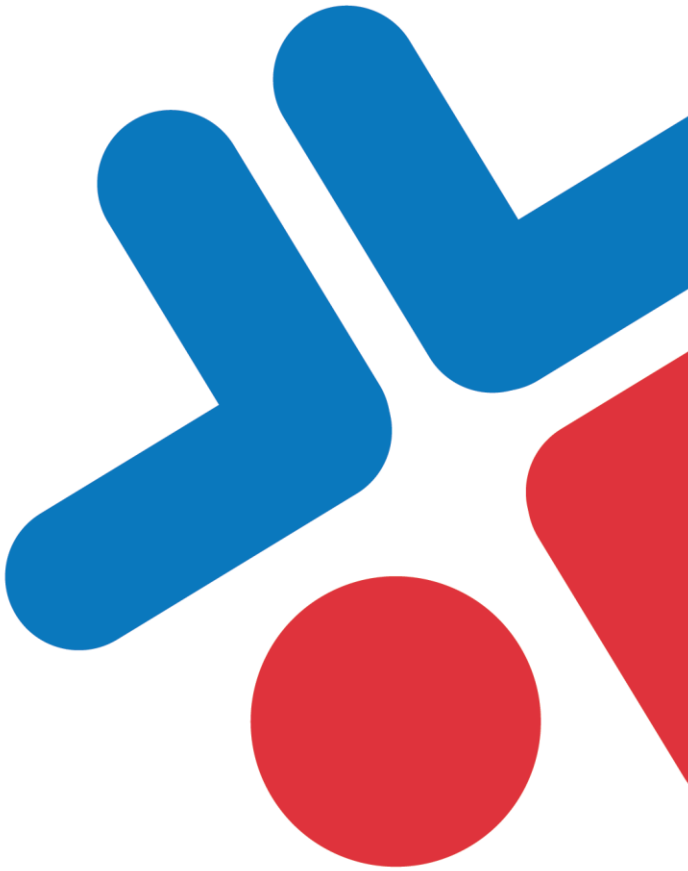
netwrix
#1 for change auditing

The Audit Zone: Five Stories of Suspense and Security



www.netwrix.com | **Toll-free**: 888.638.9749

Table of Contents

Introduction

You're traveling through another dimension, a dimension not only of operations and technology, but of security; a journey into a strange land whose boundaries are that of compliance and policy. That's the signpost up ahead – your next stop, the Audit Zone.

These days, the IT department can't just focus on keeping servers up and running, getting users the access they need, and bringing new services online to benefit the business. IT is, unfortunately, also the last line of defense in the organization's security compliance. Whether your organization needs to meet external legislative or industry rules, or you simply have a strict internal set of security policies, making sure you're compliant is an absolute requirement of the modern IT environment. With good reason: Failing to enforce those security policies can result in significant damage.

Unfortunately, the native security tools in Windows, SharePoint, Exchange Server, SQL Server, and so on don't always provide the robust level of auditing, reporting, and alerting that you need to make sure your security is in place at all times, and that it's being managed properly.

In a way, that's what IT security all comes down to, really: Auditing. Keeping track of what's in place, what's changing, and what's happening.

Welcome to the Audit Zone.

Story #1: The Thief in Broad Daylight

Martin knew it was going to be a rough week when the suits started running around first thing Monday morning, speaking in urgent, hushed tones. It hit the news on Wednesday: Some of the company's most critical intellectual property, the real details about their new and as-yet-unreleased product, had leaked to the competition, who was rapidly modifying their own upcoming product to squash any competitive advantage Martin's company might have had. The stockholders were screaming for someone's head, and management was looking for the culprit.

They started with the security cameras, and after reviewing a few evenings' worth of footage, decided that it had probably been an inside job. As word spread through the office grapevine, Martin simply put his head down on his desk and moaned. He knew what was coming next.

"Martin," his boss asked, strolling into Martin's cube, "can we talk in my office for a minute? It's about the leak," he finished ominously.

Safely ensconced in his boss' office, Martin admitted that there was almost no way to know who had last accessed those files. The problem, Martin said, as that the files' current Access Control List (ACL) contained a domain user group that definitely should not have been there. Having that group on the ACL, Martin explained, gave almost the entire company read-only access to the file. And no, he added, there was no way to determine who had modified the ACL. The company simply didn't have the tools in place.

"That stuff isn't logged?" his boss fumed.

Martin admitted that it was, but said that it had happened long enough ago that the records had been overwritten by now. He explained that the Windows-based file server they used simply didn't provide any capabilities for archiving security logs. In reality, events only stayed in the log for a few days. Someone had clearly been planning this for a while, and had modified the permissions first – then just waited until they were likely to have been overwritten before using those new permissions. They could have then easily copied the files whenever they wanted to – right during the regular work day – and never have been caught. The company didn't currently log each and every successful access to every file, since doing so would generate an enormous amount of log traffic, causing log entries to be overwritten that much more quickly.

Martin left his boss' office with a firm directive to find a way to rectify the situation. He needed a way to permanently archive security entries, and he was really hoping to find a way to get real-time alerts as soon as permissions on critical files, or changes to critical groups, were made. He also needed a better way to search through the mass of entries in each security log to find specific activity, if this happened again

Story #2: Laziness Sinks the Audit

"We just failed our corporate security audit!"

Jennifer's boss was furious. His face was beet-red, and that one vein on his forehead was threatening to explode, it was bulging so much. With good reason: Not only had IT failed a security audit, they had failed it on something stupid. Rather than the strong password policy that domain was supposed to have, the auditors discovered that the password policy had essentially been turned off. For an unknown length of time, users' passwords hadn't been expiring. Now, not only did they have to correct the policy – easy enough – but they'd probably start fielding an enormous volume of help desk calls as users' passwords expired simultaneously. That's not what her boss was most concerned with, however.

"Who did it?!?!"

Jennifer looked at her coworkers. The company had more than two dozen people in the super-trusted Domain Admins group, and any of them could have made the change. The password policy was defined in a top-level Group Policy object (GPO) that contained thousands of other settings. All of them made changes to that GPO almost weekly, and while they audited access to it, the audit long didn't contain any information about which settings were changed. Any of them could have done it – even accidentally – and there would be no way of proving it. Joachim, one of the newer administrators, nervously explained this to their manager, who wasn't happy about it.

"So," he said slowly, "someone either accidentally or deliberately modified this setting, and we have no way of determining who." Everyone in the room nodded. Even though they archived the Windows security logs, combing through months of back logs from two dozen different domain controllers was impractical at best, and even then the logs wouldn't contain the information they needed.

"Nobody wants to volunteer? Come clean?" the manager asked. Nobody did. In the past three months alone they'd lost four administrators, and it was easy enough to put the blame on one of them. "Any suggestions as to why someone would do this, if it wasn't an accident?"

Jennifer shrugged. "They were probably dealing with a user who couldn't make up a complex-enough password. Easy enough to shut off the policy. Some of us have done that in the past to get a user back online quickly, and then turned the policy back on afterwards and worked with the user to get the right password in place. Maybe someone just forgot to turn the policy back on." Not exactly what he'd wanted to hear, Jennifer guessed, seeing his face take a deeper shade of red.

She knew her company needed better auditing capabilities, specifically of what was changed in a GPO, when the change happened, and who made it. They also needed a better way of storing the log events, so that they could quickly narrow down to just GPO modification entries – preferably without having to search each domain controller's log independently.

Story #3: The Trouble with Tribbles Virtual Machines

It's never a good day when your performance monitoring system starts sending out panicked emails and text messages, and it's an even worse day when the subject of those alerts is the company's core virtual machine infrastructure. John met six of his fellow administrators, each bolting for the datacenter with a single, shared purpose: To find out why the monitoring system was telling them that the company's for main virtualization host servers were metaphorically melting into pools of goo because they were being seriously overworked. Four admins each logged onto a different host server's console, while the other three pulled up the monitoring software to find out what was happening.

"Why am I seeing two hundred virtual machines on here?" Keith asked, aghast.

"I've got one-fifty," John said, staring at an impossible number of running virtual machines. "And we're overcommitted on memory by a factor of six. I don't even know what most of these things are for," he added. He started to shut down the virtual machines he wasn't familiar with, trying to get the server responsive again.

"The dates on these are pretty old, but it looks like they were all started up just a few minutes ago. They're all running Windows 7?" another admin said, confused. "Since when did these servers become part of a virtual desktop infrastructure?"

"Never," growled John. "We only run virtualized servers on these. This one's our Exchange Server, for pity's sake – nobody's getting email right now."

"They're also not getting into the corporate apps," Juan piped in, furiously typing at another console. "This host has a hundred extra virtual machines on it, and none of them are moving. I'm trying to shut them down as fast as I can, but I'm not getting a lot of responsiveness."

A few hours later, with the virtualization hosts running smoothly again, the team met to discuss what had happened. "Where did all of those virtual machines come from?" John asked, opening the conversation. Everyone shook their heads; they had no idea. "Don't we have any kinds of logs?" More head-shaking. "We're going to have to review who has permission to create VMs, and go talk to everyone."

"At this point, nobody's going to confess," Juan said. "They probably know this was their fault."

"Well what else can we do? Management is demanding answers, and other than interviewing everyone – which is about six dozen people, by the way – we have nothing to show them."

The team nodded sadly. It was going to be a pretty awful week. What they needed was some actual audit logging on those virtualization hosts. A centralized, consolidated log that could quickly show them who'd been creating hundreds of new virtual machines on those hosts, and perhaps more importantly who had started all of those virtual machines at practically the same time.

Story #4: Mindreading… or Malfeasance

"Tom, I just got off the phone with the Securities and Exchange Commission, and they have a few questions for us." Tom gulped. He was in the CEO's office, and the CFO and CTO were right there with him.

"Questions about what?" he asked.

"Well, they're accusing us of some rather serious violations, including insider trading. This is still confidential – well, as confidential as it can be since it appears that the word is out – but I'm going to be resigning from the company next month. Nobody apart from my colleagues here," he added, indicating the CFO and CTO, "knew about this. I haven't even presented my resignation to the board. And yet the board does know, the news has made it out to the analysts, and our stock has been taking a major hit because we didn't have the opportunity to present this in a positive light."

"Um, okay," Tom stammered.

"We'd only discussed this in person and in a few emails between us," the CTO said gently. "Is there any way someone could have accessed those emails without our knowing."

Tom nodded. "Absolutely. A lot of the permissions in the Exchange Server are pretty messed-up. You guys had asked us to give your assistants permission to access your mailboxes when you were out of the office, and the permissions on your mailboxes in particular are pretty complicated. It's possible one of them, or someone else, has the ability to get into your mail." The three executives stared at Tom.

"We trust our assistants," the CFO said, "but who else might have permissions."

Tom shrugged. "I can look, but I'm not the only one who can modify permissions. It's possible to put someone on the allowed list, let them access your mailbox, and then take them off. You've had us to do it before when you needed something but couldn't get in remotely."

Tom's CTO rubbed his eyes. "Okay, well, can we check the logs and see who has been accessing our mailboxes?"

Tom fidgeted. "We really don't capture that information in the logs. It's kind of difficult to do natively, and there's no way to really pull a report or anything out of the logs anyway."

The executives looked at each other. "We'll deal with this, then," the CEO said. "But Tom, start finding a way to make sure this never happens again without our being able to find out who did it. And fix up those mailbox permissions right now."

Tom's going to be shopping for an auditing solution that can not only capture that non-owner mailbox access activity, but actually report on it quickly and accurately. He'll also want something that can catch mailbox permission changes, perhaps alerting him when permissions on those sensitive mailboxes are changed in the future.

Story #5: A Trojan for All

"Linda, I've called you in because you've been with the company for a long time, and I trust you. What we discuss right now needs to remain confidential."

Linda nodded. She'd never seen the IT director look so serious. "What's the matter?"

"We've noticed a few unusual things happening throughout the environment. Things being changed, permissions being deleted, that kind of thing. We've checked the audit logs, and these things are being done by pretty much every administrator. Even you," he said. He raised his hand as Linda started to object, "No, you're not under suspicion. I had a security consultant from headquarters come and look at the servers. He found a Trojan of sorts installed on all of our servers. It's a custom piece of work, because none of our anti-malware systems caught it. Essentially, every time one of you logs onto a server, this thing runs and does something under your permissions. It seems to have a very explicit set of instructions for what to do, although it also does a lot of random stuff that is making it difficult for me to figure out what its goal is."

Linda's eyes were wide. "How long has it been there?"

"We don't know," the director said, grimacing, "although I'm guessing for about six months. You remember when all of those bogus logins were created on the SQL Server machines last April?" Linda nodded. "We think that was one of its first major actions. That looked like Stacy made the changes, but she swore she didn't, so we tabled the issue. Now it looks like it's this Trojan. We've uninstalled it, but I need to know if there's a way for us to find out who put it there?"

Linda thought about it, and then slowly shook her head. "The audit logs show who logs onto a server console, but that's it. We all do that, several times a day. It could have been any of us. Once you're logged on, we don't really audit any local activity – just stuff like Active Directory activity."

The director nodded. "I was afraid of that. And in the past year, we've let more than two dozen employees and contractors go, meaning this could have been set up by any of them before they left, as well as anybody on staff now. Okay – well, we've removed the Trojan, like I said. Corporate security wants us to put measures in place to make sure we can catch this the next time. Start looking for ideas."

Linda left the office, her head spinning. Back in her cube, she started trying to think of a way to capture the activity an administrator performed locally on a server once logged in. Perhaps a logon script that started some kind of monitoring agent? But installing software wasn't something she knew how to even monitor for. Maybe just looking for file system or registry changes? But logging the information into a native event log would be no good, since an admin could clear the log easily and cover their tracks. Sighing, she opened Google and started punching in keywords, hoping to run across someone who'd already figured this out.

What Linda's looking for is a solution that can audit local activity, such as software installation, registry keys, and other local configuration settings. Such a solution will need to log activity to a central database, rather than to the native logs, and provide real-time alerts for this kind of suspicious activity.

Mastering the Audit Zone

Many organizations have the mistaken belief that native auditing features will solve all of their security needs.

Not so.

Modern needs have outstripped the capabilities that the native auditing features were ever meant to provide. While the event logs in Windows, SQL Server, SharePoint, Exchange and other systems can all capture a great deal of information, they lack key capabilities that can contribute directly to the terrible situations you've just read about. The players in those tragedies are going to be looking for something more robust. Specifically, they're going to need:

- Consolidated auditing that tracks who is making what changes and where in the entire IT infrastructure: Windows, file servers, Active Directory, VMware, Exchange Server, SQL Server, Group Policy, SharePoint, and other systems.
- A single, centralized audit log with solid long-term archival capabilities.
- Rapid reporting, providing the ability to locate specific activity in just moments, answering **who**, **what**, **when**, **where** and **why** questions easily.
- Real-time alerts, calling attention to especially critical changes so that they can be mitigated or remediated immediately if needed.
- An audit trail that can't readily be cleared by the same administrators they're trying to monitor – something that the native Windows event logs can't provide.

In some cases, our protagonists are going to be looking for information that isn't captured in the native audit logs, but is instead available directly through supported, under-the-hood application programming interfaces.

They could choose to try and tap these interfaces themselves, or try to get by with the native event logs. Alternatively, they could choose to download an evaluation of Netwrix Auditor, a powerful, all-in-one change and configuration auditing solution that will fulfill their every need. Netwrix Auditor's AuditAssurance™ technology captures the **who**, **what**, **when**, and **where** for every change, in many cases also capturing a "**before**" and "**after**" values for modified settings that makes it easy to roll back unwanted changes. They'll get easy-to-understand reports that make auditing and troubleshooting accurate and fast – mastering the Audit Zone.

About Netwrix Corporation

Netwrix Corporation is the leading provider of change auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solutions with the broadest coverage of audited systems and applications available today. Founded in 2006, Netwrix has grown to have thousands of customers worldwide. The company is headquartered in Irvine, California, with regional offices in New Jersey, Ohio, Georgia and the UK.

Netwrix Corporation, 20 Pacifica, Suite 625, Irvine, CA 92618, US

Regional offices: New York, Atlanta, Columbus, London

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-318-0261