Framework Mapping:
Cisco Secure Network Analytics
+ CIS Controls v8.1

Background

Cisco Secure Network Analytics (SNA) gives organizations a practical way to connect CIS Critical Security Controls v8.1 requirements to network detection and response capabilities they can deploy, operate, monitor, and document. SNA can provide broad visibility into users, devices, applications, and traffic flows across on-premises, cloud, hybrid, branch, data center, and remote-access environments. It helps customers understand what is communicating, detect suspicious behavior, investigate policy violations or threats, and preserve evidence for audit and security operations.

For organizations using CIS as a security controls roadmap, SNA can be especially useful where safeguards depend on passive asset discovery, network traffic and flow visibility, audit log and telemetry collection, centralized security event alerting, network monitoring and defense, behavioral analytics, encrypted traffic analytics, threat hunting, forensic investigation, and incident response evidence. These are areas where network telemetry and behavioral context can provide operational protection and evidence for audit and security program reviews.

The mapping is intentionally scoped to what Cisco SNA can reasonably provide. Some CIS safeguards require endpoint configuration management, identity lifecycle controls, anti-malware deployment, vulnerability remediation, web or email security controls, backup and recovery, workforce training, service-provider oversight, software development security, or broader governance processes. In those areas, SNA may still provide meaningful support through visibility, detection context, or evidence that customers can use with the appropriate process owner and adjacent security platforms.

CIS Controls v8.1 Overview

The CIS Critical Security Controls v8.1 are a prioritized set of safeguards for defending systems and networks against prevalent cyber attacks. For Cisco customers, the framework can be useful because it turns broad security outcomes into specific safeguards that can be mapped to technology capabilities, operational ownership, and evidence.

CIS Controls v8.1 updates v8 with current alignment to industry standards and frameworks, revised asset classes and safeguard wording, and the Govern security function introduced in NIST Cybersecurity Framework 2.0. CIS publishes mapping resources and the CIS Controls Navigator so teams can see how CIS safeguards relate to other security standards and to the broader programs they already manage.

This crosswalk value matters in a multi-framework environment. CIS publishes individual mappings to frameworks such as NIST CSF 2.0, NIST SP 800-53 Rev. 5, NIST SP 800-171, ISO/IEC 27001, PCI DSS, SOC 2, and additional regulatory or industry frameworks. A CIS mapping can therefore help Cisco customers explain how firewall enforcement, monitoring, logging, segmentation, and policy-management evidence supports more than one compliance conversation.

Implementation Groups

Implementation Groups (IGs) are CIS's recommended prioritization model. IG1 is essential cyber hygiene: the baseline set of safeguards every enterprise should consider first because they address common attacks with practical, foundational controls. IG2 builds on IG1 for organizations with more complex environments, greater regulatory exposure, or higher operational risk. IG3 includes the full CIS Controls safeguard set and is designed for

significant risk exposure, or a need for the most comprehensive coverage.

In the mapping tables, the IG1/IG2/IG3 columns show where each safeguard sits in that adoption path. This lets a customer use the same Cisco firewall and FMC mapping for a phased roadmap: start with IG1 priorities, expand into IG2 as the program matures, and use IG3 where the organization requires full CIS coverage.

Major Controls at a Glance

The CIS Controls v8.1 provide a prioritized set of 18 cybersecurity best practices designed to help organizations strengthen their security posture, reduce cyber risk, and improve resilience against modern threats. The controls are organized around key areas of security governance, asset management, vulnerability management, access control, monitoring, and incident response. Together, they offer a practical, risk-based framework that helps organizations establish foundational security capabilities while aligning security resources to the most effective defensive measures. The following table summarizes the 18 CIS Controls at a high level. Detailed descriptions for each control are provided in subsequent sections of this document.

Table 1. CIS Controls v8.1

Control Number	Control Title
Control 1	Inventory and Control of Enterprise Assets
Control 2	Inventory and Control of Software Assets
Control 3	Data Protection
Control 4	Secure Configuration of Enterprise Assets and Software
Control 5	Account Management
Control 6	Access Control Management
Control 7	Continuous Vulnerability Management
Control 8	Audit Log Management
Control 9	Email and Web Browser Protections
Control 10	Malware Defenses
Control 11	Data Recovery
Control 12	Network Infrastructure Management
Control 13	Network Monitoring and Defense
Control 14	Security Awareness and Skills Training
Control 15	Service Provider Management
Control 16	Application Software Security
Control 17	Incident Response Management
Control 18	Penetration Testing

Cisco Secure Network Analytics Overview

Cisco Secure Network Analytics (SNA) helps organizations turn the network into a source of security visibility, detection, investigation, and response evidence. SNA can analyze ongoing network telemetry across on-premises, cloud, hybrid, branch, data center, and remote-access environments so security teams can understand users, devices, applications, and traffic flows without requiring a full endpoint-agent footprint.

Within the context of CIS Controls v8.1, SNA has relevant alignment where safeguards depend on passive asset discovery, network traffic and flow visibility, audit log and telemetry collection, centralized security event alerting, network intrusion and anomaly detection, threat hunting, forensic investigation, and incident response evidence. SNA does not replace broader security processes, but it can provide useful network context and evidence for a customer's cybersecurity program.

SNA uses behavioral analytics, machine learning, policy-violation detection, encrypted traffic analytics, historical flow records, reporting, and integrations with the Cisco and third-party security ecosystem. These capabilities can help customers identify suspicious behavior, investigate lateral movement or data exfiltration, enrich response workflows, and document how network activity is monitored over time.

How to Interpret the Mapping

The CIS Controls mappings in this document describe Cisco SNA's contribution to each safeguard. Meets indicates that this mapping identifies SNA as providing the primary technical mechanism for the safeguard within its network visibility, traffic-flow logging, behavioral analytics, event alerting, Data Store, forensics, or incident response scope. Supports indicates that SNA contributes meaningful visibility, telemetry, context, detection, reporting, or evidence, but complementary technologies, processes, or organizational controls may be needed to address the safeguard.

Many CIS safeguards are not typically addressed by network detection and response technologies. Where a safeguard focuses primarily on endpoint configuration, identity lifecycle management, software development security, backup and recovery, user training, service-provider governance, or business process ownership, SNA may provide supporting visibility or evidence rather than the primary control implementation.

Table 2. CIS alignment value

Capability Area	Cisco Secure Network Analytics Benefits
Network Visibility and Flow Telemetry	Supports safeguards for asset visibility, audit evidence, network infrastructure monitoring, and network monitoring.
Behavioral Analytics and Anomaly Detection	Supports monitoring, detection, investigation, and incident-response safeguards.
Encrypted Traffic Analytics	Helps customers detect threats where payload inspection is limited by encryption or privacy requirements.
Threat Investigation and Forensics	Supports audit log management, threat hunting, forensic investigation, and post-incident evidence needs.
Response and Ecosystem Integration	Helps customers move from detection to triage, containment, and documented response.

Detailed CIS Controls Mapping Tables

The following sections provide a detailed mapping of Cisco SNA capabilities to the CIS Controls v8.1. Each control is evaluated against its associated safeguards to show where SNA can meet or support CIS implementation.

For each control, the mapping tables include the applicable Implementation Group (IG1, IG2, and IG3), asset type, security function, and SNA rating. Blank status cells indicate that SNA is not identified in this mapping as meeting or supporting that safeguard.

Safeguards are categorized as either:

- **Meets** – Directly provides capabilities that satisfy the intent of the safeguard.
- **Supports** – Contributes to the implementation of the safeguard but may require complementary technologies, processes, or organizational controls to fully address the requirement.

Not all CIS Controls and safeguards are directly addressed by network security technologies. Controls focused on governance, policy, risk management, or workforce training may not include a mapping table but are included for completeness and context within the CIS Controls framework.

Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices	Identify	X	X	X		Supports
1.2	Address Unauthorized Assets	Devices	Respond	X	X	X		Supports
1.3	Utilize an Active Discovery Tool	Devices	Detect		X	X		Supports
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Devices	Identify		X	X		Supports
1.5	Use a Passive Asset Discovery Tool	Devices	Detect			X	Meets	

Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
2.1	Establish and Maintain a Software Inventory	Applications	Identify	X	X	X		Supports
2.2	Ensure Authorized Software is Currently Supported	Applications	Identify	X	X	X		Supports
2.3	Address Unauthorized Software	Applications	Respond	X	X	X		Supports
2.4	Utilize Automated Software Inventory Tools	Applications	Detect		X	X		Supports

Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
3.3	Configure Data Access Control Lists	Data	Protect	X	X	X		Supports
3.8	Document Data Flows	Data	Identify		X	X	Meets	
3.10	Encrypt Sensitive Data in Transit	Data	Protect		X	X		Supports
3.12	Segment Data Processing and Storage-Based on Sensitivity	Network	Protect		X	X		Supports
3.13	Deploy a Data Loss Prevention Solution	Data	Protect			X		Supports
3.14	Log Sensitive Data Access	Data	Detect			X		Supports

Control 4: Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
4.1	Establish and Maintain a Secure Configuration Process	Applications	Protect	X	X	X		Supports
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Network	Protect	X	X	X		Supports
4.6	Securely Manage Enterprise Assets and Software	Network	Protect	X	X	X		Supports
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Devices	Protect		X	X		Supports

Control 5: Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
5.1	Establish and Maintain an Inventory of Accounts	Users	Identify	X	X	X		Supports
5.3	Disable Dormant Accounts	Users	Respond	X	X	X		Supports
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Users	Protect	X	X	X		Supports
5.6	Centralize Account Management	Users	Protect		X	X		Supports

Control 6: Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
6.1	Establish an Access Granting Process	Users	Protect	X	X	X		Supports
6.2	Establish an Access Revoking Process	Users	Protect	X	X	X		Supports
6.5	Require MFA for Administrative Access	Users	Protect	X	X	X		Supports
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Users	Identify		X	X		Supports
6.7	Centralize Access Control	Users	Protect		X	X		Supports
6.8	Define and Maintain Role-Based Access Control	Data	Protect			X		Supports

Control 7: Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
7.1	Establish and Maintain a Vulnerability Management Process	Applications	Protect	X	X	X		Supports
7.2	Establish and Maintain a Remediation Process	Applications	Respond	X	X	X		Supports
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Applications	Identify		X	X		Supports
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Applications	Identify		X	X		Supports
7.7	Remediate Detected Vulnerabilities	Applications	Respond		X	X		Supports

Control 8: Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
8.1	Establish and Maintain an Audit Log Management Process	Network	Protect	X	X	X		Supports
8.2	Collect Audit Logs	Network	Detect	X	X	X	Meets	
8.3	Ensure Adequate Audit Log Storage	Network	Protect	X	X	X		Supports
8.4	Standardize Time Synchronization	Network	Protect		X	X		Supports
8.5	Collect Detailed Audit Logs	Network	Detect		X	X	Meets	
8.6	Collect DNS Query Audit Logs	Network	Detect		X	X		Supports
8.7	Collect URL Request Audit Logs	Network	Detect		X	X		Supports
8.9	Centralize Audit Logs	Devices	Detect		X	X	Meets	
8.10	Retain Audit Logs	Network	Protect		X	X	Meets	
8.11	Conduct Audit Log Reviews	Network	Detect		X	X		Supports
8.12	Collect Service Provider Logs	Data	Detect			X		Supports

Control 9: Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement

This control is primarily addressed through technologies and processes that protect users from malicious email and web content. Cisco Secure Network Analytics (SNA) does not directly provide email or web browser protection capabilities; however, it complements this control by continuously monitoring network activity and detecting anomalous or malicious communications resulting from phishing attacks, malicious downloads, compromised accounts, or browser-based threats. Through behavioral analytics and threat detection, SNA helps organizations identify and investigate indicators of compromise associated with email- and web-based attack vectors, supporting a broader defense-in-depth strategy.

Control 10: Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
10.5	Enable Anti-Exploitation Features	Devices	Protect		X	X		Supports
10.7	Use Behavior-Based Anti-Malware Software	Devices	Detect		X	X		Supports

Control 11: Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
11.2	Perform Automated Backups	Data	Recover	X	X	X		Supports
11.3	Protect Recovery Data	Data	Protect	X	X	X		Supports
11.5	Test Data Recovery	Data	Recover		X	X		Supports

Control 12: Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
12.1	Ensure Network Infrastructure is Up-to-Date	Network	Protect	X	X	X		Supports
12.2	Establish and Maintain a Secure Network Architecture	Network	Protect		X	X		Supports
12.3	Securely Manage Network Infrastructure	Network	Protect		X	X		Supports
12.4	Establish and Maintain Architecture Diagram(s)	Network	Identify		X	X		Supports

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
12.6	Use of Secure Network Management and Communication Protocols	Network	Protect		X	X		Supports
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Devices	Protect		X	X		Supports

Control 13: Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
13.1	Centralize Security Event Alerting	Network	Detect		X	X	Meets	
13.3	Deploy a Network Intrusion Detection Solution	Network	Detect		X	X	Meets	
13.4	Perform Traffic Filtering Between Network Segments	Network	Protect		X	X		Supports
13.5	Manage Access Control for Remote Assets	Devices	Protect		X	X		Supports
13.6	Collect Network Traffic Flow Logs	Network	Detect		X	X	Meets	
13.8	Deploy a Network Intrusion Prevention Solution	Network	Protect			X		Supports
13.9	Deploy Port-Level Access Control	Devices	Protect			X		Supports
13.10	Perform Application Layer Filtering	Network	Protect			X		Supports
13.11	Tune Security Event Alerting Thresholds	Network	Detect			X	Meets	

Control 14: Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

This control is primarily addressed through organizational policies, processes, and employee education programs. While Cisco SNA does not directly provide security awareness or training capabilities, it complements this control by detecting suspicious network activity that may result from human error, social engineering, or compromised credentials, supporting overall cybersecurity monitoring and response efforts.

Control 15: Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
15.4	Ensure Service Provider Contracts Include Security Requirements		Protect		X	X		Supports
15.5	Assess Service Providers		Identify			X		Supports
15.6	Monitor Service Providers		Identify			X		Supports
15.7	Securely Decommission Service Providers	Data	Protect			X		Supports

Control 16: Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
16.8	Separate Production and Non-Production Systems	Applications	Protect		X	X		Supports
16.10	Apply Secure Design Principles in Application Architectures	Applications	Protect		X	X		Supports
16.13	Conduct Application Penetration Testing	Applications	Protect			X		Supports
16.14	Conduct Threat Modeling	Applications	Protect			X		Supports

Control 17: Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents		Respond	X	X	X		Supports
17.4	Establish and Maintain an Incident Response Process		Respond		X	X		Supports
17.6	Define Mechanisms for Communicating During Incident Response		Respond		X	X		Supports
17.7	Conduct Routine Incident Response Exercises		Recover		X	X		Supports
17.8	Conduct Post-Incident Reviews		Recover		X	X		Supports
17.9	Establish and Maintain Security Incident Thresholds		Recover			X		Supports

Control 18: Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	SNA Meet	SNA Supports
18.3	Remediate Penetration Test Findings	Network	Protect		X	X		Supports
18.4	Validate Security Measures	Network	Protect			X		Supports
18.5	Perform Periodic Internal Penetration Tests		Identify			X		Supports

Key Observations

1. Relevant Alignment to Network Visibility and Monitoring:

- Cisco Secure Network Analytics aligns with CIS safeguards focused on network visibility, traffic-flow monitoring, passive asset discovery, and centralized security event analysis.
- SNA helps customers understand which users, devices, applications, and systems are communicating across on-premises, cloud, hybrid, branch, data center, and remote-access environments.

2. Support for Audit Log Management and Evidence Collection:

- SNA supports CIS audit and monitoring outcomes through network telemetry, flow records, historical activity, reporting, and event context that can be used during investigation and audit or framework review.
- These capabilities are especially valuable where customers need to document how network activity is collected, reviewed, retained, and used to detect or understand security events.

3. Behavioral Analytics and Threat Detection:

- Cisco Secure Network Analytics contributes to proactive defense through behavioral analytics, machine learning, anomaly detection, policy-violation detection, and encrypted traffic analytics.
- This supports CIS safeguards tied to identifying suspicious behavior, detecting lateral movement, investigating data exfiltration indicators, and improving network monitoring and defense.

4. Incident Investigation and Response Support:

- SNA provides meaningful support for CIS incident response outcomes by giving security teams historical flow data, entity context, alerts, dashboards, and forensic evidence during triage and investigation.
- The platform helps customers move from detection to investigation and documented response, especially when unusual network behavior is the first indicator of compromise.

5. Complementary Role in Broader CIS Programs:

- Cisco Secure Network Analytics is especially relevant for network detection and response use cases, but some CIS safeguards require endpoint controls, identity management, vulnerability remediation, backup and recovery, training, governance, or application security processes.
- In those areas, customers can use SNA as a supporting source of visibility, detection context, and evidence alongside the broader security program.

Summary

Cisco Secure Network Analytics can support CIS Controls v8.1 alignment efforts by helping customers see, monitor, analyze, investigate, and document network activity across complex environments. Its relevant contributions include passive asset visibility, network traffic and flow telemetry, security event alerting, behavioral analytics, anomaly detection, policy-violation detection, threat hunting, forensic investigation, and incident response evidence.

The value of SNA is especially clear when customers need to connect framework requirements to observable activity on the network. SNA can help security teams understand what is communicating, identify suspicious changes in behavior, investigate threats such as lateral movement or data exfiltration, and preserve evidence that supports audit and response workflows. For safeguards outside the SNA product boundary, customers can use SNA as a supporting control alongside endpoint, identity, vulnerability, backup, training, governance, and application security programs.

Resources

For more information, please refer to the following:

- CIS Critical Security Controls v8.1
- CIS Critical Security Controls Implementation Groups
- CIS Controls Navigator and framework mappings
- Cisco Secure Network Analytics product page
- Framework Mapping: SNA + NIST CSF 2.0