WHITE PAPER

The New Center for Internet Security Controls

How Tripwire Solutions Align with CIS Controls v7

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The Center for Internet Security (CIS) maintains a procedural list of 20 cybersecurity best practices. The CIS Controls serve as the go-to cyber readiness rulebook for organizations and agencies across the world. The controls were first developed in 2008 by the U.S. government to help organizations achieve cyber integrity with a cost-effective, practical methodology. Before they were managed by CIS, they were managed by the SANS Institute and referred to as the SANS Top 20 and the Critical Security Controls.

CIS Controls v7

Basic 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 Configurations 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

The CIS Controls v7

The 20 CIS Controls are listed in order of priority. It's recommended that you start with the first six to establish basic security hygiene. Then you can work your way through the foundational and organizational controls' action items to optimize your security posture one step at a time.

Each control contains several subsections detailing specific benchmarks. The controls employ the Pareto Principle, also known as the 80/20 principle—the assertion that 80 percent of effects result from 20 percent of causes in most systems. To give you an idea of how this works within the CIS Controls, one agency prevented 85 percent of targeted cyber intrusions using the first four controls alone[1].

The controls are updated regularly to reflect new advances in cybersecurity as well as trends and changes in the threat landscape. As of March 2018, the CIS Controls are now in their seventh iteration. Version seven incorporates two high-level updates:

New categories: The controls are now broken into three categories: basic, foundational and organizational. The first six basic controls are strongly recommended for all organizations and agencies as a bare minimum strategy. The foundational controls (7–16) build on those essentials with recommendations that offer clear security benefits. Organizational controls (17–20) focus on people and processes, and refine the security posture established by implementing the basic and foundational controls.

Structural changes: The latest version refines several sub controls to make them easier to enact and measure, communicating only one requirement per subcontrol for increased comprehension and clarity.

Most organizations and agencies must take a pragmatic approach to align themselves with the controls. Attempting to match the requirements of all 20 at once is generally cost-prohibitive, which is why it's smart to start with the basics and build from there. However, it should be in your security team's strategy to comply with all 20 controls as soon as possible to ensure the best cyber integrity you can.

Let's take a look at each of the controls, along with the key takeaways you'll want to remember for each. We'll also cover the ways Tripwire solutions do the heavy lifting for you in implementing each of the controls.

Control 1: Inventory and Control of Hardware Assets

There's no way to secure your network without an accurate view of what devices connect to it—especially in modern-day BYOD environments. Tripwire® IP360™ and Tripwire Log Center® let you actively and passively discover hardware devices connected to your network.

Active discovery not only identifies hosts, but collects application and operating system data as well. For passive discovery, Tripwire Log Center mines log data for previously unknown assets. Once identified, Tripwire Enterprise can collect and monitor configuration details about the previously unknown assets.

Key takeaways:

» **Avoid manual inventorying:** You may be tempted to use a spreadsheet to keep track of your hardware assets. In addition to being inefficient and unscalable, manual inventorying can miss new or occasionally-connected devices—ostensibly creating a blindspot your cyber adversaries can take advantage of.

» **Use standardized data formats:** Unfortunately, other controls list out standardized data formats such as SCAP. As you begin scanning and gathering data, use common data formats that more complex tools utilize so you don't need to lose valuable data when deploying new tools.

Control 2: Inventory and Control of Software Assets

During asset discovery, Tripwire IP360 catalogs the software running on your assets, linking your hardware and software inventories. Tripwire Enterprise also discovers new software when it's installed and can compare it against a whitelist, alerting you to the existence of unauthorized applications in your environment. Through integration with ITSM products, Tripwire Enterprise can facilitate the removal of unauthorized software.

Key takeaways:

» **Merge the first two controls:** Only attempt to scan hardware that is already in your asset database. If a system isn't in the asset database, revisit Control 1 to figure out why. Treat these first two controls as one when you're looking at how to implement them efficiently.

» **Focus on file integrity monitoring:** Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems. Use file integrity monitoring (FIM), such as available in Tripwire Enterprise, to scan the environment for new software. Let automated tools like these be the driver for populating your inventory databases.

> The CIS Controls are a free cybersecurity best practices resource for any organization to download and implement. They provide clear, prioritized guidance to help organizations tackle the most pervasive cybersecurity threats[3].
>
> — Center for Internet Security, 2018

Control 3: Continuous Vulnerability Management

A robust vulnerability management (VM) program powered by the correct tools will empower your organization to take control of its own security and manage risks presented by both internal and external threats. Tripwire IP360 is a powerful 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 unique vulnerability scoring provides a 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.

Key takeaways:

» **Run regular scans:** Utilizing remote and credentialed scans gives you a holistic view of your network that allows you to better understand threats before they become a problem. When you review and compare your results, you will quickly know what has changed and what risks those changes introduce.

» **Use risk scoring:** VM programs like Tripwire IP360 expose a plethora of faults and flaws in even the most secure networks. Don't be alarmed; simply apply risk-ratings and break the work into smaller, more manageable portions.

Control 4: Controlled Use of Administrative Privileges

Phishing and other common cyberattacks take advantage of poorly-controlled admin privileges. Tripwire Enterprise monitors systems to ensure that administrative access and privileges are configured securely, and if those configurations ever 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.

Key takeaways:

» **Take credentials seriously:** Attackers would love to get their hands on your admin credentials—Control 4 is in the top six for that very reason. Administrative credentials are as valuable as the data you're trying to protect. Provide the level of care with those as you would with your organization's most sensitive data.

» **Adopt multi-factor authentication:** There is guidance on enabling multi-factor authentication (MFA) for administrative users, but why not all users? And not just when accessing the VPN, but all the time. This may

initially be a cost or resource issue, but most organizations and agencies are well overdue for making this a requirement.

Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

The default configurations on your endpoints are likely geared toward ease of use, not security. Tripwire Enterprise can compare your configurations against a secure image or template and 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. Additionally, Tripwire Enterprise can integrate with ITSM tools like ServiceNow to bring security configuration management (SCM) work items into your overall IT workflow.

Key takeaways:

» **Assume your configurations need attention:** Some vendors recommend configuration guidelines in terms of performance and security. Most software and operating systems are configured in an open and insecure state, so use external sources such as CIS hardening guides and DISA STIGs for essential guidance.

» **Prepare for incidents:** Control 5 will be tightly coupled with Control 19. A configuration change can lead to a configuration vulnerability, which can lead to a breach. Make sure SCM resources are part of your incident response program when you begin implementing Control 19.

Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Logs are the lifeblood of cybersecurity. Tripwire Log Center aggregates logs from multiple sources. It then correlates events of interest to detect anomalies, suspicious behaviors, changes and patterns known to be threats or indicators of compromise. Tripwire Enterprise monitors to ensure logging is enabled and configured correctly, and detects when logging is disabled.

Key takeaways:

» **Know where to look:** The theft of data often mirrors physical theft in terms of where disruption takes place. A bank robber is going to break many laws and create disruption at the bank, but they'll likely obey as many laws as possible fleeing the scene. Likewise, a digital attacker may disrupt an endpoint while leaving little trace on the network, or vice-versa. You need to collect logs from as many systems as possible to get an accurate picture of what's taking place.

» **Establish consistent time and naming conventions:** Time consistency issues make it harder to correlate events. Coordinating with UTC so you can track an event across the globe is essential. You'll also need to make sure metadata is named identically across all logs. For example, you don't want to have to search for ip, ipv4 and ipv4 to look for the same thing.

Control 7: Email and Web Browser Protections

Cyber adversaries try to manipulate human behavior through email and browser interaction. Tripwire IP360 can identify which applications (including web browsers and email clients) and versions are present on a system. Tripwire Enterprise can then identify and flag unauthorized applications or versions.

Key takeaways:

» **Block email images:** Embedded single pixel tracking images are a way for attackers to gain information into employee activity. Malicious images embedded or loaded from external sites can also be an attack vector. Consider disabling auto-loading images in emails and requiring users to click a button to see the fancy graphics.

» **Leverage hardening benchmarks:** The CIS has hardening guidelines for Microsoft Exchange and Office, although leveraging those isn't called out explicitly in Control 7. Even though software is covered under Control 5, be aware that CIS and DISA offer hardening templates for both Exchange and Office.

Control 8: Malware Defenses

In order to keep up with the creative ways malware aims to override defenses, your cybersecurity solution must employ around-the-clock monitoring of anti-malware. Tripwire Enterprise can be used to validate that anti-malware is deployed, running and correctly configured. Tripwire Log Center can receive and centrally manage logs and events from anti-malware tools. These events can then be correlated against a list of known malicious domains.

Key takeaways:

» **Return to the basics:** Install anti-malware and update it regularly. This has been ingrained in IT professionals minds' for decades. Make sure the anti-malware solution meets the needs of your organization.

» **Integrate your security tools:** Many security tools can work together to orchestrate the response to a malware infection. While an anti-malware product can quarantine and delete an infected file, integrating with change management and other SCM tools may be able to remediate an entire system back to a clean state.

Control 9: Limitation and Control of Network Ports, Protocols and Services

Poor default configurations on endpoints make for easy cyberattack targets. Tripwire Enterprise combined with Tripwire Whitelist Profiler can create an up-to-date report of which network ports and services are active on each asset in the environment. It can compare current open ports and services to a known list of acceptable services. Furthermore, either alone or in conjunction with Tripwire IP360,

Tripwire Whitelist Profiler can scan the environment for unauthorized ports and services.

Key takeaways:

» **Reduce your attack surface:** The focus of Control 9 is about limiting the external attack surface of a system. This is always the first step in securing an endpoint.

» **Look at business needs:** Network ports, protocols and services are often open and available by default, serving no explicit purpose and leaving your systems more vulnerable to attacks. Automated scans can help you find these vulnerabilities so you can determine whether or not they fulfill an actual business need.

Control 10: Data Recovery Capabilities

There are numerous reasons why you want to perform backups. Historically, availability is the goal that drove this control. Now that ransomware is prevalent across many industries, this can be a driver to show additional ROI for backup solutions. Tripwire Enterprise can validate that systems are running backup software and are correctly configured for regular backups.

Key takeaways:

» **Establish regular backups:** After getting hit with ransomware, some companies have ponied up millions in ransom. While a Fortune 500 company may be able to take that type of hit, the vast majority cannot. The importance of testing data backups is just as critical as actually creating the backups. This doesn't have to be a complex procedure; a sample file on a non-critical server can be quickly tested in a matter of minutes.

» **Define "regular":** What does testing on "a regular basis" mean to your organization or agency? This is a great question when it comes to how often you need to run a full, incremental or differential backup. The CIS recommends that backups be administered at least weekly.

Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

Misconfigured assets are an open door for attackers, and SCM minimizes these vulnerabilities. Tripwire Enterprise helps you 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.

Key takeaways:

» **Leverage existing controls:** If you already implemented Control 5 to monitor the configuration and change on your endpoints, then you probably already have the tools and expertise needed to address Control 11. Increase the efficiency of your security strategy by identifying solution overlap.

» **Treat network devices like computers:** These controls match exactly what you would do for any other computer in the enterprise. Don't forget to give them attention as well.

Control 12: Boundary Defense

According to the CIS, "Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts[2]."

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, and Tripwire Log Center can receive and centrally manage logs from network boundary devices.

Key takeaways:

» **Quick and powerful wins:** Use tools at your disposal to quickly address network scanning and logging requirements. For even greater impact, implement boundary decryption (such as SSL) to raise your awareness, as well as multi-factor authentication to reduce your attack surface.

» **Use premium feeds:** There are recommendations for threat intelligence as well as IDS/IPS signature-based tools throughout Control 12. A paid-for and/or curated feed is highly recommended. You'll generally get what you pay for when it comes to using free versus premium feeds.

Control 13: Data Protection

By collecting audit logs across devices, you can achieve some level of insight into data exfiltration of sensitive data with existing tools. Tag assets that store sensitive data and closely monitor them. Leverage baselines for both network and file data so anything suspicious can quickly be flagged. Tripwire Enterprise can validate that data protection features are configured and enabled on systems.

Key takeaways:

» **Rely on hardening standards:** Both CIS and DISA have hardening guidelines for mobile devices. These guidelines have recommendations on encrypting the drive as well as locking down USB access.

» **Take a process-oriented approach:** Some of these recommendations, such as blocking access to cloud storage providers, can be considered quick wins. Others, such as creating an inventory of sensitive information, can be a never-ending process. This is one of the more difficult controls to fully implement—and for good reason. Protecting data is the primary goal of everyone in information security.

Control 14: Controlled Access Based on the Need to Know

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. Tripwire Enterprise provides best-in-class FIM capabilities to monitor changes in real-time, including information on who made the change.

Key takeaways:

» **FIM is about more than files:** In the latest version of the Controls, FIM only appears explicitly in section 14.9. However, FIM is a key capability across a number of the controls from beginning to end. Utilizing FIM should be considered an essential control for most organizations.

» **Automation and integration:** Automating security tasks is usually going to be a force multiplier for your security staff. While not directly touched on, integrating tools is going to be another area to amplify the workforce. By bolting together technologies, you'll obtain greater visibility into the network.

Control 15: Wireless Access Control

Creating a baseline is the starting point in securing any part of the enterprise network. You can then configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network. Tripwire IP360 discovers wireless access points on the network. Tripwire Enterprise audits configuration settings to ensure wireless access points are configured securely, and then monitors settings for changes.

Key takeaways:

» **Reduce your attack surface:** Much of Control 15 is about limiting the use of wireless technologies. Where you are using wireless, utilize best practices with encryption to prevent successful attacks on wireless data.

	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	

Tripwire solutions support nearly every CIS Control, including nearly complete support for the six highest-impact Basic controls.

» **Use efficient tools:** Using a vulnerability scanner or wireless intrusion detection system for detecting rogue access points is often overkill. If you already have a scanning tool at your disposal, reuse it without having to use more budget.

Control 16: Account Monitoring and Control

Camouflaging as a legitimate user account is a popular tactic among cybercriminals. 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.

Key takeaways:

» **Don't forget the logs:** Enabling a lot of the later sections of this control will require gathering logging data from endpoints into a centralized location, such as a SIEM. The security intelligence of the organization will be in your logs, so collect as much as you can without overburdening the tool or necessitating that analysts review the logs.

» **Block common attacks:** Many common attacks that have been made public hit on a lot of the requirements in Control 16. While a zero-day attack gets all of the press at security conferences, attackers are after valid credentials to make their attacks stealthier. Controlling authentication mechanisms and valid accounts is a cornerstone of building a proper security architecture.

Control 17: Implement a Security Awareness and Training Program

It's not just your security team that needs to understand the best practices laid forth by the CIS and other cybersecurity experts. Employees across the entire organization or agency must also gain a basic understanding of what they can do in their everyday roles to deter cyberattacks.

Key takeaways:

» **Be inclusive:** From system engineers to end users who are susceptible to social engineering, be as broad as possible in who you include in your security hygiene trainings.

» **Outsourcing continues to be ideal:** Security teams are already understaffed, underfunded and overworked. Establishing an awareness training program from scratch will be a time-consuming process that may be better suited for a third-party to develop and deliver.

Control 18: Application Software Security

Keeping tabs on the software used within your agency or organization is an ongoing process. Using the newest versions is paramount, as you may be missing out on necessary patches otherwise. 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.

Key takeaways:

» **Understand your risk:** The first great addition to Control 18 is the requirement to run both static and dynamic code analysis utilities on in-house developed code. The second is creating the ability for vulnerabilities to be reported to the company, especially from outside parties. Both of these are going to uncover vulnerabilities to the business which previously may have remained hidden for long periods of time.

» **Layer security strategies:** This is iterated over and over again in Control 18. Start by training developers how to write secure code, testing the code they write, hardening the environment around the code, then installing security tools in front of the code. The goal is to have multiple security layers to stop an attack long before it succeeds.

A Cybersecurity Ventures report found the global costs of ransomware exceeded $5 billion in 2017—a 15 percent increase in just two years. The report estimates ransomware attacks will grow by 350 percent annually[4].

Control 19: Incident Response and Management

Do you have a detailed action plan in place for handling cybersecurity incidents? Your plan should include the exact steps you'll take to remove the intruder from your system, quarantine the damage and return to a secure baseline. The CIS calls this type of plan an "incident response infrastructure."

Key takeaways:

» **Plan and Test:** One core component of Control 19 is to make sure you plan and test for an event before it happens. As with any emergency, you don't want to be figuring things out in the heat of the moment.

» **Define roles:** Make sure your incident response infrastructure results in written records of any incidents, as well as clearly defined organizational roles and responsibilities. The National Institute of Standards and Technology (NIST) provides a framework you can use for reference.

Control 20: Penetration Tests and Red Team Exercises

Red team exercises and penetration tests are an excellent way to gain deeper insight into system vulnerabilities from an attacker's point of view. Tripwire IP360 integrates with penetration testing tools to make testing efforts more effective. Tripwire Log Center can track and monitor accounts used in penetration tests to ensure they're not used after testing is complete.

Key takeaways:

» **Rely on the previous controls:** Control 20 leverages sections of the earlier Controls. Understanding your attack

surface from Controls 1 and 2 can help scope sections 1–3 of Control 20. Control 3 is going to define your vulnerability management toolset, which can be utilized across most of the sections in this control. The findings from your red team exercises are going to help mature your coverage in every previous control.

» **Test for a diverse range of attacks:** If you're just beginning, don't try to tackle the full blend of attacks at once. Start with something you may have expertise in or a critical finding from a vulnerability scan. Over time, you can get to having the full blend of attacks in your arsenal, such as wireless, client-based and web application attacks.

Summary

The CIS Controls offer a straightforward path to cyber integrity in a prioritized fashion. Trying to implement each of these controls manually or ad-hoc rather than holistically is generally unrealistic from both a budgetary and organizational perspective. Tripwire solutions like Tripwire Enterprise, Tripwire IP360 and others provide the built-in security procedures and workflows you need in order to meet the majority of the CIS Controls.

References

1 https://www.sans.org/reading-room/whitepapers/analyst/basics-focus-first-cis-critical-security-controls-37537

2 https://www.cisecurity.org/controls/boundary-defense/

3 https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/

4 https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc

WPNCISC1a 1806