netwrix
#1 for change auditing

2014 SIEM Efficiency Survey Report

Hunting out IT changes with SIEM

74%

OF USERS ADMITTED THAT DEPLOYING A SIEM SOLUTION DIDN'T PREVENT SECURITY BREACHES FROM HAPPENING

Contents

Introduction

Security violations have become a hot topic among IT pros, for whom ensuring efficiency of security policies has always been a stumbling block. Devastating consequences of information leaks affect the whole society and demonstrate how vulnerable IT infrastructures are and how easily sensitive information can be compromised.

800

OF IT PROS HAVE BEEN INTERVIEWED

30+

INDUSTRIES COVERED

72%

OF COMPANIES ARE SMBs

Ensuring the security of the entire IT infrastructure should become a priority of the highest level to all organizations, no matter whether they fall under compliance regulations or not. Compromised sensitive information like personal data, Social Security numbers, health information, credit card numbers and other data go directly to the hands of cyber thieves. Companies that experience a security breach are forced to pay huge fines for noncompliance, lose customer demand and ruin their honorable reputation; banks have to reissue millions of credit cards at their own expenses; IT organizations are frantically searching for solutions that will enforce IT infrastructure security and prevent any information leaks in the future.

More important than the risk to a company's reputation is loss of intellectual property or even

the slowdown of output, which can cost an organization even more than the penalties imposed for noncompliance. Consider the financial impact if a breach led to the shutdown of your manufacturing line. What if your competitor now has access to your future plans as well as your new product that hasn't been released yet? What would the impact be if someone were able to change all of the salaries in the organization due to a misconfigured connection to your payroll processing system? In healthcare, while privacy is important, what if the HVAC system was reversed and this allowed infectious disease transmission?

A recent Verizon Data Breach Investigations Report revealed that the majority of insider misuse results from privilege abuse and recommended minimizing access to sensitive information. Deploying a Security Information and Event Management (SIEM) solution is a bold step toward delivering visibility to your security posture. SIEM solutions allow you to look into security logs and gather information that helps manage user and service privileges, as well as identify and report on security threats and suspicious activity. Knowing what is going on across the entire IT infrastructure by continuous monitoring of changes made to system configurations and data is key when it comes to ensuring security and meeting compliance regulations.

Netwrix Corporation recently conducted a survey to find out how IT professionals are leveraging their SIEM solutions to provide visibility across the entire IT infrastructure and how this helps them strengthen IT security.

Highlights

- We have interviewed 800 IT professionals who work for companies involved in more than 30 industries, the majority of which are small or medium businesses.

- 62% of surveyed IT pros stated that they have encountered security violations of their IT infrastructures. The survey also showed that large enterprises experience security incidents more often than small and medium businesses. However, SMBs are not immune, as half of them have to deal with security incidents.

- 73% of SMBs make little effort to ensure security of their IT infrastructures and struggle to monitor changes made to sensitive information and system configurations.

- 74% of IT professionals admitted that deploying a SIEM solution didn't prevent security incidents from happening.

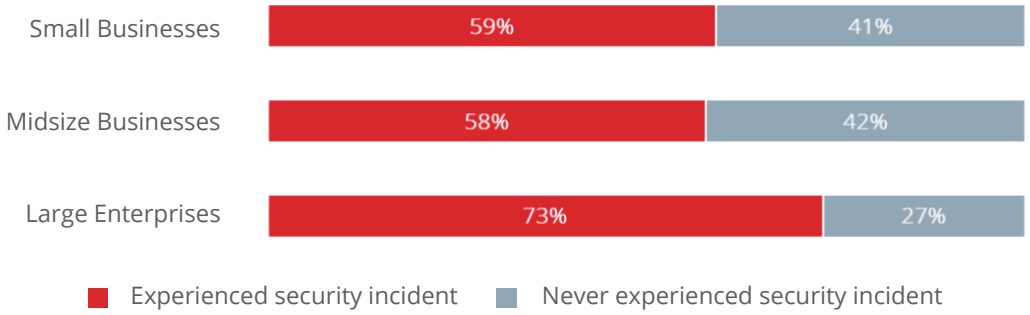
- The survey also revealed that the majority of IT pros who have a SIEM solution agreed that, when it comes to auditing changes, SIEM has noise, gaps in audited data and hard-to-read change auditing reports.

Part 1: Security Concern

Security is still an issue

The majority of IT pros interviewed during the survey stated that the security of their IT infrastructures has been violated at least once. According to the survey, more than 70% of large enterprises and more than half of SMBs have become victims of a security breach.

This fact once again proves that security incidents have become common for companies of all sizes, and IT organizations should make efforts to ensure security of sensitive information and, in case a security breach occurs, be able to quickly provide necessary information to help the investigation process.



OF IT PROS HAVE EXPERIENCED SECURITY VIOLATIONS

Industries at risk of security violations

An interesting fact was revealed when we decided to find out which industries suffer the most from security incidents. Banking, Consulting, Education, Health Care, Manufacturing and Technology turned out to be the most sensitive to security violations.

Among the companies interviewed, there are organizations that deal with sensitive information (e.g., personal or financial data) and, therefore, fall under the scope of compliance regulations; however, the majority of them hardly succeed in assuring security of sensitive data and fail to meet the requirements.

Top 6 industries most vulnerable to security incidents

19% Technology

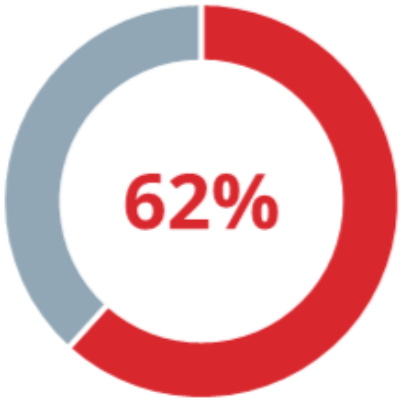
14% Manufacturing

12% Education

10% Health Care

10% Banking

8% Consulting

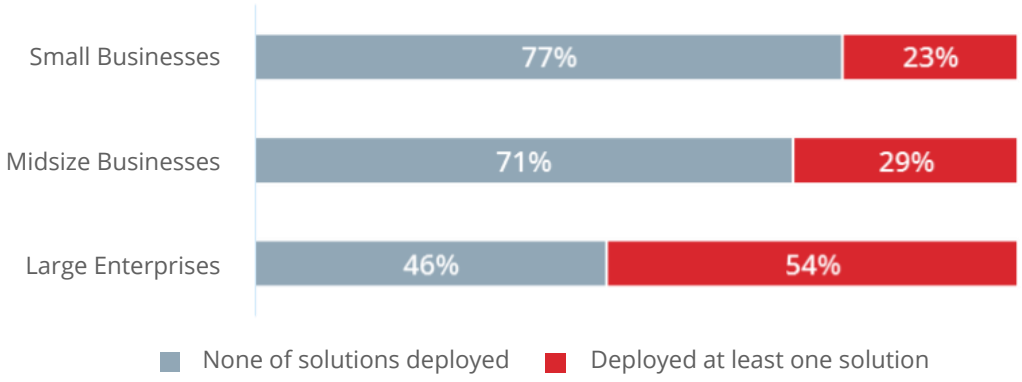


OF ORGANIZATIONS THAT ARE OBLIGED TO MEET COMPLIANCE STANDARDS STILL SUFFER FROM SECURITY BREACHES

The state of IT infrastructure monitoring

The majority of large enterprises take the problem of ensuring security seriously and make efforts to enforce their security policies with implementing either SIEM or a change auditing solution, or in some cases they take it one step further and deploy both solutions.

At the same time, small and midsize enterprises turned out to be lax about maintaining the security of their IT infrastructures, so only a third of them have taken certain steps to strengthen security by deploying an automated solution to monitor their IT systems and report on suspicious activity.



OF SMBs DO NOT MONITOR THEIR IT INFRASRTUCTURES WITH AUTOMATED SOLUTIONS

SIEM is not a magic bullet if security is a concern

SIEM is a powerful solution that allows you to collect log data from a variety of systems across the entire IT infrastructure to identify and report on security threats and suspicious activity. However, the overwhelming majority of IT pros who were asked during the survey said they still suffer from security violations, despite implementing SIEM.

Although it is a reliable solution for ensuring security and analyzing security events across the IT infrastructure, SIEM has shown itself not to be as efficient in auditing changes as it seems to be.

So let us drill down into the details and find out what SIEM solutions lack most of all and why they do not satisfy IT professionals when it comes to auditing changes.

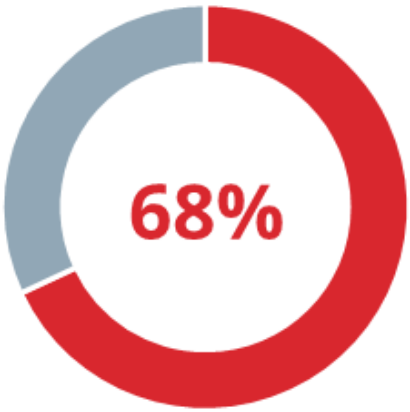
OF USERS WHO DEPLOYED SIEM STILL EXPERIENCE SECURITY BREACHES

Part 2: SIEM In Use

Auditing changes with SIEM

SIEM solutions gather and analyze information on security alerts generated by network hardware and applications, track security data logs for unauthorized access, indications of network threats, etc., and generate reports that are used to pass compliance audits by gathering logs from a variety of devices and attempting to correlate them.

Auditing changes is a key point when it comes to ensuring the security of the entire IT infrastructure, as both Verizon and Gartner acknowledge in their reports. Knowing who did what, when and where helps detect suspicious activity and prevent security breaches at early stages by tracking how often changes are made.



OF USERS WHO HAVE SIEM DEPLOYED USE IT TO AUDIT CHANGES

SIEM weak points in auditing changes

IT professionals recognize SIEM solutions as an effective security measure for ensuring the consistency of processed and archived data. SIEM helps to meet the ultimate goal of any company by providing a level of visibility and awareness to protect critical information and system configurations.

However, when used for change and configuration auditing purposes, SIEM solutions demonstrate weaknesses.

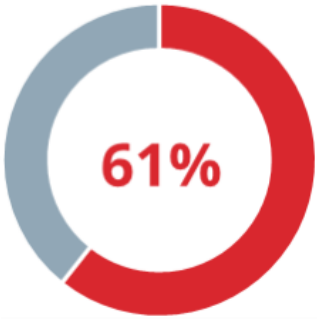
Too much noise data

The majority of respondents complain that SIEM change auditing reports contain too much noise data, e.g., many log entries for every change made to data or system configurations. Unfortunately, the need to dig through that much information will take away not only efforts but also time, which is worth its weight in gold during investigation of a security incident. Many hours are spent fine-tuning these solutions, and any reduction in noise drastically improves the visibility in the environment.

OF USERS THINK THAT SIEM REPORTS CONTAIN TOO MUCH NOISE DATA

Gaps in audited data

The majority of interviewed IT pros who had experienced a security breach stated that information on changes they get in the SIEM reports has gaps; e.g., there are no audit data for certain changes or there are no before/after values. The change auditing report doesn't contain important information, which was probably erased, overwritten or otherwise tampered with.



OF USERS THINK THAT SIEM REPORTS ARE NOT COMPLETE

Hard-to-comprehend audit reports

Among IT pros who had experienced a security incident, more than half stated that they had had difficulties reading and understanding SIEM change auditing reports. They claimed that it was not clear to them who changed what, when and where across their IT infrastructure.

OF USERS FIND SIEM REPORTS HARD TO UNDERSTAND

Part 3: Change Auditing

Change auditing proved to be helpful when investigating security incidents

Finally, we decided to find out what IT pros think of change and configuration auditing solutions. The majority of those who are already auditing their IT infrastructures appreciate change auditing and its assistance in providing complete visibility across their IT systems.

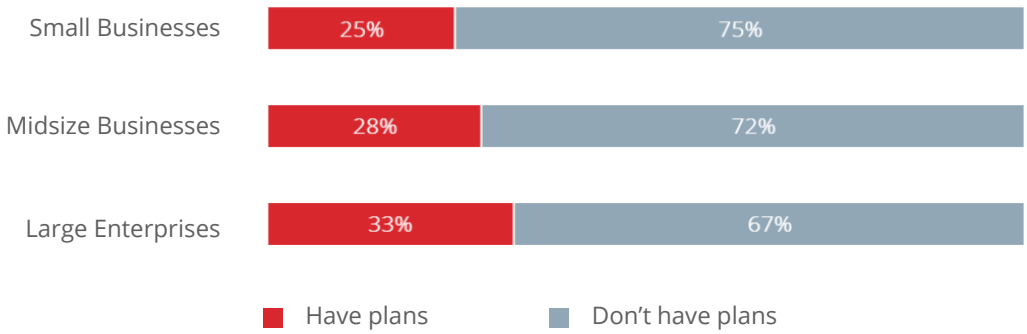
More than 70% of respondents among those who had deployed such a solution agreed that change auditing helped them when there was a need to find out details of malicious changes to data, user accounts or system configurations that resulted in a security violation.

OF USERS WHO HAVE DEPLOYED A CHANGE AUDITING SOLUTION CONSIDER IT HELPFUL WHEN DIGGING INTO BREACH DETAILS

Plans to strengthen security with change auditing

Although change and configuration auditing has shown itself to be useful when tracking changes across the entire IT infrastructure, only 28% of respondents who don't audit IT systems now are planning to do so in future and intend to deploy a change auditing solution.

Paradoxically, despite suffering from security violations and inability to know who did what, when and where across the entire IT infrastructure, organizations still struggle to implement a simple auditing solution that audits the IT systems and tracks changes to data and system configurations, thus providing IT staff with complete visibility across the entire IT infrastructure.



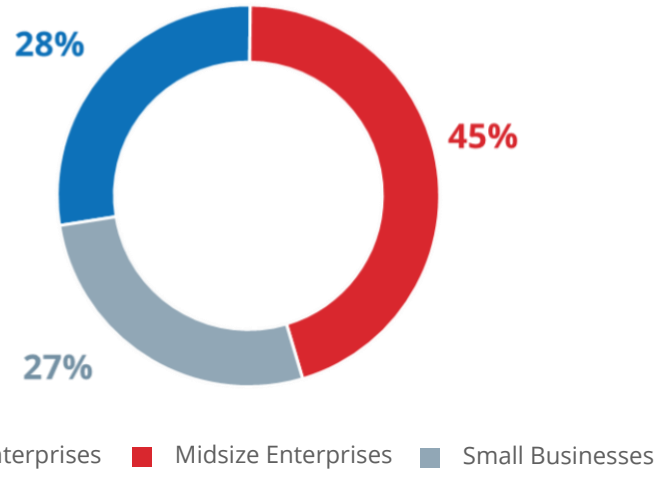
OF USERS WHO DON'T USE A CHANGE AUDITING SOLUTION ARE PLANNING TO ENFORCE SECURITY WITH DEPLOYMENT

Respondent Demographics

Organization size

We grouped organizations by size according to Gartner's* definition of small businesses (1-99 employees), midsize enterprises (100-999 employees) and large enterprises (more than 1000 employees).

The majority of IT pros work for midsize businesses, and equal shares of one third demonstrate representatives of large enterprises and small businesses.



* Based on Gartner definition of small and midsize business (SMB) by the number of employees.

Industry vertical

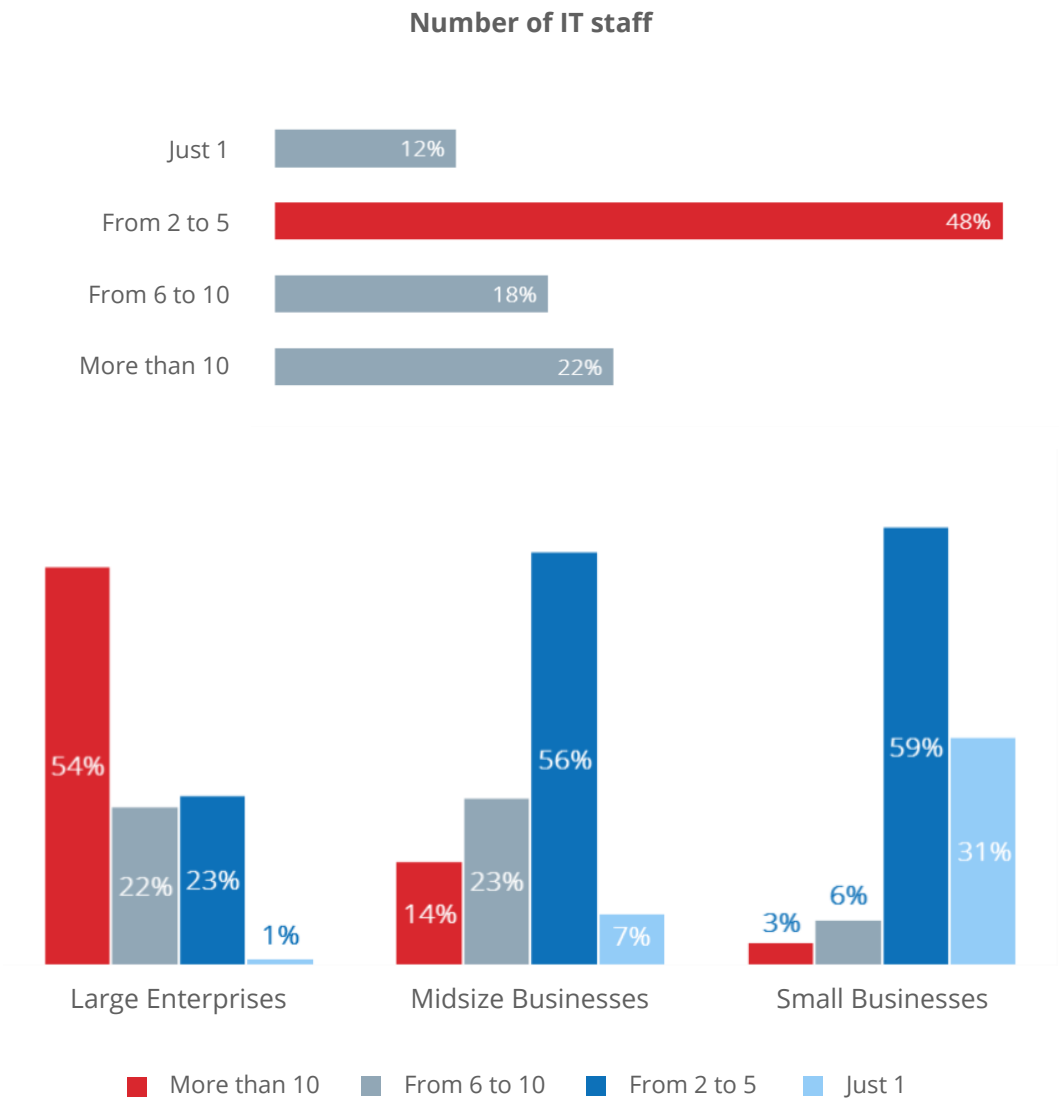
We have interviewed IT pros that represent more than 30 industries. The majority of respondents come from Technology, Manufacturing, Education, Health Care, Banking, Consulting, Retail and Wholesale, and Service.

Top 8 industries represented in the survey

OF SURVEYED IT PROS WORK FOR ORGANIZATIONS THAT ARE COMPLIANT

IT organization size

The number of IT staff varies from one to more than 10 specialists. The majority of SMBs hire from 2 to 5 employees, whereas large enterprises mostly need more than 10 IT pros to maintain their IT infrastructure.



Conclusions and Recommendations

SMBs, watch out!

The 2014 SIEM Efficiency Survey Report revealed that the majority of organizations suffer from security breaches. If large enterprises have a more responsible approach to security issues, small and midsize businesses act more carelessly when it comes to securing sensitive information. SMBs should become more proactive in establishing security policies. They should deploy a SIEM solution and enable continuous auditing of their IT infrastructures.

Compliance is not a joke

A common requirement of compliance standard (HIPAA, PCI, SOX, FISMA and other) states the necessity to regularly monitor IT infrastructure and be able to provide QSA with relevant reports ensuring that security policies in place are working. Organizations that deal with sensitive information turn out to be incredibly lax about maintaining security. They are recommended to enforce their security policies with a SIEM solution that will provide monitoring and reporting on security threats and malicious activities, thus allowing IT organizations to ensure that sensitive information is protected and pass compliance audits smoothly.

Enforce SIEM with change auditing

As the survey revealed, establishing a SIEM solution is not enough to achieve complete visibility of what is going on across the entire IT infrastructure. Too much noise, gaps in audited data and hard-to-read change auditing reports are key SIEM weak points when it comes to auditing changes. To know exactly who changes what, when and where across all IT systems and be able to detect malicious activity at early stages, it is recommended to enforce SIEM with a comprehensive change auditing solution. This will provide complete visibility across the entire IT infrastructure and add more value to an established SIEM solution.

About Netwrix Corporation

Netwrix Corporation, the #1 provider of change and configuration auditing solutions, delivers complete visibility into who did what, when and where across the entire IT infrastructure. This streamlines compliance, strengthens security and simplifies root cause analysis. Founded in 2006, Netwrix is ranked in the Top 100 US software companies in the Inc. 5000 and Deloitte Technology Fast 500. Netwrix software is used by 160,000 users worldwide. For more information, visit www.netwrix.com.

Netwrix Corporation, 8001
Irvine Center Drive, Suite 820, Irvine,
CA 92618, US

Regional offices: New Jersey,
Atlanta, Columbus, London

netwrix.com/social

Toll-free: 888-638-9749

Int'l: 1-949-407-5125

EMEA: +44 (0) 203 318 0261