FORTRA™

10 Common Security Misconfigurations and How to Fix Them

Does your organization have an established security configuration management (SCM) program, or are you relying on default security settings? Misconfigurations are a leading cause of unauthorized access and security breaches, creating entry points for hackers in servers, file systems, networks, firewalls, websites, software, workstations, and cloud infrastructure.

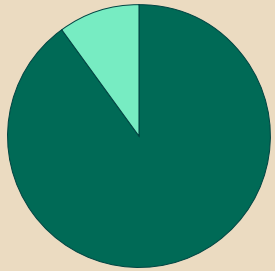
The **Open Worldwide Application Security Project** includes security misconfigurations in their **OWASP Top 10** list of web application security risks: "*With more shifts into highly configurable software, it's not surprising to see this category move up.*"[1] And the problem isn't limited to the cyber criminals alone—it's an issue of human error as well, with misconfigurations making up 21 percent of error-related breaches.[2]

Fortunately, security misconfigurations are easy enough to prevent and correct when you're equipped with the right knowledge and tools. When the options, permissions, and modes of all assets in your environment are configured securely, the chance of a successful security breach declines significantly.

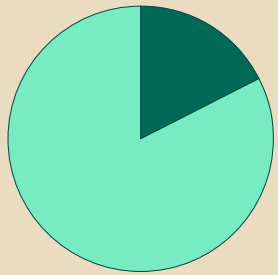
This guide highlights ten of the most common types of security misconfigurations and explains how SCM can help with some. But first, let's start with a concise definition of misconfiguration. The National Institute of Standards and Technology (NIST) defines a misconfiguration as "*An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.*"[3]

MISCONFIGURATION STATS

OWASP reported finding misconfigurations in **90%** of the applications they examined.[4]



Verizon's ***2023 Data Breach Investigations Report*** (DBIR) noted 602 incidents resulting from miscellaneous errors, and 126 (**21%**) of those were due to misconfigurations.[5]



10 Common Security Misconfigurations

1. DEFAULT SOFTWARE AND APPLICATION CONFIGURATIONS

One of the first places to look for misconfigurations is in your default software and application settings. Most settings aren't secure by default. For example, new vendor-supplied software comes with default configurations created for convenient installation. Manufacturers create these settings with one goal in mind: ease of use. So as soon as you onboard a new service or tool, ensure settings are as secure as possible.

WHAT IS A MISCONFIGURATION?

An incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.

2. WEAK PASSWORD POLICIES

Employees may want to use a password that is easy to remember, but it's critical to enforce a strong password policy to prevent bad actors from entering your systems using automated password cracking tools. Passwords need to be adequately long and combine upper and lowercase letters, numbers, and symbols while avoiding complete words—especially words that could be guessed based on context clues or social engineering. Additionally, it's best to implement multi-factor authentication (MFA) for all employees and require passwords be updated on a regular basis.

3. PUBLIC CLOUD MISCONFIGURATIONS

Cloud service providers (CSPs) such as Amazon Web Services (AWS) or Google Cloud Platform (GCP) don't provide securely configured environments for your data by default. Unfortunately, threat actors use automated tools to find misconfigured cloud accounts and storage, including AWS S3 buckets and Azure/GCP Blobs. While they are responsible for the security of the networks and data centers enabling their cloud infrastructure, the customer is ultimately responsible for securing the data, devices, and accounts that interface with that infrastructure.

4. MISCONFIGURED REMOTE ENDPOINTS

Remote endpoints are more common than ever and pose a number of significant misconfiguration risks. When employees use their devices on home Wi-Fi networks or while traveling they are often at greater risk of exposure due to limited security knowledge and the increasing prevalence of rogue public access points. Cyber criminals can leverage misconfigurations in remote endpoint accounts, password storage, and management tools.

5. UNSECURED PROTOCOLS AND NETWORK SERVICES

Unsecured communication protocols such as Telnet, Hypertext Transfer Protocol (HTTP), and Trivial File Transfer Protocol (TFTP) pose another major misconfiguration risk. Telnet, for example, transmits data in plain text that hackers can easily exfiltrate and is a prime target for credential stuffing. And TFTP doesn't use encryption, access control, or authentication controls, making it suitable for publicly available information only.

6. UNPROTECTED FIREWALLS

Firewall settings must be proactively and securely configured or else they can become an easy access point for cyber criminals. Organizations can use network scanning tools to continuously search for misconfigured firewalls, allowing security personnel to act fast and close potential attack vectors.

7. INCOMPLETE NETWORK MONITORING

As modern enterprise networks become increasingly large and complex, the risk of incomplete network monitoring is much more rampant. Without a complete view of your network, you can't be sure of what—or who—is present on it. Change monitoring is only an effective cybersecurity control when the entire network and its traffic is known.

8. UNMONITORED FILES AND FOLDERS

Files and folders are another potential open door for cyber criminals if they aren't configured securely and monitored closely. When organizations monitor continuously for suspicious changes to files and folders, they can catch and correct unwanted changes before a breach occurs. File integrity monitoring (FIM) is an essential security control for differentiating between good changes (such as patches) and changes that increase cyber risk.

DID YOU KNOW?

The National Security Agency (NSA) cites misconfiguration as the most prevalent type of cloud vulnerability.[6]

9. UNSECURED API INTEGRATIONS

Application Programming Interface (API) integrations can contain misconfigurations on the network level, application level, and everything between. Some examples of API misconfigurations can be found in the absence of Transport Layer Security (TLS), incorrect sharing policies, outdated and unpatched systems, and cloud service permissions. API misconfigurations can be exploited using credential stuffing, code injection, server-side request forgery (SSRF), and other tactics.

10. DISABLED SECURITY CONTROLS

Disabled security controls are one way human error creates exploitable misconfigurations. While employees are less likely to disable such controls with bad intentions, the truth is that security controls can be seen as an inconvenience. An end-user with local admin access might temporarily disable antivirus, for example, because they need to do so to run an installer. Re-enabling it may not be top-of-mind for that employee, especially if your organization doesn't conduct regular security training to instill the right mindset.

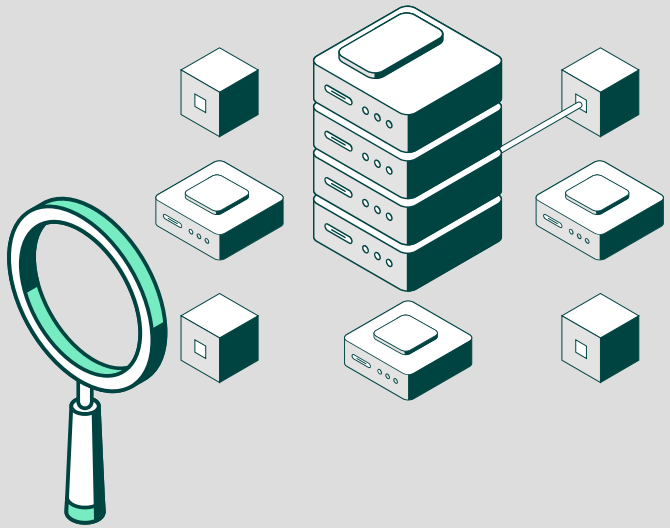
How to Prevent and Correct Security Misconfigurations

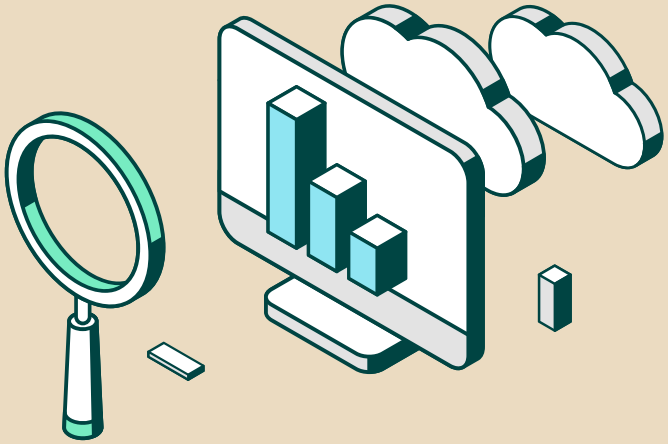
It's important to continuously monitor for misconfigurations and get alerted so you can close gaps in your armor before bad actors take notice.

A successful SCM program is made up of several independent processes that work together to shrink an organization's attack surface for maximum levels of security and uptime.

ACCURATE ASSET INVENTORY

Getting a comprehensive view of devices and software on your network provides the foundation for effective SCM and compliance. Simply put, you can't scan it if you don't know it's there. Asset inventory also includes identifying active applications, open ports on the network, running services, and more.



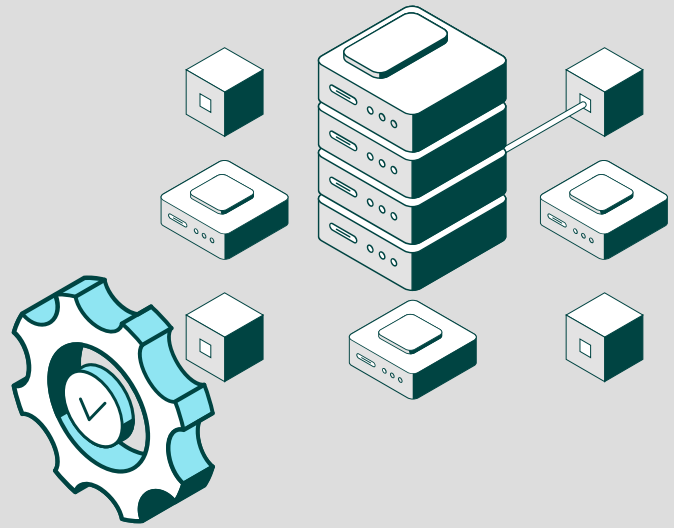


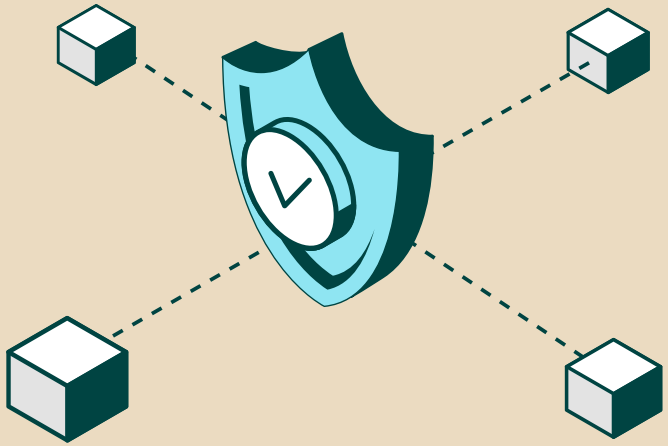
CONTINUOUS, AUTOMATIC MISCONFIGURATION DETECTION

Continuous monitoring against a secure baseline is the core of any powerful SCM solution. You can also use automated tools to fix misconfigurations before bad actors find them. Continuous monitoring gives organizations deep, unparalleled visibility into the security of their systems and clear information on current misconfigurations—and how to fix them.

ALIGNMENT WITH ESTABLISHED BEST PRACTICE FRAMEWORKS

Most industries are mandated to follow regulatory compliance frameworks such as the Payment Card Industry Data Security Standard (PCI DSS). But in addition to mandatory requirements, there are also voluntary best practice frameworks that anyone can use in the same way to strengthen overall cybersecurity at their organization, including the Center for Internet Security's CIS Controls, MITRE ATT&CK, and the National Institute of Standards and Technology (NIST).





A CULTURE OF CYBERSECURITY AWARENESS

Employee training is essential in creating a cyber-aware culture at your organization. Each employee should feel confident about knowing how to spot and respond to suspicious activity. Employees should also understand the importance of established policies on passwords, MFA, and other security protocols.

Fortra's Approach to SCM

Fortra provides fully integrated solutions for compliance, file integrity, and security configuration management across your entire digital environment. Our solutions lead the way in SCM using unparalleled asset discovery, baselining, change management, policy enforcement, and remediation capabilities.

Fortra's Approach to SCM

ASSET DISCOVERY

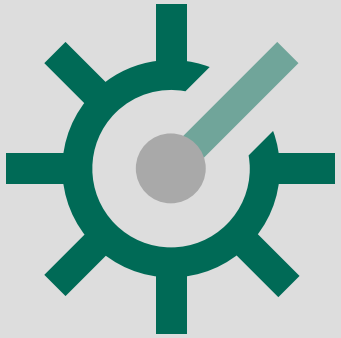
Fortra provides thorough and accurate asset discovery across on-premises and cloud environments. Discover devices, hosts, applications, services, and ports to give you total visibility into your organization's assets (authorized and unauthorized) along with their potential misconfiguration risks. In the cloud, it classifies and scans new assets when they connect in dynamic environments and delivers a baseline state to monitor those cloud assets—even if they are short-lived. You can opt for automatic offboarding and set your own parameters on how long ephemeral asset data is retained.

BASELINING

Before you can identify new misconfigurations, you must first define what a secure configuration baseline looks like. Fortra's Tripwire SCM solution helps you establish a secure baseline that it uses to detect changes and change data (such as who made the change, whether it was authorized, and whether it resulted in a misconfiguration). During the monitoring process, deviations from the known baseline result in test failures—which you can then quickly remediate.

CHANGE MANAGEMENT

Fortra provides thorough and accurate asset discovery across on-premises and cloud environments. Discover devices, hosts, applications, services, and ports to give you total visibility into your organization's assets (authorized and unauthorized) along with their potential misconfiguration risks. In the cloud, it classifies and scans new assets when they connect in dynamic environments and delivers a baseline state to monitor those cloud assets—even if they are short-lived. You can opt for automatic offboarding and set your own parameters on how long ephemeral asset data is retained.



POLICY ENFORCEMENT

Tripwire has the largest and broadest library of supported policies and platforms—over 4,000 policies that cover the largest array of platform OS versions and devices. This includes best practice frameworks such as the **CIS Controls**, **National Institute of Standards and Technology (NIST)**, and more. You can also create custom policies for internal compliance rules.

REPORTING & REMEDIATION

Rather than inundating you with excess alert noise, Tripwire's clear dashboarding helps organizations identify and tackle their biggest security issues first and optimize from there. Its large portfolio of customizable, ready-to-use reports help stakeholders and auditors understand your organization's configuration state. Tripwire's remediation capability automates and guides you for rapid repair of many security and compliance misconfigurations.

TRIPWIRE ENTERPRISE

Fortra's 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.

Thousands of organizations trust Tripwire Enterprise to serve as the core of their cybersecurity programs. Backed by decades of experience, it's capable of advanced use cases unmatched by other solutions.

FORTRA™

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.

Sources

1. https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
2. https://www.verizon.com/business/resources/T750/reports/2023-data-breach-investigations-report-dbir.pdf
3. https://csrc.nist.gov/glossary/term/misconfiguration
4. https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
5. https://www.verizon.com/business/resources/Ta89/reports/2023-data-breach-investigations-report-dbir.pdf
6. https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF

fta-tw-gd-1023-r1-hm