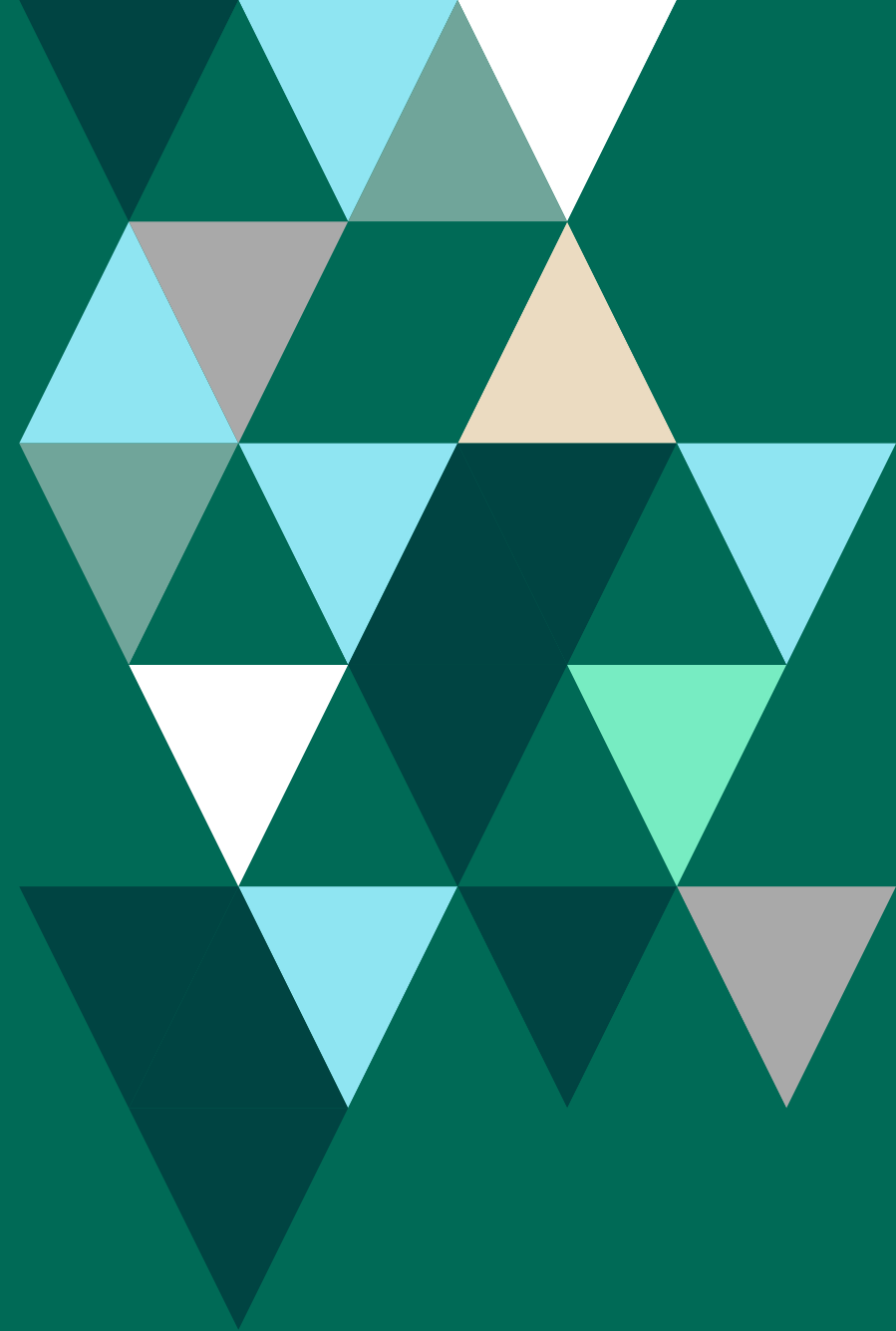


FORTRA

**Tripwire Solutions
and the
CIS Controls v8
Detailed Mapping**



The goal of the Center for Internet Security's CIS Controls (formerly known as the SANS Top 20 and the Top 20 Critical Security Controls) is to protect critical assets, infrastructure and information by strengthening an organization's defensive posture through continuous, automated protection and monitoring of sensitive information technology infrastructure to reduce compromises, minimize the need for recovery efforts, and lower associated costs. The Controls can be applied to any organization, industry, maturity level, and likely threat vectors.

The strength of the CIS Controls is that they reflect the combined knowledge of actual attacks and effective defenses from experts in many organizations that have exclusive and deep knowledge about current threats. This has ensured that the Controls are the most effective and specific set of technical measures available to detect, prevent and mitigate damage from the most common and damaging of those attacks.

Experts endorsing the CIS Controls come from multiple agencies of the U.S. Department of Defense, Nuclear Laboratories of the U.S. Department of Energy, the U.S. Computer Emergency Readiness Team of the U.S. Department of Homeland Security, the United Kingdom's Centre for the Protection of Critical Infrastructure, the FBI and other law enforcement agencies, the Australian Defence Signals Directorate, and government and civilian penetration testers and incident handlers.

Fortra’s Tripwire Solution Support for the CIS Controls v8

CIS CONTROL	Tripwire® Enterprise		Tripwire IP360™	Tripwire LogCenter®	Tripwire Industrial Solutions	Tripwire ExpertOps
	Configuration Management	File Integrity and Change Monitoring	Vulnerability Management	Log Management	Industrial Applications	Tripwire Services
1: Inventory and Control of Enterprise Assets	✓		✓	✓	✓	✓
2: Inventory and Control of Software Assets	✓	✓	✓		✓	✓
3: Data Protection				✓		
4: Secure Configuration of Enterprise Assets and Software	✓		✓		✓	✓
5: Account Management						
6: Access Control Management						✓
7: Continuous Vulnerability Management			✓		✓	✓
8: Audit Log Management	✓			✓		✓
9: Email and Web Browser Protections						
10: Malware Defenses						
11: Data Recovery						
12: Network and Infrastructure Management			✓		✓	✓
13: Network Monitoring and Defense		✓		✓		
14: Security Awareness and Skills Training						✓
15: Service Provider Management						
16: Application Software Security						
17: Incident Response Management						
18: Penetration Testing						✓

Legend: P=Provides, S=Supports, V=Validates

CIS Control	Description	How Tripwire Can Help	Tripwire Enterprise	Tripwire State Analyzer	Tripwire IP360	Tripwire LogCenter
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					
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Tripwire IP360 can scan the environment to discover assets, including operating system, installed applications, and other identifying information.			P	
1.2	Address Unauthorized Assets	Tripwire IP360 can help identify unauthorized assets in the environment as part of this process.			S	
1.3	Utilize Active Discovery	Tripwire IP360 provides active discovery capabilities. Tripwire LogCenter can provide discovery of assets through log data. Tripwire Enterprise can validate that active discovery tools are in place.	V		P	S
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Tripwire LogCenter can collect DHCP logs and provide a mechanism for reviewing them. Tripwire Enterprise can validate that systems are configured to log correctly.	V			S
1.5	Use a Passive Asset Discovery Tool	Tripwire LogCenter can discovery assets through log data.				S
Control 2: Inventory and Controls 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.					
2.1	Establish and Maintain a Software Inventory	IP360 can automatically discover assets and the applications on them. Tripwire Enterprise can fully enumerate the software installed on systems it monitors.	P	S	P	
2.2	Ensure Authorized Software is Currently Supported	IP360 contains checks for unsupported software as required by the PCI Data Security Standard. Tripwire State Analyzer allows customers to build an allowed list of software against which the environment is assessed.	S	P	P	
2.3	Address Unauthorized Software	Tripwire products support this requirement by providing data about unauthorized software into the process to address it.	S	S	S	
2.4	Utilize Automated Software Inventory Tools	Tripwire Enterprise and Tripwire IP360 function as automated software inventory tools. Tripwire State Analyzer can support this process with AllowedLists of software.	P	S	P	
2.5	Allowlist Authorized Software	Tripwire products can support creating an allowlist of software, but do not actively block execution	S	S	S	
2.6	Allowlist Authorized Libraries	Tripwire products can support creating an allowlist of libraries, but do not actively block execution	S			
2.7	Allowlist Authorized Scripts	Tripwire products can support creating an allowlist of scripts, but do not actively block execution	S			
Control 3: Data Protection	Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.					
3.1	Establish and Maintain a Data Management Process					
3.2	Establish and Maintain a Data Inventory					
3.3	Configure Data Access Control Lists					
3.4	Enforce Data Retention	Tripwire Enterprise can validate that data retention settings are properly configured. Tripwire Log Center can be configured to retain log data to support this requirement	V			S
3.5	Securely Dispose of Data					

Legend: P=Provides, S=Supports, V=Validates

CIS Control	Description	How Tripwire Can Help	Tripwire Enterprise	Tripwire State Analyzer	Tripwire IP360	Tripwire LogCenter
3.6	Encrypt Data on End-User Devices	Tripwire Enterprise can validate that end-user devices are configured to be encrypted.	V			
3.7	Establish and Maintain a Data Classification Scheme					
3.8	Document Data Flows					
3.9	Encrypt Data on Removable Media	Tripwire Enterprise can validate that removable media are configured to be encrypted.	V			
3.10	Encrypt Sensitive Data in Transit	Tripwire Enterprise can validate that systems are configured to encrypt communications. IP360 can discover unencrypted communication protocols.	V		S	
3.11	Encrypt Sensitive Data at Rest	Tripwire Enterprise can validate that data is configured to be encrypted.				
3.12	Segment Data Processing and Storage Based on Sensitivity					
3.13	Deploy a Data Loss Prevention Solution	Tripwire Enterprise can validate that DLP is deployed and configured.	V			
3.14	Log Sensitive Data Access	Tripwire LogCenter can collect logs for access to sensitive data.				P
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).					
4.1	Establish and Maintain a Secure Configuration Process	Tripwire Enterprise can be the cornerstone of a secure configuration management process as the primary tool for establishing and validating configurations against a policy.	P			
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Tripwire Enterprise can be the cornerstone of a secure configuration management process as the primary tool for establishing and validating configurations against a policy.	P			
4.3	Configure Automatic Session Locking on Enterprise Assets	Tripwire Enterprise can validate this configuration setting	V			
4.4	Implement and Manage a Firewall on Servers	Tripwire Enterprise can validate this configuration setting	V			
4.5	Implement and Manage a Firewall on End-User Devices	Tripwire Enterprise can validate this configuration setting	V			
4.6	Securely Manage Enterprise Assets and Software	Tripwire Enterprise can be the cornerstone of a secure configuration management process for enterprise assets and software. Tripwire State Analyzer can provide an extended means of evaluating lists of allowed objects, including software. Tripwire IP360 can be used to detect unmanaged or insecure systems and software.	P	P	P	
4.7	Manage Default Accounts on Enterprise Assets and Software	Tripwire Enterprise can be used to validate that default accounts are not configured. Tripwire State Analyzer can be used to identify default accounts in usage through an AllowedList. IP360 can identify default accounts in use through active assessment.	V	V	V	
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Tripwire Enterprise can be used to validate that unnecessary services are disabled. Tripwire State Analyzer can use an AllowedList to ensure that only allowed software and services are running, including assessing assets for open ports. Tripwire IP360 can identify unwanted services through active scanning.	V	V	V	
4.9	Configure Trusted DNS Servers on Enterprise Assets	Tripwire Enterprise can validate which DNS servers are configured on assets.	V			
4.10	Enforce Automatic Device Lockout on Portable End-User Devices	Tripwire Enterprise can validate this configuration setting	V			
4.11	Enforce Remote Wipe Capability on Portable End-User Devices	Tripwire Enterprise can validate this configuration setting	V			
4.12	Separate Enterprise Workspaces on Mobile End-User Devices					

Legend: P=Provides, S=Supports, V=Validates

CIS Control	Description	How Tripwire Can Help	Tripwire Enterprise	Tripwire State Analyzer	Tripwire IP360	Tripwire LogCenter
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.					
5.1	Establish and Maintain an Inventory of Accounts	Tripwire State Analyzer can be used to create an AllowedList of accounts and identify unauthorized accounts in use.		S		
5.2	Use Unique Passwords	Tripwire Enterprise can validate that unique passwords are required in configurations.	V			
5.3	Disable Dormant Accounts	Tripwire Enterprise can identify accounts that have been dormant for a specified period of time.	V			
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Tripwire Enterprise can validate that administrative privileges are not assigned to non-administrative accounts. Tripwire Log Center can identify suspicious login activity related to administrative actions.	V			S
5.5	Establish and Maintain an Inventory of Service Accounts	Tripwire State Analyzer can be used to create an AllowedList of accounts and identify unauthorized accounts in use.		V		
5.6	Centralize Account Management	Tripwire Enterprise and IP360 can be used to identify account management systems in use that are not authorized.	V		V	
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.					
6.1	Establish an Access Granting Process					
6.2	Establish an Access Revoking Process					
6.3	Require MFA for Externally-Exposed Applications	Tripwire Enterprise can validate the MFA is configured	V			
6.4	Require MFA for Remote Network Access	Tripwire Enterprise can validate the MFA is configured	V			
6.5	Require MFA for Administrative Access	Tripwire Enterprise can validate the MFA is configured	V			
6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems	Tripwire IP360 can be used to identify authentication and authorization systems in the environment.				S
6.7	Centralize Access Control	Tripwire Enterprise can validate which access control systems an asset is configured to use.	V			
6.8	Define and Maintain Role-Based Access Control	Tripwire Enterprise can support this requirement by identifying access control configurations	S			
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.					
7.1	Establish and Maintain a Vulnerability Management Process	Tripwire IP360 can be the cornerstone of a vulnerability management process.				P
7.2	Establish and Maintain a Remediation Process	Tripwire IP360 can validate the vulnerabilities have been remediated. It can also provide key data to support a risk-based approach to remediation.				V
7.3	Perform Automated Operating System Patch Management	Tripwire IP360 can validate the vulnerabilities have been remediated. It can also provide key data to support a risk-based approach to remediation.				V
7.4	Perform Automated Application Patch Management	Tripwire IP360 can validate the vulnerabilities have been remediated. It can also provide key data to support a risk-based approach to remediation.				V
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Tripwire IP360 can perform automated vulnerability scans				P
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Tripwire IP360 can perform automated vulnerability scans				P

Legend: P=Provides, S=Supports, V=Validates

CIS Control	Description	How Tripwire Can Help	Tripwire Enterprise	Tripwire State Analyzer	Tripwire IP360	Tripwire LogCenter
7.7	Remediate and Detect Vulnerabilities	Tripwire IP360 can validate the vulnerabilities have been remediated. It can also provide key data to support a risk-based approach to remediation.			V	
Control 8: Audit Log Management	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.					
8.1	Establish and Maintain an Audit Log Management Process	Tripwire LogCenter can be the cornerstone of your log management program				P
8.2	Collect Audit Logs	Tripwire LogCenter collects audit logs				P
8.3	Ensure Adequate Audit Log Storage	Tripwire LogCenter stores audit logs				P
8.4	Standardize Time Synchronization	Tripwire Enterprise can validate that assets are configured to use a time server.	V			
8.5	Collect Detailed Audit Logs	Tripwire Enterprise can validate that logging is configured. Tripwire LogCenter can receive these logs.	V			S
8.6	Collect DNS Query Audit Logs	Tripwire Enterprise can validate that logging is configured. Tripwire LogCenter can receive these logs.	V			S
8.7	Collect URL Request Audit Logs	Tripwire Enterprise can validate that logging is configured. Tripwire LogCenter can receive these logs.	V			S
8.8	Collect Command-Line Audit Logs	Tripwire Enterprise can validate that logging is configured. Tripwire LogCenter can receive these logs.	V			S
8.9	Centralize Audit Logs	Tripwire LogCenter can provide a centralized logging destination.				P
8.10	Retain Audit Logs	Tripwire LogCenter can retain logs				P
8.11	Conduct Audit Log Reviews	Tripwire LogCenter can facilitate the review of audit logs.				S
8.12	Collect Service Provider Logs	Tripwire LogCenter can receive these logs.				S
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.					
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Tripwire IP360 can check for browsers that have vulnerabilities. Tripwire Enterprise can validate browser configurations. Tripwire State Analyzer can be used to create an AllowedList of specific browsers and versions	V	V	V	
9.2	Use DNS Filtering Services	Tripwire Enterprise can validate the configuration of DNS filtering services	V			
9.3	Maintain and Enforce Network-Based URL Filters	Tripwire Enterprise can validate the configuration of network-based URL filters. Tripwire LogCenter can support this requirement by collecting relevant logs for review.	V			S
9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Tripwire Enterprise can validate the configuration of browsers and email clients. Tripwire LogCenter can support this requirement by collecting relevant logs for review.	V			S
9.5	Implement DMARC	Tripwire Enterprise can validate the configuration of DMARC. Tripwire LogCenter can support this requirement by collecting relevant logs.	V			S
9.6	Block Unnecessary File Types	Tripwire Enterprise can validate the configuration of email gateways. Tripwire LogCenter can support this requirement by collecting relevant logs for review.	V			S
9.7	Deploy and Maintain Email Server Anti-Malware Protections	Tripwire Enterprise can validate the configuration of email servers. Tripwire LogCenter can support this requirement by collecting relevant logs for review.	V			S

Legend: P=Provides, S=Supports, V=Validates

CIS Control	Description	How Tripwire Can Help	Tripwire Enterprise	Tripwire State Analyzer	Tripwire IP360	Tripwire LogCenter
Control 10: Malware Defenses	Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.					
10.1	Deploy and Maintain Anti-Malware Software	Tripwire Enterprise can validate that anti-malware tools are installed and configured correctly. Tripwire IP360 can detect whether anti-malware tools are installed.	V		V	
10.2	Configure Automatic Anti-Malware Signature Updates	Tripwire Enterprise can validate that anti-malware tools are installed and configured correctly.	V			
10.3	Disable Autorun and Autoplay for Removable Media	Tripwire Enterprise can validate that anti-malware tools are installed and configured correctly.	V			
10.4	Configure Automatic Anti-Malware Scanning of Removable Media	Tripwire Enterprise can validate that anti-malware tools are installed and configured correctly.	V			
10.5	Enable Anti-Exploitation Features	Tripwire Enterprise can validate that anti-malware tools are installed and configured correctly.	V			
10.6	Centrally Manage Anti-Malware Software					
10.7	Use Behavior-Based Anti-Malware Software					
Control 11: Data Recovery	Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.					
11.1	Establish and Maintain a Data Recovery Process					
11.2	Perform Automated Backups	Tripwire Enterprise can validate that automated backups are configured.	V			
11.3	Protect Recovery Data	Tripwire Enterprise can validate that controls are configured for recovery data.	V			
11.4	Establish and Maintain an Isolated Instance of Recovery Data					
11.5	Test Data Recovery					
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.					
12.1	Ensure Network Infrastructure is Up-to-Date	Tripwire State Analyzer can validate the software versions are part of an AllowedList. Tripwire IP360 can identify unsupported systems in the environment.		V	V	
12.2	Establish and Maintain a Secure Network Architecture					
12.3	Securely Manage Network Infrastructure	Tripwire Enterprise can validate that network infrastructure is configured appropriately. IP360 can identify versions and insecure protocols through active scanning.	V		V	
12.4	Establish and Maintain Architecture Diagram(s)					
12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)	Tripwire Enterprise can validate that network devices are configured to use the centralized AAA	V			
12.6	Use of Secure Network Management and Communication Protocols	Tripwire Enterprise can validate that systems are configured to use security protocols. IP360 can identify insecure protocols in use through active scanning.	V		V	
12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Tripwire Enterprise can validate that VPN systems are configured to use the centralized AAA	V			
12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Tripwire Enterprise can validate that these dedicated computing resources are appropriately segregated and configured.	V			
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.					
13.1	Centralize Security Event Alerting	Tripwire LogCenter can provide centralized log collection, event correlation and alerting.				P
13.2	Deploy a Host-Based Intrusion Detection Solution	Tripwire Enterprise can provide host-based intrusion capabilities.	P			
13.3	Deploy a Network Intrusion Detection Solution					

Legend: P=Provides, S=Supports, V=Validates

CIS Control	Description	How Tripwire Can Help	Tripwire Enterprise	Tripwire State Analyzer	Tripwire IP360	Tripwire LogCenter
13.4	Perform Traffic Filtering Between Network Segments	Tripwire Enterprise can validate access control configurations for network traffic filtering are in place.	V			
13.5	Manage Access Control for Remote Assets	Tripwire Enterprise can validate that assets are compliant with organizational configuration policies for connecting. IP360 can validate that assets meet vulnerability risk requirements.	V		V	
13.6	Collect Network Traffic Flow Logs	Tripwire LogCenter can collect and facilitate review of these logs.				P
13.7	Deploy a Host-Based Intrusion Prevention Solution	Tripwire Enterprise can validate that EDR or other endpoint solutions are installed, running and configured correctly.	V			
13.8	Deploy a Network Intrusion Prevention Solution	Tripwire Enterprise can validate that network based intrusion prevention systems are configured correctly.	V			
13.9	Deploy Port-Level Access Control	Tripwire Enterprise can validate that infrastructure is configured to use port-level access control.	V			
13.10	Perform Application Layer Filtering	Tripwire Enterprise can validate that application layer filtering is configured correctly.	V			
13.11	Tune Security Event Alerting Thresholds					
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.					
14.1	Establish and Maintain a Security Awareness Program					
14.2	Train Workforce Members to Recognize Social Engineering Attacks					
14.3	Train Workforce Members on Authentication Best Practices					
14.4	Train Workforce on Data Handling Best Practices					
14.5	Train Workforce Members on Causes of Unintentional Data Exposure					
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents					
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates					
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks					
14.9	Conduct Role-Specific Security Awareness and Skills Training					
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.					
15.1	Establish and Maintain an Inventory of Service Providers					
15.2	Establish and Maintain a Service Provider Management Policy					
15.3	Classify Service Providers					
15.4	Ensure Service Provider Contracts Include Security Requirements					
15.5	Assess Service Providers					
15.6	Monitor Service Providers					
15.7	Securely Decommission Service Providers					
Control 16: Applications 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.					
16.1	Establish and Maintain a Secure Application Development Process					
16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities					
16.3	Perform Root Cause Analysis on Security Vulnerabilities					
16.4	Establish and Manage an Inventory of Third-Party Software Components					
16.5	Use Up-to-Date and Trusted Third-Party Software Components					

Legend: P=Provides, S=Supports, V=Validates

CIS Control	Description	How Tripwire Can Help	Tripwire Enterprise	Tripwire State Analyzer	Tripwire IP360	Tripwire LogCenter
16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities					
16.7	Use Standard Hardening Configuration Templates for Application Infrastructure	Tripwire Enterprise can provide secure hardening templates and validate that system configurations comply with them.	P			
16.8	Separate Production and Non-Production Systems					
16.9	Train Developers in Application Security Concepts and Secure Coding					
16.1	Apply Secure Design Principles in Application Architectures					
16.11	Leverage Vetted Modules or Services for Application Security Components					
16.12	Implement Code-Level Security Checks					
16.13	Conduct Application Penetration Testing					
16.14	Conduct Threat Modeling					
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.					
17.1	Designate Personnel to Manage Incident Handling					
17.2	Establish and Maintain Contact Information for Reporting Security Incidents					
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents					
17.4	Establish and Maintain an Incident Response Process	Tripwire Enterprise and Tripwire LogCenter can provide important data to support incident response, including logs and changes from the environment.	S			S
17.5	Assign Key Roles and Responsibilities					
17.6	Define Mechanisms for Communicating During Incident Response					
17.7	Conduct Routine Incident Response Exercises					
17.8	Conduct Post-Incident Reviews					
17.9	Establish and Maintain Security Incident Thresholds					
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.					
18.1	Establish and Maintain a Penetration Testing Program					
18.2	Perform Periodic External Penetration Tests					
18.3	Remediate Penetration Test Findings					
18.4	Validate Security Measures					
18.5	Perform Periodic Internal Penetration Tests					

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.