FORTRA™

GUIDE (TRIPWIRE)

# The Security Configuration Management Buyer's Guide

Reduce Risk by Ensuring Systems Are Properly Configured for Security and Compliance

Agile enterprises need to adapt quickly to business digitalization and new IT models to ensure availability while controlling risk. What is constant is change. There are changes that organizations are adapting to and have control over, such as system virtualization, cloud deployment, and which endpoint devices they will accept (BYOD).

However, they have less control over the threat landscape and where exploited vulnerabilities might hamper their operation. Organizations require platforms and technologies that can adapt and provide resilience to both these expected and unpredictable changes. Modern organizations encompass much more than traditional on-premises data centers, so security teams must be equipped to defend an ever-changing attack surface using sophisticated security controls like security configuration management (SCM).

One technical challenge is collecting relevant data from all parts of the enterprise. While organizations may have a large volume of data, they are still not collecting complete data — or in some cases none at all — from the vast number of endpoints in their environment.

This buyer's guide contains everything you need to know to get started on the journey to finding the best SCM solution for your organization. We will cover the business drivers behind SCM, the security processes it encompasses, what to look for in your SCM solution, and the ten questions you should be asking potential vendors.

## Business Drivers of SCM

### Digital Globalization

Today, a digital form of globalization has opened the door for developing countries, small companies, and billions of individuals to take part. Large companies can also manage their international operations in leaner, more efficient ways.

Using digital platforms and tools, they can sell in fast-growing markets while keeping virtual teams connected in real time. This is a moment for companies to rethink their organizational structures, products, assets, and competitors.

IT has also turned to the cloud as individual business units are now running their own IT infrastructures. These BUs are often subscribing to central IT services through services bureaus from the corporate IT organization. That, in and of itself, presents several challenges, such as having the right people, processes, and technologies in place to pass compliance audits or maintain up-time requirements. .

### New IT Models

One example of a new IT model organizations are considering is the convergence of Information Technology with Operational Technology (OT). The Internet of Things means more and more devices are connecting, and industrial networks are no exception. And these "things" aren't just the controllers and related computers "owned" by the OT department or the computers and network devices "owned" by the IT department. The "things" might also include everything from physical security IP cameras and networked badge readers to HVAC systems. A single vulnerable system is a potential pathway to other systems. All of these new and connected systems present security, operations, and compliance requirements and challenges that now need to be maintained and managed.

**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]

### Endpoint Intelligence Data Management

A current perception is that there is a data management problem: too much data. In reality, there is a data collection problem. Data collection can be categorized by volume and flow. Here's an example of how data volume hampers IT operations and security: Silos of data that are focused on a particular tool or business unit don't allow the collaboration or integration needed to piece together a timely or focused response to cyber incidents. In addition, multiple tools often collect the same data from the same systems, creating redundancy that must be managed.

Many organizations are also reluctant to install agents on every endpoint, citing agent drag or performance concerns. Endpoints are not static, meaning they are not connected in the same manner or at the same IP as might be expected. Data collection flow is hampered by network dark zones where connections are intermittent or communication is tightly controlled. Together, these real problems with data collection reinforce the perception that there is too much data. Actually, there is not enough of the right data and too much agent management overhead.

### Attack Vectors: What's Old is New

Many successful attacks are caused by simple operational failures. Whether it's an inability to patch in a timely fashion or to maintain secure configurations, far too many people leave the proverbial doors open on their devices. Attackers also frequently target users via social engineering, in which employees unknowingly open the doors for attackers and enable data compromise.

# The SCM Controls

## Security Configuration Management

Security configuration management exists at the point where IT security and IT operations meet. It's a core security control that combines elements of vulnerability assessment, automated remediation, and configuration assessment. The goal of SCM is to reduce security risks by ensuring that systems are properly configured — or hardened — to meet internal and/or regulatory security and compliance standards.

## Configuration Management Process

Let's take a high-level look to see how it works.

1. **Discovery:** First 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 configuration baselines:** First define acceptable secure configurations for each managed device type. Many organizations start with the benchmarks from the Center for Internet Security (CIS) or National Institute of Standards and Technology (NIST) for granular guidance on how devices should be configured.
3. **Assess, alert, and report changes:** Once devices are discovered and categorized, define a frequency for assessments. How often will you run a policy check? Real-time assessments may be available but are not required for all use cases.
4. **Remediate:** Once a problem is identified, either it needs to be fixed or someone needs to grant an exception. You are likely to have too much work to handle all issues immediately, so prioritization is a key success criterion. You will also need to verify that expected changes actually took place for the audit.

## What to Look For in an SCM Solution

Configuration management tools have been around for a while and are reasonably mature. There's significant leverage to be gained from a single platform which handles both periodic endpoint security and IT management functions.

- **Coverage (OS and apps):** Of course, your configuration management offering must support your operating systems and applications.
- **Discovery:** You can't manage configurations you don't know about, so you need to ensure you have a way to identify new and "invisible" devices. You also don't want to clutter your environment, and should retire deprecated devices. Supported standards and benchmarks: The more available policies and configurations offered by the solution, the better your chance of finding something you can easily adapt to your own requirements.
- **Policy editing:** Policies generally require customization to satisfy your requirements. Your configuration management solution should offer a flexible policy editor to define policies and add new baseline configurations and/or benchmarks.
- **Scalability:** Scanning each device for configuration changes can be demanding on endpoints and the network, so understand how to distribute scanners effectively and make sure scanning frequency, impact, and scope is flexible.
- **Dealing with remote devices:** How does assessment work for a remote device? This could be a field employee's laptop or a device in a remote location with limited bandwidth. What kinds of recovery features are built in to ensure the correct remediation is implemented? And finally, can you be alerted to devices that haven't been recently assessed, perhaps because they haven't connected?
- **Integration with operational process:** Make sure any identified configuration issues are reported to the central help desk system to close the operational loop in order to ensure a proper process for authorizing and applying changes.
- **Process to deal with policy exceptions:** As mentioned above, there may be situations where a configuration change represents an authorized exception. To complicate things further, authorization is often granted after configuration management detects (and perhaps reverses) the change. You must be able to reduce the possibility of false positives.

## File Integrity Monitoring

File integrity monitoring (FIM), also called change monitoring, means monitoring files, operating systems, servers, endpoints, and more to see if and when they change, how they changed, who changed them, and what will it take to change them back. This active security control allows you to define a known, secure baseline and watch for changes.

**Here are a few scenarios where FIM is particularly useful:**

- **Unauthorized changes:** These may not be malicious but can still cause serious problems. Many things, including operational failure and bad patches, can cause them, but ill intent is not necessary for exposure.
- **Malware detection:** Malware can load software and change configurations and registry settings, but another common activity is to change system files.
- **PCI compliance:** The Payment Card Industry Data Security Standard (PCI DSS) is a widespread prescriptive regulatory mandate that requires file integrity monitoring to alert personnel to unauthorized modification of critical system, configuration, or content files.

### FIM Process

Again we start with a process that can be used to implement file integrity monitoring.

- **Set policy:** Start by defining your policy, identifying which assets need to be monitored.
- **Baselining:** Then ensure that the assets you assess are in a known good state. This may involve evaluating version, creation, and modification date, or any other attribute to provide assurance.
- **Monitor:** Next, actively monitor changes. This is easier said than done because you may see hundreds of changes on a normal day on a single system, so knowing a good change from bad is essential. You need a way to minimize false positives by auto-promoting expected changes.
- **Alert:** When an unauthorized change is detected, the appropriate staff must be notified.
- **Report:** FIM is required for PCI and other regulatory compliance requirements, so you may need to substantiate effective usage for your auditor with solution-generated reports.

### What to Look For

Now that you have the process in place, you need some technology to implement FIM.

**Here are some factors to keep in mind when evaluating these tools:**

- **Policy granularity:** · Policy granularity: You will want to make sure your product can support different policies by device. For example, a point of sale device in a store (within PCI scope) needs to have certain files under control, while an information kiosk on a segmented internet-only network in your lobby may not need the same level of oversight.
- **Lightweight agent:** In order to implement FIM, you might install an agent on each protected device. Agents should be flexible to turn off functionality when not in use and pluggable to be able to add functions as they become necessary.
- **Monitoring frequency:** You need to determine whether you require true continuous monitoring, or whether scheduled assessment is acceptable.
- **Integration with threat intelligence sources:** Additive to internal research is integration with third-party threat intelligence sources, as they likely have the most up to date information on new attack vectors and indicators of compromise.
- **Research and intelligence:** A large part of successful FIM is identifying a good change from a potentially bad one. Besides integration with threat intelligence sources, it requires integrated operational intelligence.
- **Change detection algorithm:** Is a change detected based on file hash, version, creation date, modification date and/or privileges? Or all of the above? Understanding how the vendor identifies changes enables you to ensure all your threat models are factored in.
- **Version control:** Remember that even a legitimate file may not be the right one — for example, you're updating a system file, but an older legitimate version is installed instead.
- **Forensics:** In the event of a breach, you'll want forensics capability, such as a log of all file activity. Knowing what data was accessed, by which programs — and

what was done — can be very helpful for assessing the damage of an attack and nailing down the chain of events which resulted in data loss.

- **Closed loop change audit:** Thousands of file adds, deletes and changes happen — and most are authorized and legitimate. But for both compliance and operational reliability you should be able to reconcile the changes you expect against the changes that actually happened.
- **Platform integration:** There's no reason to reinvent the wheel, especially for cross-functional capabilities such as discovery, reporting, agents, and agent deployment/updating/maintenance. So, leverage your SCM platform to streamline implementation and facilitate operations.

## Policy Management

For policy creation, the system you use should provide baselines to get you started. Every environment has its own unique characteristics, but the platform vendor should provide out-of-the-box policies to make customization easier and faster. All policies should be usable as templates for new policies.

The more complex a policy, the easier it is to create internal discrepancies or accidentally define an incorrect remediation. Most administrators tend to prefer interfaces that use clear, graphical layouts for policies, preferably with an easy-to-read grid showing the relevant information for each policy.

### What to Look For

Technologies for implementing policy compliance are numerous and varied.

**Here's what to look for:**

- **Supported standards and benchmarks:** The more built-in standards and/or configuration benchmarks offered by the tool, the better your chance of finding something you can easily adapt to your own requirements.
- **Policy editing:** Policies optimize systems and services to improve availability and performance, and also reduce the attack surface. They generally require customization to satisfy your requirements. Your configuration management tool should offer a flexible policy editor to define policies and add new baseline configurations and/or benchmarks.
- **Policy updates:** Regulatory policies are updated constantly; systems should quickly (even automatically) update through content download for the solution.
- **Automated asset classification:** When new assets are discovered, the system should evaluate and make recommendation to what kind of assets it is and which policies are appropriate.

# Platform Considerations

## Platform Selection

User-selectable elements and defaults for technical and non-technical users save time and increase efficiency by taking the guesswork out of configuration.

**Let's list the platform capabilities you need:**

- **Dashboard:** 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.
- **Discovery:** You can't protect an endpoint (or any other device, for that matter) if you don't know it exists. Make sure you know about new devices as quickly as possible.
- **Asset repository integration:** Closely related to discovery is the ability to integrate with an enterprise asset management system/CMDB to get a heads-up whenever a new device is provisioned.
- **Policy creation and management:** Alerts are driven by the policies you implement in the system, so policy creation and management is also critical to adapt the solution to the unique requirements of your environment.
- **Alert management:** Time is of the essence during any potential breach, so the ability to provide deeper detail via drill down then provide information to an incident response process is critical. This allows administrators to monitor and manage policy violations which could represent a breach.
- **Agent vs. agentless:** Does the configuration management vendor use an agent to perform assessment, or do they perform agentless scans? How do they apply changes? Environments may require a combination in order to gather endpoint intelligence and avoid blind spots.
- **Reporting:** As we mentioned under specific controls, compliance tends to fund and drive these investments, so substantiating their efficacy is necessary. Look for a mixture of customizable prebuilt reports and tools to facilitate ad hoc reporting — both at the specific control level and across the entire platform.

## Enterprise Integration Points

No platform really stands alone in an organization. You already have plenty of technology in place, and anything you buy to manage endpoint security should integrate with your other solutions to maximize your investments. Make sure your vendor can provide sufficient integration, or at a minimum an SDK or API to pull data from it for other systems.

**Enterprise integration points include:**

- **Operations management** – Including device building/provisioning, software distribution/licensing, and other asset repositories
- **Vulnerability management** – For discovery, vulnerabilities, and patch levels
- **Endpoint protection** – Including anti-malware and full disk encryption, potentially leveraging agents to simplify management and minimize performance impact
- **SIEM/Log management** – For robust data aggregation, correlation, alerting, and reporting
- **Backup/recovery** – Many endpoints house valuable data, so make sure device failure doesn't risk intellectual property

## 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. What products, devices, and applications are supported by your endpoint security management offerings?
3. What standards and/or benchmarks are offered out of the box as part of your configuration management offering?
4. What kinds of 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 endpoint security management product better?
6. What kind of agent is required for your products? Is the agent persistent or dissolvable? How are updates distributed to managed devices? How do you ensure agents are not tampered with?
7. How do you handle remote and disconnected devices?
8. 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?
9. What is your plan to extend your offering to virtual desktops (VDI)?
10. What have you done to ensure the security of your endpoint security management platform? Is strong authentication supported? Have you done an application pen test on your console? Does your engineering team use any kind of secure software development process?

This list can't replace a more comprehensive RFI/RFP, but can give you a quick idea of whether a vendor's product family can meet your requirements. As we have described, security configuration management is mature technology — so look less at specific feature/capability differentiation and more at policy integration, console leverage, and user experience. That approach will usually yield the most effective solution for your environment.

### FORTRA'S APPROACH TO SCM

You can rely on Fortra's Tripwire to continuously monitor your digital environments for misconfigurations that impact security and compliance along with clear guidance for remediation. Trusted by thousands of organizations worldwide, Tripwire's SCM solutions integrate with the other tools in the tech stack and bridge on-premises, cloud, and industrial environments.

#### Tripwire Enterprise: Superior Security, Continuous Compliance

Fortra's Tripwire® Enterprise is the leading compliance monitoring solution powered by SCM and FIM. Backed by decades of experience, it's capable of advanced use cases unmatched by other solutions.

#### Tripwire ExpertOps: Instant Expertise with Managed Cybersecurity

Fortra's Tripwire® ExpertOps℠ is a managed cybersecurity service that equips you with the SCM advice and support needed to protect your data from cyberattacks while maintaining regulatory compliance.

Learn more at **www.tripwire.com**.

Sources:
1. https://csrc.nist.gov/glossary/term/security_configuration_management

FORTRA™

Fortra.com

**About Fortra**

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

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.