Framework Mapping:
Cisco Secure Workload + CIS Controls v8.1

Background

Cisco Secure Workload gives organizations a practical way to connect CIS Critical Security Controls v8.1 requirements to workload protection and microsegmentation capabilities they can deploy, operate, monitor, and document. Secure Workload can help see how applications communicate, identify workload and software package context, discover application dependencies, apply segmentation policies, and provide supporting information for audit and security operations.

For organizations using CIS as a security controls roadmap, Secure Workload can be especially useful where safeguards depend on workload visibility, application dependency mapping, software package inventory, vulnerability context, least-privilege segmentation, policy monitoring, host-based workload enforcement, and incident investigation evidence. These are areas where workload telemetry, policy discovery, vulnerability context, and microsegmentation can provide operational protection and evidence for audit and security program reviews.

The mapping is intentionally scoped to what Cisco Secure Workload can reasonably provide. Some CIS safeguards require enterprise Identity Access Management (IAM), DNS/web/email security, endpoint anti-malware deployment, backup and recovery, workforce training, service-provider oversight, software development security, or broader governance processes. In those areas, Secure Workload may still provide meaningful support through visibility, segmentation evidence, vulnerability context, or investigation data that organizations 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 explain how Secure Workload visibility, software package context, application dependency mapping, microsegmentation policy, vulnerability context, and enforcement evidence may support broader audit, risk, and security program conversations.

Implementation Groups

Implementation Groups (IGs) are CIS's recommended prioritization model. IG1 is essential cyber hygiene: the baseline safeguards every organization 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 organizations with mature security programs, 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. Organizations can use the same Cisco Secure Workload mapping to support a phased roadmap: start with IG1 priorities, expand into IG2 as the program matures, and use IG3 where the organization is working toward 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 Workload Overview

Cisco Secure Workload can help organizations improve visibility and control for applications and workloads across data center, cloud, hybrid, virtualized, bare-metal, container, and Kubernetes environments. It can collect workload telemetry, map application dependencies, identify software packages and process activity, and use that context to help security teams understand how applications communicate.

Within the context of CIS Controls v8.1, Secure Workload has relevant alignment where safeguards depend on workload inventory, application dependency mapping, software package visibility, vulnerability context, segmentation policy, workload-level enforcement, policy monitoring, and evidence for investigation or audit review. Secure Workload does not replace broader security processes, but it can provide useful workload context and segmentation evidence for an organizations's cybersecurity program.

Secure Workload supports agent-based and agentless approaches for visibility and segmentation use cases. Depending on deployment design, it can use workload agents, cloud telemetry, network telemetry, labels, and integrations with Cisco and third-party systems to support policy discovery, microsegmentation, vulnerability prioritization, policy monitoring, and incident investigation workflows.

How to Interpret the Mapping

This document provides a mapping of Cisco Secure Workload to the CIS Controls framework. It highlights how the platform functions as a primary technical mechanism for securing workloads through visibility, application dependency mapping, and microsegmentation.

Additionally, the mapping details how Secure Workload provides valuable telemetry, context, and evidence for broader enterprise security initiatives, such as identity management, vulnerability assessment, and policy monitoring.

While some CIS safeguards fall outside the core scope of workload protection, Secure Workload remains an important component in supporting an organization's overall security posture by providing essential, evidence-based data for compliance and risk management activities.

Table 2. CIS alignment value

Capability Area	Cisco Secure Workload Benefits
Workload Visibility and Inventory	Supports safeguards for asset visibility, software visibility, audit evidence, and investigation.
Application Dependency Mapping	Helps customers understand workload relationships and build segmentation policies from observed activity.
Microsegmentation Policy Enforcement	Supports least-privilege access, containment, and reduce unnecessary east-west traffic where policies are deployed and maintained.
Vulnerability and Package Context	Supports prioritization and response workflows where workload vulnerability context is relevant.
Policy Monitoring and Evidence	Supports audit review, incident response evidence, and ongoing segmentation policy management.

Detailed CIS Controls Mapping Tables

The following sections provide a detailed mapping of Cisco Secure Workload capabilities to the CIS Controls v8.1. Each control is evaluated against its associated safeguards to show where Cisco Secure Workload 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 Secure Workload rating. Blank status cells indicate that Secure Workload 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. 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	Secure Workload Meets	Secure Workload 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	Secure Workload Meets	Secure Workload Supports
2.1	Establish and Maintain a Software Inventory	Applications	Identify	X	X	X	Meets	
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	Meets	
2.5	Allowlist Authorized Software	Applications	Protect		X	X		Supports
2.6	Allowlist Authorized Libraries	Applications	Protect		X	X		Supports
2.7	Allowlist Authorized Scripts	Applications	Protect			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	Secure Workload Meets	Secure Workload Supports
3.3	Configure Data Access Control Lists	Data	Protect	X	X	X	Meets	
3.6	Encrypt Data on End-User Devices	Devices	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	Meets	
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	Secure Workload Meets	Secure Workload 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
4.4	Implement and Manage a Fiewall on Servers	Devices	Protect	X	X	X	Meets	
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	Respond		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	Secure Workload Meets	Secure Workload 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	Secure Workload Meets	Secure Workload 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	Meets	
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	Secure Workload Meets	Secure Workload 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
7.3	Perform Automated Operating System Patch Management	Applications	Protect	X	X	X		Supports
7.4	Perform Automated Application Patch Management	Applications	Protect	X	X	X		Supports

Sub-Control	Title	Asset Type	Security Function	IG1	IG2	IG3	Secure Workload Meets	Secure Workload Supports
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Applications	Identify		X	X	Meets	
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	Secure Workload Meets	Secure Workload 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	
8.8	Collect Command-Line 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

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

Cisco Secure Workload does not directly protect against malicious email or web content. It complements this control by providing visibility into workload communications, detecting anomalous behavior resulting from compromised systems, and enforcing microsegmentation policies that help contain threats originating from email- and web-based attack vectors. This reduces the potential for lateral movement and supports incident detection and response activities.

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	**Secure Workload Meets**	**Secure Workload Supports**
10.1	Deploy and Maintain Anti-Malware Software	Devices	Protect	X	X	X		Supports
10.2	Configure Automatic Anti-Malware Signature Updates	Devices	Protect	X	X	X		Supports
10.5	Enable Anti-Exploitation Features	Devices	Protect		X	X		Supports
10.6	Centrally Manage Anti-Malware Software	Devices	Protect		X	X		Supports
10.7	Use Behavior-Based Anti-Malware Software	Devices	Detect		X	X	Meets	

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	Secure Workload Meets	Secure Workload 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	Secure Workload Meets	Secure Workload 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	Meets	
12.3	Securely Manage Network Infrastructure	Network	Protect		X	X		Supports
12.4	Establish and Maintain Architecture Diagram(s)	Network	Identify		X	X	Meets	
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	Secure Workload Meets	Secure Workload Supports
13.1	Centralize Security Event Alerting	Network	Detect		X	X	Meets	
13.2	Deploy a Host-Based Intrusion Detection System	Devices	Detect		X	X		Supports
13.3	Deploy a Network Intrusion Detection Solution	Network	Detec		X	X		Supports
13.4	Perform Traffic Filtering Between Network Segments	Network	Protect		X	X	Meets	
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	
13.7	Deploy a Host-Based Intrusion Prevention Solution	Devices	Protect			X		Supports
13.8	Deploy a Network Intrusion Prevention Solu-tion	Network	Protect			X		Supports
13.9	Deploy Port-Level Access Control	Devices	Protect			X	Meets	
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.

Cisco Secure Workload does not directly provide security awareness or training capabilities. It supports this control by detecting anomalous workload behavior that may result from human error, social engineering, or credential compromise and by enforcing segmentation policies that help contain potential threats and support incident response activities.

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	Secure Workload Meets	Secure Workload 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	Secure Workload Meets	Secure Workload Supports
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	Applications	Protect		X	X		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	Secure Workload Meets	Secure Workload 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	Meets	

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	Secure Workload Meets	Secure Workload 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 Workload Visibility and Application Mapping:

- Cisco Secure Workload aligns with CIS safeguards focused on workload inventory, software package visibility, process telemetry, and application dependency mapping.
- These capabilities help organizations understand how applications and workloads communicate across hybrid, multicloud, data center, and containerized environments.

2. Support for Microsegmentation and Least-Privilege Access:

- Secure Workload contributes to CIS safeguards requiring segmentation, access control, containment, and reduction of unnecessary east-west traffic through workload-level policy discovery and enforcement.
- Organizations can use Secure Workload to help build and monitor policies that align application communication with business need.

3. Vulnerability and Software Package Context:

- Secure Workload supports security controls workflows by combining software package visibility, vulnerability context, workload labels, and application behavior to inform prioritization and response.
- This context is useful where CIS safeguards depend on understanding workload exposure and taking action based on risk.

4. Policy Monitoring, Investigation, and Evidence:

- Cisco Secure Workload can provide telemetry, reporting, and historical context that may support audit and review evidence.
- This can support incident investigation, segmentation policy review, and documentation of workload security control operation.

5. Complementary Role in Broader CIS Programs:

- Cisco Secure Workload is especially relevant for workload protection and micro-segmentation use cases, but some CIS safeguards require enterprise IAM, endpoint controls, anti-malware, backup and recovery, training, governance, or application security processes.
- In those areas, organizations can use Secure Workload as a supporting source of workload context, segmentation evidence, vulnerability context, and investigation data alongside the broader security program.

Summary

Cisco Secure Workload can support CIS Controls v8.1 alignment efforts by helping customers see, analyze, segment, monitor, and document workload activity across complex environments. Its relevant contributions include workload inventory, application dependency mapping, software package visibility, vulnerability context, microsegmentation policy discovery, workload-level enforcement, policy monitoring, and investigation evidence.

The value of Secure Workload is especially clear when organizations need to connect framework requirements to application behavior and workload communication. Secure Workload can help security teams understand workload relationships, apply segmentation policies based on observed communication, monitor policy behavior, prioritize workload risk, and retain context that may support audit and response workflows. For safeguards outside the Secure Workload product boundary, customers can use Secure Workload as a supporting control alongside identity, endpoint, 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 Workload product page
- Cisco Secure Workload Platform datasheet
- CIsco Zero Trust Microsegmentation guide
- Framework Mapping: Secure Workload + NIST CSF 2.0