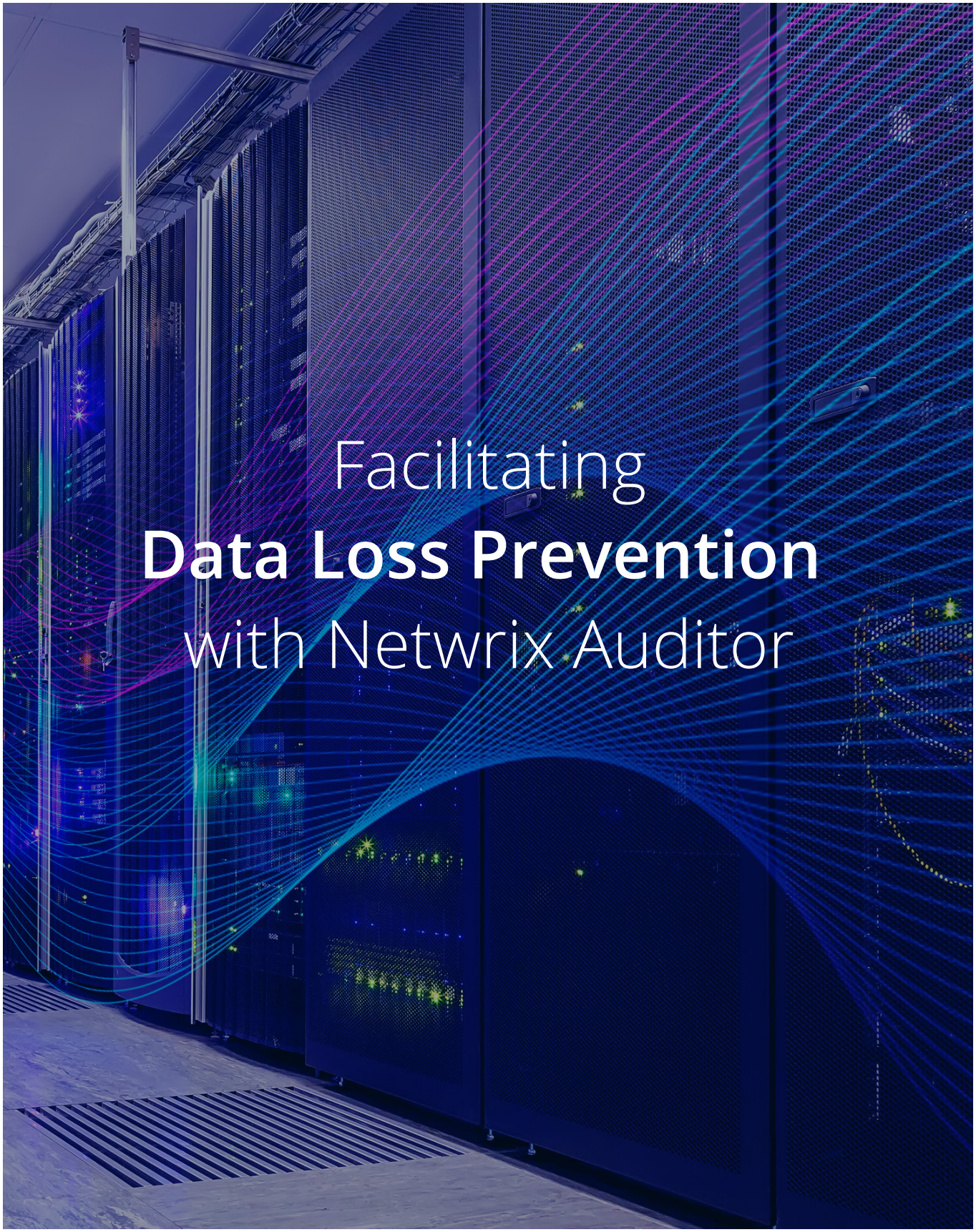
netwrix



Facilitating **Data Loss Prevention** with Netwrix Auditor

Table of Contents

Introduction

In its recent analytical report, "How to Choose Between Enterprise DLP and Integrated DLP Approaches," Gartner urges organizations to explore the data loss prevention (DLP) capabilities of the products they already have before adopting an enterprise DLP solution. By leveraging their existing solutions to their full potential, the report notes, organizations can gain visibility into and control over how users handle sensitive data. The report identifies a number of vendors who provide such solutions, sorted into categories such as Secure Web Gateways, Cloud Access Security Brokers and Endpoint Protection Products.

Netwrix is included in the list of vendors in the Data Discovery product category. But exactly how does Netwrix Auditor help with data loss prevention? And what specific functionality does it offer to aid in data discovery?

We crafted this eBook to answer these interesting questions and show how Netwrix Auditor can help your organization prevent data loss. Chapter 1 discusses what data loss prevention is and elaborates on Gartner's "integrated DLP" approach as we understand it. Chapter 2 offers specific evidence to support Gartner's characterization of Netwrix as an IT vendor that offers a visibility solution with an integrated DLP feature set, providing numerous examples of how particular Netwrix Auditor capabilities can support the DLP needs of many organizations.

1. Finding the Right DLP Approach for Your Organization

1.1 The Importance of Data Protection

You've probably seen models of the cosmos from ancient or medieval times, with Earth at the center of the universe and everything else circling it. A similar model could accurately depict the modern enterprise, with information at the center and everything else revolving around it. Together, the structured and unstructured data an organization has amassed and the tacit knowledge developed by its employees comprise one of its most strategic assets.

Accordingly, protecting corporate data is of paramount importance — how well you perform at this task can determine whether your organization prospers, decays or dies a sudden death. But it's critical to recognize that the old cliché "there is no such thing as 100% safe" reflects reality when it comes to data protection: Every business is a potential target for cyber attacks by both insiders and external malefactors. Every organization is vulnerable to data exposure. Your goal should not be to build a fortress, since it will inevitably be breached from the outside and attacked from within. Rather, your goal should be to become more resilient by building a layered defense strategy that helps you minimize your attack surface and spot suspicious behavior in time to respond effectively.

1.2 The Value and Limitations of Enterprise DLP Solutions

Even though the need to protect sensitive corporate and customer data from loss is both critical and urgent, Garner urges organizations to resist the impulse to adopt a DLP solution as soon as possible. Data loss prevention extends far beyond implementing a particular DLP technology, even if the product selected is a full-featured enterprise DLP platform. Preventing data leaks needs to be recognized as just one part of a broader corporate data security governance strategy. Therefore, before you leap into any purchases, it's critical to think through your internal requirements for data protection, clarify organizational objectives and risks, and look critically into how the new solution could be integrated into your existing security procedures. Gartner considers DLP to be not a product, but a well-defined data security process that should be bolstered by well-managed supporting technology.

One way to get some of that supporting technology is to adopt an enterprise DLP solution. These highly specialized products are designed with large enterprises in mind, so they typically offer a broad set of features, from network traffic analysis and active blocking of outbound communications to user notifications for policy violations and alerts sent to security teams about detected unauthorized data transfers. But don't mistake even the most comprehensive enterprise DLP solution for a panacea. Improving data security requires much more, such as establishing and enforcing information security policies and procedures, and gaining visibility into access entitlements, system access, data ownership, data usage and data movement. Exfiltration is the endmost link of a kill chain, and prevention shouldn't focus on that last piece of the puzzle.

Remember, data itself is not the problem in data exfiltration and loss — it's a people problem, because it is human intentions that stand behind most data exfiltration cases.

Moreover, enterprise DLP products have a reputation for being overly complex for basic use cases — a reputation that Gartner says is well earned. That is not to say these products are bad or ineffective. Rather, it means they are not always a good fit. They often fail to meet a company's expectations because decision makers fail to carefully consider their organization's specifics, such as company size, data volumes, the complexity of the networks, regulatory requirements, business objectives, and human and financial resources available for operating and maintaining the enterprise DLP solution. Instead, many purchase decisions are made in response to an immediate organizational need, such as the need to act upon an improvement notice from a regulatory compliance authority or to demonstrate a strong commitment to security after a data leak made the headlines.

Many IT managers and C-level security leaders new to DLP do not realize that enterprise DLP products will not be used to full capacity (or even to half capacity) in a low-complexity environment or one in which granular control over users and data is not required across all silos of the organization. These products, however, will likely cost as much as a little jet plane and require onerous initial implementation and further upkeep.

1.3 Why Integrated DLP Can Be a Cost-Effective Alternative to Enterprise DLP

Fortunately, organizations often have an alternative to enterprise DLP: taking full advantage of the products and applications they already have. While technologies like antivirus, firewalls, endpoint protection, IT asset management, identity management, secure web and email gateways, log analysis, data discovery, and data classification are not DLP products in a conventional sense, they all deliver data protection in one way or another. In fact, the Gartner report notes, an organization's existing products often have features that can provide business leaders with enough insight into information security gaps and deliver adequate protection for sensitive data. Gartner refers to these capabilities as "integrated DLP."

For many smaller or less complex organizations, integrated DLP is a cost-effective alternative to enterprise DLP. The DLP capabilities of the security tools the organization already owns can be equivalent to those of an enterprise product, while coming at significantly less cost and creating far less complexity. In fact, as Gartner explains, integrated DLP features can actually be superior to their enterprise counterparts. In particular, existing security tools that provide integration capabilities enable organizations to automate security processes and share data between different tools to strengthen DLP, thereby delivering functionality lacking natively in an enterprise DLP product.

Of course, budget is often the most important factor in the technology selection process at many organizations. Finding out that there is a less costly yet effective alternative to a highly priced enterprise DLP solution can be welcome news for C-level security executives — especially if they discover that they underestimated the initial investment, staffing requirements or ongoing operational costs of an enterprise DLP solution. The integrated DLP approach can offer significant savings because the initial investment costs are much smaller, or even non-existent, and the DLP-related capabilities of existing tools can be managed by the IT pros who are already using other features of the tools.

1.4 How to Choose the Best Approach for Your Organization

To determine which DLP approach is the best fit for your organization, your security and business leaders should contemplate the following questions:

- What are the objectives of having a DLP solution in place? Is it about covering your entire organization and protecting a large amount of intellectual property on multiple user endpoints, networks, and on-premises and cloud storages; demonstrating the uniformity of policies and workflows applied to data leaving the environment across all points of data egress; and complying with a wide set of regulatory controls? Or is it more about gaining better visibility into how users interact with smaller amounts of sensitive data in the context of a lower risk environment and a less demanding regulatory landscape? While enterprise DLP might seem like a reasonably effective technology in either scenario, in the second case it would be economically unjustified — you'd be spending a lot of money for functionality you'll never use while adding unnecessary complexity to your environment. Remember, there is no silver bullet when it comes to security: Not even the most comprehensive enterprise DLP solution will catch one hundred percent of attacks and make your organization immune to breaches.
- How much time, effort and money are available for the investment in DLP? Would it be acceptable if months of deployment and tuning are required before the enterprise DLP solution starts to protect data? Are the costs of initial purchase and ongoing upkeep really affordable? If not, then looking into other security tools with strong DLP functionality is obviously a good option. If the tools are already in your security arsenal, you can economize significantly on implementation, tuning, managed services, and staff costs, including hiring and training. If extra tools still need to be purchased, chance are these tools will have shorter implementation periods and a lower initial price than any enterprise DLP solution.

2. Improving DLP with Netwrix Auditor

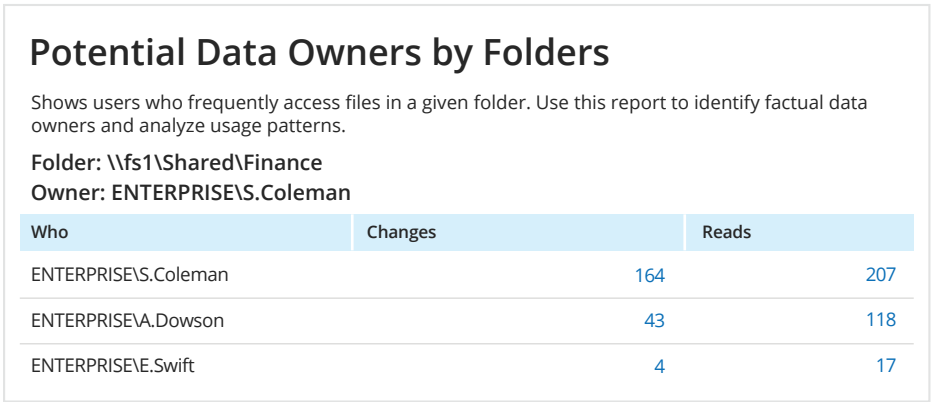
2.1 The Role of Data Discovery in DLP

As we mentioned in the introduction, Gartner includes Netwrix in its list of integrated DLP vendors in the Data Discovery category. Data discovery is focused on answering questions such as: What data does the organization have and who owns it? Where does sensitive and other valuable data reside? And who has access to which data?

Without answers to these questions, a specialized DLP solution cannot effectively interpret incidents and respond appropriately by blocking unauthorized data transfers, encrypting sensitive data flows or notifying security administrators of likely exfiltration attempts. In other words, without the results of the data discovery process, a DLP product is missing the ability to define appropriate rules and accurately apply them to data. That is why data discovery is commonly the first step in the DLP process and a necessary feature of DLP tools.

2.2 Getting the Data Discovery You Need with Netwrix Auditor

Netwrix Auditor's capabilities intersect in several ways with those of specialized data discovery tools or the data discovery modules in enterprise DLP solutions. Specifically, Netwrix Auditor provides insight into **how data is currently being used, who uses which data, who can and who cannot access data, who has excessive access permissions and who lacks access rights to which specific datasets**, as well as **data ownership details**. With this visibility, security teams can better analyze data security risks and understand whether the data is exposed or properly guarded, and how it can be lost. Moreover, Netwrix Auditor aggregates analytical insights and presents them in an easy to consume form, speeding response and lightening the load on already overburdened IT teams.



Potential Data Owners by Folders

Shows users who frequently access files in a given folder. Use this report to identify factual data owners and analyze usage patterns.

Folder: \\fs1\Shared\Finance
Owner: ENTERPRISE\S.Coleman

Who	Changes	Reads
ENTERPRISE\S.Coleman	164	207
ENTERPRISE\A.Dowson	43	118
ENTERPRISE\E.Swift	4	17

Figure 1. Reviewing who actually uses a particular piece of data helps you establish data ownership and spot improper access.

2.3 Enforcing a Least-Privilege Model

The least privilege principle is a security best practice that requires access permissions to be granted strictly on a need-to-know basis. Establishing and enforcing a least privilege model limits the amount of data that malicious insiders, attackers with compromised credentials, and malware using a user or computer account can access, minimizing data loss.

But many organizations are unable to ensure that access rights aren't assigned or delegated without proper approval and a solid business need, and they fail to regularly review permissions for accuracy and revoke them in a timely way as needed. In some cases, the organization has these information security controls but no way to enforce them; in other cases, the policies exist only in people's minds, if they exist at all. As a result, unnecessary access entitlements and lingering excessive permissions put the security of sensitive data in jeopardy.

Netwrix Auditor closes the awareness gap between provided access permissions and user activity, and helps security administrators establish and enforce a least privilege model. It provides a full holistic view of the current state of privileged access entitlements and makes it easy to track how privileges have changed over time for a particular user or data object. Furthermore, it saves a history of all past states of permissions, and enables easy comparison of the current state with any past state or the baseline configurations. This visibility helps you identify suspicious changes that could pose a risk.

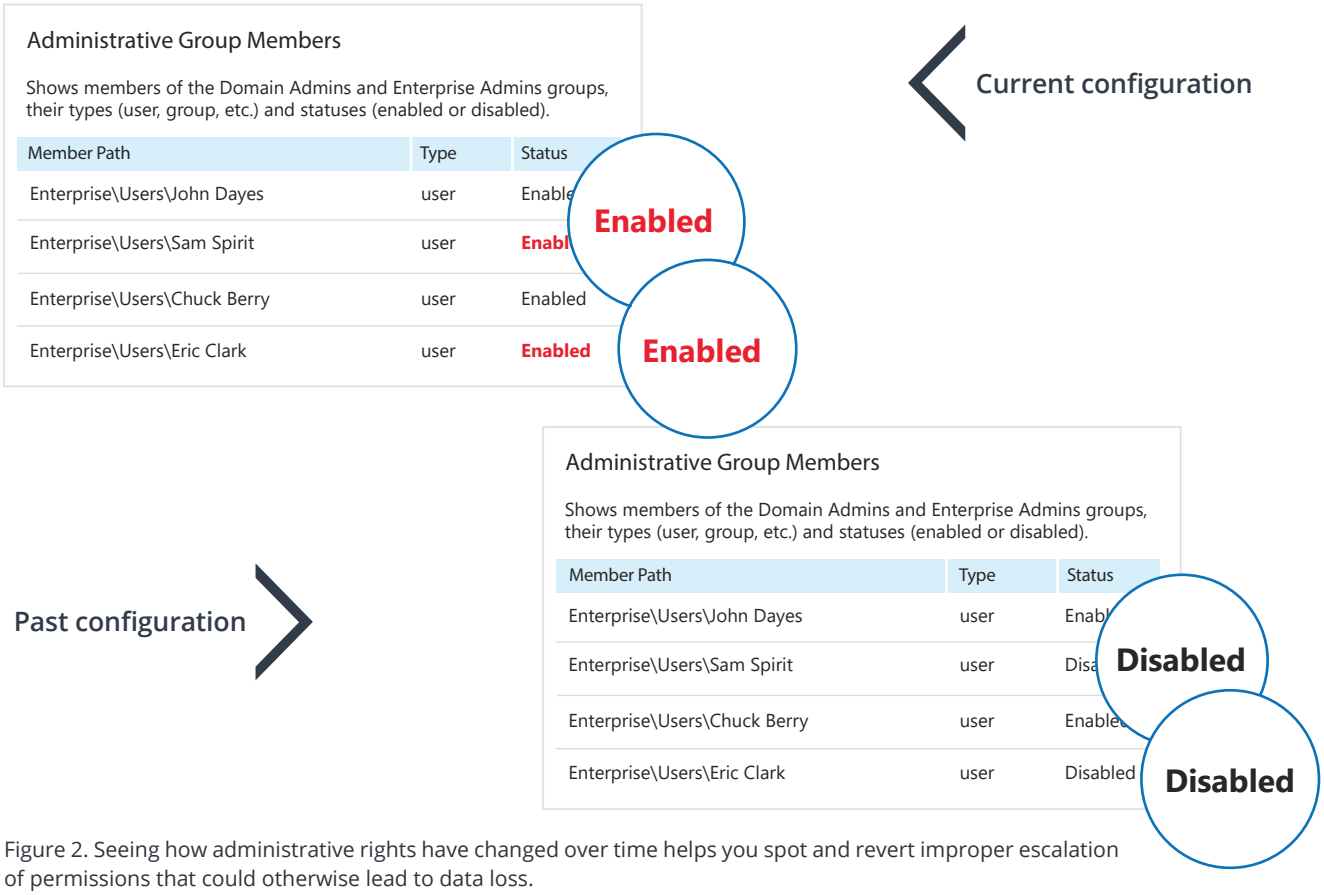


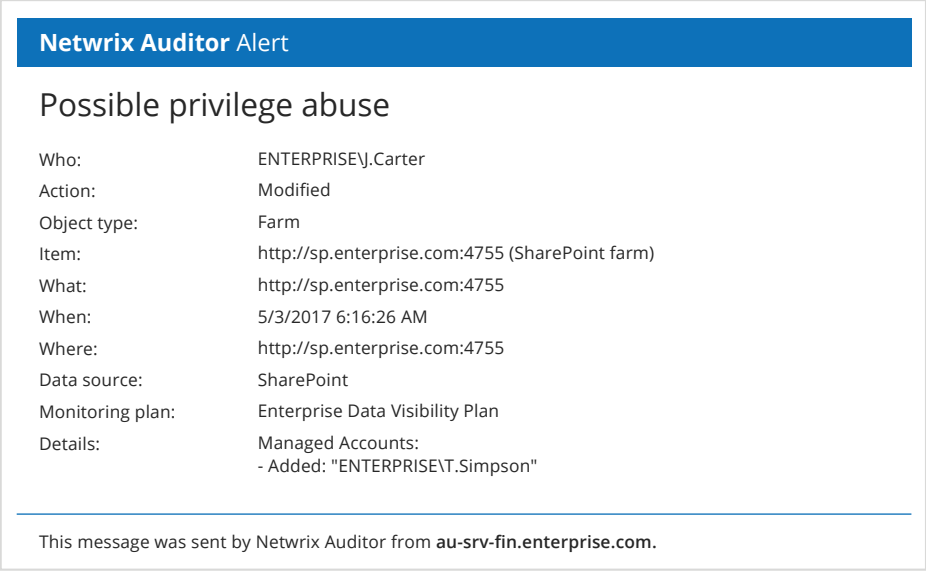
Figure 2. Seeing how administrative rights have changed over time helps you spot and revert improper escalation of permissions that could otherwise lead to data loss.

2.4 Spotting Suspicious Actions

Netwrix Auditor provides capabilities to help organizations quickly detect privilege abuse, privilege escalation and potential identity theft. Specifically, the solution includes reports that keep security administrators informed about a variety of suspicious actions, such as the addition of members to any privileged group, including additions that are reverted soon thereafter, and abnormal activity outside of business hours.

It also offers predefined and custom alerts that enable timely response to critical events, such as the addition of a user account to the Domain Admins group in Active Directory, new role assignments in Oracle Database or the addition of users to Managed Accounts in SharePoint.

Both reports and alerts include the critical details about who assigned permissions and who received them, what level of permissions were granted, and what actions were performed using the account in question.



Netwrix Auditor Alert

Possible privilege abuse

Who:	ENTERPRISE\J.Carter
Action:	Modified
Object type:	Farm
Item:	http://sp.enterprise.com:4755 (SharePoint farm)
What:	http://sp.enterprise.com:4755
When:	5/3/2017 6:16:26 AM
Where:	http://sp.enterprise.com:4755
Data source:	SharePoint
Monitoring plan:	Enterprise Data Visibility Plan
Details:	Managed Accounts: - Added: "ENTERPRISE\T.Simpson"

This message was sent by Netwrix Auditor from **au-srv-fin.enterprise.com.**

Figure 3. Alerts on suspicious behavior help you respond in time to prevent misuse or loss of data.

2.5 Spotting Threats Faster with User Activity Intelligence

Spotting threats to your data is not always a matter of noticing one particular action. You also have to be able to gather and correlate information about user behavior across your environment and over time and be able to tell when something unusual is going on. Netwrix Auditor provides security teams with user-centric audit and protection capabilities that enable them to centrally monitor the activity of user (and computer) accounts in an environment in relation to specific datasets. While Netwrix Auditor cannot block data transfers, quarantine applications or encrypt data, it can alert security staff to potentially harmful developments initiated by either users or applications across the entire IT environment, so they can immediately review incidents based on severity to identify and respond to rogue users or outliers who bypassed security.

This user-centric approach ensures organizations get deep visibility into how data is being used, and whether employee behavior deviates from known normal, which reduces the risk of unauthorized data access, improper usage and loss.

Netwrix Auditor brings together activity data from multiple sources, not just system logs, across multiple on-premises and cloud-based systems and applications, and transforms the cryptic machine data into noise-filtered human-readable insights. The results are displayed as actionable intelligence in a variety of reports and dashboards, through a single pane of glass associated with a unified platform. As a result, organizations ensure faster incident detection, investigation and response.

To ensure actions can be scrutinized in full detail or reviewed within the broader context of all activities in the IT environment, Netwrix Auditor offers several display options. Security administrators can review all activity by a particular user in one particular system, in several specific systems, or in all systems. In the basic case, no switching of reports or interfaces will be required. Alternatively, security staff can concentrate on specific use cases and see, for example, only failed user attempts to read files on a critical file server, or just successful SQL Server logons by a particular user. And they can also investigate user activity using the Interactive Search capabilities if a very specific use case applies or if they need to perform a sequential inquiries into what someone did or what happened to a certain set of data.

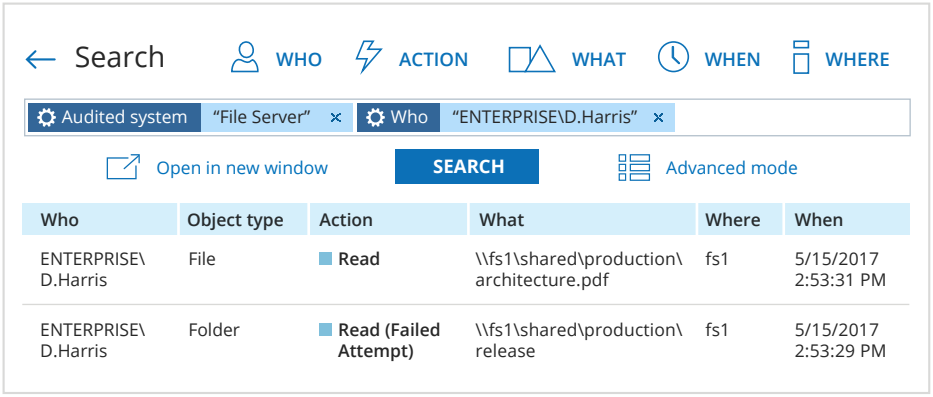
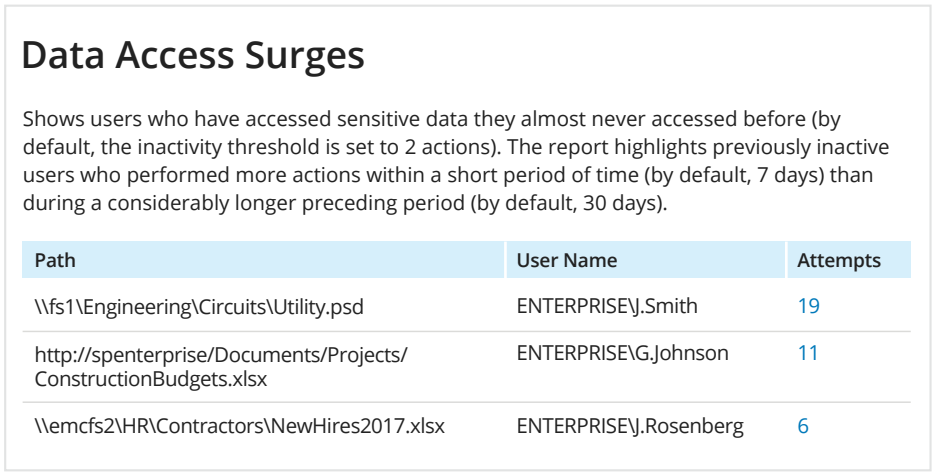


Figure 4. Search capabilities enable you to quickly review a particular user's actions. You can just as easily review all activity related to a particular set of data.

Apart from reporting and alerting on specific events, Netwrix Auditor also provides higher level security insights that help you proactively reduce the risk to your valuable data. For example, it includes predefined reports on the placement of potentially harmful files on file shares, the creation of files likely to contain sensitive data, and logons by a single user from multiple endpoints or by multiple users from a single endpoint.

It also helps you spot signs of an attacker trying to access your systems and data, with dashboards that highlight spikes in successful file reads, changes and deletions, or that visualize spikes in failed activity.



Data Access Surges

Shows users who have accessed sensitive data they almost never accessed before (by default, the inactivity threshold is set to 2 actions). The report highlights previously inactive users who performed more actions within a short period of time (by default, 7 days) than during a considerably longer preceding period (by default, 30 days).

Path	User Name	Attempts
\\fs1\Engineering\Circuits\Utility.psd	ENTERPRISE\J.Smith	19
http://spenterprise/Documents/Projects/ConstructionBudgets.xlsx	ENTERPRISE\G.Johnson	11
\\emcfs2\HR\Contractors\NewHires2017.xlsx	ENTERPRISE\J.Rosenberg	6

Figure 5. Monitoring surges in unusual data access activity can help you respond quickly to an attack and protect your data.

2.6 Addressing Compliance Requirements

As noted earlier, the purchase of DLP solutions is often driven by the need to comply with regulatory standards, such as HIPAA, PCI DSS or GLBA. But it's important to remember that the primary goal of compliance regulations is to improve the security of sensitive data — and you likely already have solutions in place to help you keep your data secure. Therefore, it's smart to consider whether the integrated DLP features of those solutions can help not only with security but compliance as well. You may find that they can help you address a multitude of compliance requirements, demonstrate the maturity of your security programs and controls to auditors, and earn acceptable grades in assessments — without spending an extra penny or adding unnecessary complexity to your IT infrastructure.

Netwrix Auditor is not a DLP solution in a conventional sense; however, thousands of IT departments in companies in heavily regulated industries successfully use its capabilities to enforce policies, validate controls, excel at demonstrating compliance to auditors and avoid penalties. The platform helps simplify iterative reviews of security controls as mandated by various compliance regulations. Many of the reports Netwrix Auditor provides are preconfigured right out of the box to deliver insights into the state of security in many critical areas: access entitlements, user access to systems, computer policies, data usage, attempts to change or destroy data, and more.

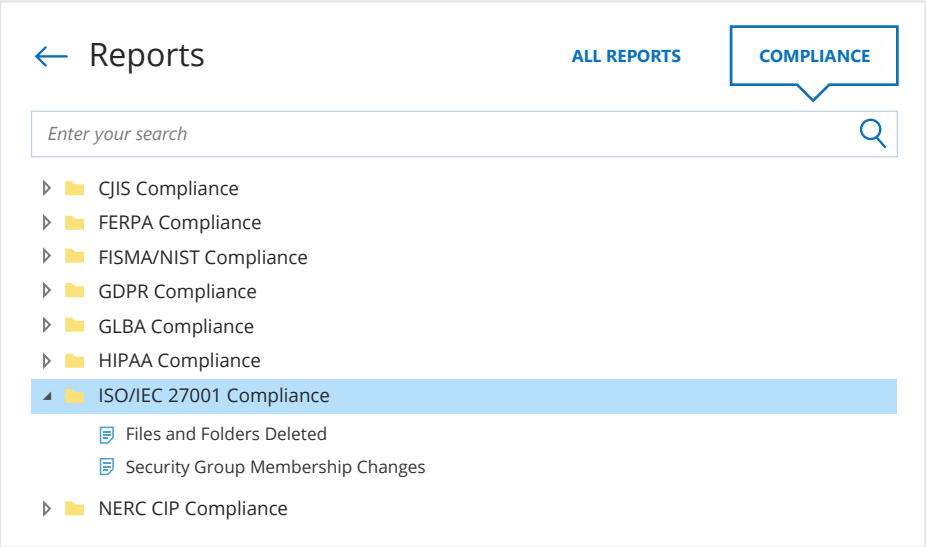


Figure 6. Preconfigured reports help organization achieve and prove compliance with a variety of regulations.

The entirety of Netwrix Auditor features and capabilities help the participants in the compliance process respond quickly to identified policy violations or areas lacking control. Users can craft a new alert, report subscription or search in seconds to address specific requests and recommendations from auditors on the fly.

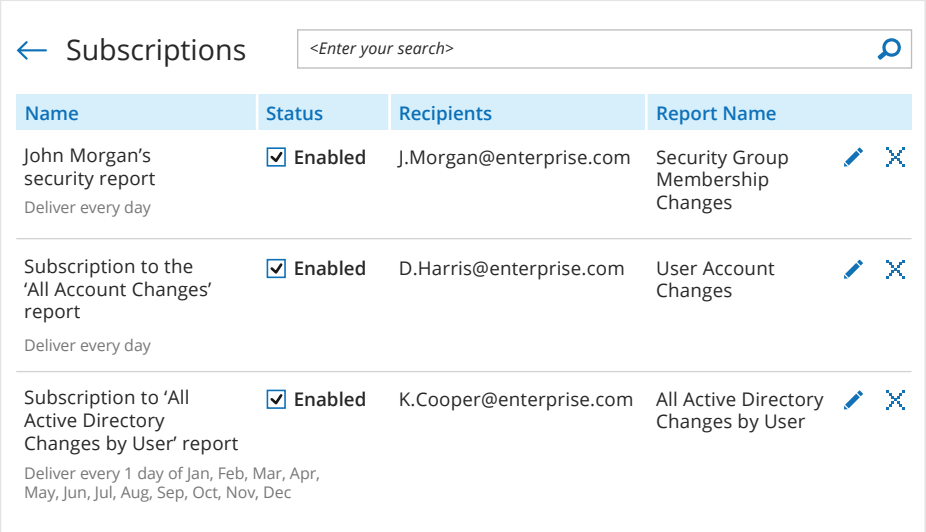


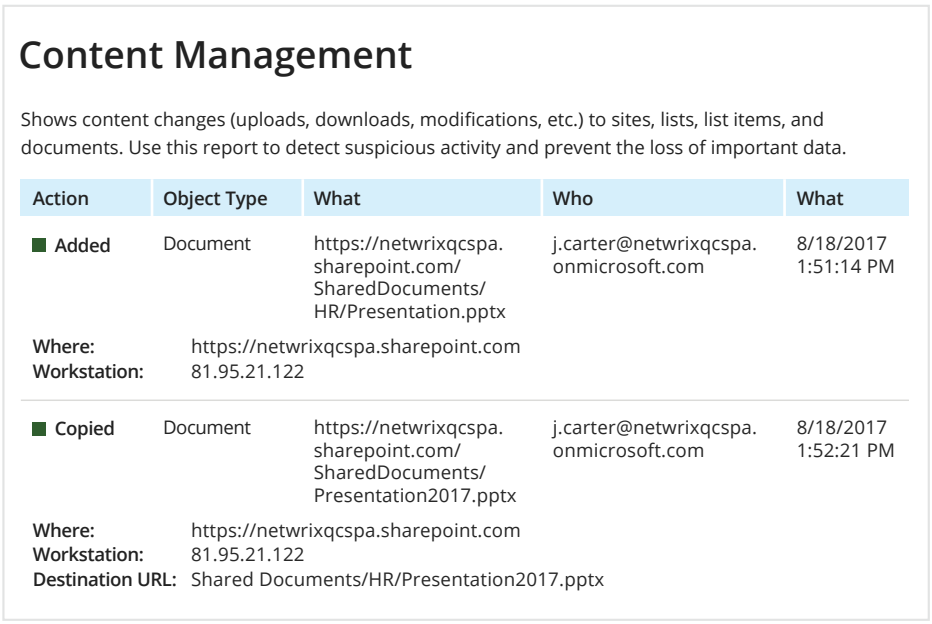
Figure 7. Alerts and report subscriptions are simple to set up, alter and manage.

2.7 Protecting Data in the Cloud

There are many places in an organization through which sensitive data can leak. The ones that allow data to leave corporate boundaries and flow out into the internet are of a particular concern because these egress channels are difficult to control. As enterprises use more and more cloud services, sensitive data that once resided only in a secure, on-premises repository is now often being uploaded to less secure cloud environment.

For example, suppose an operations team member needs data from a secure database in order to fulfill an order. That data is moved into documents stored on a file share, which is less protected than the database. The employee then decides to copy those files to a personal laptop, which is even less secure, and then to OneDrive storage to be shared with colleagues who also need it. All of this data transfer — and the corresponding increased risk of data loss — happens without any approval from data owners and without awareness of the security team.

Not all enterprise DLP solutions provide visibility into and control over user uploads of data into cloud storage services, because many of them are focused on only the network perimeter. Netwrix Auditor enables security administrators to gain visibility into what happens in cloud services like SharePoint Online, OneDrive for Business and Exchange Online. They can stay updated on any data uploads, downloads and modifications, which facilitates data loss prevention.



Content Management

Shows content changes (uploads, downloads, modifications, etc.) to sites, lists, list items, and documents. Use this report to detect suspicious activity and prevent the loss of important data.

Action	Object Type	What	Who	What
Added	Document	https://netwrixqcspa.sharepoint.com/SharedDocuments/HR/Presentation.pptx	j.carter@netwrixqcspa.onmicrosoft.com	8/18/2017 1:51:14 PM
Where:	https://netwrixqcspa.sharepoint.com			
Workstation:	81.95.21.122			
Copied	Document	https://netwrixqcspa.sharepoint.com/SharedDocuments/Presentation2017.pptx	j.carter@netwrixqcspa.onmicrosoft.com	8/18/2017 1:52:21 PM
Where:	https://netwrixqcspa.sharepoint.com			
Workstation:	81.95.21.122			
Destination URL:	Shared Documents/HR/Presentation2017.pptx			

Figure 8. Monitoring the movement of data, especially to the cloud, helps prevent data loss.

2.8 Expanding Protection through Integrations

As noted earlier, security tools that provide integration capabilities enable organizations to automate security processes and share data between different tools to strengthen DLP, thereby delivering unique functionality that enterprise DLP products may lack. According to Gartner, these integrations not only give birth to useful capabilities based on a synergetic effect but also help organizations avoid the "policy fatigue" that arises from having to utilize DLP capabilities from multiple point solutions separately.

Netwrix Auditor can be easily integrated with other existing on-premises and cloud applications because it offers open RESTful API. For example, it can be integrated with change management, threat intelligence, log aggregation and analysis, service desk, and compliance tools. Both data-in and data-out integration scenarios are supported.

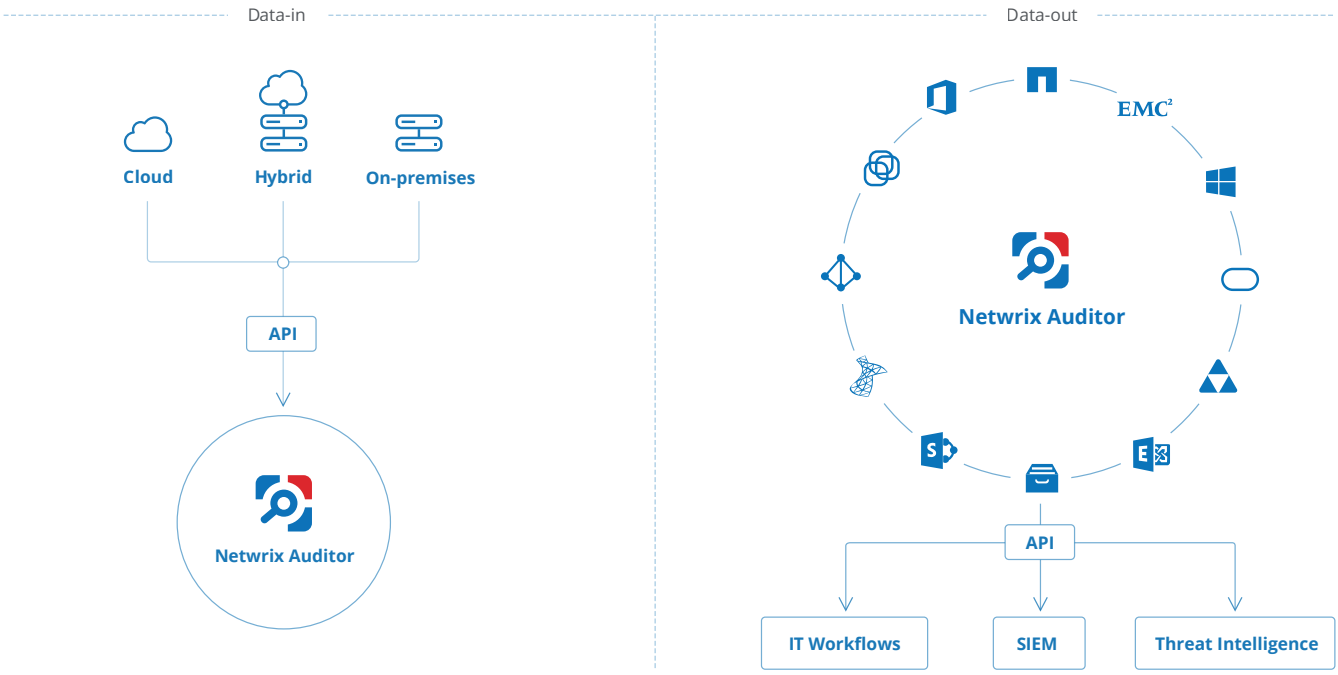


Figure 9. Integrating Netwrix Auditor with other solutions you already have can improve your DLP capabilities.

For example, suppose you already use the cloud-based application ServiceNow IT Service Management. Many critical security events in your environment might not be supplied to ServiceNow. If no ticket is created, odds are there will be no incident investigation and response. And even when the incidents are supplied to ServiceNow ITSM, operators might not have filled in all the required fields of the ticket form, which slows investigation and response. Moreover, on its own, ServiceNow doesn't provide cross-referencing with previous related incidents.

By integrating Netwrix Auditor with ServiceNow ITSM, you use Netwrix Auditor's core competency to improve the incident discovery and handling processes. Netwrix Auditor will supply ServiceNow with alerts about incidents across the IT environment. All necessary information about those incidents will be automatically entered into the appropriate fields in the ticket, eliminating the gaps possible during manual input. Incidents reported through the integration are cross-referenced and can be combined into a larger single ticket, further streamlining review and investigation. This faster and more accurate handling of incident improves your organization's ability to prevent data loss.

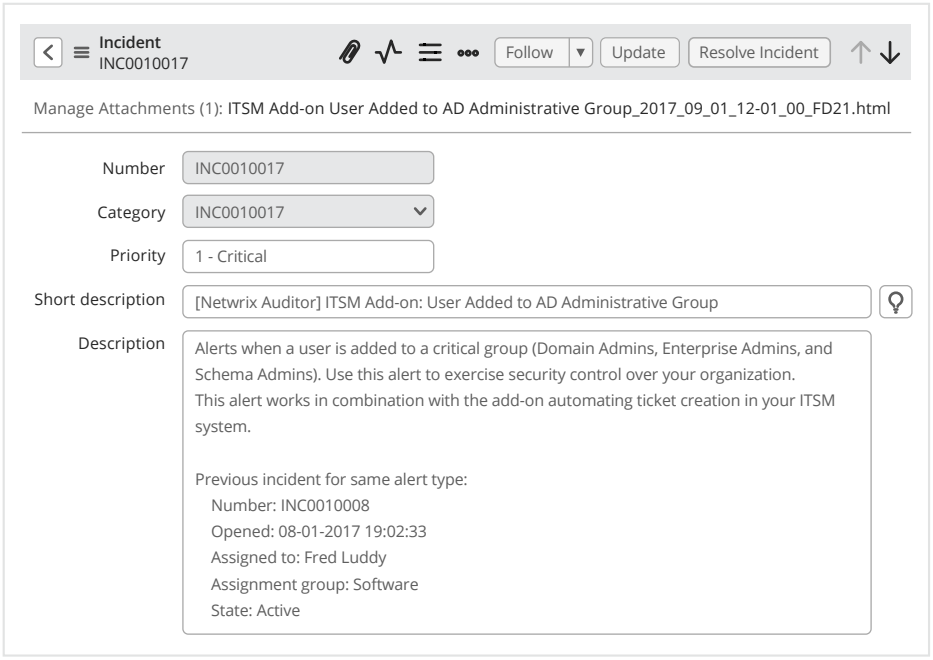


Figure 10. Integrating Netwrix Auditor with ServiceNow ITSM enables you to handle incidents better and faster.

Conclusion

Data is one of the most valuable assets any organization has, and protecting it from the growing array of modern threats is both critical and urgent. But, as Gartner argues, organizations should not simply rush to purchase an all-encompassing enterprise DPL solution. Instead, they should carefully consider whether they actually need the comprehensive functionality these products offer, and whether they have the budget and resources to operate and maintain such complex solutions. Otherwise, they may find themselves forced to bear expenditures that exceed all their expectations while a product that is used to half or less of its potential adds unwanted complexity to the IT environment.

Once they determine what DLP functionality they actually need, Gartner says, they should review the integrated DLP capabilities of the security tools they already have or could acquire with far less effort and expense. These integrated DLP features might be a better fit, and they can almost always be up and running much faster than a new enterprise DLP solution.

According to Gartner, Netwrix can help in the area of data discovery, which is an important part of any DLP process. Netwrix Auditor provides both data-centric and user-centric audit and protection capabilities that thousands of organizations already use to improve security and streamline compliance. Plus, it can easily be integrated with other security tools and processes, creating opportunities for organizations to fully benefit from the combined functionality of those solutions, as well as have a quick win in the areas of security and compliance as compared to the option of investing in enterprise DLP.

About Netwrix

Netwrix Corporation was the first vendor to introduce a visibility platform for user behavior analysis and risk mitigation in on-premises, hybrid and cloud IT environments. Founded in 2006, Netwrix has earned more than 100 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises and cloud-based IT systems in a unified way.

More than 160,000 IT departments worldwide rely on Netwrix Auditor to detect insider threats on premises and in the cloud, pass compliance audits with less expense, and increase the productivity of IT security and operations teams.

For more information, visit www.netwrix.com

If you want to evaluate Netwrix Auditor in your environment, choose one of the deployment options below. To see Netwrix Auditor in action online without having to download and install it, visit netwrix.com/testdrive.

On-Premises Deployment

Download a free 20-day trial

netwrix.com/go/freetrial

Virtual Appliance

Download our virtual machine image

netwrix.com/go/appliance

Cloud Deployment

Deploy NetwrixAuditor in the cloud

netwrix.com/go/cloud

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social