FORTRA

Frequent Security Misconfigurations and How to Mitigate Them

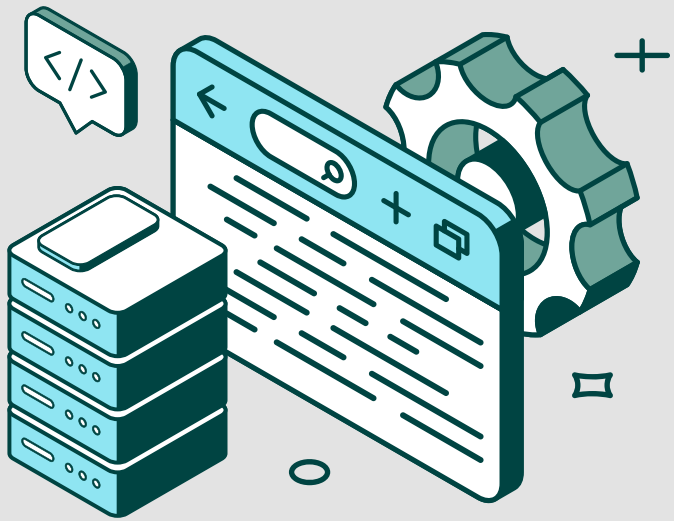
Intro

If your home alarm system is doing its job, it will sound when an intruder comes in. But if it was assembled incorrectly, it may not utter a single beep.

Even worse than having no security system is having one that you think is working – but isn't. In that scenario, you're resting easy with a false sense of security.

The same thing can happen with IT environments, whether security-based or not. Imagine if your front door was installed incorrectly, or your windows – same thing. The end result is that faulty craftsmanship leads to weak points that attackers can use to get in.

Misconfigurations in both cloud and on-prem environments create vulnerabilities that attackers can exploit. In fact, research suggests that SaaS misconfigurations account for up to 63% of security incidents. In this guide, we'll explore common ones to look out for and provide the steps you can take to shore them up before attackers find them out.



Cloud Misconfigurations

1. Misconfigured cloud storage permissions

The Problem: A lot can go wrong when setting up cloud storage repositories. This can lead to:

- Accidentally granting public access
- Granting excessive permissions
- Storing private encrypted keys in publicly available places

A Gartner survey noted that eight out of ten security breaches arise from misconfigurations, and predicted that through 2025, 99% of cloud security failures "will be the customer's fault." This is something to take heed of 0020, as many cloud customers are under the assumption that a cloud services provider (CSP) will provide all the security protections they need.

The truth is that cloud security operates under a shared responsibility model in which the CSP provides a basic level of cybersecurity, and the customer is accountable for the rest. Configuring security settings is often within the direct purview of the customer, encompassing firewalls, databases, services, and storage in the cloud. However, on-premises skillsets do not always transfer directly to the cloud, and it is easy for errors to be made by the untrained. Cloud security experts are needed to ensure proper cloud configuration. For this reason, many teams turn to managed security service providers when implementing strategic cloud security.

The Impact: The impact can be disastrous; take this example from an online software development storage and collaboration platform. Last year, 12.8 million secrets were leaked on GitHub. Per Bleeping Computer, "The exposed secrets include account passwords, API keys, TLS/SSL certificates, encryption keys, cloud service credentials, OAuth tokens, and other sensitive data that could give external actors unlimited access to various private resources and services, leading to data breaches and financial damage."

In this case, the GitHub repository was forked, meaning that a new copy of the original GitHub repository was created. When this copy was created, certain environmental variables were also copied over to the forked repository - including secrets like API keys, passwords, and tokens. Considering this, all attackers would need to do is find a vulnerable repository and fork it if they wanted to steal the sensitive information inside.

In another example, a misconfigured AWS S3 bucket led to a high-profile airline breach in which 23 million files were left unprotected, source code was exposed, and sensitive flight data was leaked. According to the Safety Detectives cybersecurity team, this included "software...[used] for aircraft navigation, takeoff/landing, refueling, safety procedures, and various other in-flight processes." Noted the researchers, "These files were left accessible and could allow anyone to delete, modify, or upload data to additional encrypted or password-protected databases, files, and folders on the bucket."

Perhaps nowhere is a defense-in-depth approach more valuable than in a cloud environment, which is why it is crucial for organizations to carefully consider their part of the shared responsibility model and plan accordingly.

TLDR: Organizations need to approach cloud security with eyes wide open, realizing how much of it is their responsibility. Cloud misconfigurations can result in millions of dollars in losses; regularly conducting security audits with automated scanners can help proactively identify these issues before an attacker does.

2. Insecure API management

The Problem: According to Broadcom, 88% of organizations use APIs. And for good reason—they enable companies to scale quickly, interface with other technologies and platforms seamlessly, and scale quickly without changing an organization's underlying systems, they continue to be a popular choice among developers. Companies earning more than $10 billion annually claim to manage over 1,400 APIs overall, and another figure indicates that APIs underpin nearly 40% of an organization's revenue-generating digital assets. Needless to say, the market (and the attack surface) is saturated with application programming interfaces, and not all are properly protected.

Shadow APIs are a pernicious threat, originating innocently as forgotten test APIs or legitimate APIs that are no longer in use. These old APIs – unprotected yet still capable of connecting to sensitive data, in many cases – are hot targets for today's attackers. In 2023, 29% of all web attacks targeted APIs, and a 2022 report noted that 31% of all malicious requests were aimed at unknown and unmanaged APIs.

Per the report, web-based API threats typically include:

- Cross-site scripting
- SQL injection
- Session hijacking
- Data harvesting ploys

While common API runtime problems encompass:

- Unauthorized attempts to access critical data
- API requests containing malformed data
- Data scraping attempts
- API activity with unexpected data types

The Impact: In May of 2024, a threat actor created a fake business account and scraped a Dell partner portal API for no less than 49 million customer records. The API gave up so much information because it was not only (too) easy to access, but no rate limiting was applied. The siphoned data included a catalog of purchases for millions of monitors, notebooks, desktops, and more, and was eventually sold on a hacking forum.

API attacks don't stop at mere data exfiltration alone. Designed to be a multi-vector point of connection, cybercriminals have long since abused Microsoft Graph API to establish covert channels of communication for nefarious purposes. Once compromised, they use it to "facilitate communications with command-and-control (C&C) infrastructure hosted on Microsoft cloud services."

Forgotten in the rush of API creation, testing, and deployment, lingering APIs are often queried for sensitive information because they lack proper authentication and access controls. Due to their rare role in connecting applications, services, and systems, these computing "nerve centers" have the capability to severely cripple an enterprise if exploited.

TLDR: APIs are nearly ubiquitous among digitized entities today, and form an integral part of flexible, scalable growth. Because of their function as multi-faceted communication hubs, they are high-value targets for attackers seeking to exploit them for access to sensitive information. Proactive security techniques like vulnerability management and penetration testing can help discover unprotected APIs and secure them.

3. Improper identity and access management (IAM)

The Problem: One reason that IAM is so tricky in the cloud is the sheer level of complexity afforded by the cloud; another is the amount of access given by cloud-based credentials. Usernames and passwords have become targets of even higher value in recent years because they sit in front of SaaS applications that are tantalizingly connected to a myriad of cloud resources back-end. Now, attackers could breach a connected app and end up nearly anywhere in the enterprise's cloud estate given the right lucky breaks. And because cloud security configuration, visibility, and permissions also struggle under the same load of complexity, those breaks are often easy to come by.

Additionally, the rising tide of machine identities – or services used to communicate with other services – adds an additional opportunity for weak IAM to lead to high-value hacks, as these entities often have elevated permissions. And when you factor in multi-cloud environments, the nuances of identity and access management between the different providers can also provide a point of weakness in which attackers can gain the advantage if organizations aren't completely cyber-savvy as to the distinctions.

The Impact: When your IAM system is configured incorrectly, you're often the last one to know. Meanwhile, attackers can crack poor authentication methods and run around your internal systems disguised as "authorized" users. This leads to a host of troubles, including:

- **Insider threats**, or something that functions very much like them. With their "unauthorized access" - which looks authorized because they've taken over a legitimate account – they can escalate privileges, exfiltrate data, and do much of it without sounding any alarm bells.
- **Business Email Compromise (BEC)**, or disguising oneself as a legitimate client, coworker, or even employer and duping an unsuspecting user into transferring money for "business purposes," when in reality the funds go directly to a cybercriminal. Hacking an email account gives the threat actor the ability to send messages as a clean fellow employee, adding credibility to the ruse.
- **Compliance consequences** when your IAM practices fall below industry or regulatory standards. This can result in the usual litany of fines, penalties, failed audits, reputational damage, and loss of trust both among potential partners and current customers.

Identity-related attacks are only growing as organizations invest more in remote and cloud resources. With the latter trends not showing signs of stopping, organizations need to find ways to find and shore up instances of weak authentication within their environments.

TLDR: Decentralized cloud resources make identity and access management harder than ever as teams seek to manage different rules in different environments. All too often, things slip through the cracks and attackers are able to gain access to a myriad of cloud-hosted resources via a single cloud login. To combat this, organizations can leverage penetration tests to proactively identify improper IAM configurations.

On-Premises Misconfigurations

4. Misconfigured firewalls and open ports

The Problem: The rules of a firewall are designed to keep out malicious traffic, but if these rules are configured incorrectly, all bets are off. The same goes for ports that should be closed (to protect against dangerous probes) and aren't.

When configured correctly, firewalls generally do their job of examining data packets and weeding out the ones that are harmful and unauthorized. There are some highly sophisticated threats that manage to sneak by, but the statistics indicate that those count for the vast minority of successful attacks. According to Gartner, 99% of firewall breaches between 2019 and 2023 were due to firewall misconfigurations, not firewall flaws.

Unfortunately, even when firewalls are configured correctly, open ports can allow attackers to go around them and infiltrate the network directly. Open port vulnerabilities can result in:

- Credential-stuffing attacks via an open RDP connection
- SQL injection and cross-site request forgery attacks via open web service ports
- Man-in-the-middle attacks re-routing unencrypted traffic on exposed ports (like email traffic)
- Denial-of-Service (DoS) attacks which jam web ports to disrupt a particular service
- The Impact: A misconfigured firewall or open port can give threat actors blatant access to your network, resulting in:
- The probing and pinpointing of network weaknesses
- Exploited software vulnerabilities
- System takeover
- Eavesdropping on running services

Misconfigured firewalls and open ports are not a new issue—but they remain a dangerous one. Perhaps one of the highest-profile examples is when a breached firewall at CapitalOne compromised the information of roughly 106 million customers. The data included Social Security numbers and bank account numbers and caused an immediate 6% dip in the company's stock price when the market opened the following Tuesday. The incident was noted by the Associated Press as being "among the largest security breaches of a major U.S. financial institution on record."

Perhaps the most critical danger of open ports and misconfigured firewalls is that all the while teams are operating under the assumption that their assets as safe—and this disconnect between perceived and actual security status can have severe consequences. As organizations add new assets, it's important to keep in mind that this can potentially disrupt or affect the established configuration of other tools. So it's never a bad idea to ensure that the foundational staples of IT infrastructure are still secure.

TLDR: Improper configuration is one of the leading causes of firewall breaches, vastly more so than built-in flaws. Even when firewalls are properly configured, open ports can undermine network safety by providing attackers with open and unauthorized access. Implementing a regular vulnerability management program and performing penetration tests can help teams identify these weaknesses before they are forgotten.

5. Outdated or Unpatched Software

The Problem: Unpatched software vulnerabilities have always been a problem, but in today's technological climate, they can do more damage than ever. The Verizon 2024 Data Breach Investigations Report noted that vulnerability exploitation in 2023 was nearly three times (180%) what it was in 2022.

When used in the right hands—yours, the security practitioner's—vulnerability scanning is great, even recommended. But in the wrong hands, it proves disastrous. As we all know, AI is being weaponized by both sides. The numbers indicate that many organizations are being subjected to vulnerability scans whether they know it or not. The question is, by whom?

The Impact: As early as 2019, a Ponemon report noted that 60% of breach victims admitted they were compromised due to vulnerabilities they knew about and failed to patch. Imagine how many more had vulnerabilities they knew nothing about. Now imagine how many more applications, services, software, and devices are in use today, a half-decade later, and the impact they have on the number of vulnerabilities that could be out there today. One industry report notes that unpatched vulnerabilities as old as 2017 are still being exploited in a wide array of attacks.

As we've seen, one weak link can bring down the entire chain. The 2017 WannaCry event was a prime example. Hitting hundreds of thousands of computers around the world, the ransomware exploited a Microsoft vulnerability for which a patch had been offered two months prior. Knowing about vulnerabilities is the first step, but it is not enough. To be effective, a complete cybersecurity strategy needs to regularly patch, manage, and mitigate them as well.

TLDR: Attackers often look for the low-hanging fruit, and unpatched software is a particularly susceptible target. Even vulnerabilities as much as a decade old are more are still being exploited, compromising organizations that have long since forgotten about them. Proactive measures like a patch management program, vulnerability scans, and penetration tests can be put in place to ensure that in a climate of rapid development, outdated software and unpatched vulnerabilities don't get left behind.

Mitigations

While the problems may be diverse, the answers can be contained in Fortra's range of cloud-ready solutions. Because the demands of securing a cloud environment can be much more exacting than the demands of protecting an on-premises environment, organizations need tools that can operate at the cloud level so that both environments can be secure.

Organizations need a security strategy that leans on automation and cutting-edge research to keep ahead of misconfigurations in the cloud, on-premises, and anywhere. Fortra's vast portfolio of best-in-class tools provides the key.

1. Fortra VM | Vulnerability Management

To stay ahead of firewall changes, updates, and the errors that can occur, it is essential to have a habit (quarterly, if not more) of vulnerability scans which can catch those kinds of mistakes. A good VM program will give teams early visibility into any outdated or unpatched software components, identify rogue APIs, and find open ports and misconfigured firewalls. Fortra VM comes equipped with in-depth features suited for finding vulnerabilities across cloud or on-premises environments, including:

- The ability to **identify trending vulnerabilities** used in today's attacks so companies can prioritize the most likely vectors first.
- A **network map** of your total assets and overall security posture. Customize the map with network asset scan groups and single out subsets to view their collective risk.
- **Peer insights** to see how your security risk levels, vulnerability management program, and threat priorities stack up to others in the industry.
- A customized **Security GPA** score to help benchmark baselines and measure improvements other systems may overlook.

With Fortra VM, security teams are not only able to gain transparency into their vulnerability landscape but prioritize remediation based on the severity of the CVEs and create simple, powerful reports that can make the business case to the C-suite.

This process can be implemented as part of an overall Security Configuration Management (SCM) approach. For organizations that handle a large number of assets across a digital environment, this automated alternative to manually assessing, correcting, and monitoring myriads of configurations is one of the only ways teams can keep up. The ability to monitor regularly for misconfiguration prevents configuration drift, hidden vulnerabilities, and eventual exploitation.

2. Core Impact | Penetration Testing

Another tool that can provide invaluable information regarding which vulnerabilities present the highest threat is Fortra's penetration testing solution, Core Impact. Core Impact automated pen testing software walks security administrators through industry-level penetration tests, subjecting the organization to the same techniques used by today's threat actors.

Penetration testing can not only determine which CVEs are "most easily exploitable," but also help find Shadow APIs (in the reconnaissance phase), probe for improper IAM and firewall configurations, compromise open ports, and exploit unpatched software solutions so teams know which identified risks present the greatest threats and carry the greatest consequences.

Included in Core Impact are a set of advanced features, including:

- Rapid Penetration Tests (RPTs) that use automation to execute the most common and repetitive tasks of high-level pen testing so that teams can "get the job done" while optimizing resources, simplifying, and focusing on higher-level penetration testing tasks.
- An exploit library full of professionally written, commercial-grade exploits, updated constantly with new pen testing tactics as they become available for different platforms.
- Our patented Impact Agents that execute your penetration testing orders for the remote host and take care of all of the technical aspects behind the scenes, helping your team bridge the pen testing knowledge gap.

And that's not all. This centralized tool has programmable self-destruct capabilities for agents no longer in use, teaming collaboration technology that allows multiple testers to interact in the same session, and automated reporting capabilities to help prioritize remediation and prove compliance with frameworks like GDPR, HIPAA, and PCI DSS.

3. Cobalt Strike | Red Teaming

Red teaming is especially effective at providing transparency into which misconfigurations can be leveraged to do the most damage across an enterprise. With a post-exploitation agent and covert channels, Fortra's Cobalt Strike enables organizations to replicate the same advanced techniques of advanced adversaries – both on-premises and in the cloud.

While vulnerability management and penetration testing can help find misconfigurations and let you know how likely they are to be successfully exploited, red teaming opens a world of possibilities and tells you everything else an advanced attacker could possibly do with those same opportunities. Additionally, the practice of being "under attack" in creative, sophisticated ways – from social engineering to spear phishing to APTs and more – gives your team real-world experience dealing with the potential downstream consequences of misconfigurations.

If nothing else, it is a powerful object lesson of where unchecked vulnerabilities can lead, hopefully prompting a more stringent misconfiguration management strategy across your enterprise.

TLDR: As infrastructures continue to become more complex, misconfigurations will remain a pervasive challenge every organization will need to manage. A proactive strategy that layers offensive security solutions like vulnerability management, pen testing, and red teaming can efficiently identify threats to protect your critical assets. Fortra offers a single source portfolio of offensive security solutions with Fortra VM, Core Impact, and Cobalt Strike, providing a consolidated approach to help effectively manage misconfigurations while reducing the complexity that often comes with managing multiple separate tools.

Conclusion

The cloud is one of the best breeding grounds for mistakes, misconfigurations, and misplaced technologies. With Shadow IT, firewall errors, and weak authorization rampant in both serverless and on-premises environments, organizations need powerful tools able to maneuver both worlds and find weaknesses where they're least expected.

That is why the importance of continuous monitoring, proactive configuration management, and the right tooling cannot be underestimated. By anticipating the most impactful threats and errors across any environment, Fortra's range of solutions, from vulnerability assessment to penetration testing, helps arm today's organizations with the technologies they need to secure both cloud and on-prem infrastructures.

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.

fta-ip-gd-1124-r1-db