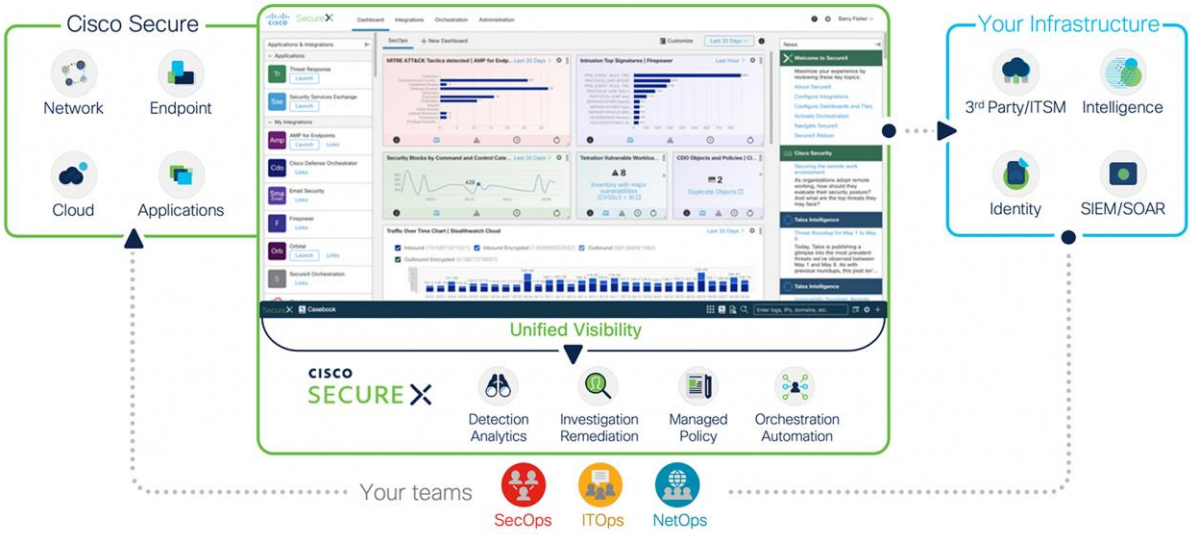
CISCO
SECURE

Data sheet
Cisco public

SecureX

Contents

Platform overview



Introducing Cisco SecureX

A cloud-native, built-in platform experience within our portfolio.

SecureX is a cloud-native, built-in platform experience within our Cisco Secure portfolio and connected to your infrastructure, which is integrated and open for **simplicity**, combines multiple otherwise disparate sensor and detection technologies into one unified location for **visibility**, and provides automation and orchestration capabilities to maximize operational **efficiency**, all to secure your network, users and endpoints, cloud edge, and applications.

With SecureX, security teams can:

- **Radically reduce the dwell time and human-powered** tasks involved with detecting, investigating, and remediating threats to counter attacks or securing access and managing policy to stay compliant – make faster decisions with less overhead and better precision with less error.
- **Enable time savings and better collaboration** involved with orchestrating and automating security across SecOps, ITOps, and NetOps teams, which helps advance your security maturity level using your existing resources and realizes more desired outcomes with measured, meaningful metrics.
- **Speed time-to-value and reduce costs** with real benefits in 15 minutes – even if you start small with a single product and grow as your needs dictate over time to consolidate security vendors without compromising security efficacy.

Every Cisco Secure customer is entitled to Cisco SecureX, without a separate license. In other words, SecureX is included at no additional charge with purchase of any SecureX-capable product.

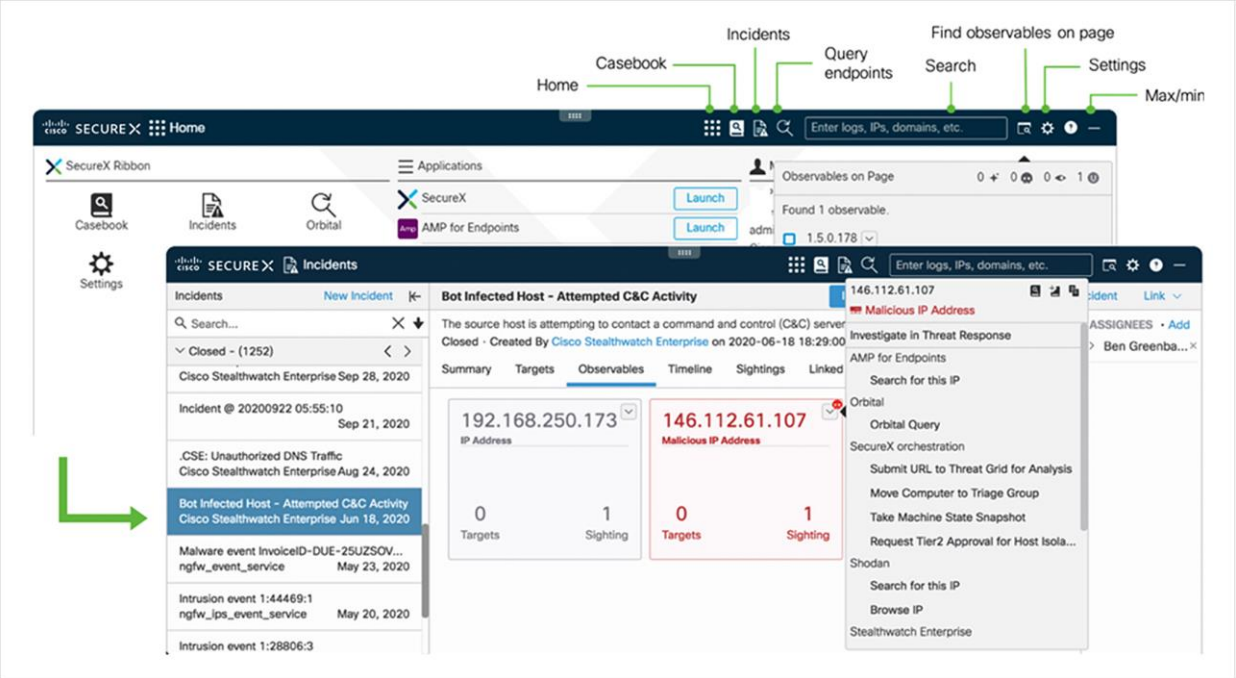
Primary customer use cases

Customer Use Case	Description	Outcomes
Incident prioritization	Prioritize most critical situations w/ metrics and operational measures across products and pivot to product drill down.	• Faster investigations • Investigating the right things
Threat hunting	Proactively search for active threats across control points in your environment with a holistic, integrated approach to see the full extent of a compromise through shared context and case management.	• More ability to find threats that did affect you and respond appropriately.
Incident response	Manage the aftermath of an attack in your environment by aggregating multiple security technologies for shared context and case management to conduct a holistic investigation and remediate in a single console.	• Faster responses • Reduce adversary dwell time and damage
Automated and orchestrated workflows	Automate workflows for SecOps, NetOps, and ITOps use cases to manage endpoint, network, and cloud policy and defense more efficiently and repeatably. Share playbooks between SecOps, NetOps, ITOps.	• Automated and orchestrated workflows
Strategic security management	Awareness of threats targeting our environment. One view into the current security landscape – the high-level management and protection – in the organization.	• Strategic security management

Key Capabilities

Capability	Description	Benefit
Ribbon	The SecureX ribbon is a transport framework for functionality: it allows you to take the capabilities of SecureX and integrated products with you when you pivot to any other product console. It helps share and maintain context, provides unified experiences, with broad response capabilities. The ribbon apps - casebook, incidents, and Orbital – are brokered by SecureX and provided by SecureX and other products.	• Carry the most relevant security context and threat intelligence with you across all products • Have your tools handy regardless of what console you are in
Threat response	SecureX threat response is a core platform application that aggregates and correlates global intelligence and local context across Cisco Secure and third-party technologies, in one view.	• Accelerate threat investigations and incident management for lower threat dwell times
Orchestration	SecureX orchestration with pre-built workflows aligned to common use cases and a no/low-code, drag-drop canvas to build your own workflows to eliminate friction in your processes and automate routine tasks	• Accelerate time to remediate and automate workflows to lower operational costs • Reduce or eliminate repetitive tasks and broaden scope of cloud orchestration • Reduce human error and improve collaboration
Device Insights	SecureX device insights provides comprehensive endpoint inventory in a single unified view. Endpoint searching and reporting allows you to assess device security configuration on employee-owned, contractor-owned, company owned, and IoT/OT devices—without risking business disruption.	• Gain a holistic view of your device data to help you simplify and automate security investigations. • Identify gaps in control coverage, build custom policies, and create playbook driven automation options
Dashboard	The SecureX dashboard is the first page users see upon logging in. It gives one view across your security infrastructure for unified visibility and aggregated, actionable intelligence across your security environment.	• Customizable for what matters to you including operational metrics • Visibility into emerging threats, and access to new products in one click
Sign-on	SecureX sign-on with Duo-protected multi-factor authentication allows you to access all of your Cisco Secure products with one set of credentials, from any device, anywhere. It provides secure and resilient identity that meets the highest industry standards including FedRAMP, SOC 2, and ISO 27001.	• Easily access all of your applications and maintain context through workflows • Centrally protect and manage credentials in one secure portal
Integrations	SecureX has built-in integrations with Cisco Secure products, and integrates with third-party solutions through built-in, pre-packaged, or custom integrations for a connected backend architecture and consistent frontend experience.	• Simplify your existing ecosystem for greater threat efficacy and lower threat dwell times

Key Capability: Ribbon



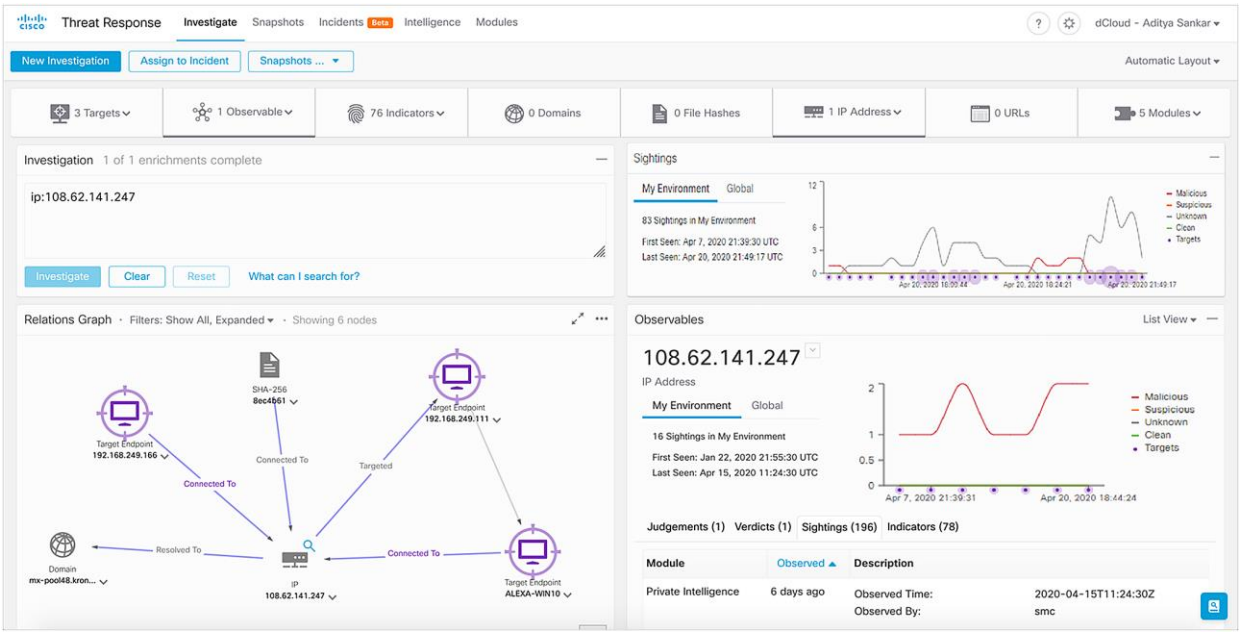
Part of the SecureX design philosophy is that you shouldn't have to navigate to multiple different consoles to get all the functions you need for one business task. The SecureX ribbon brings this philosophy to reality across the portfolio. Via the ribbon, a persistent bar in the lower portion of the UI of all ribbon-capable products, you have access to all the functions lent to SecureX by all your deployed SecureX-capable technologies. The ribbon is collapsible and expandable to open ribbon apps, launch integrated applications, and view your account profile. From the ribbon, you can pivot between SecureX or the console of any integrated product, into any other integrated product. And also search the current web page for malicious file hashes, suspicious domains and other cyber observables. You can then also add observables to a case or investigate observables in the threat response app.

You're in the Cisco Secure Endpoint (formerly AMP for Endpoints) console, and discover a domain that you need to block? The ribbon allows you to do so right there, without having to leave Secure Endpoint to go to the Cisco Umbrella interface.

The ribbon is a unified experience, providing access to capabilities of all integrated products and allows broad response actions. The ribbon maintains and shares security context and threat intelligence when navigating across SecureX and all Cisco Secure products. The ribbon apps are brokered by SecureX, and can be provided by either SecureX or other Cisco Secure products. See the list of available applications below.

Ribbon Apps	Description	Benefit
Casebook	Tool that allows to gather observables in groups, assign the case a name and a description, take and save notes on the case, add other observables at any time. You can immediately see verdicts, take actions, and share cases between staff.	• All cases in one cloud casebook, easy to find, and share.
Incidents	Automate triage and prioritization of alerts currently from Cisco Secure Firewall and Cisco Secure Network Analytics, with more in the future. Maintain a single list for security incidents across all supported products; assign, open, close and work tickets through the lifecycle; quick pivots into investigations and response actions.	• Save time and human effort by investigating and enriching events with context from product integrations prioritizing response to high-urgency incidents
Orbital	Query endpoints with Cisco Orbital Advanced Search, a feature of Secure Endpoint. Orbital provides endpoint visibility in a familiar SQL format, with an intuitive graphical interface and a catalog of pre-built queries for threat hunting and incident response.	• Trigger deep and detailed system status queries in parallel across your entire deployment in seconds.

Key Capability: Threat Response

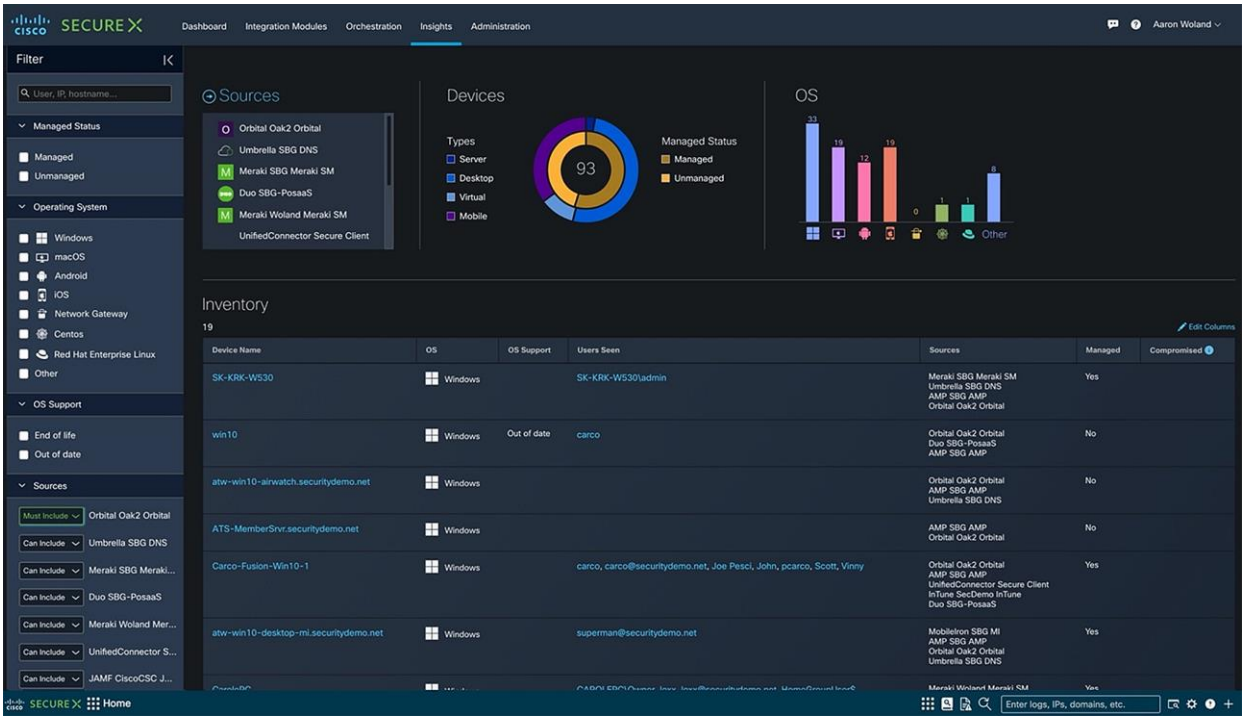


SecureX threat response is a security investigation and incident response application. It simplifies threat hunting and incident response by accelerating detection, investigation, and remediation of threats. The threat response application provides your security investigations with context and enrichment by connecting your Cisco security solutions (across endpoint, network, and cloud) and integrating with third-party tools, all in a single console.

To understand whether a threat has been seen in your environment as well as its impact, SecureX threat response aggregates contextual awareness from Cisco security product data sources along with global threat intelligence from Talos® and third-party sources via APIs. Threat response identifies whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious or malicious, and whether you have been affected by them. It also provides the ability to remediate directly from the interface and block suspicious files, domains, isolate hosts, and more without pivoting to another product first.

Functionality	Description	Benefit
Relations graph	Visualization of all the observables found during the investigation and indicates relationships between them.	• Easily determine the nature of the events and the relationships.
Incidents	Automated triage and prioritization of alerts from Cisco Secure Firewall and Cisco Secure Network Analytics.	• Investigate and enrich events with context from integrations across security products as well as responding to high-urgency incidents.
Browser plugin	Browser extension that allows for pulling IP addresses or domains from anywhere an observable is seen, for an investigation.	• Quickly and easily pull in indicators of compromise from any webpage or browser-based console, Cisco or otherwise, and start an investigation.
Casebook	Tool for saving, sharing, and enriching threat analysis that allows documentation of all the analysis in a cloud casebook and to save snapshots from all integrated or web-accessible tools. *Casebook is also accessible via the browser plugin.	• Seamlessly work a case across multiple tools, Cisco or otherwise. Improve collaboration between staff.
Snapshots	Document the state of an investigation within a specific organization at a point in time. Save the current investigation and graph for further retrieval and analysis.	• Improve collaboration between staff.
Intelligence	Enrichments, sightings from local context, observables from threat intelligence aggregated and correlated in one view.	• Access to multiple sources of threat intelligence in one view, to accelerate investigations.
Pivot menu	Act on observables, including: • Copy to clipboard or casebook • Further research in integrated products • Take response actions	• Quick access to the next steps in investigating or remediating.
Response actions	Enforce protective controls such as: • Block files • Block URLs • Block domains • Isolate hosts • Orchestrated workflows (new)	• First strike response in one console without pivoting to other product consoles

Key Capability: Device Insights

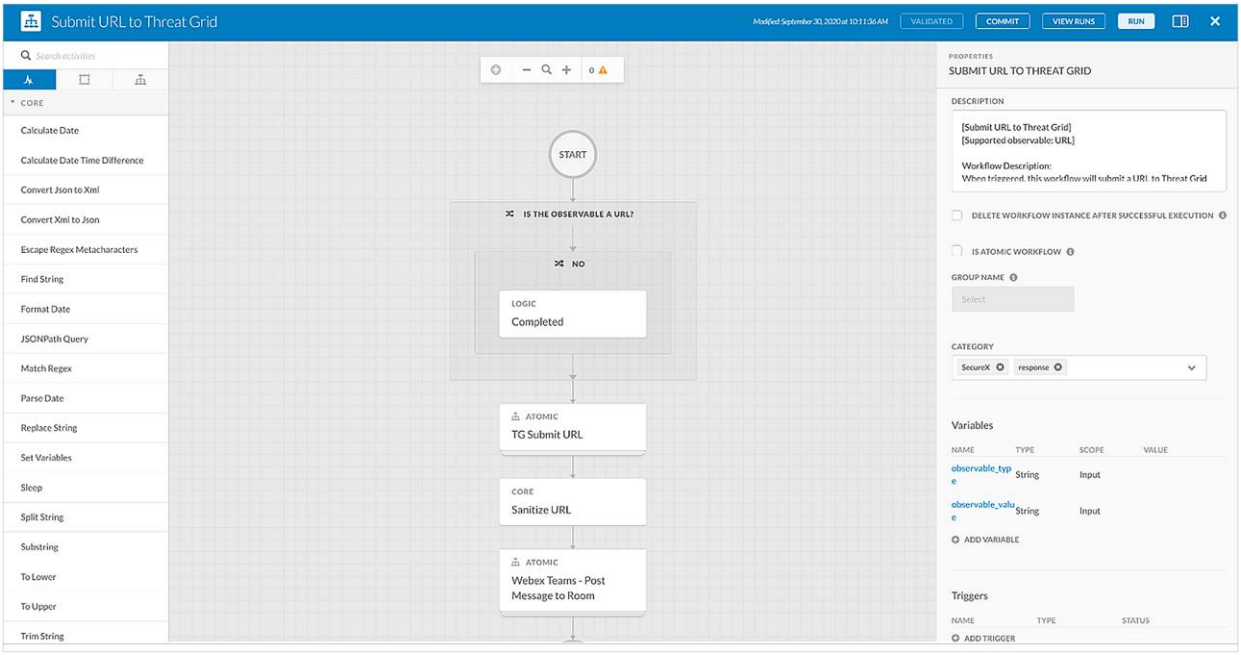


Consolidate information from multiple device managers, endpoint detection and response tools, and other endpoint security products and then bring the details they provide into a unified view within SecureX. Device Insights helps you identify gaps in your control coverage, build custom policies, and explore opportunities for playbook driven automation. You can use correlated endpoints for contextual awareness to identify and isolate endpoints ensnared in cyber-attacks.

Device Insights also gives you comprehensive endpoint inventory within SecureX. You can keep track of device inventory counts and better understand the expanding and changing nature of your endpoint landscape. Furthermore, endpoint searching and reporting allows you to assess device security configuration on employee-owned, contractor-owned, and IoT/OT devices—without risking business disruption. Stop threats before problems occur!

Functionality	Description	Benefit
Asset Visibility Sources	Visualization of all the asset sources on your network which provides information on performance over time and record synchronization.	Gain a holistic view of the assets connected to your network
Security Configuration	Charts and tables which break down the devices within your environment and status of device encryption, firewall, screen lock, AMP definitions, and SMB ports.	Easily keep track of device compliance across your environment
Inventory	Complete device inventory with details on OS, users seen, sources, management status, device model and compromise state. Can get full details on a single device and see full history of how it has been used, who has used it, and gain further insight into device vulnerabilities and incidents. Can use filters to create custom reports which can be exported to CSV.	Get detailed information about all the devices on your network. Easily assess critical vulnerabilities and incident history

Key Capability: Orchestration



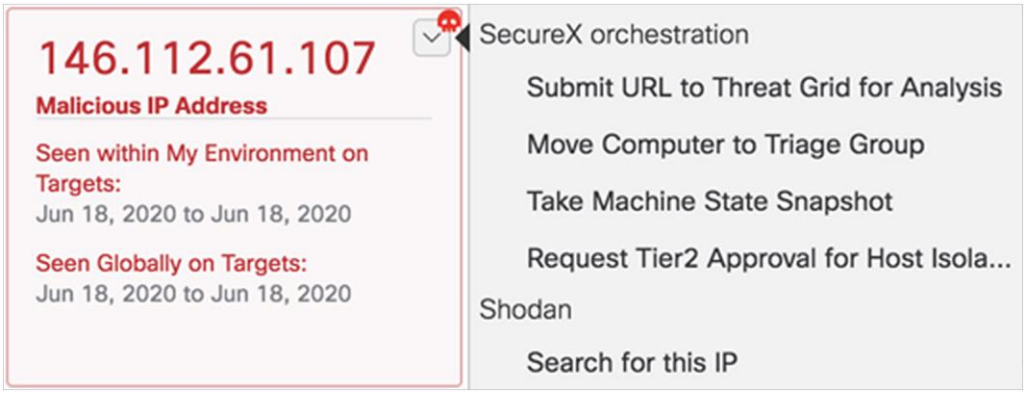
SecureX orchestration is a key capability in SecureX, automating repetitive and critical security tasks such as threat investigation, hunting, and remediation use cases. SecureX orchestration provides pre-built workflows and response capabilities or you can build your own with a no/low-code, drag-drop canvas to strengthen operational efficiency and precision, and lower operational costs.

SecureX orchestration enables you to define workflows that reflect your typical security processes; the automation steps (activities), the logic or flow between these steps, and how to flow data from one step to the next. With SecureX, you can leverage Cisco Secure and third-party multi-domain systems, applications, databases, and network devices in your environment to create these workflows.

Examples of pre-designed automated workflows that can be built:

Workflow	Who is this for	Description
Automate response workflows from triggered events	SecOps	Automatically extract new observables from threat blogs that SecOps read, enrich and add sightings of observables across your environment, create a new case only if a target is found; accelerating threat response with actionable insight.
Automate workflows for vulnerability management	ITOps	Automatically query endpoints to identify vulnerabilities and create incident tickets in your ITSM to strengthen breach defense.
Optimize VPN capacity for securing remote access	NetOps	Automatically monitor VPN head-end load. If too high, request authorization from NetOps and automatically deploy virtual head-ends to scale on-demand for increasing remote worker traffic.

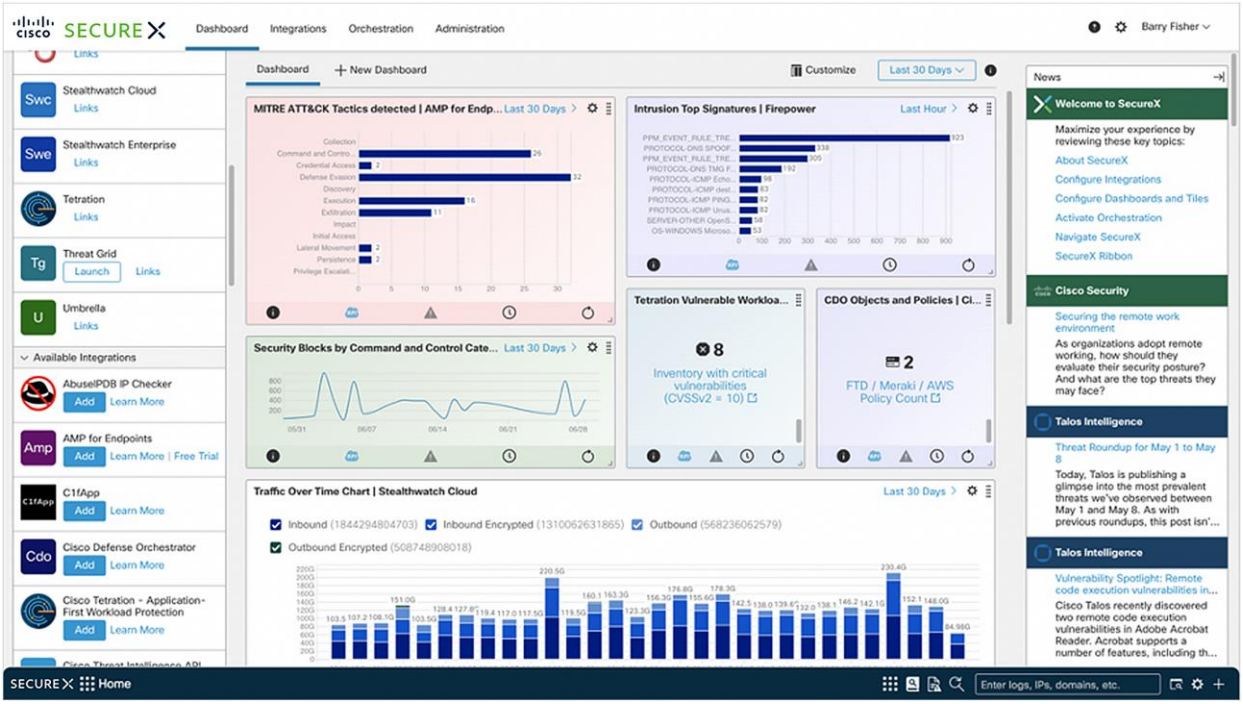
Since SecureX orchestration is integrated into the Cisco Secure platform, it can also enhance your investigation and response processes with “response” workflows. These workflows can be triggered from pivot menus within SecureX threat response, the SecureX ribbon, and across many other product interfaces.



Below are five response workflows to work with, right out of the box:

Workflow	Description
Move Computer to Endpoint Triage group	Take an IP address, hostname, or AMP Computer GUID and moves the corresponding endpoint to a triage group.
Submit URL to Threat Grid workflow	Allow the user to submit URL to Threat Grid workflow takes a URL and submits it to Threat Grid for analysis.
Take Orbital forensic snapshot	Take an IP address, hostname, or AMP computer GUID and initiates an Orbital forensic snapshot for the corresponding endpoint.
Take forensic snapshot and isolate	Take an IP address, hostname, or AMP computer GUID, requests an Orbital forensic snapshot for the endpoint, and then enables AMP host isolation using the response action.
Endpoint host isolation with tier 2	Take an AMP computer GUID and request approval to enable host isolation for the corresponding endpoint using the response action for AMP host isolation from SecureX threat response.

Key Capability: Dashboard



The SecureX dashboard is the first thing the users see upon logging into SecureX. It gives one view across your security infrastructure for unified visibility and aggregated, actionable intelligence across your security environment.

From the dashboard:

- On the upper left panel: View and launch your integrated products, with links to support resources
- On the lower left panel: View and self-provision trials for other available product integrations
- In the center: Configure up to 20 customizable dashboards per user to view metrics and operational measures from integrated products across your security environment
- On the right panel: in the News feed, users can learn about recent notable threats and product innovations

Key Capability: Sign-on

SecureX sign-on with Cisco Secure Access by Duo MFA (Multi-Factor Authentication) provides an adaptive, layered, and simplified authentication. Duo MFA is embedded into SecureX – it does not require purchase of a separate Secure Access license. Get instant access to SecureX and all of your applications with one push notification and one tap. Easily manage and invite users to your organization. Maintain context and pivot between product consoles during an investigation and have access to all applications and respective capabilities. For example, with SecureX sign-on, you can see firewall security intelligence incidents from within the Secure Endpoint console.

Key Capability: Integrations

SecureX has built-in integrations with Cisco Secure products, and integrates with third-party solutions that are built-in, pre-packaged, or custom for a connected backend architecture and consistent frontend experience.

SecureX has modules to integrate with Cisco Secure products and third-party solutions. Each source of global or local intelligence is provided by a module, which is linked via an API key. Modules must be configured for each product integrations, so the data is available in SecureX. Existing integrations with SecureX threat response will automatically migrate to SecureX.

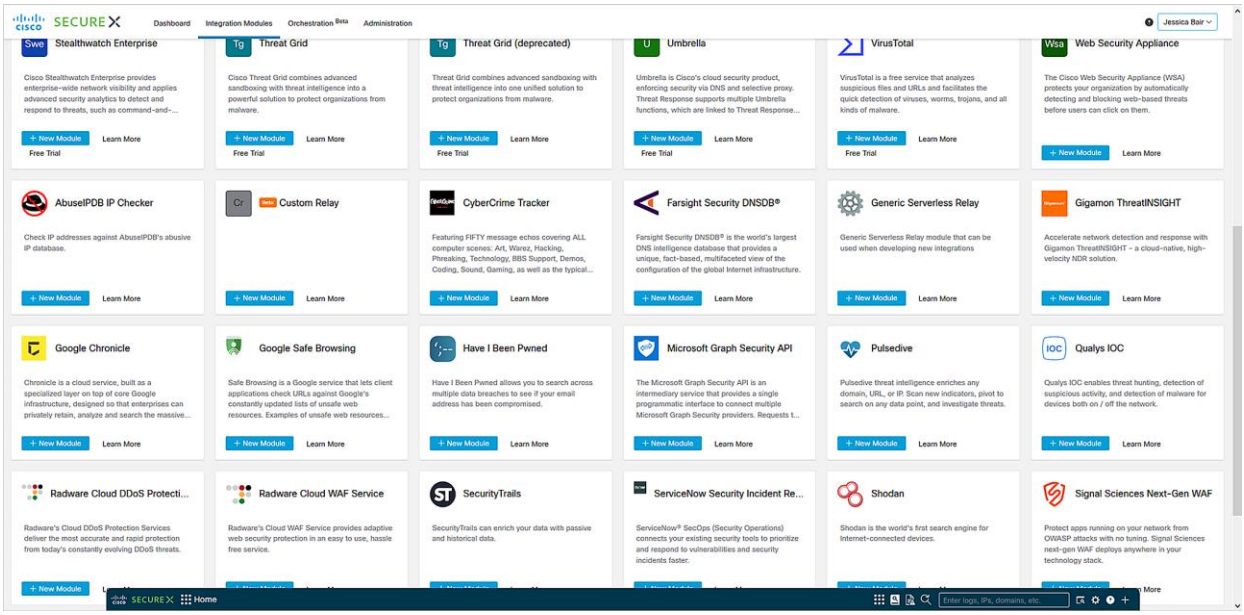
Cisco Secure product integrations with SecureX

Integration	Value to SecureX	Outcomes
Cisco Secure Endpoint (formerly AMP for Endpoints)	Secure Endpoint provides agent-driven, cloud-managed protection for physical and virtual endpoint systems. In SecureX, Secure Endpoint can be used as a sensor, to detect the presence of files or network connections to specific hosts. It can also be used to take common and critical endpoint-related response actions. Also in SecureX, Secure Endpoint provides tiles to the dashboard, as well as actions for orchestration so customers can build automated workflows. Additionally, Secure Endpoint incorporates the SecureX ribbon, allowing SecureX functions to be leveraged from any page in the Secure Endpoint console.	• Quickly determine in a single click if a file or network resource has been seen by up to tens of thousands of globally distributed endpoints within your environment. • Remotely isolate a potentially infected host, anywhere in the world, from anywhere you have a browser and an internet connection.
Cisco Orbital	Orbital provides a deep structured query language that treats system state like a database, allowing detailed probing system inspections to be carried out simultaneously across the environment in real time. A catalog provides a set of pre-built queries for threat hunting, incident response, and more – and users can write their own using the familiar SQL-like structure. In SecureX, Orbital is one of the ribbon apps, and is therefore accessible quickly from within the console of any ribbon-capable product. Additionally, it is available via the pivot modules driven by the SecureX threat response app.	• Trigger deep and detailed system status queries in parallel across your entire deployment in seconds.
Cisco Secure Malware Analytics (formerly Threat Grid)	Secure Malware Analytics is Cisco's automated, malware inspection and threat intelligence solution. In SecureX, it allows users to get detailed intelligence about malware, associated network traffic, system changes, and more.	• Heightened malware threat intelligence gained via automated detonation of suspected files from a global user base.
Cisco Secure Network Analytics (formerly Stealthwatch)	Secure Network Analytics is a Network Detection and Response (NDR) solution that provides agentless visibility across the private network and public cloud. In SecureX, Secure Network Analytics enriches threat detection and response with agentless behavioral and anomaly detection capabilities. SecureX integrations with other sources of global threat intelligence and internal visibility will affirm and enrich Secure Network Analytics findings with confirmed threat intel and local sightings. Integrations with Cisco control devices provide two-click mitigation and resolution. Also in SecureX, Secure Network Analytics provides tiles to the dashboard, as well actions for orchestration so customers can build automated workflows. Additionally, Secure Network Analytics incorporates the SecureX ribbon, allowing SecureX functions to be leveraged from any part of the Secure Network Analytics console.	• Save time and respond more holistically and effectively by using SecureX to process and manage high-priority alerts from Secure Network Analytics (and any other configured alerting technologies). • In addition, the ability to query all configured Secure Network Analytics devices in SecureX threat response and then use them in coordinated, single click defenses, simplifies visibility and increases response efficiency.

Integration	Value to SecureX	Outcomes
Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud)	Secure Cloud Analytics provides behavioral analytics across your network for better visibility to help identify advanced threats faster, from the private network to the public cloud. In SecureX, Secure Cloud Analytics provides tiles to the dashboard, as well as actions for orchestration so customers can build automated workflows. Additionally, Secure cloud Analytics incorporates the SecureX ribbon, allowing SecureX functions to be leveraged from any part of the Secure Cloud Analytics console.	• Accelerate investigations with better visibility.
Cisco Secure Email (formerly Email Security)	Secure Email provides threat defense capabilities that detect, block, and remediate threats in incoming email faster. In SecureX, this integration allows you to understand email as a threat vector by visualizing message, sender, and target relationships in the context of a threat. You can search for multiple email addresses, subject lines, and attachments at once to understand how a threat has spread. Also in SecureX, Secure Email provides tiles to the dashboard, as well as actions for orchestration so customers can build automated workflows. Additionally, Secure Email incorporates the SecureX ribbon, allowing SecureX functions to be leveraged from any part of the Secure Email console.	• Get better insight into context of a threat with email as a threat vector. Combat phishing attacks, business email compromise, malware, and ransomware.
Cisco Umbrella	Umbrella DNS and cloud security provides protection against domain-based threats across the enterprise, including the cloud. In SecureX, Umbrella provides: • Global threat intelligence from their rich database of multi-faceted domain reputation. • Local security insight by reporting sightings of investigated domains • The ability to block domains immediately and enterprise-wide in two clicks. Also in SecureX, Umbrella provides tiles to the dashboard, as well as actions for orchestration so customers can build automated workflows. Additionally, Umbrella incorporates the SecureX ribbon, allowing SecureX functions to be leveraged from any part of the Umbrella console.	• Enrich all investigations with leading reputational insight on domains and more. Discover - and quickly block - the sources of attacks, the recipients of potential or discovered data leakage, or other parts of adversary infrastructure.
Cisco Secure Firewall	Secure Firewall devices protect network edges and boundaries with state-of-the-art packet inspection and intrusion protection and prevention engines, leveraging advanced TALOS threat intelligence. In SecureX, Secure Firewall provides sightings of IP addresses, URLs, and domain. Additionally, users can leverage Secure Firewall devices via SecureX to block IPs at the perimeter. Lastly, Secure Firewall devices can be configured to provide alerts to Cisco's cloud event storage platform to be triaged and correlated such that the most pressing alerts are displayed to the user in SecureX incident manager. Also in SecureX, Secure Firewall provides tiles to the dashboard, as well as actions for orchestration so customers can build automated workflows.	• Save time and respond more holistically and effectively by using SecureX to process and manage high-priority alerts from all Firewall devices (and any other configured alerting technologies). • In addition, the ability to query all configured Firewall devices in SecureX threat response and then use them in coordinated, single click defenses, simplifies visibility and increases response efficiency.

Integration	Value to SecureX	Outcomes
Cisco Defense Orchestrator	Cisco Defense Orchestrator is a cloud-based management solution that allows you to manage security policies and device configurations across your Cisco and cloud-native security products. In SecureX, Defense Orchestrator provides tiles to the dashboard. Additionally, Defense Orchestrator incorporates the SecureX ribbon, allowing SecureX functions to be leveraged from any part of the Defense Orchestrator console.	• Consistent policy and visibility, by streamlining security policies and device management across your extended network.
Cisco Secure Web Appliance (formerly Web Security Appliance)	The Secure Web Appliance leverages multiple technologies and provides SecureX users with visibility into connections with internet-based threats. In SecureX, the integration of Secure Web Appliance with other sources of global threat intelligence and internal visibility will affirm and enrich Secure Web Appliance findings with confirmed threat intel and local sightings. Also in SecureX, Secure Web Appliance provides tiles to the dashboard, as well as actions for orchestration so customers can build automated workflows.	• Protect your network against the most common threat vector whether users are browsing the web in the office, on the road, and everywhere in between.
Cisco Secure Workload (formerly Tetration)	Cisco Secure Workload is a hybrid-cloud workload protection and microsegmentation solution designed to secure compute instances in both on-prem data centers and public clouds. In SecureX, Secure Workload provides tiles to the dashboard, as well as actions for orchestration so customers can build automated workflows.	• Greater visibility to protect critical application workloads with a zero-trust approach.
Cisco Secure Access by Duo	Cisco Secure Access by Duo provides multi-factor authentication, verifying user identity and device health at every login attempt with a zero-trust model. In SecureX, Secure Access by Duo provides actions for orchestration so customers can build automated workflows.	• Secure your workforce by providing trusted access to your applications and establish device trust.
Additional Cisco Secure Resources	Access to several threat intelligence sources is included in the free licensing for SecureX. These include the TALOS database, the default Cisco Secure Threat Intelligence Architecture, and a private repository into which users can upload their own threat intelligence, whether generated in house or acquired from other sources.	• Simultaneously enhance all investigations with additional information about adversaries and adversary infrastructure from multiple sources.

Third-party integrations with SecureX



SecureX is an open platform for customers to integrate Cisco Secure products with third-party products. In SecureX, you can aggregate and correlate threat intelligence available from Cisco Talos with network and security data from Cisco and third-party security products deployed within your organization. It brings together threat intelligence and local security context and control in one place. By connecting your existing infrastructure with Cisco Secure in SecureX, you can better understand threats and the impact on your entire environment. SecureX enables built-in or pre-packaged integrations for third-party security tools, and its open APIs allow for third parties to write custom integrations to make their tools SecureX-capable. Each source of global or local intelligence is provided by a module, which is linked via an API key.

There are two pathways to integrating with SecureX -- threat response and orchestration. Documentation on the integration workflows can be found on Readthedocs:

Integration pathway	Integration type	Resources
SecureX threat response	Threat intelligence	https://developer.cisco.com/threat-response/ https://github.com/search?q=topic%3Athreat-response+org%3ACiscoSecurity
SecureX orchestration	Workflows/playbookxs	https://github.com/CiscoSecurity/sxo-05-security-workflows

Sample use cases for integrating your existing third-party tools with SecureX:

- Aggregating and pulling in threat intelligence
- Threat hunting
- Incident response
- Automating workflows

Key third-party partners	Use Case
ServiceNow	• Threat intelligence source – query ServiceNow intel data in SecureX threat response. • Operational – query/share SecureX threat response data within ServiceNow Security Operations.
IBM	• Operational – query/share SecureX threat response data within IBM QRadar Query IBM X-Force Exchange threat intelligence in SecureX threat response.
Splunk	• Operational – query/share SecureX threat response data within Splunk Enterprise and Splunk Phantom.
Microsoft	• Threat intelligence source – query intel data from Microsoft Graph Security in SecureX threat response
Google	• Threat intelligence source – query intel data from Google Chronicle in SecureX threat response

Learn more: SecureX threat response partner ecosystem and SecureX on DevNet.

Activation information

Cisco Secure customers can get started today at: security.cisco.com, no additional license required. For help, check out this quick login guide.

Not yet a Cisco Secure customer? Evaluate our products with a free trial here.

Platform specifications

Cisco SecureX is a cloud-native platform available in three regional clouds:

- U.S. cloud
- EU cloud
- Asia Pacific cloud

Browser requirements: current and preceding versions of Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari.

Cisco security buying programs

The Security Choice Enterprise Agreement is a Cisco enterprise agreement option. The Cisco enterprise agreement is a cross-architecture buying program that lets organizations purchase and manage software and supporting services spanning all architectures through a single, flexible, 3- or 5- year agreement. The Security Choice Enterprise Agreement gives you the flexibility to deploy what you need now, and add more in the future.

Our new simplified buying programs make it financially compelling to experience our broad portfolio, while SecureX helps you multiply the benefits and capabilities of your investments with us. You can gain financial predictability with our "not-to-exceed" pricing guarantee that allows for your org to grow by 20% annually without additional costs.

Find additional information here: https://www.cisco.com/c/en/us/products/software/security-enterprise-license-agreement/index.html.

Resources

- SecureX online help - For complete documentation about SecureX, see the online help in the platform. Review the Resources topic to access videos to learn more about the features in SecureX.
- SecureX getting started guide
- SecureX login guide
- Cisco Community
- SecureX videos (YouTube)
- SecureX webinars
- Privacy datasheet

Support

If you require technical assistance with SecureX, you can open a case in Support Case Manager. The Cisco security product(s) through which you have access to Cisco SecureX entitle you to a number of technical services. You would need your product serial number or product service contract to create a support case. Alternatively, you can either manually select "SecureX" in the technology window and bypass the entitlement or contact Cisco Support at X 800 553 2447.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-744985-00 08/21