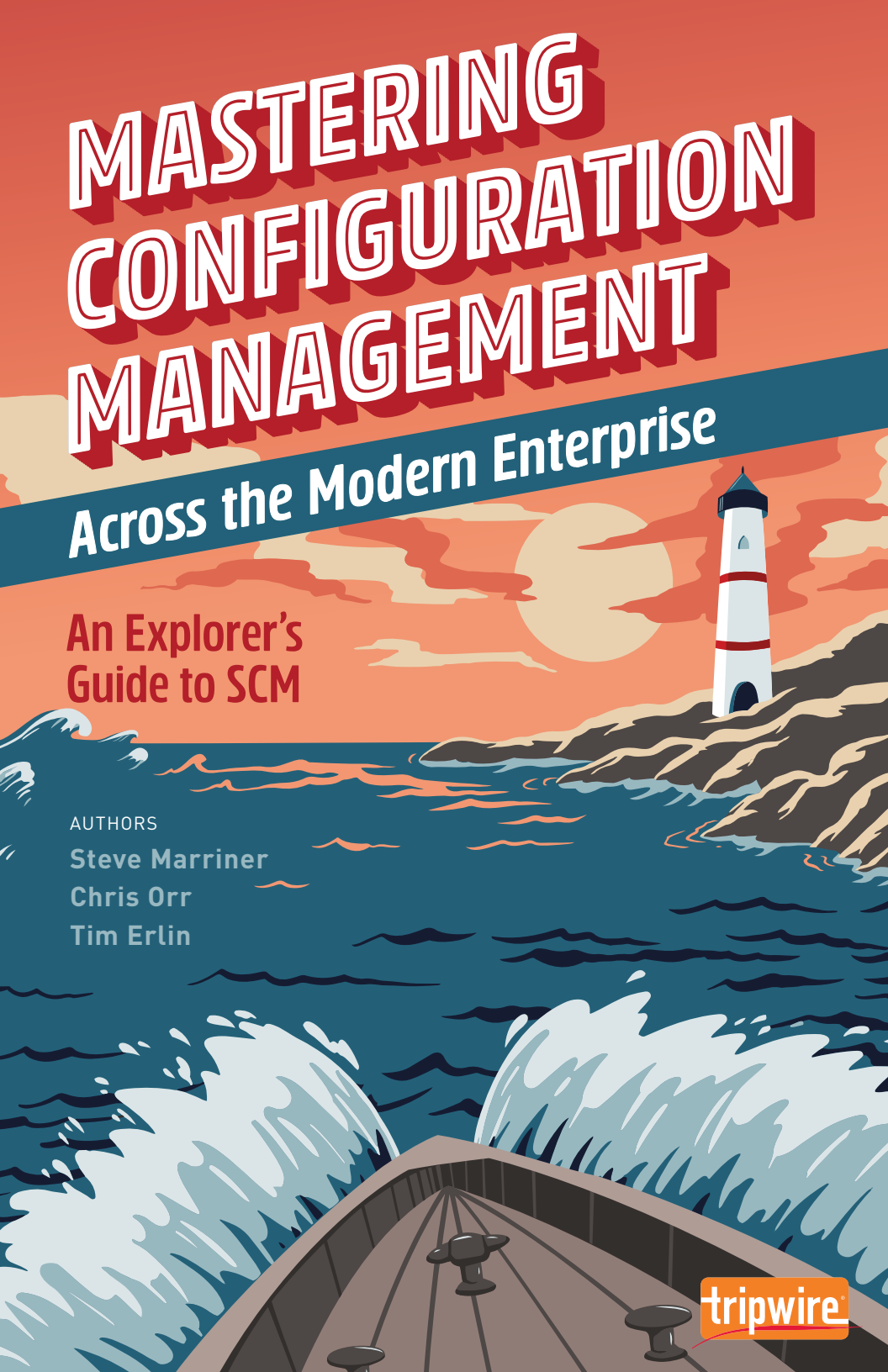
MASTERING CONFIGURATION MANAGEMENT

Across the Modern Enterprise

An Explorer's Guide to SCM

AUTHORS
Steve Marriner
Chris Orr
Tim Erlin



tripwire

TABLE of CONTENTS

INTRODUCTION

Security configuration management (SCM) isn't the newest technology for protecting your organization from cyberattacks, but it's absolutely one of the most important. In an industry where cybercriminals invent new methods every day to penetrate the defenses of modern enterprises, basic security controls like SCM still offer your best chance of preventing, detecting and remediating potential breaches and staying compliant.

In this book, we'll start with the basics of SCM to help you make sure your security program is solid and seaworthy—and why it matters so much in the first place. We'll cover the differences between SCM and other security controls to use alongside it. Then we'll map out the challenges modern enterprises face, such as the skills gap, expanding cloud infrastructures, and industrial environments.

We'll explore what successful SCM looks like in practice with an overview of system baselining, configuration monitoring, policy libraries, and utilizing compliance frameworks for smoother sailing in your next audit. We'll also dive into what you should look for in an SCM solution and explore a few advanced topics to help you make sure SCM is being implemented correctly for your specific environment.

TESTING THE WATERS

Configuration Management 101

Security Configuration Management is the cybersecurity practice of making sure your systems are properly configured to meet security and compliance standards, reducing cyber risk in the process. When a system is configured securely, we say it is "hardened" against cyberattacks. Another term you may come across is "attack surface," meaning the areas of a system that are exposed to attack; SCM is designed to shrink your attack surface.

This process of detecting and remediating misconfigurations combines elements of integrity monitoring, configuration validation, vulnerability assessment and system remediation. It spans on-premise and cloud configurations and requires participation from both security and operations teams. SCM isn't something you can implement in a day, but it will serve as a critical component of your systems' defenses for the long haul.

Without SCM in place, organizations are more likely to suffer security oversights such as weak passwords or utilizing protocols like Telnet or TFTP (trivial file transfer protocol) that can put sensitive data within cybercriminals' reach. SCM can provide two critical types of benefits to an organization: security and compliance.

WHAT IS SCM?

The National Institute of Standards and Technology (NIST) defines security configuration management as "The management and control of configurations for an information system to enable security and facilitate the management of risk."[1]

SCM FOR SECURITY

Misconfigurations create entry points for hackers. This is why properly configured systems are so critical for reducing the chance of a breach.

Before you can identify new misconfigurations, you must define what a secure configuration baseline looks like. Then deviations from this known baseline will result in test failures in your assessment process, and you can continuously test your current state against it.

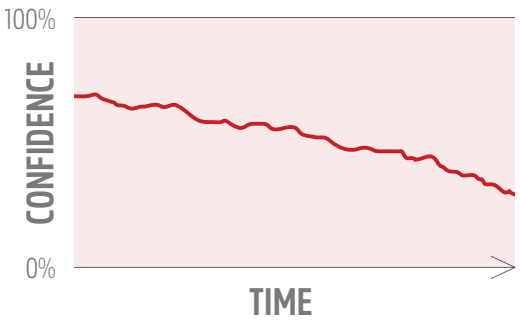
Organizations should define acceptable secure configurations as baselines for each type of managed device. Once you know that your systems are configured securely, SCM becomes about continuously monitoring those configurations for dangerous drifts from the secure and compliant state.

By setting a gold standard configuration for your systems and continuously monitoring for indicators of compromise, you can quickly identify a breach that would otherwise go unnoticed on your systems. Detecting breaches early is key to mitigating the damage of an attack.

SCM FOR COMPLIANCE

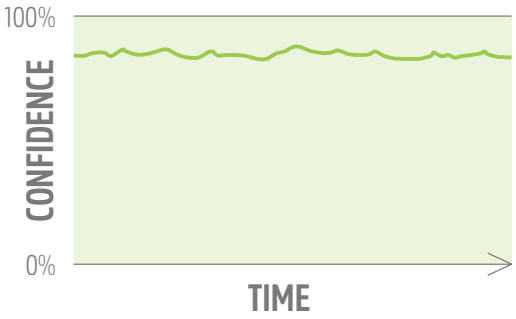
Configuration security is so crucial that almost all industry standards and regulations incorporate some version of an SCM mandate for specifying how configurations should be set up. SCM tools help you substantially reduce the time it takes to prepare for an audit, and speed up the actual audit process as well.

SCM is also about helping you continuously maintain a compliant system state post-audit. It's not enough to know that you were aligned with your compliance mandates under the scrutiny of an auditor. The goal should be having the ability to know your exact compliance level at any point in time—audit or not.



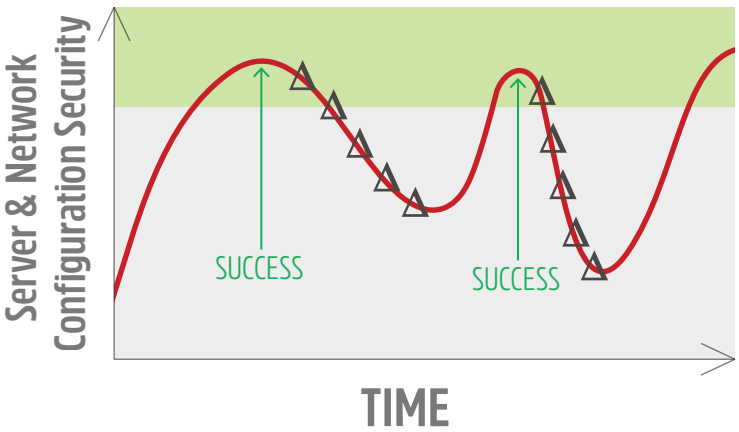
When new assets are deployed and hardened, the confidence in the functionality of those assets is usually high. But as users and administrators interact with it—as software and operating systems are upgraded, and settings are changed—that confidence degrades over time.

The continuous monitoring provided by an SCM solution, however, tracks these changes as they're made. That means you can immediately see when changes take your organization out of compliance and then take steps to remediate back to your baseline state. That way, you can maintain a consistently higher level of confidence in those assets over time.



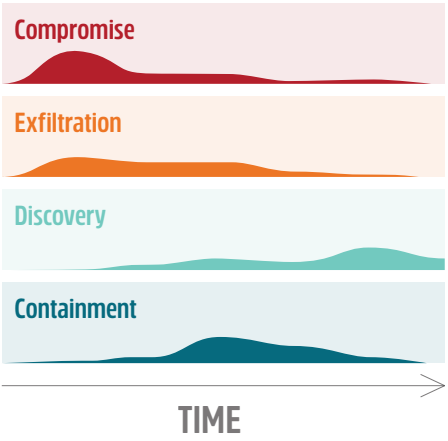
Without an SCM solution in place, the amount of time it takes to prepare for an audit can be extensive and expensive. Once you pass the audit, one common pitfall is that all of the pent-up work held back leading up to the audit is unleashed—meaning the secure baseline state is lost until the organization starts preparing for the next audit all over again. Your organization faces increasing risk the longer you allow your environment to drift out of compliance.

SCM can serve to enforce general or industry-specific hardening framework like CIS, NIST and ISO 27001 as well as compliance standards enforced by audits—such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX) or Health Insurance Portability and Accountability Act (HIPAA), depending on your industry's regulations.



ACT ON MISCONFIGURATIONS BEFORE HACKERS DO

It can only take a few minutes for a system to be compromised, but many organizations still take days, months or longer to realize an intruder has accessed their data and start to take corrective action. Verizon's annual *Data Breach Investigations Report*[2] reaffirmed the continuation of this unfortunate trend that has plagued organizations across the globe for years.



The time between a bad actor compromising a system and exfiltrating sensitive data—versus that breach being discovered and contained—is one of the key ways SCM works to your advantage. When you are instantly notified of misconfigurations that leave you vulnerable to attack, you can take proactive action to close the gap.

But don't take our word for it. Cybersecurity organizations like the Center for Internet Security (CIS) advise modern enterprises to implement SCM as one of the very first foundational security steps they take.

"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, 2020

THE TOP CIS CONTROLS

The 20 CIS Controls are listed in order of priority, and it's recommended that you start with the first six to establish a basic cybersecurity program for your organization. You can then work your way through the remainder of the controls to optimize your security posture one step at a time. SCM is so fundamental that it's listed fifth in the CIS Controls.

1 Inventory and Control of Hardware Assets

This control is paramount given the scale of the modern enterprise—without proper hardware management, it's impossible to know what's on your network to begin with.

2 Inventory and Control of Software Assets

This goes beyond operating systems, covering a range of software assets like embedded code, applications and services.

3 Continuous Vulnerability Management

Vulnerability scanning, while a critical part of your security program, doesn't replace the need for SCM. It does, however, help you identify and prioritize vulnerability risks.

4 Controlled Use of Administrative Privileges

A major part of an effective cybersecurity program is simply controlling who has access to what, such as credit card information or personally identifiable information (PII).

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

This is the main control around SCM. Once your system is configured as you need it using SCM, it must be maintained with the help of other processes like file integrity monitoring (FIM) to ensure that unauthorized changes aren't being made to files and other related assets.

> ***TRIPWIRE TIP:*** Before you can execute SCM effectively, you need to have a basic understanding of your environment. You gain this knowledge by implementing the first four CIS Controls: Inventory your hardware and software assets, deploy vulnerability management (VM), and control administrative privileges. You have to know what you have before you can make sure it's configured correctly and not vulnerable.

SMOOTH SAILING WITH COORDINATED PROCESSES

SCM isn't meant to be used alone: A strong SCM program is one that's tightly integrated with other core cybersecurity processes. By sharing data among your tools, you can create a more holistic picture of your exposure and the potential impact of a specific misconfiguration or system change.

Enterprise Integrity

Another way of thinking about security is to focus on the processes and controls needed to maintain integrity. True integrity means not allowing any variance from a current or expected state. Changes often occur, and can be internal or external, authorized or unauthorized, intentional or accidental, benign or malicious—all could potentially affect the integrity of the system. Managing integrity is at the core of foundational security.

Integrity is also at the heart of the "CIA Triad." The CIA Triad is a widely used information security model that provides organizations a framework to make sound information security policies. The CIA Triad refers to confidentiality, integrity and availability. Integrity is a necessary precondition and essential element for enabling confidentiality and availability.

The concept of integrity is indispensable when it comes to creating a cybersecurity program that protects the entire enterprise. You can use integrity as your organizing principle in setting goals for your systems, network, and data in order to align diverse types of environments under one well-coordinated program.

When viewed in this broader context, integrity emerges as a way to understand what matters to an organization and what to focus on to prevent undesired consequences. As the basis for trust and reliability, integrity becomes the ultimate measure of enterprise security. SCM is a core component of validating the integrity of your infrastructure—but is most effective when paired with robust change management processes. And FIM is a key component of successful change management.

The Importance of File Integrity Monitoring

To detect breaches early, you first need to first detect the changes that make them possible. You must consistently determine which changes are bad from a security or compliance standpoint. FIM goes hand-in-hand with SCM to quickly detect and assess the impact of all suspicious change events.

WHAT IS FIM?

FIM is the security process that monitors and detects changes in your environment to alert you to cybersecurity threats and helps you remediate them. FIM data is the engine that drives SCM success—you can't have one working optimally without the other.

Whereas SCM focuses specifically on assessing whether the current configuration is consistent with a predefined policy or expected state, FIM detects changes to files and system attributes that deviate from their prior baseline, including changes to servers, network devices, databases, virtual images, cloud service accounts, and more.

Two additional security processes that are often implemented to complement an SCM program are VM and Log Management (LM).

Vulnerability Management and SCM

An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. It is different from a misconfiguration, though both can lead to making your environment more vulnerable.

Vulnerability Management is the process of scanning networks for known vulnerabilities (often referring to a list of CVEs, or common vulnerabilities and exposures), then prioritizing and remediating those vulnerabilities in order based on risk severity. Tools that can display combined SCM and VM data can give you a more holistic picture of your environment and help you prioritize remediation efforts based on their potential impact.

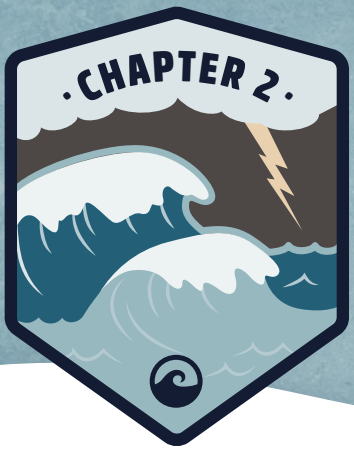
WHAT MAKES A FIM TOOL SEAWORTHY?

There are plenty of FIM solutions in the sea, and their capabilities vary quite a bit. FIM tools that don't help you differentiate expected from unexpected changes lead to excess "noise" that actually distracts security teams from important risks. An advanced FIM solution gives you the context around each change—like who made the change and when—along with tools that differentiate between good and bad changes. Other capabilities that make for successful FIM are real-time change detection and automated reconciliation of bad changes.

Log Management and SCM

Log Management is the process of collecting the log output of all of the devices and applications in your infrastructure. The centralization and aggregation of these logs allows your organization to search for events of interest that are part of a chain of events from seemingly unrelated devices. The data derived from SCM can add valuable context to these events to allow you to focus your efforts on high-value assets.

These are just a few of the primary cybersecurity processes that you should run in tandem with SCM to round out a robust cybersecurity toolkit.

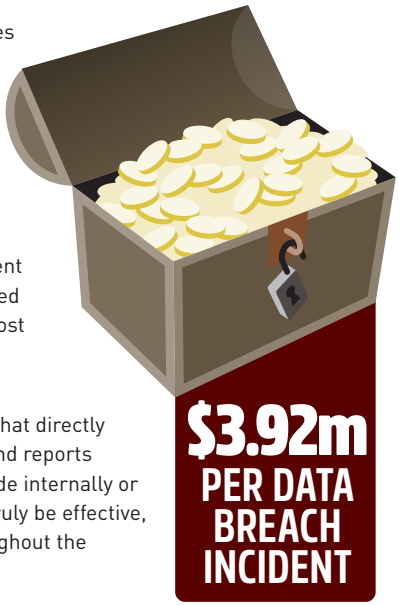


STORMY SEAS

Threats to the Modern Enterprise

One of the greatest challenges faced by modern enterprises is attempting to defend an expanding attack surface that is borderless, porous, and interdependent. The numbers and types of computing assets are exploding, with most endpoints connected directly to the corporate network or indirectly via the internet. Each of these devices represents a potential entry point for hackers and cybercriminals.

In this environment, older approaches such as perimeter-based security and network defenses have become untenable. Focusing on keeping attackers out of a perimeter is an unworkable strategy, as the perimeter is increasingly fluid and porous. Following a decade of exponential growth of incidents causing massive financial, privacy and intellectual property losses, we know with certainty that bad actors exist in the environment and that traditional security solutions have failed to keep them out. On average, data breaches cost organizations to the tune of $3.92 million per incident.[4]



SCM, then, provides a critical security control that directly monitors the state of the assets themselves, and reports deviations from expected values—whether made internally or externally, accidentally or maliciously. But to truly be effective, these controls must be deployed broadly throughout the organization.

Modern enterprises are composed of much more than traditional on-premises data centers. Security teams have to simultaneously monitor and manage computing resources across the organization, whether they're laptops being used by remote users, distributed systems, physical servers, network devices, assets deployed in the cloud, or applications running as a SaaS.

That being said, don't be overwhelmed by the amount of work it will take to implement SCM and the other basic CIS Controls. It's just a matter of getting started and prioritizing your efforts from there. If you think in terms of risk management, your best bet is to set your sights on thwarting your most serious threats first and then continuously optimizing.

SHRINKING YOUR ATTACK SURFACE

How would your security program run differently if your perspective was shaped around attack surface reduction? It's a great way to reframe the way your organization approaches security, especially when it comes to implementing the same basic controls that continue to be your very best line of defense against cyberattacks.

First off, what does "attack surface" mean? To understand the attack surface, you first need to understand what an attack vector is. An attack vector is simply an avenue that a bad actor can use to exploit your systems and networks and gain access to your sensitive information.

The attack surface, then, is just the sum of all the attack vectors for your organization—the total surface area of potential system exposure, be it on-prem, cloud, industrial, or any combination of hybridized environments you may have.

In this chapter, we'll take a look at how SCM functions in different environments commonly found in the modern enterprise—along with specific risks to be aware of.

BASIC SCM

The configurations on your network devices, databases, directory servers, POS terminals, workstations, laptops, tablets, operating systems and applications aren't secure by default. In fact, default settings on new devices are often set with ease-of-installation in mind, not proper security settings.

Configuration changes that leave systems vulnerable occur inadvertently through what's called "configuration drift." Configuration drift can take many forms, like privilege escalation, open communication ports, or open AWS (Amazon Web Services) S3 bucket access.

Adding to this complexity is the fact that your organization will have these assets scattered around an office building, home office, campus, distributed data centers, and even multiple cloud vendors. The fabric that ties all of these things together is also subjected to configuration drift. A small, seemingly innocuous change to a router configuration can disconnect entire networks and prevent employees from performing their tasks or allow unfettered access from the internet.

The key on-prem SCM practice of your security teams should be monitoring device and application configuration settings to keep them at a secure baseline. This must be done as a continuous practice rather than an occasional project. Even organizations that routinely assess their configurations or pass audits are only secure for a moment in time.

Risk increases every second that passes after an audit or assessment. And after each second, the known and trusted configuration state becomes less of a reality and more of a belief, inviting the conditions for a breach to take place.

> ***TRIPWIRE TIP:*** Dynamic environments offer their own SCM challenges. The term "dynamic environment" covers many types of deployments—such as a data center with hardware assets that are routinely retired and replaced. If your SCM tool doesn't monitor on- and off-boarding for dynamic assets, you won't have an accurate picture of your configuration state.

Example Attack Vectors Blocked by Basic SCM

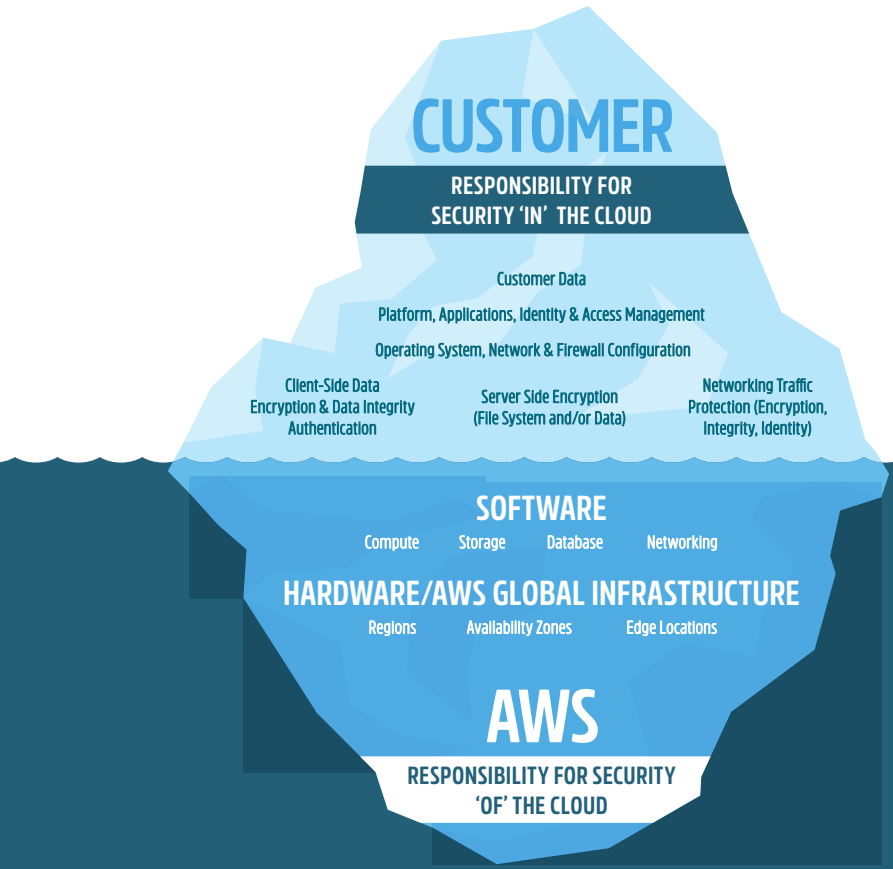
- Privilege escalation
- Credential access
- Insecure services and protocols like Telnet and TFTP

SCM IN THE CLOUD

The typical modern enterprise isn't operating on a strictly on-prem or cloud binary. The norm is now a combination of both modalities, due to the fact that organizations can get the best of both worlds by embracing elements of each that serve a range of business, IT and security goals. This blending of cloud and on-prem assets is what we call a "hybrid" environment.

Hybrid environments—while invaluable in terms of IT benefits such as scalability, cost savings, and granular infrastructure customization—do complexify your attack surface. What's more, it's also commonplace for hybrid organizations to use more than one cloud provider in order to take advantage of a wider array of cloud services and to avoid vendor lock-in.

Multi-cloud security requires automated SCM tools that can extend beyond the physical systems that you have on-site and conduct the same degree of configuration monitoring in the clouds. The configurations of AWS S3 buckets is one cloud attack vector that requires continuous management. The Verizon *DBIR* found that cloud storage misconfigurations are a leading cause of error-related breaches.[1]



It's tempting to assume your data and system configurations are secured automatically by your cloud provider. In reality, you share security responsibilities with them. It's important to know the clear delineations of how your security responsibilities fit in with your providers' such as AWS, Google Cloud Platform, Azure and others. You're required to protect your data and applications, but you are also responsible for managing the configurations of your cloud accounts.

DevOps is another area that deserves particular attention from cybersecurity teams. Since DevOps teams aim to move through the CI/CD pipeline as quickly and efficiently as possible, security can take a backseat to dangerous effect. The software development lifecycle was much longer before containerization; now, new builds can be promoted at the speed of business needs. Now when an application is rolled out, it's often been containerized. There's been a shift from thinking of applications and services as discrete units. Container and image misconfigurations need to be seen as their own continuously-checked quality gate in order to bring DevOps under the SCM umbrella.

Example Attack Vectors Blocked by SCM in the Cloud

- » Public cloud storage misconfigurations
- » DevOps containers
- » Unsecured GitHub repositories
- » Exposed admin credentials

INDUSTRIAL SCM

Industrial environments like critical infrastructure plants or discrete manufacturing facilities inherently complicate SCM because they incorporate the operational technology (OT) sphere in addition to IT. Moreover, they're home to the quickly-expanding array of industrial internet of things (IIoT) devices. IIoT devices connect once-isolated physical equipment to organizations' digital infrastructures and the internet—expanding the attack surface in new and sometimes unpredictable ways.

Industrial control systems (ICS) require SCM processes to correctly configure endpoints like operational workstations, SCADA equipment, programmable logic controllers, and human-machine interfaces. Like their IT counterparts, the name of the game here is continuous monitoring of configurations in alignment with compliance standards. The added obstacle is that many of these control systems are fragile, and you need low-impact or even "no-touch" approaches to scanning the devices to obtain the needed configuration data.

Example Attack Vectors Blocked by Industrial SCM

- Remote access via privilege escalation
- Misconfigured workstation endpoints
- Misconfigured ICS and IIoT devices

REMOTE WORK AND SCM

In addition to the environments we've covered in this chapter, the surge in remote work and its associated tools introduces new configuration management concerns. Shifting from a majority office to a majority remote workforce drastically changes the network perimeter and expands the attack surface.

It's easy to focus on the laptops that people use in their home offices when considering the information security challenges of a work-from-home environment, but they're only a part of the equation. Supporting a sizable and widely-distributed remote workforce isn't just about giving people laptops and permission. There is a host of infrastructure required to provide supporting services such as remote access, authentication and helpdesk.

In order to effectively implement SCM in a majority-remote working environment, you must start by inventorying the systems involved in delivering that capability. With an inventory in hand, you can then deploy SCM to all of the components involved. Doing so effectively allows you to ensure that users are being authenticated securely, that remote access is configured securely, and finally that the remote endpoints themselves are configured to be both secure and compliant.

Example Remote Work Attack Vectors Blocked by SCM

- Misconfigured remote endpoints (e.g. laptops)
- Misconfigured DNS
- Misconfigured access control

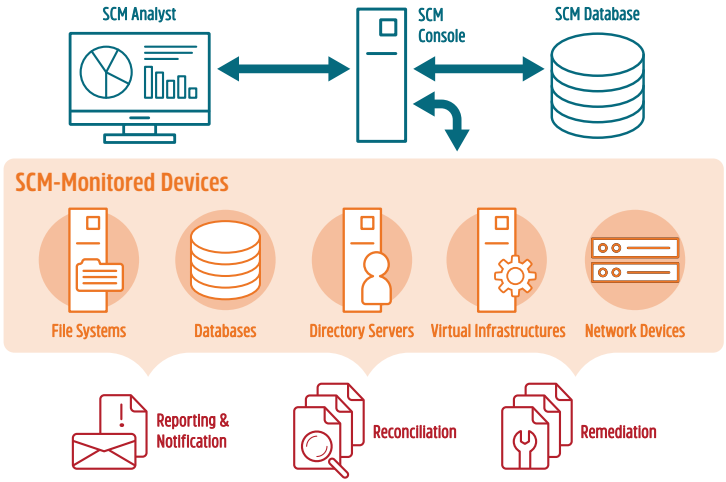
SETTING SAIL

SCM in Practice

Tracking configurations on even a single server can potentially be a colossal task—with thousands of ports, services and settings. If you multiply those same ports, services and settings across your entire enterprise of servers, hypervisors, routers, switches and firewalls, the only way to track all of those configurations is through automation.

Your SCM console will collect data from these numerous endpoints and can be used to remediate issues based on your compliance policies of choice. The components of your particular SCM solution may differ, but architecturally there will be a console of some sort that is used to manage, configure and report SCM data. There will be a backend database that will store all of the baseline, change and compliance information.

Finally, you will have a combination of agent-based and agentless technologies that will allow you to capture the SCM information you need from a variety of endpoints ranging from laptops and workstations to routers, switches and firewalls, servers, databases, directory servers and other assets—whether they be physical, virtual or cloud-based.



THE FOUR CARDINAL POINTS OF STRONG SCM

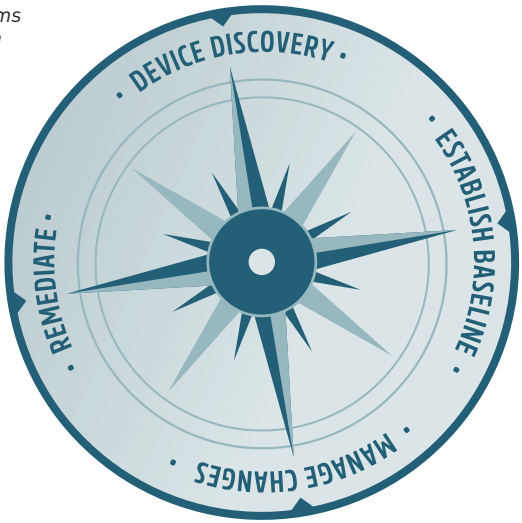
Device discovery, the establishment of configuration baselines, change management, and remediation are the four integral processes of SCM. A worthwhile SCM tool automates those tasks for you and provides deep system visibility at the same time. The moment your system becomes misconfigured, you should be notified and offered detailed remediation instructions in order to bring the misconfiguration back into alignment.

1. **Device Discovery:** *You can't manage what you don't know. First, you'll need to find the devices that need to be managed. Ideally, you can leverage an SCM platform with an integrated asset management repository. You will also want to categorize and tag assets to avoid starting unnecessary services. Engineering workstations, for example, require different configurations than finance systems.*

2. **Establish Your Baseline:** *In order to establish a secure baseline, you need to define acceptable configurations for each managed device type. Many organizations start with benchmarks from trusted establishments like CIS or NIST (the National Institute of Standards and Technology) for granular guidance on how various devices should be configured.*

3. **Manage Changes:** *Your SCM tool should get to work identifying and alerting on changes once your baseline is defined. And once devices are discovered and categorized, the next step is to define a frequency for SCM assessments. Determine how often you will run policy checks. Real-time assessments are not required for all use cases (more on that later).*

4. **Remediate:** *Identified problems either need to be fixed or granted an exception. You will also need to verify that expected changes actually took place for the audit. You are likely to have too much work to handle immediately when first implementing your SCM solution, so prioritization is key.*



DEEP-DIVE SCM PROCESSES TO KNOW

The four-part process of discovery, baselining, change management and remediation acts as the foundation of your SCM program. We'll now dive into what you need to know about policy libraries, understanding how SCM assessment works in practice, and leveraging SCM dashboards and reporting to their full potential.

MAINTAINING POLICY LIBRARIES

An SCM policy is a collection of standards to which monitored systems on your organization's network must conform in order to comply with either internal or external regulations. Make sure the tool you use has built-in policy content for testing against frameworks like the CIS Controls and PCI DSS. An advanced solution will also allow you to test against internal compliance policies. This is done by creating custom policy tests within the SCM tool itself.

WHAT MAKES GOOD POLICY CONTENT?

Good policy content is accurate and current. Accuracy is about correctly interpreting often-vague compliance requirements into effective controls that will be accepted by your auditors. Currency is about keeping up with the myriad of changes that are constantly being introduced into all modern compliance policies.

Custom Policies

A good SCM solution will allow you to import a number of additional policies as well as offer the flexibility needed to create your own custom policies. Each policy will have the following four components:

- **Tests** that check the state of a specific configuration setting
- **Scores** that measure the overall conformity of a system or device
- **Weights** that indicate the relative importance of a test
- **Thresholds** that separate the most urgent failures from the rest

Policy waivers

A waiver is an exception that can be granted to a test or a policy due to a business requirement or other mitigating factors. For example, your organization may be running a legacy application that can only run on Microsoft Windows 2003. In most cases, an auditor would ding you for running an operating system so far out of date. But a documented waiver showing why you need to run it and that the business has signed off on the risk will allow the auditor to move on.

> ***TRIPWIRE TIP:*** Look for an SCM tool that allows waivers to be dynamically assigned to assets based on groups and tags, rather than just hard associations between specific assets and tests. This allows ephemeral and dynamic assets to be waived from policy tests as they spin up and down based on details that would associate them with the appropriate asset group or tag. This brings waiver implementation to dynamic, cloud environments.

Multi-policy capabilities

Often an organization will have multiple compliance or security requirements. Your company may be a public company that processes credit cards, for example. As such, it will have to be compliant with both SOX (the Sarbanes-Oxley Act) and PCI. A complete SCM solution lets you apply multiple policies against your assets with little additional effort.

Asset tagging

Larger enterprises are complex and have many layers. It's important that your SCM solution can reflect that complexity to get the best actionable information out of it. You may have your company divided into location, system owner, business owner, application, and so on. Being able to tag your assets by the logical schema that maps your organization allows you to better report on your SCM compliance.

MONITORING

Having well-defined processes and policies is a great start, but they're ineffectual without the means to monitor the asset they're applied to. By actively monitoring these assets for change, you ensure that your organization's processes and policies are being correctly followed and that the appropriate personnel are alerted when deviations occur.

Agents vs agentless

Assets can typically be monitored in one of two ways: using a program specifically installed on the target system to do monitoring, called an agent, or via remote access. Some vendors can provide both. Agent-based monitoring generally provides more detailed information, as it can directly interact with the asset in question. Agentless monitoring may be best when an agent would be disruptive (such as in industrial networks) or incompatible with some aspects within your monitored environment (such as systems running embedded Windows or Linux). Agentless monitoring requires you have the correct credentials to access those systems remotely.

Real-time vs periodic

Most SCM tools monitor for changes on a periodic basis and then compare the results with the previous baseline. For certain critical systems or dynamically changing environments, having the option for real-time change detection can be a big advantage. You can be immediately alerted of a potentially dangerous change, and also capture exactly who made the change and when. At the same time, not all monitored nodes support agents, such as routers, network switches and firewalls, so you will need to configure your SCM solution to scan these on a periodic basis.

REMEDIATION WORKFLOWS

Knowing which of your assets are out of compliance with your policies is only half the battle. Being able to correct or fix the issues on a timely basis is the other half. A complete SCM solution has policy content that not only describes the issue but also provides remediation guidance so that the system or application owners have the details they need to effectively deal with the problem.

When combined with a change management process—or better yet, when integrated with an automated change management solution—an effective SCM solution can help drive the remediation process in a well-documented manner that allows business units to maintain availability.

REPORTS AND DASHBOARDS

You will need to consider how you want to receive the information collected by SCM. Not only do you want to think about the technical information you want, but the higher-level reports as well. Remember all of the stakeholders, both technical and non-technical, who can use the SCM reports.

Well-defined reports and dashboards are a requirement for an effective SCM solution. Organizations of any size need to be able to draw the crucial information out of the potentially massive amount of data that can be generated. When combined with asset tagging, these reports will allow the administrator to present only the information that is required by the business.

Good SCM Looks Like High-Visibility Dashboarding

Dashboarding is a crucial part of good SCM tools because it helps stakeholders across the organization get an at-a-glance understanding of security and compliance—both right now and over time. Keep in mind that you'll want user-selectable elements and defaults for technical and non-technical users. You should be able to only show certain elements, policies, and/or alerts to authorized users or groups, with entitlements typically stored in the enterprise directory. Using a good reporting system will highlight areas where you aren't aligned with your desired configuration state and help you drill down for remediation guidance.

KEEPING IT SHIPSHAPE

Using SCM to Stay Compliant

In addition to hardening your attack surface against intrusion, SCM also helps auditors track compliance improvements over time. When it comes time to supply your auditor with documentation, you can pull reports from any point in time to demonstrate your configurations' alignment with various compliance standards.

Compliance efforts can be geared toward both internal and external audits. Your organization may have its own unique set of internal controls that are enforced via in-house audits on a regular basis in addition to externally-conducted audits for legally-mandated regulatory standards such as PCI DSS or HIPAA.

"Developing configuration settings with good security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices. Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security 'decay' as software is updated or patched, new security vulnerabilities are reported, and configurations are 'tweaked' to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network-accessible services and client software."[5]

—Center for Internet Security

BEST PRACTICE FRAMEWORKS

It's important to distinguish between best practice frameworks and enforced regulatory standards. Best practice frameworks provided by organizations such as CIS and NIST are resources you can adhere to in order to maintain a modern, effective cybersecurity program.

They recommend basic security practices like SCM, but they are not enforced by audit. Mandated standards, on the other hand, also call for SCM—so implementing it will get you one step closer to adherence with both.

There are a handful of frameworks available to help you create an effective cybersecurity program, including the CIS Controls, NIST and MITRE ATT&CK. These aren't the only frameworks you can leverage to help build a well-oiled SCM machine, but they are a few of the most widely used.

THE CIS CONTROLS

As mentioned in Chapter 1, the Center for Internet Security's CIS Controls is the cybersecurity industry's gold standard for organizations to use to secure their systems. The 20 controls are prioritized by importance, so you'll get the most benefit from the controls by implementing them in order. SCM is covered in Control 5: "Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers."

The CIS Controls

Basic CIS Controls

1. *Inventory and Control of Hardware Assets*
2. *Inventory and Control of Software Assets*
3. *Continuous Vulnerability Management*
4. *Controlled Use of Administrative Privileges*
5. *Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers*
6. *Maintenance, Monitoring and Analysis of Audit Logs*

Foundational CIS Controls

7. *Email and Web Browser Protections*
8. *Malware Defenses*
9. *Limitation and Control of Network Ports, Protocols and Services*
10. *Data Recovery Capabilities*
11. *Secure Configuration for Network Devices, such as Firewalls, Routers and Switches*
12. *Boundary Defense*
13. *Data Protection*
14. *Controlled Access Based on the Need to Know*
15. *Wireless Access Control*
16. *Account Monitoring and Control*

Organizational CIS Controls

17. *Implement a Security Awareness and Training Program*
18. *Application Software Security*
19. *Incident Response and Management*
20. *Penetration Tests and Red Team Exercises*

NIST

NIST is the guiding framework for federal information systems in the U.S.—closely related to the Federal Information Security Modernization Act (FISMA) regulatory standard. Their special publication (SP) 800-53 called "Security and Privacy Controls for Federal Information Systems and Organizations" is useful to private-sector organizations as well, as it helps security practitioners in any industry implement better SCM.

NIST 800-53 Control suggests automated tools for configuration management: "Automated tools can be used at the organization level, mission/business process level or system level on workstations, servers, notebook computers, network components, or mobile devices ... Automated security responses include halting selected system functions, halting system processing, or issuing alerts or notifications to organizational personnel when there 4469 is an unauthorized modification of a configuration item."[6]

SCM Compliance for Federal Agencies

The Federal Information Security Management Act (FISMA) tasks federal government agencies with ensuring data security for their systems. The standards and frameworks in this chapter don't constitute an exhaustive list—but these are a sampling of the most common regulatory standards for which your organization is likely to be audited. NIST, described in the previous section in this chapter on non-mandatory compliance frameworks, is the guiding framework for meeting FISMA compliance. The following NIST SPs are addressed by SCM:

- **NIST 800-37:** Guide for Applying the Risk Management Framework to Federal Information Systems
- **NIST 800-53:** Recommended Security Controls for Federal Information Systems and Organizations
- **NIST 800-128:** Guide for Security-Focused Configuration Management of Information Systems
- **NIST 800-137:** Information Security Continuous Monitoring for Federal Information Systems
- **NIST 800-171:** Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

"NIST is probably the most thoughtful, comprehensive, well-researched, accepted framework out there. It's robust enough to complement what large organizations are already doing but flexible enough to give smaller organizations a roadmap to improved cybersecurity."

– David Meltzer, Tripwire Chief Technology Officer

MITRE

MITRE is a non-profit organization that operates federally-funded research and development centers. Their ATT&CK framework is an incredibly useful cybersecurity model illustrating how adversaries behave and explaining the tactics you should use to mitigate risk and improve security.

Whereas CIS offers organizations a prioritized list of actions they can take to harden their systems against cyberattacks, the MITRE ATT&CK approaches its framework from the point of view of the attackers themselves.

The framework lists common adversarial tactics, techniques, and common knowledge (ATT&CK) in the form of a detailed matrix. ATT&CK techniques like privilege escalation, credential access and lateral movement can be blocked by SCM because these activities would impact configuration and be flagged and alerted on by your SCM tool.

"MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's attack lifecycle and the platforms they are known to target. ATT&CK originated out of a project to enumerate and categorize post-compromise adversary tactics, techniques and procedures (TTPs) against Microsoft Windows™ systems to improve detection of malicious activity. It has since grown to include Linux™ and MacOS™, and has expanded to cover pre-compromise tactics and techniques, and technology-focused domains like mobile devices."[7]

– MITRE

REGULATORY COMPLIANCE STANDARDS

Now that we've established a few of the main best practice frameworks for implementing SCM, let's dive into audit-enforced regulatory compliance standards. Most industries have a primary compliance standard, like HIPAA for healthcare, but some standards are more far-reaching, like GDPR (the General Data Protection Regulation). Across the board, SCM is one of the key processes for which you'll be audited.

PCI DSS

When the credit card industry moved into the digital space, it quickly realized the need to protect itself from digital fraud. Credit card fraud continues to be a major issue, with every breach in the headlines decreasing customer confidence in some of the world's biggest companies.

The PCI Security Standards Council, founded in 2006, is now a global organization with a far-reaching impact on how business is done in the digital age. In addition to helping cardholders' data stay in the right hands, PCI also helps card issuers and banks limit their liability in the event a merchant suffers losses from a breach.

Implementing effective SCM for PCI compliance requires a tool with broad support of server operating systems, POS systems, virtual systems, cloud-based assets, network devices, directory servers and databases to protect against the most common attack vectors. Your SCM tool should be able to provide guidance on how to remediate system configurations when they drift from PCI compliance. Section 11.5 specifically calls out the benefit for FIM capabilities to alert you to changes that cause drift.

HIPAA

HIPAA was formed in 1996 and is managed by the U.S. Department of Health and Human Services. To mitigate breaches to confidential patient information, HIPAA was instituted to ensure the confidentiality, integrity and availability of protected health information.

SCM tools monitor systems for unauthorized changes and prioritize vulnerabilities to ensure health data is not compromised. There are many types of environments and devices in healthcare IT that, if misconfigured, could provide cybercriminals with patient health information (PHI). Healthcare outspends other industries when it comes to the cost of cyber breaches; one stolen EMR (electronic medical record) costs healthcare organizations $429 on average[8] and can garner between $250 and $1,000 each for cybercriminals on the dark web.[9]

When you have an SCM process in place, you'll be able to see your current HIPAA compliance at a glance in your tool's reporting and dashboarding features. You can also pull reports for any point in time for proof of compliance during your audit process. Part 164, Subpart C, Section 164.312 of Title II of HIPAA explains a set of technical requirements that are addressed by SCM, such as access control.[10]

NERC

North American Energy Reliance Commission (NERC) is an international regulatory organization created by the U.S. that works to reduce risks to power grid infrastructure. They do this through the continual development of a set of regulatory standards, in addition to education, training and certifications for industry personnel.

Cybersecurity professionals who work within the bulk electric system (BES) and other critical infrastructure supply industries are mandated to comply with NERC CIP (critical infrastructure protection). NERC compliance failures can cost organizations up to $1 million per day per violation, so it's no wonder that electric utilities pour vast resources into achieving and maintaining strict NERC compliance.[11]

NERC CIP Substandard 010—*Configuration Change Management And Vulnerability Assessments*—is particularly impacted by SCM. The purpose of the substandard is "To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES."[12]

SOX

SOX requires all publicly held companies to establish internal controls and procedures for financial reporting to reduce the possibility of corporate fraud. SOX is not specific on the types of controls that are required, but points to the COBIT (Control Objective for IT) framework to provide organizations' guidance on their IT governance.

On the topic of SCM, the COBIT DS9 (delivery and support) standard DS9 is as follows: "Manage the Configuration: Ensuring the integrity of hardware and software configurations requires the establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimizes production issues and resolves issues more quickly."[13] Therefore, you can achieve SOX compliance by way of using a COBIT policy in your SCM tool.

The standards and frameworks in this chapter don't constitute an exhaustive list—but these are a sampling of the most common regulatory standards for which your organization is likely to be audited.

ALL HANDS ON DECK

Buying and Applying SCM Solutions

Let's end our odyssey with a few considerations you should be aware of when preparing to purchase and launch a new SCM solution. Configuration management tools have been around for quite some time in technology years, so you should expect a lot from yours. Now that you have a better understanding of what SCM is and what processes it includes, hold your SCM solution to the standard of managing these processes with a wide breadth of coverage and opportunities for customization.

WHAT IS "CHECKBOX" SCM?

Checkbox SCM products are ones that may provide just enough functionality to pass an audit if the auditor doesn't dig too deep, or provide a limited library of policy content focused on generic standards but not more specialized policies such as NIST or PCI. Other vendors will have products that have lots of content but do not scale well across your enterprise or lack the reporting capabilities you need. Make sure you select a solution or vendor that meets all your requirements—resist the temptation to simply check a box.

What to Assess in Your Environment

Before you decide on a new SCM tool, it's important to take a detailed look at your IT and/or OT environment to see what your unique specifications will be. These are some of the main environmental considerations to focus on:

» ***Hardware requirements**: Look closely at the hardware requirements that are needed to effectively run the SCM solution before you buy it. Does it require a six-figure server? Will you need full-time staff to run it? Does the vendor offer a hosted solution? There is*

no point in selecting a vendor if their tool only runs on Linux and most of your servers are Windows. Consider your scale as well: While your initial requirements may only cover a few dozen or hundreds of servers, can your selected solution grow with you?

- ***Distributed environments:*** *Large enterprises very seldom have all their assets in one place. Does your chosen SCM solution work in a distributed or hybrid environment? You may have some assets on-prem, some virtual, and others existing in various cloud-based environments. Comprehensive support for all of the major cloud vendors is important. If the tool you're considering only supports AWS, but you have compute loads in AWS and Azure, you will not get the coverage you need. Your SCM vendor will also need to support the dynamic nature of most cloud environments as well.*

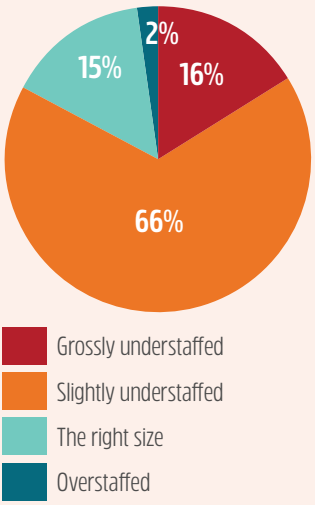
- ***Key third-party tools****: What tools and applications do you rely heavily on that are already in your environment? Define those integral tools and look for an SCM solution that gives you plenty of options to integrate with third-parties, such as threat intelligence sources, patch management and operations applications, logging and SIEM solutions, and ticketing systems.*

WHY ORGANIZATIONS USE MANAGED SCM

For years counting, the cybersecurity community has faced another challenge—one that doesn't come from cybercriminals, but from the widespread deficit of available skilled professionals to meet hiring demand. This becomes a risk when positions go unfilled or staffed by under-trained personnel. The reality of constantly-evolving standards is another issue to keep up with. Your SCM solution should be providing timely updates to the policies, but you still need to deploy and adapt them to your SCM program. Essential security processes like these can be managed remotely or run by a resident engineer supplied by cybersecurity providers offering professional services. A managed service provider can efficiently address your unique SCM challenges.[14]

Security teams continue to be understaffed

How would you characterize the size of your current security team?

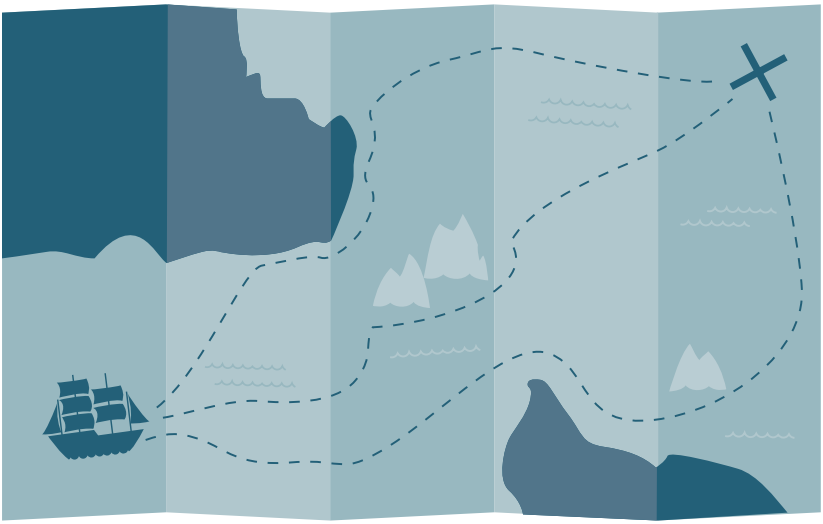


» ***The skill set of your Security and IT teams:*** *Serious consideration has to be given to the staff you currently have. Smaller organizations may only have a few admins who have to wear several hats—including security training. Large enterprises may have so many administrators that they may not all even be in the same building and rely on completely different security groups. Which group will own the SCM solution? Who will they report to when there are compliance problems? You'll also want to ensure that your selected SCM solution fits into your existing change management process, or be ready to re-engineer it.*

10 QUESTIONS TO ASK YOUR SCM VENDOR

1. **What specific controls do you offer for endpoint management?**
   Can the policies for all controls be managed via your console?
2. **Which products, devices and applications are supported?**
3. **What standards and/or benchmarks are offered out of the box?**
4. **What reports are available out of the box?**
   What's involved in customizing specific reports?
5. **Does your organization have an in-house research team?**
   How does their work make your product better?
6. **How do you handle remote and occasionally-connected devices?**
7. **Where does your management console run?**
   Do we need a dedicated appliance? What kind of hierarchical management does your environment support? How customizable is the management interface?
8. **What have you done to ensure the security of your platform?**
   Is strong authentication supported? Have you done an application penetration test on your console? Does your engineering team use any kind of secure software development process?
9. **What is the scope that the solution will cover?**
   How many of each device type needs to fall under the initial license purchase? What kind of hardware will be required to support the initial scope, and is there room to scale up?
10. **Does the vendor offer professional services and/or training options that will fit your skills, needs and budget?**

DEPLOYMENT CONSIDERATIONS



Once you have made your SCM solution selection and purchased your licenses, there will be a number of considerations to take into account for deployment. Assess your internal skill sets and determine what education and training are required to deploy the SCM solution. Consider using professional services from your vendor to help you implement or even remotely run your solution. In any case, ensure you have a well-defined project plan and statement of work from the vendor to keep costs under control.

If you will be integrating the SCM solution into other parts of the environment, make sure that the subject matter experts for these applications are available. The requirements for these integrations need to be part of the project plan and statement of work.

Know what you need to do to acquire and deploy the hardware on which the SCM tool will be installed. Make sure this hardware is ready when the vendor's professional services team gets there to avoid travel and expense cost overruns. Next, make sure you understand the solution's port and services requirements. You will need to work with the network team to ensure that all of these requirements are met.

THE TRIPWIRE APPROACH TO SCM

Tripwire provides fully-integrated solutions for policy, file integrity and remediation management. Organizations use Tripwire for a complete end-to-end SCM program to address today's pressing security and compliance challenges—while building a foundation that positions them to address tomorrow's.

Tripwire has the largest and broadest library of supported policies and platforms, with over 2000 policies covering an array of platform OS versions and devices. Get deep, unparalleled visibility into the security system state and to always know your current security posture. Tripwire's remediation capability automates and guides you for rapid repair of security and compliance misconfigurations.

TRIPWIRE® ENTERPRISE

Tripwire® Enterprise is an integrated suite that pairs the industry's most respected FIM and SCM to provide real-time change intelligence and threat detection. For the compliance officer, it delivers proactive system hardening and automated compliance enforcement—resulting in a reduction of audit cycles and cost. Thousands of organizations trust Tripwire Enterprise to serve as the core of their cybersecurity programs.

TRIPWIRE® CONFIGURATION MANAGER

Tripwire Configuration Manager gives you the ability to extend your configuration monitoring to include cloud accounts and assets executing in Amazon Web Services (AWS), Microsoft Azure, and other cloud service providers—all from a single console. It gives you the option to have your configuration rules automatically enforced and provides a risk score to prioritize all misconfigurations so that security staff can focus on the most impactful problems first.

TRIPWIRE® EXPERTOPS

Tripwire ExpertOps℠ SCM delivers a cloud-based managed services model of the industry's best SCM. A single subscription includes personalized consulting from trained experts and hands-on tool management to help you achieve and maintain compliance and critical asset security.

TRIPWIRE® INDUSTRIAL VISIBILITY

Tripwire Industrial Visibility provides ICS operators with total visibility into the devices and activity on their network. It uses change management, event logging and threat modeling to help you keep your most sensitive assets out of intruders' reach.

READY TO LEARN MORE?

DOWNLOAD THE
TRIPWIRE ENTERPRISE DATASHEET
OR SCHEDULE YOUR DEMO NOW

www.tripwire.com

THE STATE OF SECURITY
tripwire.com/blog

@tripwireinc

AUTHOR BIOS

Chris Orr

Chris Orr has been with Tripwire since September 2000. Initially hired to develop and deliver training materials for such golden oldies as Tripwire for Servers and Tripwire for Routers, he quickly moved on into the sales engineering group where he has been ever since. His role initially required him to provide technical assistance to regions covering 27 states and all of the Federal government, but as the company has grown his territory has been whittled down to everything west of the Mississippi (which, when he thinks about it, is still the largest geographic territory in the company). Currently based out of scenic Lake Stevens, Washington, when not flying to such lovely places as Winnipeg or Boise, Chris is teaching his daughter how to play guitar or going on scouting trips with his son.

Steve Marriner

Steve Marriner is the Principal of Yosemite Group. He has a broad range of technology experience with systems, applications and cybersecurity over the past 30 years. He has provided product management, marketing and strategic consulting to leading companies in the security industry including Tripwire, Voltage Security and Iovation. Steve holds a BS degree in mathematics and computer science from the University of Connecticut and an MBA from Stanford University.

Tim Erlin

Tim Erlin is VP of Product Management & Strategy at Tripwire, and the host of Tripwire's podcast, *Talking Cybersecurity*. He previously managed Tripwire's vulnerability management product line. Erlin's background as a sales engineer has provided a solid grounding in the realities of the market, allowing him to be an effective leader and product manager across a variety of products. His career in information technology began with project management, customer service, as well as systems and network administration. Erlin is actively involved in the information security community. His contributions include blogging, podcasts, press, public speaking and television.

Sources

1. Johnson, Arnold, et al. "Guide for Security-Focused Configuration Management of Information Systems." *NIST*, 31 Oct. 2019.
2. "2019 Data Breach Investigations Report." *Verizon Enterprise*, 2019.
3. "CIS Control 12: Boundary Defense." *CIS*, www.cisecurity.org/controls/boundary-defense/.
4. "2019 Cost of a Data Breach Report: *IBM Security*." IBM Security, 2019, databreachcalculator.mybluemix.net/.
5. "CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers." *CIS*, www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/.
6. "Security and Privacy Controls for Information Systems and Organizations (Final Public Draft)." *NIST CSRC*, 16 Mar. 2020, csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft.
7. Strom, Blake E., et al. "MITRE ATT&CK™: Design and Philosophy." *The MITRE Corporation*, 11 Oct. 2019, www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy.
8. Davis, Jessica. "Data Breaches Cost Healthcare $6.5M, or $429 Per Patient Record." *HealthITSecurity*, HealthITSecurity, 23 July 2019, healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record.
9. Columbus, Louis. "5 Strategies Healthcare Providers Are Using To Secure Networks." *Forbes*, Forbes Magazine, 20 Oct. 2019, www.forbes.com/sites/louiscolumbus/2019/10/20/5-strategies-healthcare-providers-are-using-to-secure-networks/#3299f9954b40.
10. "45 CFR § 164.312 - Technical Safeguards." *Cornell Law School*, Legal Information Institute, www.law.cornell.edu/cfr/text/45/164.312.
11. "NERC Compliance Regulations & Requirements." *Compliance Guidelines*, 2020, complianceguidelines.com/nerc-compliance.htm.
12. "CIP-010-1." NERC, 2020, www.nerc.com/pa/Stand/Pages/CIP0101RI.aspx.
13. Tripwire Inc. *Sustaining SOX Compliance*, www.tripwire.com/solutions/compliance-solutions/sox-it-compliance/sustaining-sox-compliance-register.
14. Tripwire Inc. 2020 *Cybersecurity Skills Gap Survey*, www.tripwire.com/misc/skills-gap-survey-2019-register/.

MASTERING CONFIGURATION MANAGEMENT

Modern enterprises are composed of much more than traditional on-premises data centers, meaning security teams must defend an attack surface that is borderless, porous, and expanding over time.

Security configuration management (SCM) is a critical security control that monitors the state of assets and reports deviations from expected values—whether made accidentally or maliciously—to keep systems aligned with a secure baseline state.

In this guide, we'll explore SCM in practice for security and compliance. Equip yourself with the skills to overcome some of the most pressing configuration challenges modern enterprises face.