly
Adding an established threat hunting practice significantly advances your security maturation.

Reduce Alert Fatigue
Through SecureX Threat Hunting your organization receives fewer, high confidence, and high impact actionable alerts.

How to Buy

To view package options, visit Packages Comparison. Then talk to a Cisco sales representative or channel partner about how Cisco Secure Endpoint can help you defend your organization from advanced cyberattacks.

Visit our website to schedule a demo and learn more.

Best in Class

- Cisco has global visibility into the threat landscape
- Cisco has an extensive view of a variety of verticals
- SecureX Threat Hunting leverages Orbital for near real-time queries
- Cisco provides guided remediation

Cisco Secure Endpoint Premier with SecureX Threat Hunting Deep Dive

Cisco Secure Endpoint Premier with SecureX Threat Hunting is just one of a number of products that Cisco offers for cybersecurity which ranges across network and end point solutions.

As the largest enterprise cybersecurity company in the world, we are committed to providing companies with the most comprehensive infrastructure security out there.

Cisco leads the way with solutions that are driving the industry in SASE, XDR, and zero trust. Integrating it all is Cisco SecureX – the security platform that provides simplicity, visibility and efficiency across your security infrastructure.

cisco SECURE

Thank you for reading

Threat Hunting with SecureX