The Executive's Guide to the CIS Controls

Key Takeaways & Action Opportunities

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Introduction

If you're like most executives, you must feel completely inundated with the volumes of material made available to you about the challenges of enterprise cybersecurity and the serious consequences of malicious hacking on business and society. Indeed, every day we are treated to a stream of news articles, television reports and government advisories about cyber risk that are 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 suitable prevention and mitigation. These solutions include technical and architectural controls, certainly, but also compliance objectives, as dictated by standardized frameworks. Because many different frameworks have been published (e.g., NIST Framework for Cyber Security, Payment Card Industry Data Security Standard (PCI DSS), and many more) 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 in the US federal government, and were original 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* is intended to provide busy readers with a comfortable, high-level understanding of these controls, without having to pour through pages of detailed documentation. It's certainly is 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, the executive 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 below introduce each control informally and provide illustrative examples, along with suggestions on how Tripwire solutions can help you implement or support the control.

CONTROL 1

Inventory and Control of Hardware Assets

Make Sure You Know What Devices You Have

This control makes perfect sense to any executive, because 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 executives should resonate with the importance of this distinction.

How Tripwire Helps

Tripwire® IP360™ and Tripwire Log Center® provide the ability to actively and passively discover devices connected to the organization's network. Active discovery not only identifies the host, but collects application and operating system data. For passive discovery, Tripwire Log Center 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

Understanding software inventory sounds easier than it is in actual practice. 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, Tripwire IP360 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 can facilitate the removal of unauthorized software.

CONTROL 3

Continuous Vulnerability Management

Check for and Fix Vulnerabilities Continually

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 IP360 is 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. Tripwire IP360's unique vulnerability scoring provides a robust prioritization mechanism that includes the risk a vulnerability presents, the threat of exploit, and the time elapsed since the vulnerability was publically known. Reports can provide validation that vulnerabilities have been remediated in a timely manner.

CONTROL 4

Controlled Use of Administrative Privileges

Manage Administrative Privileges Carefully

The control of administrative privileges should be obvious in its importance to enterprise security. Hackers will always target accounts with high privilege, so these privileges need to be inventoried and controlled using tools that monitor and manage all types of activity from these powerful system vantage points.

How Tripwire Helps

Tripwire Enterprise can monitor systems to ensure that administrative access and privileges are configured securely, and if those configurations change. It can also detect when users with administrative privileges are added or removed. Tripwire Enterprise policy content can be used to ensure systems are configured to prevent unauthorized users from executing malicious scripts and other malicious techniques. Tripwire Log Center can monitor logs and alert when administrative accounts are added or removed.

CONTROL 5

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Configure Your Systems Properly

The systems in scope with 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 good 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 like ServiceNow to integrate secure configuration management work items into your overall IT workflow.

CONTROL 6

Maintenance, Monitoring and Analysis of Audit Logs

Pay Attention to Your Audit Logs

Most systems in the enterprise generate useful 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 Log Center 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.

CONTROL 7

Email and Web Browser Protections

Use Only Trusted Email Clients and Browsers

Attackers commonly 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

Tripwire IP360 can identify which applications (i.e. web browsers and e-mail clients) and versions are present on a system. Tripwire Enterprise can identify and flag unauthorized applications or versions present.

CONTROL 8

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 can be used to validate that anti-malware is deployed, running and correctly configured. Tripwire File Analyzer works with Tripwire Enterprise to determine and report file and executable behaviors, which may be malicious. Tripwire Log Center can receive and centrally manage logs and event from anti-malware tools. These events can be correlated against a list of known malicious domains.

CONTROL 9

Limitation and Control of Network Ports, Protocols, and Services

Limit What's Allowed on Your Network

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, combined with either the Tripwire Whitelist Profiler app or Tripwire State Analyzer, can create an up-to-date report of which network ports and services are active on each asset in the environment. In addition, it can compare current open ports and services to a known list of acceptable services. Furthermore, they can scan the environment for unauthorized ports and services, either alone or in conjunction with Tripwire IP360.

CONTROL 10

Data Recovery Capabilities

Make Sure You Can Recover Lost Data

Increasingly, hackers understand that data theft is only one dimension of the cyber offensive equation. In addition, they have come to recognize the potential to tamper with the integrity of data and systems. Ransomware is an 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 11

Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

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. Tripwire IP360 is consistently updated with the latest vulnerability information and can scan network devices for those vulnerabilities.

CONTROL 12

Boundary Defense

Build a Multi-Layered Boundary Defense

Defense in depth is the preferred architectural paradigm for security engineers, especially with the evolution of the enterprise to hybrid cloud services. The old perimeter model has been supplanted by the view that boundary defenses can be created closer to both data and computing resources, such as in cloud environments.

How Tripwire Helps

Tripwire IP360 can be used to scan across network boundaries and identify unauthorized connections. Tripwire Enterprise can validate that systems are configured to record network traffic. Tripwire Log Center can receive and centrally manage logs from network boundary devices.

CONTROL 13

Data Protection

Focus on Protecting Your Data

Modern tools exist that can prevent or detect the leakage or loss of proprietary data. These tools include encryption-based technologies to maintain proper access to sensitive data. In addition, advanced data loss prevention tools examine behaviors to help determine if perhaps a disgruntled or malicious insider is leaking data.

How Tripwire Helps

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

CONTROL 14

Controlled Access Based on the Need to Know

Use Need-to-Know for Access

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

How Tripwire Helps

Tripwire Enterprise provides best-in-class File Integrity Monitoring capabilities to monitor changes in real-time, including who made the change. As opposed to audit-logging everything that happens on a system, Tripwire Enterprise can be used to limit the scope of what is monitored and send only relevant data to your SIEM, making monitoring for changes to sensitive files and data far more effective and efficient.

CONTROL 15

Wireless Access Control

Control Your Wireless Devices

The explosion of wireless and mobile devices in business is staggering, and executives should recognize that wireless access control, device authentication, inventory and access management are not only sensible, but are absolutely required to keep malicious actors from wreaking havoc on an enterprise.

How Tripwire Helps

Tripwire IP360 can discover wireless access points on the network. Tripwire Enterprise can audit configuration settings to ensure wireless access points are configured securely, and then monitor settings for changes.

CONTROL 16

Account Monitoring and Control

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 (like Active Directory) to inventory accounts and monitor active and disabled accounts. Tripwire Log Center can monitor, correlate and alert on unauthorized access activities.

CONTROL 17

Implement a Security Awareness and Training Program

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.

Tripwire products do not assist with this control

CONTROL 18

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, Tripwire IP360 can identify version info and identify vulnerabilities. Tripwire IP360 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.

CONTROL 19

Incident Response and 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 cases, 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.

Tripwire products do not assist with this control

CONTROL 20

Penetration Tests and Red Team Exercises

Test Your Network by Breaking In

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

How Tripwire Helps

Tripwire IP360 integrates with penetration testing tools so they can be used in concert to make penetration testing efforts more effective. Tripwire Log Center can track and monitor usage of accounts used in penetration tests to ensure they are not used after testing is complete. Tripwire also offers penetration testing through Professional Services.

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, leaving the reams of requirements detail to other compliance structures. Each of the controls is simple to understand, and focused on real-world cybersecurity problems that encountered in the field by practitioners.

If you're wondering about your next management steps—well, there are three specific actions the Tripwire team recommends…

☑ 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 referencing the existence of the Controls, perhaps referencing during discussions or meetings certain controls that are meaningful to you, 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—nearly all of the first six, and many more—of the CIS Controls without great effort or expenditure, including through Tripwire ExpertOps^{SM} managed services. Contact us!

Tripwire and the CIS Controls

	CIS CONTROL	Overall Tripwire Solution Support
Highest Impact Controls	Control 1: Inventory and Control of Hardware Assets	●
	Control 2: Inventory and Control of Software Assets	●
	Control 3: Continuous Vulnerability Management	●
	Control 4: Controlled Use of Administrative Privileges	◕
	Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	●
	Control 6: Maintenance, Monitoring and Analysis of Audit Logs	●
Foundational Controls	Control 7: Email and Web Browser Protections	◔
	Control 8: Malware Defenses	◑
	Control 9: Limitation and Control of Network Ports, Protocols, and Services	●
	Control 10: Data Recovery Capabilities	◔
	Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	●
	Control 12: Boundary Defense	◔
	Control 13: Data Protection	◔
	Control 14: Controlled Access Based on the Need to Know	◔
	Control 15: Wireless Access Control	◔
	Control 16: Account Monitoring and Control	◑
Organizational Controls	Control 17: Implement a Security Awareness and Training Program	○
	Control 18: Application Software Security	◑
	Control 19: Incident Response and Management	○
	Control 20: Penetration Tests and Red Team Exercises	◕

In their white paper **Back to Basics: Focus on the First Six CIS Critical Security Controls**, SANS states that the biggest security gains against the most common threat vectors can be simply and inexpensively achieved by implementing Controls 1–6.

Getting started is the most important step, and the CIS Controls apply to virtually every enterprise—Tripwire can help!

> *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.*
>
> —SANS, *Back to Basics: Focus on the First Six CIS Critical Security Controls*

Conclusion

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 sales@tripwire.com with any inquiries regarding this content.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

The State of Security: **News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook