Framework Foundations: CIS Controls v8.1

Introduction to the CIS Controls

The CIS Critical Security Controls (CIS Controls) are prioritized best practices developed by the Center for Internet Security to strengthen organizational cybersecurity. The latest version, CIS Controls v8.1, was released in 2024 and reflects modern IT environments, including cloud, hybrid, and remote workforces as well as securing the supply chain.

CIS Controls v8.1 also aligns with major security frameworks such as NIST CSF v2, ISO 27001, HIPAA, and PCI DSS, and provides a clear migration path for organizations updating from previous versions.

Applicable to organizations of all sizes, CIS Controls are especially useful for small to medium-sized enterprises seeking a clear path to stronger cybersecurity.

Objectives

- **Prioritize cyber defense:** Focus on the most effective actions to reduce risks from known threats
- **Simplify implementation:** Offers clear steps for organizations of any size
- **Support Compliance:** Maps to regulatory frameworks and industry standards
- **Adapt to modern environments:** Addresses cloud, hybrid, and remote infrastructure
- **Enables continuous improvement:** Encourages regular assessments and maturity progression

Key Requirements

The CIS Controls are widely recognized as a foundational framework for effective cyber defense. The core tenets and actions required to align with CIS Controls include:

Implementation of Safeguards

The CIS Controls are structured into a set of 18 top-level safeguards (formerly controls), each containing several sub-safeguards. These cover a range of cybersecurity activities, from basic cyber hygiene to more advanced defense measures, including inventory and control of enterprise assets, secure configuration of enterprise assets and software, data protection, access control management, vulnerability management, incident response management, and security awareness and skills training.

Prioritization of Safeguards

The CIS Controls are designed to be implemented in a prioritized manner, focusing first on safeguards that provide the greatest risk reduction and are most effective against common threats. This prioritization helps organizations allocate resources efficiently and achieve meaningful security improvements early in their cybersecurity journey. The safeguards are ranked based on real-world data and expert consensus, ensuring that organizations address the most critical areas first.

Using Implementation Groups (IGs)

The CIS Controls are grouped into three IGs to simplify and tailor their adoption based on organizational needs.

- **IG1 (basic cyber hygiene):** Focuses on essential safeguards for small and medium-sized organizations with limited resources, aiming to defend against common attacks.
- **IG2:** Builds on IG1 with additional safeguards for organizations with moderate resources and risk.
- **IG3:** Encompasses all safeguards from IG1and IG2, plus additional advanced safeguards for organizations with significant resources and a higher risk tolerance, often dealing with sensitive data or critical infrastructure.

How Cisco Security + Splunk Support Compliance

- Cisco and Splunk offers a comprehensive portfolio of security solutions that can help organizations meet the requirements of the CIS Controls framework:

CIS Control	How Cisco + Splunk Support Compliance	Relevant Products
Control 1. **Inventory and Control of Enterprise Assets**	Identifies and monitors enterprise assets across networks and cloud, aggregating data for centralized visibility and anomaly detection.	Cisco Identity Services Engine (ISE), Cisco Secure Endpoint, Cisco Secure Network Analytics (SNA), Cisco Secure Workload, Splunk Asset and Risk Intelligence (ARI), Splunk Enterprise Security (ES)
Control 2. **Inventory and Control of Software Assets**	Detects installed software across endpoints and networks, correlating inventories with threat intelligence and policy violations.	Cisco Secure Endpoint, Cisco Secure Workload, Splunk Asset and Risk Intelligence (ARI), Splunk ES
Control 3. **Data Protection**	Enforces encryption, data loss prevention, and secure access while monitoring data flows and alerting on unauthorized access or exfiltration attempts.	Cisco Secure Endpoint, Cisco ISE, Cisco SNA, Cisco Secure Firewall, Cisco Secure Email, Cisco Duo, Splunk ES, Splunk UBA, Splunk Attack Analyzer, Splunk SOAR
Control 4. **Secure Configuration of Enterprise Assets and Software**	Applies secure configurations to devices and cloud assets, auditing changes and flagging deviations from baselines.	Cisco Secure Endpoint, Cisco ISE, Cisco Secure Workload, Cisco Secure Firewall, Cisco Duo, Splunk ES, Splunk SOAR, Splunk ARI
Control 5. **Account Management**	Manages identities and enforces access policies, tracking account lifecycle events and privilege changes for compliance.	Cisco ISE, Cisco Duo, Splunk ES, Splunk UBA, Splunk SOAR
Control 6. **Access Control Management**	Enforces multi-factor authentication and network segmentation, monitoring access attempts and flagging least privileged violations.	Cisco Duo, Cisco ISE, Cisco Secure Firewall, Cisco SNA, Splunk ES, Splunk UBA, Splunk SOAR

CIS Control	How Cisco + Splunk Support Compliance	Relevant Products
Control 7. Continuous Vulnerability Management	Identifies vulnerabilities using threat intelligence and telemetry, ingesting scan results and prioritizing remediation.	Cisco Secure Endpoint, Cisco Secure Workload, Cisco XDR, Splunk ES, Splunk SOAR, Splunk ARI, Splunk Attack Analyzer
Control 8. Audit Log Management	Generates logs across security tools, centralizing ingestion, parsing, and analysis for audit and investigation.	Cisco XDR, Cisco SNA, Splunk ES, Splunk SOAR
Control 9. Email and Web Browser Protections	Filters malicious email and web traffic, analyzing logs to detect phishing, malware, and risky user behavior.	Cisco Secure Email, Cisco Umbrellas, Cisco Secure Endpoint, Cisco Secure Access, Cisco XDR, Splunk ES, Splunk UBA, Splunk Attack Analyzer
Control 10. Malware Defenses	Blocks malware across endpoints, networks, and cloud, correlating alerts and supporting incident response workflows.	Cisco Secure Endpoint, Cisco Secure Firewall, Cisco Secure Email, Cisco Umbrella, Cisco Secure Access, Cisco SNA, Cisco XDR, Splunk ES, Splunk SOAR, Splunk UBA, Splunk Attack Analyzer
Control 11. Data Recovery	Supports network and device configuration backups, storing historical logs to aid forensic analysis and recovery planning.	Cisco XDR, Cisco SNA, Cisco Secure Firewall, Cisco ISE, Cisco Secure Endpoint, Cisco Secure Workload, Splunk ES, Splunk SOAR
Control 12. Network Infrastructure Management	Manages network infrastructure securely, monitoring device logs for performance, configuration drift, and security events.	Cisco ISE, Cisco Secure Firewall, Cisco SNA, Cisco XDR, Splunk ES, Splunk SOAR, Splunk ARI
Control 13. Network Monitoring and Defense	Detects threats via intrusion prevention and network analytics, correlating flow data and alerts for real-time detection.	Cisco Secure Firewall, Cisco SNA, Cisco Umbrella, Cisco Secure Access, Cisco XDR, Splunk ES, Splunk UBA, Splunk Attack Analyzer

CIS Control	How Cisco + Splunk Support Compliance	Relevant Products
Control 14. Security Awareness and Skills Training	Provides security awareness and skills training for network defense, Incident response, threat detection, and security analytics.	Cisco U., Cisco Networking Academy, Splunk Learning Services, Cisco Security Workshops
Control 15. Service Provider Management	Secures third-party access and monitors interactions, ingesting external logs and tracking service provider activity.	Cisco ISE, Cisco Secure Access, Cisco Duo, Cisco Secure Firewall, Cisco SNA, Cisco XDR, Splunk ES, Splunk SOAR, Splunk UBA, Splunk ARI
Control 16. Application Software Security	Secures APIs and monitors application behavior, analyzing logs and WAF data to dtect vulnerabilities and attacks.	Cisco Secure Application, Cisco Hypershield, Cisco Web Application and API Protection (WAAP), Cisco Secure Workload, Cisco XDR, Splunk ES, Splunk UBA, Splunk SOAR, Splunk Attack Analyzer
Control 17. Incident Response Management	Detects and responds to threats using XDR and endpoint tools, orchestrating response actions and supporting incident investigations.	Cisco Secure Endpoint, Cisco XDR, Cisco SNA Cisco Secure Firewall, Cisco Duo, Cisco Secure Email, Cisco Secure Workload,, Cisco Hypershield, Splunk ES, Splunk SOAR, Splunk UBA, Splunk Attack Analyzer, Talos Emergency IR Services
Control 18. Penetration Testing	Hardens systems to reduce attack surface, monitoring penetration test activity and providing insights for remediation.	Cisco XDR, Cisco Secure Endpoint, Cisco Secure Firewall, Cisco SNA, Cisco Secure Workload, Cisco Hypershield, Splunk ES, Splunk SOAR, Cisco UBA, Cisco Attack Analyzer, Cisco ARI

CIS Controls Compliance with Cisco Security + Splunk

As organizations adopt AI and expand into hybrid and cloud environments, they encounter new layers of complexity, control challenges, and visibility gaps that demand a more integrated approach to cybersecurity.

Cisco and Splunk help organizations implement CIS Controls efficiently. Cisco XDR offers end-to-end visibility, automated threat detection, and fast response across endpoints, networks, cloud, and apps. Splunk adds strong analytics, log management, and orchestration to turn data into actionable insights, boosting security operations. This enables:

- Streamlined implementation of CIS Safeguards, from asset inventory to incident response.
- Real-time threat detection and response, powered by Cisco XDR and Splunk SOAR.
- Scalable compliance and audit readiness, with centralized visibility and reporting.
- Reduced complexity and vendor sprawl, through platform integration and automation.

Together, Cisco and Splunk offer a future-ready foundation for cybersecurity maturity, operational resilience, and continuous improvement.

Resources

For more information and guidance on CIS Controls compliance, please refer to the following resources:

- CIS Critical Security Controls
- CIS Critical Security Manual Assessment Tool (CSAT)
- Cisco Security Portfolio
- Splunk Security Products