

# Cisco Secure Endpoint





# Contents

Product overview .....3

Benefits.....3

Prevention .....4

Detection.....5

Talos Threat hunting .....6

Response .....7

Cisco Secure MDR for Endpoint .....9

Cisco Secure Endpoint independent third-party tests ..... 11

Platform support and compatibility..... 11

Ordering information ..... 12

Warranty information..... 12

Cisco environmental sustainability..... 12

Cisco Capital..... 13

For more information ..... 13

## Product overview

Cisco® Secure Endpoint integrates comprehensive prevention, detection, threat hunting, and response capabilities in a single-agent solution leveraging the power of cloud-based analytics. Secure Endpoint will protect your Windows, Mac, Linux, Android, and iOS devices through a public or private cloud deployment.

Cisco Secure MDR for Endpoint adds to Secure Endpoint's superior capabilities, Cisco's managed security operations expertise to dramatically reduce the mean time to detect and respond to threats.

## Benefits

In the rapidly evolving world of cybersecurity, threats are becoming harder and harder to detect. Threat actors abuse legitimate workspace applications and system utilities to perform malicious actions as part of living off the land attacks. The most advanced 1% of these threats, those that will eventually enter and wreak havoc in your network, could potentially go undetected. However, Secure Endpoint provides comprehensive protection against that 1%. Secure Endpoint prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes endpoint activity and behaviors to rapidly detect, contain, and remediate threats that can evade front-line defenses.

Cisco Secure MDR for Endpoint adds further value to Cisco Secure Endpoint by combining human and machine intelligence, leveraging an elite team of Cisco security researchers, investigators, and responders who utilize integrated threat intelligence, defined investigation, and response playbooks supported by Cisco Talos threat research. We can identify and then stop threats, block malware, and contain and recommend remediation actions for even advanced threats that evade front-line defenses 24x7x365 from our dedicated, global Security Operations Centers (SOCs).

## Prevention

Stopping threats at the earliest point in time ensures minimal damage to endpoints and less downtime after a breach. Secure Endpoint employs a robust set of preventative technologies to stop malware and malicious behaviors, in real-time, protecting endpoints against today's most common attacks as well as emerging cyberthreats.

**File reputation:** Secure Endpoint contains a comprehensive database of every file that has ever been seen and a corresponding good or bad disposition. As a result, known malware is quickly and easily quarantined at the point of entry without any processor-intensive scanning.

**Antivirus:** Secure Endpoint includes constantly updated, definition-based antivirus engines for Windows, Mac and Linux endpoints. All endpoints also benefit from custom signature-based detection, allowing administrators to deliver specific control capabilities and enforce blocklists. The antivirus signature database resides locally on each endpoint, meaning it does not rely on cloud connectivity to operate. This ensures that your endpoints are protected both on- and offline.

**Polymorphic malware detection:** Malware actors will often write different variations of the same malware to avoid common detection techniques. Secure Endpoint can detect these variants, or polymorphic malware through loose fingerprinting. Loose fingerprinting will look for similarities between the suspicious file's content and the content of known malware families, and convict if there is a substantial match.

**Machine learning analysis:** Secure Endpoint is trained by algorithms to "learn" to identify malicious files and activity based on the attributes of known malware. Machine learning capabilities in Secure Endpoint are fed by the comprehensive data set of Cisco Talos™ to ensure a better, more accurate model. Together, the machine learning in Secure Endpoint can help scale detections and detect never-before-seen malware at the point of entry.

**Exploit prevention:** Memory-based attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes. The exploit prevention feature leverages moving target defense to defend endpoints from system and application exploitation, including zero-days, and other fileless injection attacks.

**Behavioral protection:** Secure Endpoint's enhanced behavioral analysis continually monitors all user and endpoint activity to protect against malicious behavior in real-time by maintaining state and matching streams of activity records against a set of attack activity patterns which are dynamically updated as threats evolve. For example, this enables granular control and protection from the malicious use of living-off-the-land tools and ransomware by terminating the processes of the offending behavior and stopping the attack.

**Script protection:** Secure Endpoint provides enhanced visibility into scripts executing on your endpoints and helps protect against script-based attacks commonly used by malware and threat actors. Script control provides additional protection by preventing certain scripting DLLs from being loaded by commonly exploited desktop applications and their child processes.

**Device Control:** Secure Endpoint lets you control the usage of USB mass storage devices and prevent attacks from these devices. With visibility, endpoint administrators can review device connect/disconnect events, access violation events, use the API to manage device control configurations and rules, among others. With control, administrators define the default behavior when devices are connected and create granular rules to further support varied approaches to controlling these devices.

**Host Firewall:** Monitor and enable fast, more effective response by allowing or blocking network connections using IPv4 and IPv6 5-tuple rules, or apply application-based rules for greater control. Simplify your security stack by managing firewall rules centrally for Windows and macOS from the Secure Endpoint console or through the API.

## Detection

Though upfront prevention techniques are necessary for a complete next-generation endpoint security solution, combating advanced threats requires additional measures. Secure Endpoint continuously monitors endpoints to help accelerate the detection of new and unknown threats.

**Cloud-based indicators of compromise:** Cisco's industry-leading threat intelligence organization, Talos, constantly analyzes malware and threat actor groups to discover new threat types and build behavioral and forensic profiles for emerging threats, otherwise known as Indicators of Compromise (IoCs). The forensic data, such as file locations or modifications to registry key values, are all data that Secure Endpoint can use to help administrators identify systems that have been breached.

**Host-based IoCs:** Administrators can write their own custom IoCs for use in incident response to scan for post-compromise indicators across the entire endpoint deployment. Custom IoCs are written in an open standard format (OpenIOC) making it easy to leverage data from any existing intelligence feeds.

**Low prevalence:** Secure Endpoint will automatically identify unique executables that exist in low numbers across your endpoints and automatically analyze those samples in our cloud-based sandbox to uncover new threats. These often include applications that have been trojaned or otherwise tampered with by a threat actor. Targeted malware or advanced persistent threats will often fly under the radar and start on only a few endpoints, but with low prevalence, Secure Endpoint will automatically surface these evasive executable files to uncover the 1% of threats that would have otherwise gone unnoticed.

**Vulnerabilities:** For customers on Advantage or Premier Tier, Secure Endpoint automatically taps into Cisco Vulnerability Management (formerly Kenna Security) for vulnerability inference to identify known OS and Application vulnerabilities in your environment to help you proactively reduce the attack surface and/or gain vulnerability context into a compromised endpoint. Endpoints that have known vulnerabilities are marked with a Risk Score that reflects beyond common vulnerability scores to real world vulnerability exploitation data, which enables administrators to prioritize remediation.

**Advanced search:** Advanced Search is an advanced capability in Cisco Secure Endpoint Advantage or Premier Tier, designed to make security investigation and threat hunting simple by providing over a hundred Cisco Talos curated queries, allowing you to quickly run complex queries on any or all endpoints. This enables

you to gain deeper visibility on what happened to any endpoint at any given time by taking a snapshot of its current state. Whether you are doing an investigation as part of incident response, threat hunting, IT operations, or vulnerability and compliance, Advanced Search gets you the answers you need about your endpoints fast.

## Talos Threat hunting

Talos Threat Hunting is a proactive analyst-centric approach to detecting evasive advanced threats built into Cisco Secure Endpoint. This capability is offered exclusively as part of the Premier license tier within Secure Endpoint to augment the product with specialized Cisco Talos Threat Hunters hunting across your endpoint telemetry to find potential threats. A Talos Threat Hunt report tells the incident responders an attack chain narrative of how an attack was first identified, how it evolved and provides recommendations on what to do next in terms of response. The purpose is to discover and thwart attacks before they cause any damage. As a side-effect of leveraging regular and continuous threat hunting, an organization increases their knowledge of vulnerabilities and risks which further allows the hardening of their security environment.

Talos Threat Hunting leverages the expertise of both Talos and the Cisco Research and Efficacy Team to help identify threats found within the customer environment. Cisco delivers highly automated human-driven hunts based on playbooks producing high-fidelity alerts. The process uniquely combines the Orbital Advanced Search technology with expertise from elite threat hunters, with 20 years of industry experience, to proactively find more sophisticated threats.

The Secure Endpoint Premier license is available to order globally in all regions.



# Response

As the number and variety of advanced threats designed to slip past preventative measures increase, the possibility of a breach should be treated as an eventuality. With that mindset, a powerful toolset should be deployed to help easily identify compromised endpoints and understand the scope of an attack. In addition to multiple prevention and detection capabilities, Secure Endpoint offers granular

endpoint visibility and response tools to handle security breaches quickly and efficiently.

**Dashboards and inbox:** Reports are not limited to event enumeration and aggregation. The actionable dashboards built into Secure Endpoint enable streamlined management and faster response. Events and endpoints are categorized by priority and tied into workflows to track progress during investigation.

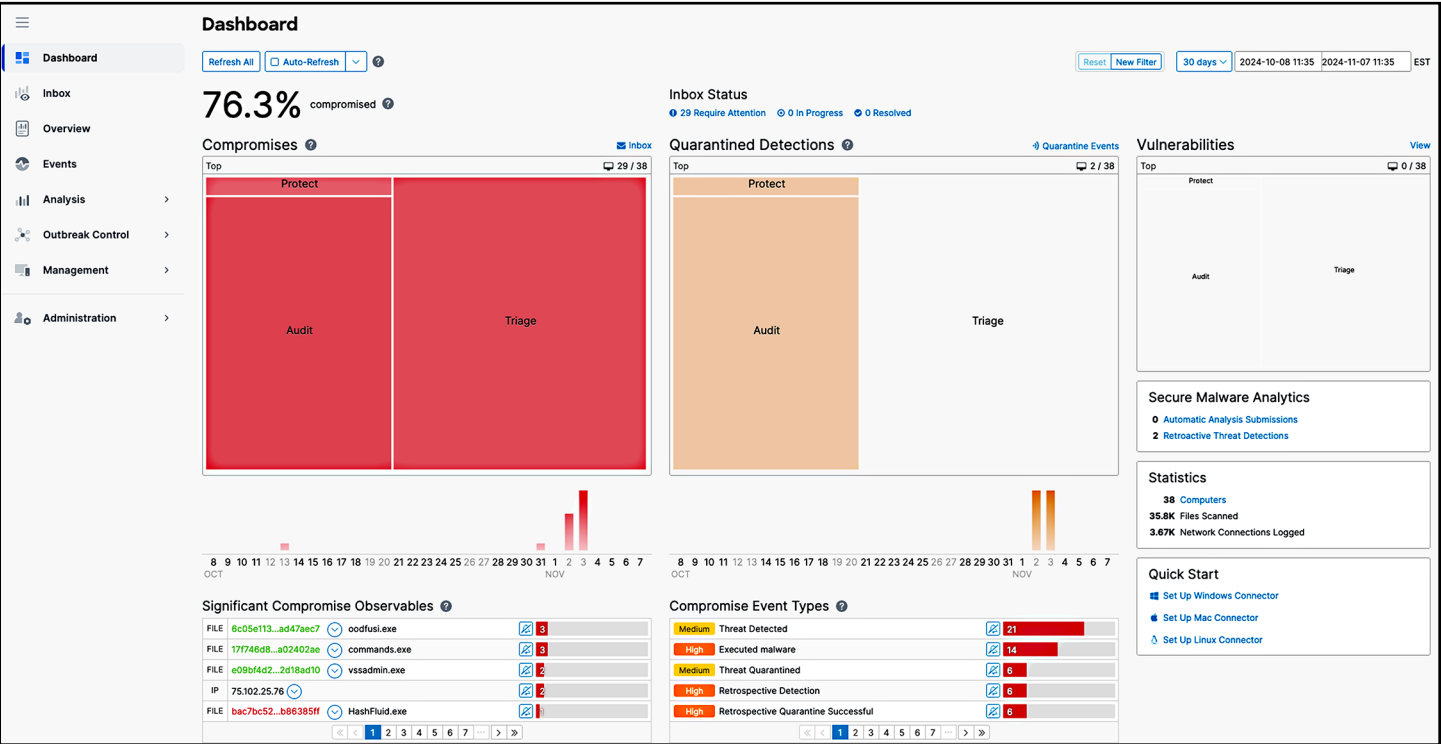


Figure 1. Secure Endpoint dashboard

**Endpoint forensics:** Powerful tools like file trajectory and device trajectory use Secure Endpoint’s continuous analysis capabilities to show you the full scope of a threat. Secure Endpoint identifies all affected applications, processes, and systems to pinpoint patient zero, as well as the method and point of entry.

These capabilities help you quickly understand the scope of the problem by identifying the attack vector for initial access, adversary tactics, techniques and procedures mapped to MITRE ATT&CK and the path that attackers are using to gain a foothold into other systems.



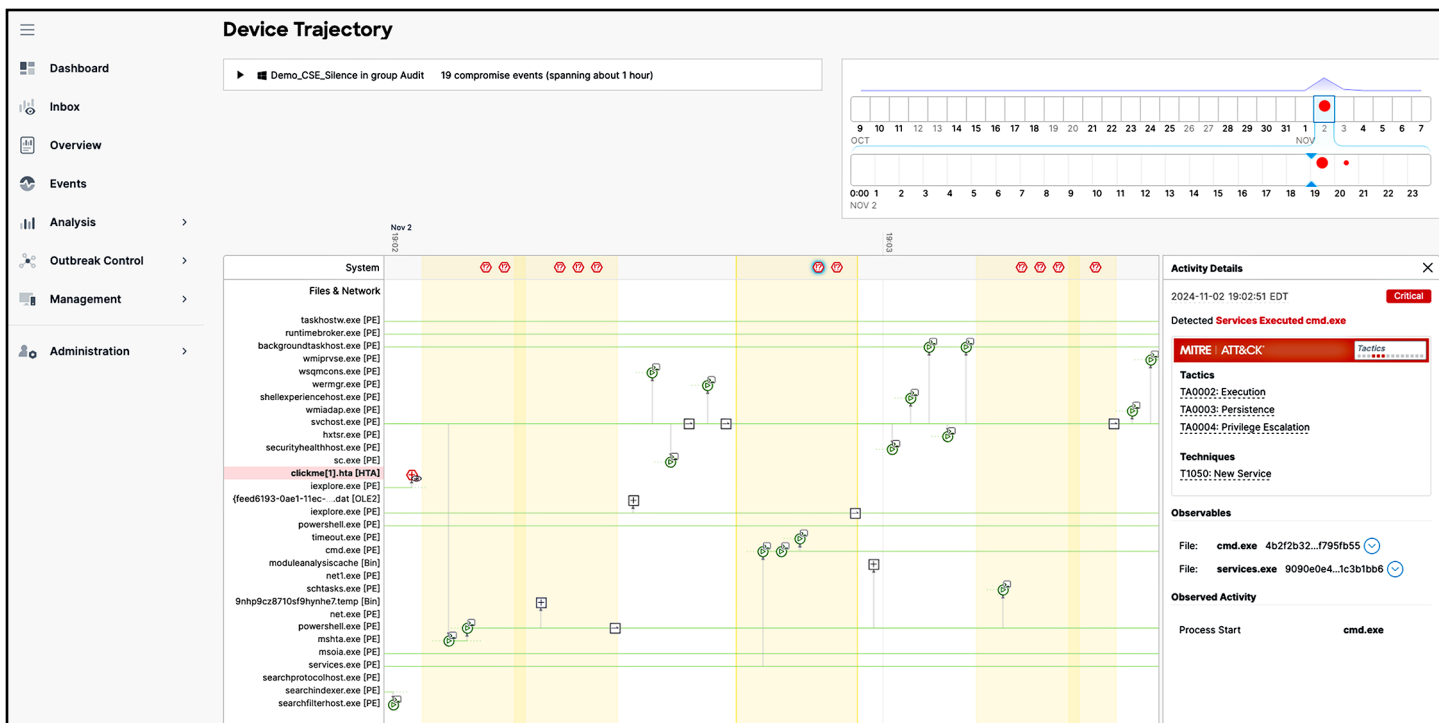


Figure 2. Secure Endpoint device trajectory

**Dynamic analysis:** Secure Endpoint includes a built-in, highly secure sandboxing environment, powered by Cisco Secure Malware Analytics, to analyze the behavior of suspect files. File analysis produces detailed information on files, including the severity of behaviors, the original file name, video replay and screenshots of the malware execution, and sample packet captures. Armed with this information, you'll have a better understanding of what is necessary to contain the outbreak and block future attacks.

**Retrospective security:** Secure Endpoint employs patented technology that automatically uncovers advanced threats that have entered your environment. Powered by Cisco's collective threat intelligence cloud and continuous monitoring, Secure Endpoint correlates new threat information with your past history and automatically blocks and/or quarantines files across the Cisco Malware Defense Ecosystem of Endpoint, Email and Network security control points, the moment they start to exhibit malicious behavior. This automated response to the latest threats provides a faster time to detection and greatly reduces the proliferation of the malware.

**Command line visibility:** Gaining visibility into command line arguments helps to determine if legitimate applications, including Windows utilities, are being used for malicious purposes. Secure Endpoint can uncover hard-to-detect behavior, such as the use of vssadmin to delete shadow copies or disable safe boots; PowerShell-based exploits; privilege escalation; modifications of access control lists; and attempts to enumerate systems.

**Endpoint isolation:** It is critical to isolate endpoints that have been compromised to contain threats from spreading and prevent them from communicating with their C&C for exfiltration while at the same time allowing triage and recovery with trusted resources such as the Secure Endpoint cloud. Endpoint Isolation allows one-click isolation of an infected endpoint along with the ability to whitelist trusted network resources. The endpoint can be de-isolated by a single click by the admin or through an unlock code by the user.



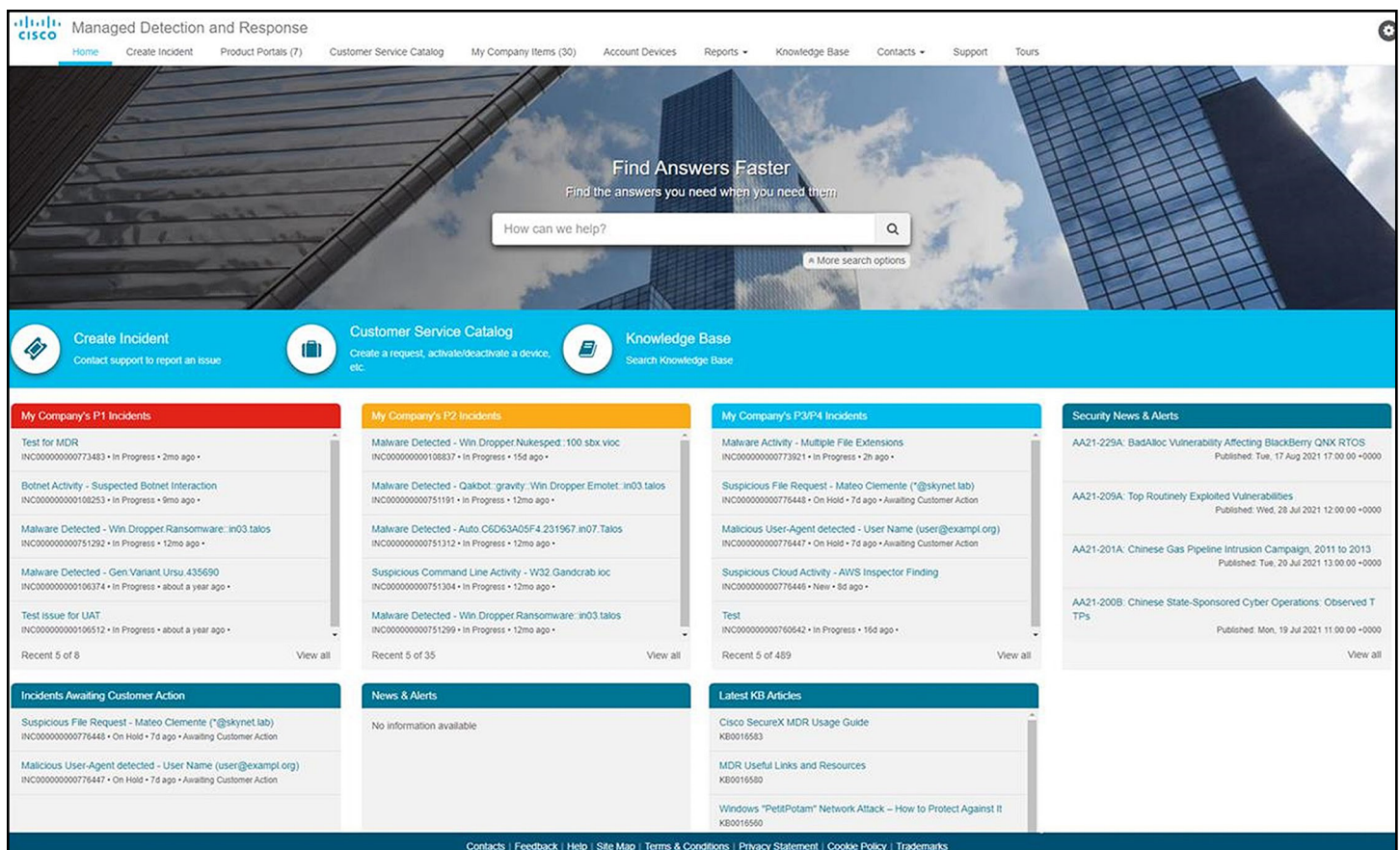
**Remote Scripts:** Remote scripts are a companion to Advanced Search and are available in the Advantage and Premier tiers. Scripts provide the ability to contain, eradicate and recover from threats impacting the endpoint. Used in combination with Secure Endpoint's

isolation feature, Remote Scripts can contain the attack by cutting off lateral movement and disabling persistence, to accelerate mean time to response and recover from a breach.

## Cisco Secure MDR for Endpoint

Secure MDR for Endpoint is an optional managed Endpoint Detection and Response (EDR) service where Cisco Security Operations Centers (SOCs) take in all events from Secure Endpoint, perform investigations, enrichments, and intelligence, and review them against playbooks and use cases (with extensive automation as well as human review and enrichment). These incidents

are prioritized for you as P1-P4 (P1/P2 accompanied by direct communication) with mitigation implemented as fast as possible. Cisco will monitor the security alerts and respond appropriately within minutes of the initial event. This allows you to focus on what is important for your organization.



The screenshot displays the Cisco Secure MDR for Endpoint portal. The header includes the Cisco logo and navigation links: Home, Create Incident, Product Portals (7), Customer Service Catalog, My Company Items (30), Account Devices, Reports, Knowledge Base, Contacts, Support, and Tours. A large banner area features the text "Find Answers Faster" and "Find the answers you need when you need them," with a search bar and a "More search options" link.

Below the banner, there are three main sections: "Create Incident" (with a sub-link "Contact support to report an issue"), "Customer Service Catalog" (with a sub-link "Create a request, activate/deactivate a device, etc."), and "Knowledge Base" (with a sub-link "Search Knowledge Base").

The main content area is divided into four columns:

- My Company's P1 Incidents:** Lists incidents such as "Test for MDR" (INC000000000773483, In Progress, 2mo ago), "Botnet Activity - Suspected Botnet Interaction" (INC000000000108253, In Progress, 9mo ago), "Malware Detected - Win Dropper Ransomware: in03 talos" (INC000000000751292, In Progress, 12mo ago), "Malware Detected - Gen Variant Ursu 435690" (INC000000000106374, In Progress, about a year ago), and "Test issue for UAT" (INC000000000106512, In Progress, about a year ago).
- My Company's P2 Incidents:** Lists incidents such as "Malware Detected - Win Dropper Nukesped: 100 sbx vloc" (INC000000000108837, In Progress, 15d ago), "Malware Detected - Qakbot: gravity: Win Dropper Emotet: in03 talos" (INC000000000751191, In Progress, 12mo ago), "Malware Detected - Auto CGD63A05F4.231967 in07 Talos" (INC000000000751312, In Progress, 12mo ago), "Suspicious Command Line Activity - W32 Gandcrab ioc" (INC000000000751304, In Progress, 12mo ago), and "Malware Detected - Win Dropper Ransomware: in03 talos" (INC000000000751299, In Progress, 12mo ago).
- My Company's P3/P4 Incidents:** Lists incidents such as "Malware Activity - Multiple File Extensions" (INC000000000773921, In Progress, 2h ago), "Suspicious File Request - Mateo Clemente (\*@skynet.lab)" (INC000000000776448, On Hold, 7d ago, Awaiting Customer Action), "Malicious User-Agent detected - User Name (user@examp1.org)" (INC000000000776447, On Hold, 7d ago, Awaiting Customer Action), "Suspicious Cloud Activity - AWS Inspector Finding" (INC000000000776448, New, 8d ago), and "Test" (INC000000000760642, In Progress, 16d ago).
- Security News & Alerts:** Lists news items such as "AA21-229A: BadAlloc Vulnerability Affecting BlackBerry QNX RTOS" (Published: Tue, 17 Aug 2021 17:00:00 +0000), "AA21-209A: Top Routinely Exploited Vulnerabilities" (Published: Wed, 28 Jul 2021 12:00:00 +0000), "AA21-201A: Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013" (Published: Tue, 20 Jul 2021 13:00:00 +0000), and "AA21-200B: Chinese State-Sponsored Cyber Operations: Observed TTPs" (Published: Mon, 19 Jul 2021 11:00:00 +0000).

At the bottom, there are three additional sections: "Incidents Awaiting Customer Action" (listing "Suspicious File Request - Mateo Clemente (\*@skynet.lab)" and "Malicious User-Agent detected - User Name (user@examp1.org)"), "News & Alerts" (showing "No information available"), and "Latest KB Articles" (listing "Cisco SecureX MDR Usage Guide", "MDR Useful Links and Resources", and "Windows 'PeltPotam' Network Attack - How to Protect Against It").

The footer contains links for Contacts, Feedback, Help, Site Map, Terms & Conditions, Privacy Statement, Cookie Policy, and Trademarks.

Figure 3. Secure MDR for Endpoint portal



**Dashboards and Inbox:** The Secure MDR for Endpoint Service Portal is your main interface to the service. All incidents, support, feedback, metrics, and more are available there. You can quickly and easily contact the SOC directly via a new incident or an existing incident. The service portal provides widgets on the homepage to guide you to the latest incidents, all of which are listed by priority. The Approval Response Action interface provides a portal for rejection or approval of recommended remediation actions as well as links to incidents. We also provide a security news feed, incidents on hold for customer review, and the latest knowledge base articles.

The Service Catalog provides a way to give feedback, request support, request intelligence reports, and more.

The Secure MDR for Endpoint Knowledge base provides several useful guides and documentation around various aspects of the service and its products. Cisco Secure MDR for Endpoint provides release notes, product and service guides, best practices, license management info, and highly detailed intelligence articles and advisories directly from our dedicated intelligence team.

All State = Requested

Approval Record	Short Description	State	Created	Updated By	Due Date	Action
TASK00000000071770	Add IP Address to SWC Watchlist	Requested	2021-10-06 13:43:07	leubanks	2021-10-06 13:43:07	<button>Reject</button> <button>Approve</button>
TASK00000000071769	Add domain to Umbrella Blocklist	Requested	2021-10-06 13:42:32	leubanks	2021-10-06 13:42:32	<button>Reject</button> <button>Approve</button>
TASK00000000069305	58b947d412b325af9ce8cf60bc40a0e0cf92e35c5ade63dd768e0190d518265 - Remove file hash from AMP for Endpoints Blocklist	Requested	2021-08-26 17:27:18	mdr_user1	2021-08-26 17:27:18	<button>Reject</button> <button>Approve</button>
TASK00000000063286	178.175.12.44 - Add IP Address to SWC Watchlist	Requested	2021-05-05 19:52:03	mdr_user1	2021-05-05 19:52:02	<button>Reject</button> <button>Approve</button>
TASK00000000063285	W10-CUCKOO-MC - Isolate host via AMP for Endpoints	Requested	2021-05-05 19:52:01	mdr_user1	2021-05-05 19:52:00	<button>Reject</button> <button>Approve</button>
TASK00000000063282	fpqovmguqnxotm.xyz - Add domain to Umbrella Blocklist	Requested	2021-05-04 20:25:32	mdr_user1	2021-05-04 20:25:32	<button>Reject</button> <button>Approve</button>
TASK00000000063280	commando.skynet.lab - Isolate host via AMP for Endpoints	Requested	2021-05-04 19:41:58	mdr_user1	2021-05-04 19:41:58	<button>Reject</button> <button>Approve</button>
TASK00000000063279	ae2b55bd5d732a57de359ae3f0ab5b2de87b275c8e624fedbe1484ce54fb6665 - Add file hash to AMP for Endpoints Blocklist	Requested	2021-05-04 19:41:57	mdr_user1	2021-05-04 19:41:57	<button>Reject</button> <button>Approve</button>
TASK00000000062748	192.168.11.159 - Add IP Address to SWC Watchlist	Requested				
TASK00000000061621		Requested				

Approve

Incident Task :

TASK00000000071770

Short Description :

Add IP Address to SWC Watchlist

Description :

Attribute Type:

Destination IP

Attribute :

34.104.35.123

Response Action :

Add IP Address to SWC Watchlist

☐ By checking this box, you agree that if you approve this request for your organization, you grant Cisco permission to make the specified changes to the MDR Components. Customer accepts the risks of Cisco performing these changes.

Approve

Figure 4. The Approval Response Action interface

## Cisco Secure Endpoint independent third-party tests



## Platform support and compatibility

Secure Endpoint is compatible with the following operating systems:

- Microsoft Windows (additional details [here](#))
- Apple iOS (additional details [here](#))
- Linux (additional details [here](#))
- Google Android (additional details [here](#))
- Apple macOS (additional details [here](#))



## Ordering information

Cisco Secure Endpoint can be purchased a la carte, as part of the [Cisco User Protection Suite](#) or as part of the [Cisco Breach Protection Suite](#).

For more detailed information, find the full ordering guide [here](#).

## Warranty information

Find warranty information on the Cisco.com [Product Warranties](#) page.

## Cisco environmental sustainability

Information about Cisco’s environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the “Environment Sustainability” section of Cisco’s [Corporate Social Responsibility](#) (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the “Environment Sustainability” section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	<a href="#">Materials</a>
Information on electronic waste laws and regulations, including products, batteries, and packaging	<a href="#">WEEE compliance</a>

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

## Cisco Capital

### Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. [Learn more.](#)

### For more information

For more information, please visit the following link: [Cisco Secure Endpoint.](#)