tripwire

The Security Configuration Management Buyer's Guide

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

The Business Impact of Managing Endpoint Security & Configuration

To ensure availability while controlling risk, today's agile enterprises need to adapt quickly to business digitalization and new IT models. What is constant is change. There are changes that organizations are adapting to and have control over, such as system virtualization, cloud deployment, IT/OT conversion, 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. Customers require platforms and technologies that can adapt and provide resilience to both these expected and unpredictable changes.

Digital capabilities and response to new IT models are now a prerequisite to compete in the long term. Yet many companies seeking to go digital are still unclear about the best way to set up their IT organizations, manage digital information, and establish and maintain online services and automated processes. 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.

Business Drivers

Digital Globalization

Today, a digital form of globalization has opened the door for developing countries, small companies and start-ups, and billions of individuals to take part. Tens of millions of small and midsize enterprises worldwide have turned themselves into exporters by joining e-commerce marketplaces such as Alibaba, Amazon and eBay. Large companies can 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 too has 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 maintaining up-time requirements.

New IT Models

One example of new IT models 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.

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 OPS and Security: silos of data that are focused on a particular tool or business unit don't allow 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 what 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 today 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. In a recent Verizon DBIR study, upwards of 99% of attacks exploited vulnerabilities (CVEs) that were published over a year prior. Or attackers target users via social engineering; in the same study 50% of users opened phishing emails and clicked on bad links in the first hour. Employees unknowingly open the doors for attackers—and enable data compromise.

The Security Configuration Management Controls

Security Configuration Management

Security Configuration Management exists at the point where IT security and IT operations meet. It's a software-based solution 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—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 CIS or 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 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

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 the data about 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 to see if and when they change, how they changed, who changed them, and what will it take to change them back. Obviously many files do legitimately change over time, particularly during patch cycles. But most files are generally static, and changes to core functions (such as the IP stack and email client configuration) often indicate some type of problem. This active security control allows you to define a set of files (including both system and other files), gather a baseline for what they should look like, 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 does many bad things to your devices. It can load software and change configurations and registry settings, but another common activity is to change system files.
- **PCI compliance:** Requirement 11.5 of the 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.

> Ideally a FIM solution not only detects changes to files, but also includes capabilities that help IT immediately remediate issues caused by improper change. For more information, refer to our detailed **FIM Buyer's Guide**.

FIM Process

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

1. **Set policy:** Start by defining your policy, identifying which files on which devices need to be monitored.
2. **Baseline files:** Then ensure that the files you assess are in a known good state. This may involve evaluating version, creation and modification date, or any other file attribute to provide assurance that the file is legitimate.
3. **Monitor:** Next, actively monitor changes. This is easier said than done because you may see hundreds of file 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.
4. **Alert:** When an unauthorized change is detected you need to let someone know.
5. **Report:** FIM is required for PCI compliance. So you may need to substantiate effective usage for your assessor. That means generating reports for a compliance audit.

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:** 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 of files, 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 determines a file has changed 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 when different files were 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 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:** PCI DSS, NERC CIP, SOX, HIPAA, NIST 800-53, MAS TRM, IRS 1075, 20 CSC, COBIT, ISO 27001 to name a few. 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.
- **Policies:** For optimizing systems and services to improve availability, performance and reduce the attack surface.
- **Policy editing:** Policies 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 what policies are appropriate.

Platform Buying Considerations

We have alluded to the platform throughout this paper, but what exactly does that mean? What do you need it to do?

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 response, 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 (typically using a non-persistent "dissolvable" agent), and then 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 pre-built 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 "play nice" 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

Next Steps: 10 Questions to Ask Your Security Configuration Management 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?

Summary

Of course we could have written another 10 questions. But these hit the highlights of device and application coverage, research/intelligence, platform consistency/integration and management console capabilities. 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, endpoint security 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.

tripwire®

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

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