FORTRA®

GUIDE (TRIPWIRE)

The Executive's Guide to the CIS Controls

Key Takeaways & Action Opportunities

Introduction

If you’re like most executives, you must feel completely inundated with the volumes of material made available to you about enterprise cybersecurity challenges and the serious consequences of cyberattacks on business and society. Indeed, every day there are more news articles, television reports, and government advisories about cyber risk consistent with the warnings we receive during briefings from our chief information security officers.

To combat this risk, executives understand that a combination of security solutions is required to provide adequate prevention and mitigation. These solutions include technical and architectural controls, but also compliance objectives as dictated by standardized frameworks. Because many frameworks have been published — such as the NIST Cybersecurity Framework, Payment Card Industry Data Security Standard (PCI DSS), and many others — this is also an area of dizzying complexity.

One such framework stands out in the context of practical cyber risk management — the Center for Internet Security’s CIS Controls. The seeds of the CIS Controls were sown in 2008 as a joint initiative within the US Federal Government, and were originally known as the Consensus Audit Guidelines.

A collection of highly practical controls, they were uniquely connected to the day-to-day issues of the working professional, rather than basing its selection criteria on academic or theoretical models. The collection was quickly lauded by enterprise security teams as including controls they felt were realistic, prioritized, cost effective, and practical. Later managed by the SANS Institute (where they were known as the Critical Security Controls and the SANS Top 20), they were transferred to the Center for Internet Security in 2015.

This **Executive’s Guide to the CIS Controls** is intended to provide busy readers with a comfortable, high-level understanding of the controls — without having to pour through pages of detailed documentation. It’s certainly not intended to be used as the basis for audit, but is rather intended to be enjoyed as a friendly introduction to an important standard in cybersecurity. Once an understanding of these controls is achieved, you will be better equipped to make management decisions with respect to enterprise cyber risk.

The Controls

Each of the CIS Controls is written as a declarative objective for an enterprise cybersecurity team. Each also matches some aspect of cyber risk management that has been agreed by consensus to reduce risk in a meaningful manner.

Taken collectively, the full set of controls provides either a prescriptive means for developing new policies and programs, or a complementary means for evaluating the completeness and effectiveness of existing ones.

The entries that follow introduce each control informally and provide illustrative examples, along with suggestions on how Fortra’s Tripwire solutions can help you implement or support the control.

Control 1

Inventory and Control of Enterprise Assets

Make Sure You Know What Devices You Have

This control makes perfect sense to any executive, because asset inventory is a foundational concept in all of business, especially finance — you can’t secure what you don’t know exists. This control differentiates between authorized and unauthorized devices in the inventory, and the importance of this distinction should resonate with executives.

How Tripwire Helps

Fortra’s Tripwire LogCenter® and Fortra’s vulnerability management solution provide the ability to actively and passively discover devices connected to your network. Active discovery not only identifies the host, but also collects application and operating system data. For passive discovery, Tripwire LogCenter mines logs data for previously unknown assets. Once identified, Tripwire Enterprise can collect and monitor configuration details about the asset.

Control 2

Inventory and Control of Software Assets

Make Sure You Know What Software You Have

Undertaking a software inventory sounds easier than it actually is. License agreements can be complex, and the ease with which software can be downloaded from the Internet makes a software inventory potentially tough. Controls 1 and 2 are recommended to be worked together.

How Tripwire Helps

During asset discovery, Fortra’s vulnerability management solution can inventory the software running on your assets, linking your hardware and software inventory. Tripwire Enterprise can also discover when new software is installed and can compare installed software against an allowlist, then alert you to the existence of unauthorized applications in your environment. Additionally, through integration with ITSM products, Tripwire Enterprise facilitates the removal of unauthorized software.

Control 3

Data Protection

Focus on Protecting Your Data

Every cybersecurity professional agrees that a major challenge in the industry involves keeping up with all the vulnerabilities identified in real time across the globe. Sadly, no shortcut exists to constantly maintaining vigilance around such vulnerabilities, and taking steps to mitigate relevant ones quickly.

How Tripwire Helps

Tripwire Enterprise can validate that data protection features are configured and enabled on systems.

Control 4

Secure Configuration of Enterprise Assets and Software

Configure Your Systems Properly

The systems in scope under this control include mobile devices, laptops, workstations, servers, and other devices. The reference to proper configuration focuses on security properties such as making certain that informed decisions are made to turn off unnecessary services and properly change defaults.

How Tripwire Helps

Tripwire Enterprise can compare a system's configuration against a secure image or template, then provide a detailed report on variances. It can also provide remediation instructions on how to bring the system in line with the secure image. If you do not have an internal security standard, Tripwire provides content based on several well-known hardening guides from CIS, ISO, and NIST. Furthermore, Tripwire Enterprise can be integrated with ITSM tools such as ServiceNow to integrate secure configuration management work items into your overall IT workflow.

Control 5

Account Management

Monitor and Control Your Accounts

The "account" is the most basic unit of control in all enterprise computing and networking environments. Despite this, too many security teams have weak or non-control of the accounts in their organization. By monitoring and controlling accounts, security teams make it much harder for malicious actors to successfully attack a company and steal or damage assets.

How Tripwire Helps

Tripwire Enterprise can monitor directory servers (e.g., Active Directory) to inventory accounts and monitor active and disabled accounts. Tripwire LogCenter can monitor, correlate and alert on unauthorized access activities.

Control 6

Access Control Management

Use Need-to-Know for Access

The concept of need-to-know access control is well established throughout government agencies. Other organizations should introduce similar concepts in access management, focusing on minimizing the number of individuals who have been granted access to information or resources. This approach is also known as "least privilege."

How Tripwire Helps

Tripwire Enterprise can not only detect who made changes, but can monitor permissions assignments for changes, ensuring that least privilege is maintained and changes that impact least privilege are addressed. Tripwire's allowlisting capabilities can be used to ensure that specific individuals are included in roles and groups.

Control 7

Continuous Vulnerability Management

Use Only Trusted Email Clients and Browsers

Every cybersecurity professional agrees that a major challenge in the industry involves keeping up with all the vulnerabilities identified in real time across the globe. Sadly, no shortcut exists to constantly maintaining vigilance around such vulnerabilities and quickly taking the steps to mitigate relevant ones.

How Tripwire Helps

Fortra offers a robust vulnerability scanning solution that provides valuable insight into the current status of all scanned systems to help prioritize which are most vulnerable to compromising the security of the network. Its patented vulnerability scoring system provides detailed prioritization that factors in the risk a vulnerability presents, the threat presented by the exploit, and the time elapsed since the vulnerability became publicly known. Reports can provide validation that vulnerabilities have been remediated in a timely manner.

Control 8

Audit Log Management

Pay Attention to Your Audit Logs

Most systems in the enterprise generate helpful log output that contains useful information about potential security attack indicators. Security teams must pay attention to these logs and use them in conjunction with tools that are designed to analyze log information and generate actionable management guidance.

How Tripwire Helps

Tripwire LogCenter can aggregate logs from multiple sources then correlate events of interest to detect anomalies, suspicious behaviors, changes and patterns known to be threats and indicators of compromise. Tripwire Enterprise can monitor to ensure logging is enabled and configured correctly, as well as detect when logging is disabled. Tripwire Enterprise and Tripwire LogCenter can work together to identify the log events associated with a change and to dynamically correlate log events across tagged systems.

Control 9

Email and Web Browser Protections

Use Only Trusted Browsers and Email Clients

Attackers frequently use web browsers and email clients as entry points for code exploitation and social engineering. These applications allow users to interact with outside systems and websites, and controls need to be implemented to protect against interactions with untrusted environments.

How Tripwire Helps

Fortra's vulnerability management solution can identify which applications (e.g., web browsers and email clients) and versions are present on a system. Tripwire Enterprise can identify and flag unauthorized applications or vulnerable versions present.

Control 10

Malware Defenses

Anti-virus Integration is Key

Install AV and keep it updated. This has been ingrained in IT professionals for decades. Because so many security tools can work together to orchestrate the response to a malware infection, it is important to make sure your agency's antivirus tools integrate well with the rest of your security toolchain.

How Tripwire Helps

Tripwire Enterprise helps protect against ransomware by enabling you to identify and correct weak security configurations that are often the entry point. You can configure Tripwire Enterprise custom policies to search for specific indicators of compromise associated with a particular attack type, enabling you to identify, isolate, and restore compromised systems before the ransomware is activated. It can also be used to validate that anti-malware is deployed, running, and correctly configured. Tripwire LogCenter can receive and centrally manage logs and events from anti-malware tools. These events can be correlated against a list of known malicious domains.

Control 11

Data Recovery

Make Sure You Can Recover Lost Data

Increasingly, hackers understand that data theft is only one dimension of a cyber offense — they have come to recognize the potential to tamper with the integrity of data and systems. Ransomware is a current hot-button example. As a result, organizations must have a strong plan for dealing with recovery of lost data should preventive controls fail.

How Tripwire Helps

Tripwire Enterprise can validate that systems are running backup software and are configured for regular backups.

Control 12

Network Infrastructure Management

Secure Your Network Devices

Network devices can be viewed as the gateways to your enterprise, whether physical or virtual. As such, proper administration and secure configuration of routers, switches, firewalls, and other network devices is essential to managing ingress and egress filtering rules for enterprise policy-based protection.

How Tripwire Helps

Tripwire Enterprise can maintain a standard security configuration and evaluate network devices against that configuration, as well as report on software versions. Fortra's vulnerability management solution is regularly updated with the latest vulnerability information and can scan network devices for those vulnerabilities.

Control 13

Network Monitoring and Defense

Disable Unnecessary Ports and Services

The establishment of security policy rules that prohibit unnecessary services is one of the oldest concepts in information security. Such minimization of services at the network level makes it harder for hackers with scanners to find open ports and listening services through which to gain entry to the enterprise.

How Tripwire Helps

Tripwire Enterprise with its allowlisting capabilities can assess the environment and create an up-to-date report of which network ports and services are open on each asset in the environment. In addition, Tripwire can compare current open ports and services to a known list of acceptable services.

Control 14

Security Awareness and Skills Training

Optimize the Security Skills of Your Staff

Optimize the security skills of your staff. The security capability of staff in an enterprise is one of the most neglected aspects of cybersecurity. Executives often take for granted how hard it is for experts to keep up with the latest issues in technology and threat. Employees must also maintain high levels of current awareness of best practices in cyber hygiene.

How Tripwire Helps

Tripwire products do not assist with this control. However, Fortra’s Terranova Security provides security awareness training that reduces risk and builds threat resilience.

Control 15

Service Provider Management

Confirm That Your Service Providers Are Secure

Most organizations entrust certain processes and functions to third-party service providers who frequently have access to sensitive data. Unfortunately, service providers have become an attack vector for cybercriminals, so managing the security of your organizations' service providers is now a necessity. And this isn't just for security's sake; many compliance standards, HIPAA and PCI for example, require compliance to cover third-party service providers.

How Tripwire Helps

While Tripwire does not play a role in the evaluation of third-party service providers, our solutions help service providers themselves prove alignment with security standards. Everyone is in *someone's* supply chain, and the ability to claim and demonstrate compliance with industry standards like CIS and NIST is a good way to ensure that you're protecting your customers.

Control 16

Application Software Security

Implement an Application Security Program

The most popular target for hackers is your application base, so it's essential to implement a comprehensive program of application security controls. This should include scanning, testing, and software development lifecycle (SDLC) controls to reduce the risk of malicious insertion of Trojans and other malware into code.

How Tripwire Helps

For acquired software, Fortra's vulnerability management solution can identify version info and identify vulnerabilities. It can also be used to identify any non-standard or insecure encryption in use. For applications that require a database, Tripwire Enterprise can ensure the database is configured securely. As development increasingly moves to containers and the cloud, Tripwire can ensure that development systems are configured securely and free from vulnerabilities.

Control 17

Incident Response Management

Have a Plan for Dealing with Incidents

Even if proper cybersecurity controls are deployed across a company, incidents will certainly occur. To deal with such events, companies must have well-defined incident response plans that can help recover assets, restore integrity and reconstitute resources that might have been hacked during the incident.

How Tripwire Helps

Tripwire products do not assist with this control.

Control 18

Penetration Testing

Test Your Network by Breaking In

While penetration testing is not a great method to demonstrate the complete absence of flaws, it is an excellent way to demonstrate the presence of bugs, misconfigurations, and other security problems. Therefore it's prudent to maintain an ongoing program of security and pen testing to demonstrate progress in security across the company.

How Tripwire Helps

Fortra's vulnerability scanner integrates with penetration testing tools such as Core Impact so they can be used in concert to make pen testing efforts more effective. Tripwire LogCenter can track and monitor usage of accounts used in pen tests to ensure they are not used after testing is complete. Fortra also offers pen testing services for organizations needing a third-party assessment.

Management Actions

Based on the summary above, it should be clear that the CIS Controls are different from other frameworks. The list is succinct and to the point. Each control is easy to understand, and is focused on real-world cybersecurity problems encountered in the field by active practitioners.

If you’re wondering about your next management steps, the Tripwire team recommends the following three specific actions.

☑ ACTION 1

Evangelize the CIS Controls

As an executive, you can set the proper tone in your organization by evangelizing the CIS Controls. Just by mentioning the Controls during discussions or meetings, perhaps by referring to specific controls that are meaningful to the subject at hand, a message is sent that they are to be taken seriously by the organization.

☑ ACTION 2

Demand Simplification of Your Compliance Program

Far too much time, effort, and money are wasted on the complexity of a massive compliance program focused on multiple frameworks with duplicative objectives. Be sure to emphasize to your team that control frameworks can and should be simple, and demand that your auditors justify any complexity being unnecessarily introduced into the process.

☑ ACTION 3

Call Tripwire to Learn How Many of the Controls Can be Easily Addressed

Tripwire can help your organization better understand how automation and world-class tools can help you cover large portions of the CIS Controls without great effort or expenditure, including through Tripwire ExpertOps$^{\text{SM}}$ managed services. Contact us to learn more!

Tripwire and the CIS Controls

CIS CONTROLS	Overall Tripwire Solution Support
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	◕

Though the list may seem daunting, simply getting started is the most important step. The CIS Controls apply to virtually every enterprise and Tripwire can help nearly every step of the way — contact us today!

> *The CIS Critical Security Controls are an example of the Pareto Principle at work: 80 percent of the impact comes from 20 percent of the effort. That truism also applies to the Controls themselves.*[1]
>
> —SANS Institute

Closing

This ***Executive's Guide to the CIS Controls*** is part of a series from Tripwire intended to assist managers, executives and C-suite teams in their understanding of cybersecurity. It was produced by the Tripwire team in conjunction with Ed Amoroso, founder and CEO of TAG Cyber and well-known expert on cybersecurity, who offered his guidance and suggestions.

Please contact info@fortra.com with any inquiries regarding this content.

Source

[1] SANS Institute, Back to Basics: Focus on the First Six CIS Critical Security Controls

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.

FORTRA®

Fortra.com

Copyright © Fortra, LLC and its group of companies. Fortra®, the Fortra® logos, and other identified marks are proprietary trademarks of Fortra, LLC.