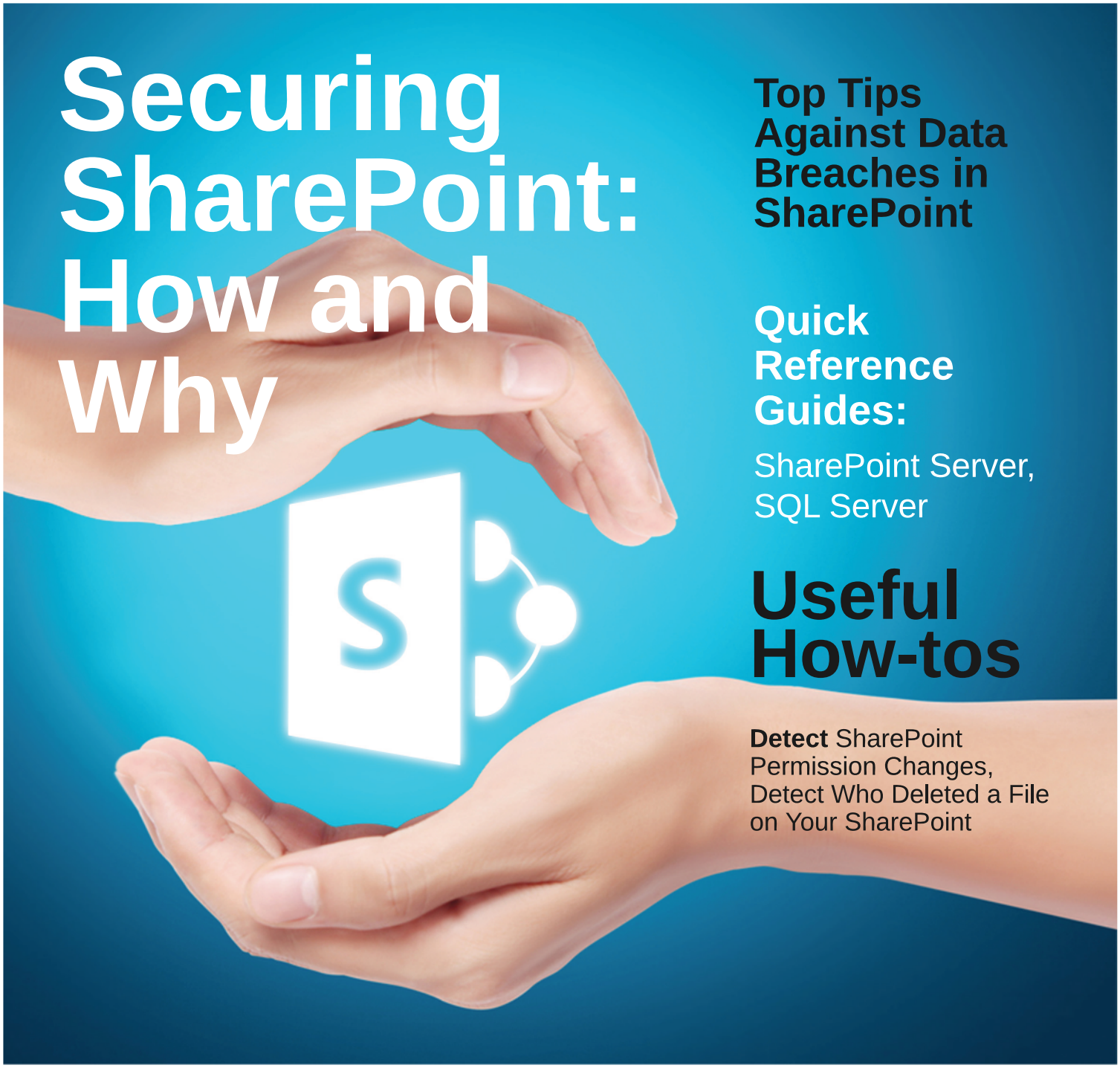
March 2015

SysAdmin Magazine



Securing SharePoint: How and Why

Top Tips Against Data Breaches in SharePoint

Quick Reference Guides:

SharePoint Server, SQL Server

Useful How-tos

Detect SharePoint Permission Changes, Detect Who Deleted a File on Your SharePoint

SysAdmin Magazine

Contents

2 **Securing SharePoint: How and Why**

by Krishna Kumar

5 **How to Detect SharePoint Permission Changes**

6 **Ten Simple Ways to Prevent Security Breaches in SharePoint Server 2013**

by Krishna Kumar

9 **Stopping Skeleton Key Malware from Causing Data Breaches**

by John O'Neill Sr.

11 **Quick Reference Guide for SharePoint Auditing**

13 **How to Detect Who Deleted a File on Your SharePoint**

15 **Quick Reference Guide for SQL Server Auditing**

Securing **SharePoint:** How and Why

by Krishna Kumar

10+ years in IT Industry specializing in designing, implementation and administration

SharePoint is one of the easiest applications to deploy and install, but it is not easy to configure with full proof security. Many administrators just perform the basic deployment without much security configuration. There is no set configuration to make it fully secure, since every environment is different and security configuration optimization varies to meet individual requirements. However, there are some basic configurations that need to be applied to make SharePoint environment secured to the maximum.

Securing SQL Server communication

SQL Server is a very important component of SharePoint: it stores most of configuration settings and libraries in its database. It is recommended to install an SQL Server and SharePoint on different servers to avoid any kind of surface attacks. Block the standard default ports - 1433 and 1434 - on the SQL Server and then to assign static port numbers on the SQL instance to allow SharePoint Server to connect. The simplest way to block these ports is through a Windows firewall.

Secure user communication

SharePoint is often exposed to Internet users and therefore it is important to secure communication between the server and user through an SSL Web server certificate. The SSL Web server certificate needs to have the subject name that matches the FQDN of the server. We could use a third-party CA certificate or an internal one. Certificate request can be generated using the Internet Information Services (IIS) Manager, then it has to be send to an internal CA or external vendor. Once you get the certificate, it needs to be updated to the IIS. Implement records management to data on SharePoint Server. Records management helps protect an edited / deleted form, delete a document with an expired retention, etc.

Disable unnecessary services and ports on SharePoint and SQL Servers

Disable unnecessary services: they can cause a security vulnerability. Only enable those services that are absolutely required for SharePoint and SQL Servers. Given below are the mandatory services which should not be disabled on a SharePoint server:

- ASP.NET State service (if you use InfoPath Forms Services or Project Server)
- View State service (if you use InfoPath Forms Services)
- World Wide Web Publishing Service
- AppFabric Caching Service
- Claims to Windows Token Service
- SharePoint Administration
- SharePoint Timer Service
- SharePoint Tracing Service
- SharePoint VSS Writer
- SharePoint User Code Host
- SharePoint Search Host Controller
- SharePoint Server Search 15
- Forefront Identity Manager service
- Forefront Identity Manager Synchronization service

Carefully review the ports required for SharePoint Server and SQL Server and block unnecessary or unused ports.

SQL and SharePoint service accounts and permissions

Service accounts are necessary to configure SharePoint Servers and SQL Servers. Using one or two service accounts for all configuration would be too risky boarding on disaster. It would end in providing unnecessary permissions, which can lead to a security threat.

Given below are the details of the service account requirements with necessary permission. It is recommended to use descriptive service accounts to identify the purpose of it and to to change the password on regularly with needed documenting.

SQL Server

- SQL Admin account to install SQL Server with local admin rights on the server
- SQL Server Agent service account
- SQL Database engine Service account

Setup user accounts

- Install SharePoint Server with local admin rights for installation
- SharePoint Product Configuration wizard

Server farm account or database access account

- Configure and manage the server farm
- Act as the application pool identity for the SharePoint Central Administration Web site
- Run the Microsoft SharePoint Foundation Workflow Timer Service

Avoid providing Anonymous and make sure the "limited-access user permission lockdown mode" is activated. SharePoint deployment and permissions need proper planning.	*Make sure only users with appropriate permissions manage SharePoint site, and not everyone on the team.*	*Define the permission model, it provides the right permissions to the right user and also helps manage SharePoint better with no performance impact.*
Never provide permissions at the level of items like calendar, tasks, etc. Managing and changing permissions will be difficult and can lead to performance issues.	*Enable auditing to track users to determine what actions have been taken on SharePoint.*	*Always provide permissions through Active Directory group membership, and provide only necessary permissions. Give full control only when necessary.*

How to Detect SharePoint Permission Changes

Native Auditing vs. Netwrix Auditor for Active Directory

Timely detection of SharePoint permission changes is extremely important for security assurance. Excessive SharePoint permissions may not only allow users to get access to sensitive data, but also to copy, modify, delete and distribute confidential files. See below how to enhance your SharePoint security and prevent information leakage.

Native Auditing

1. Navigate to Site Settings → Site Collection Administration → Site collection features → Choose “Reporting” → Press “Activate”.

2. Navigate to Site Settings → Site Collection Administration → Site collection audit settings → Mark “Editing Users and Permissions” events to audit in “List Libraries and Sites” settings.

3. Navigate to Site Settings → Site Collection Administration → Site collection audit settings → Set “Automatically trim the audit log for this site?” to “Yes” → Set trimming range time (30 days default) → Set the location you want to save the log before it will be trimmed → Click “OK”.

4. Navigate to Site Settings → Site Collection Administration → Audit log reports → Choose “Security Settings” report to view all permission changes made in your SharePoint.

Netwrix Auditor for SharePoint

1. Install and configure Netwrix Auditor for SharePoint.

2. Navigate to Netwrix Auditor → Managed Objects → Your SharePoint Server → Launch data collection by clicking “Run” button.

3. Navigate to Netwrix Auditor → Managed Objects → Your SharePoint Server → SharePoint → Reports → All Changes → All SharePoint Permission Changes by User → Specify date and time range → Click “View Report” button to view all permission changes within specified period.

See Real-Life Use Cases:

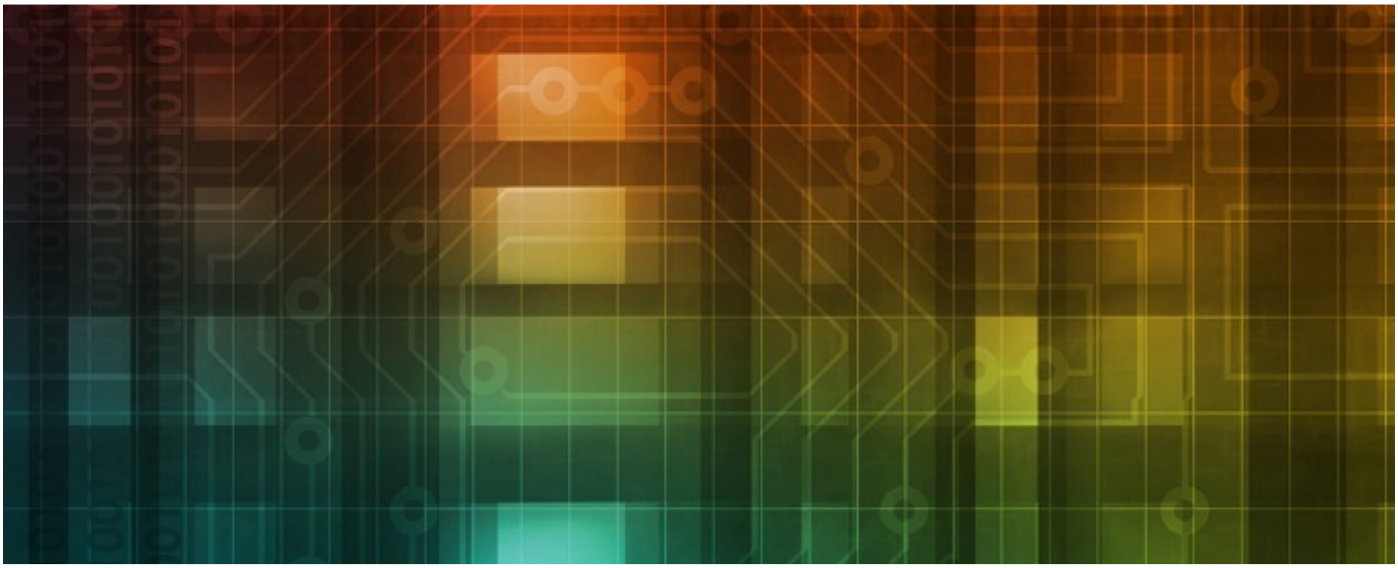
netwrix.com/go/sharepoint_permissions

Ten Simple Ways to **Prevent Security Breaches** in SharePoint Server 2013

by Krishna Kumar

10+ years in IT Industry specializing in designing, implementation and administration.

SharePoint server is one of the common applications in every organization. It's used to share information and is accessed by all the teams in the organization helping people to share documents, calendars and much more – saving time on communication. Most of the Fortune 500 companies use SharePoint, because it can be integrated with Active Directory and Microsoft Office thus establishing a collaboration platform. It plays a major role in the organization, but keep in mind that it also contains sensitive data such as legal information. Hence, it is important to secure a SharePoint server from various breaches and threats.



1. Updated Operating System

Always keep an Operating System updated with the latest service packs, patches and hotfixes. This will help you keep tabs on the loop holes in the OS. All the security patches are not required on SharePoint servers. These patches must be tested on lab machines before applying in the production systems. This is required to make sure that they don't make any negative impact.

2. SharePoint aware antivirus

SharePoint servers MUST be installed with antivirus software. Antivirus installed on the SharePoint servers should be a SharePoint aware antivirus. This helps SharePoint scan the files and documents being uploaded and downloaded from its servers.

3. Claims-based authentication

Use claim based authentication instead of traditionally integrated Windows authentication. It is based on a user obtaining security token which is digitally signed by a commonly trusted provider and contains a set of claims. Trust is established between SharePoint and identity provider. If a client

tries to access the web application, SharePoint redirects the client to a trusted identity provider. This authenticates the client and provides the token. Then the client sends the token to SharePoint, and SharePoint validates and authenticates it, and finally authorizes the user access.

Auditing can pull out the history of actions taken by a particular user or a report for a specified date range.

4. Enable auditing

It helps track users to determine what actions have been taken on SharePoint. Compliance requirements must be followed, especially when it comes to business critical information. Auditing can pull out the history of actions taken by a particular user or a report for a specified date range.

5. Records management

SharePoint 2013 archives and retains in-place records using security records management. Records management helps protect an edited / deleted form, delete a document when retention is expired, etc. In addition to the archived record and in-place record retention, SharePoint 2013 offers retention policy to SharePoint sites and Exchange 2013 mailboxes associated with the sites.

6. Avoid anonymous access

Make sure "limited-access user permission lockdown mode" is activated. This helps to prevent anonymous users from accessing application pages.

7. Managed service accounts

SQL, Setup and Farm service accounts should be domain accounts with no domain admin or special admin permissions. Also, configure e-mail accounts for all the managed users.

8. Securing ports, protocol and service

Secure SharePoint server, application server and database server by locking down the unnecessary ports, protocols and services.

9. Planned permission model

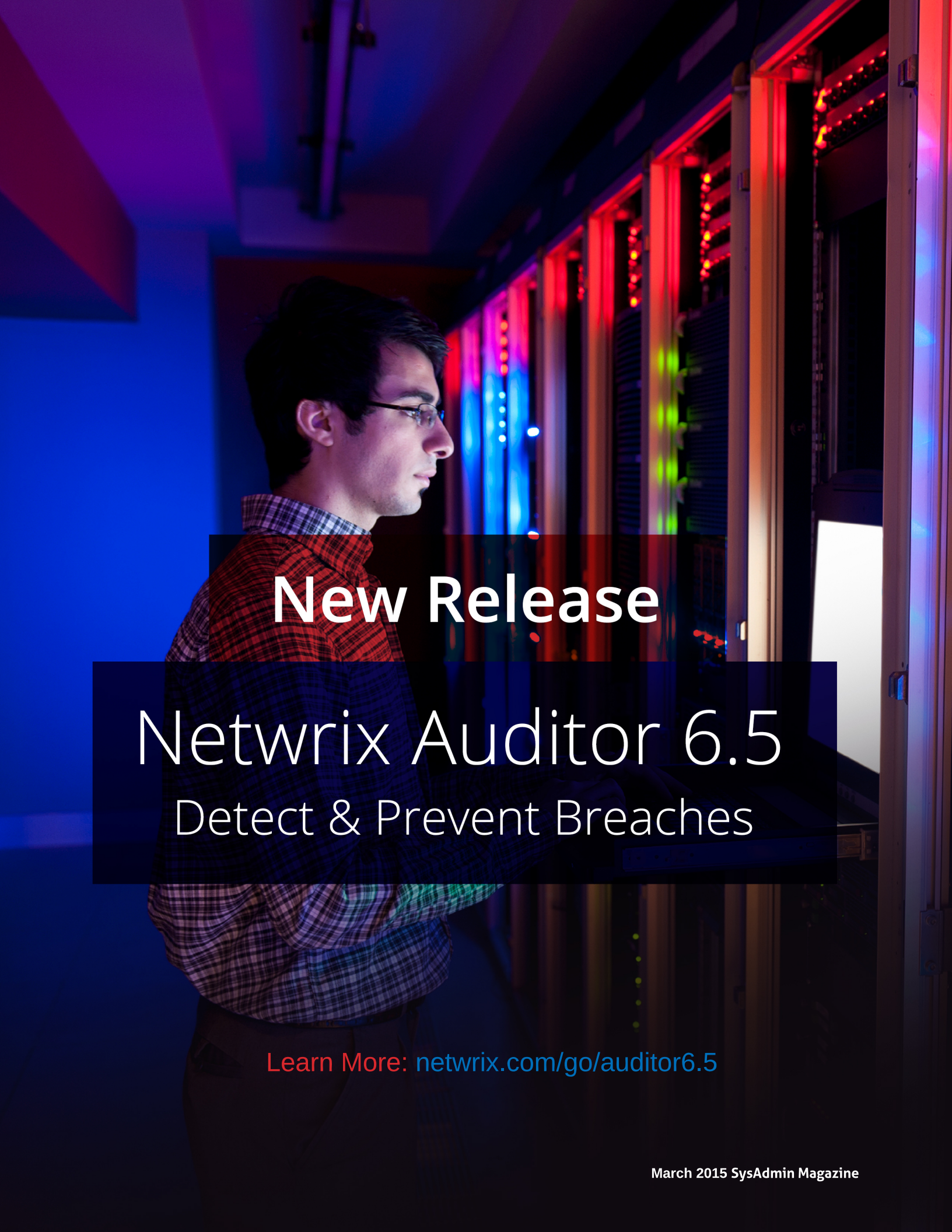
Never provide permissions at the level of items like calendar, tasks, etc. Managing and changing permissions will be difficult and can lead to performance issues. Always provide permissions through Active Directory group membership, and provide only necessary permissions. Give full control only when necessary. It can create and delete sites, SharePoint groups, manage site and library permissions, activate and deactivate SharePoint features, create and modify workflows, etc.

Never provide permissions at the level of items like calendar, tasks, etc. Managing and changing permissions will be difficult and can lead to performance issues.

10. Planning

SharePoint 2013 deployment and permissions need proper planning. Define the permission model, it provides the right permissions to the right user and also helps manage SharePoint better with no performance impact. Make sure only users with appropriate permissions manage SharePoint site, and not everyone in the team.

Hope these simple steps will help you maintain security of your SharePoint server and protect it from numerous security threats.


New Release
Netwrix Auditor 6.5
Detect & Prevent Breaches
Learn More: netwrix.com/go/auditor6.5

Stopping **Skeleton Key** Malware from Causing **Data Breaches**

by John O'Neill Sr.
20+ years in IT, consultant, architect, executive, speaker, and author

Proving the old adage that "criminals never sleep," a new piece of malware is making headlines. The aptly named Skeleton Key malware, detected in mid-January, bypasses the password authentication protection of Active Directory. Just as skeleton keys from the last century unlocked any door in a building, Skeleton Key malware can unlock access to any AD protected resource in an organization. Understanding Skeleton Key, along with methods of prevention, detection, and remediation, will empower IT admins in their fight against this latest security threat.

AD is the cornerstone of many organization's network security. It is ubiquitously integrated with virtually every type of IT system. From standard file servers to financial systems to VPN concentrators, AD is often the component authenticating username and passwords. Installed on an AD domain controller, Skeleton Key enables an attacker to authenticate as any AD user. Domain Users, Domain Admins, and even Enterprise Admins are all equally compromised. Scary stuff indeed!

Two key attributes inhibit Skeleton Key infections spreading. The malware requires direct domain controller access for installation and is only memory resident once installed. Requiring domain controller access means the DC must be compromised using other methods before Skeleton Key installation. More likely than not, Skeleton Key will travel with other malware. The initial malware opens the door to the DC allowing Skeleton Key to blast open attacker access to the entire AD protected network. Proving this point, Skeleton Key has recently been found on systems infected with backdoor.Winnti. The backdoor.Winnti trojan likely created the backdoor access for Skeleton Key installation.

Skeleton Key is an in-memory patch. This makes the malware memory resident only. A simple reboot of the DC wipes Skeleton Key from memory requiring reinstallation. Unfortunately, DCs often go weeks or even months between reboots. Likeliness of reinfection after reboot depends on the malware accompanying Skeleton Key. With slight modification, Trojans such as backdoor.Winnti might automate Skeleton Key reinfection after a DC reboot.

Installed on an AD domain controller, Skeleton Key enables an attacker to authenticate as any AD user. Domain Users, Domain Admins, and even Enterprise Admins are all equally compromised.

The best defense against Skeleton Key is multifaceted. Begin with basics including installing Windows Updates and updating malware protection on all systems in the network. Microsoft may release patches at any time that hinder Skeleton Key's effectiveness. Malware protection, in addition to detecting Skeleton Key in memory on an infected DC, may detect other enabling threats such as backdoor.Winnti on the network.

Regularly scheduled reboots of domain controllers wipe Skeleton Key from memory. Well-designed AD environments have multiple DCs allowing reboots without network downtime.

Audit all logons using domain or enterprise admin credentials anywhere on the network.

Environments with single DCs should schedule reboots at off hours. Reboots won't prevent reinfection, but they will require attackers to work harder in order to maintain access to your network via Skeleton Key.

Use robust auditing. Skeleton Key leverages PSExec to compromise systems. PSExec logs Event IDs 7045 and 7036 when used. Auditing the Event Logs for these IDs will help identify malicious vs. expected uses of the PSExec utility. Also audit all logons using domain or enterprise admin credentials anywhere on the network. Installation of Skeleton Key requires domain admin privileges or higher. Since these high level logons should be limited, identifying unusual logon activity may identify an infection quickly. Likewise, monitoring for unexpected password changes for domain and enterprise admin accounts may expose an attacker at work.

Implement multi-factor authentication. Skeleton Key only bypasses single-factor password based authentication. If a second factor is in use, such as biometrics or tokens, Skeleton Key is ineffective.

Monitoring for unexpected password changes for domain and enterprise admin accounts may expose an attacker at work.

While implementing multi-factor authentication requires some investment, its benefits are widespread.

Skeleton Key's potential to wreak havoc is significant. A Skeleton Key infection provides an attacker access to confidential files, sensitive email, and even powerful financial systems. Diligent IT pros must take sensible steps now to prevent their organization from becoming a Skeleton Key case study.

Quick Reference Guide

SharePoint Auditing

How to enable logging of important SharePoint events and view them in Audit Log Reports

Site Collection Audit Settings

- Navigate to Site Settings > Site Collection Administration > Site collection audit settings > Mark events you want to audit (Check SharePoint Built-in Audit Events) > Click “OK”
- We recommend that you select *Opening or downloading documents*, *viewing items in lists*, or *viewing item properties* for SharePoint Server sites only when absolutely needed. This option is likely to generate a large number of events that will potentially degrading the performance

Audit Log Reports

- Navigate to Site Settings > Site Collection Administration > Site collection features > Choose “Reporting” > Press “Activate”
- Navigate to Site Settings > Site Collection Administration > Audit log reports > Choose audit report you want (Check SharePoint Reports List) > Specify where to save the report once it has been generated > Click “OK” > Use “Click here to view the report” link
- The events that you select to audit are captured in audit reports in Microsoft Excel format and are available from the Auditing Reports page. You can also create a custom report that includes a number of these events over a specifid date range, within a specifi area of the site collection, or fitered to an individual user. You cannot modify events once they are logged, but site collection administrators can delete items from the audit log and confiure automatic trimming of the audit log data

Audit Log Trimming

- Navigate to Site Settings > Site Collection Administration > Site collection audit settings > Set “Automatically trim the audit log for this site?” to “Yes” > Set trimming range time (30 days default) > Set the location you want to save the log before it will be trimmed > Click “OK”

SharePoint Built-in Audit Events

Documents and items

- Editing items
- Checking out or checking in items
- Moving or copying items to another location in the site
- Deleting or restoring items
- Opening or downloading documents, viewing items in lists, or viewing item properties

Lists, Libraries, and Sites

- Searching site content
- Editing users and permissions
- Editing content types and columns

SharePoint Built-In Reports

- Content viewing
- Content modifiations
- Deletion
- Content type and list modifiations
- Policy modifiations
- Expiration and Disposition
- Auditing settings
- Security settings
- Custom report

For Detailed SharePoint Auditing, Try Netwrix Auditor — netwrix.com/go/sp-trial

- **Change auditing**: detection, reporting and alerting on all confiuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **Predefied reports and dashboards** with fitering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **AuditArchive™:** scalable two-tiered storage (fie-based + SQL database) holding consolidated audit data for 10 years or more.
- **Unified platform** to audit the entire IT infrastructure, unlike other vendors with a set of hard-to-integrate standalone tools.

Top 10 Free Tools for Change Auditing and Password Management

Track changes to Active Directory, Exchange, file servers, manage passwords and troubleshoot account lockouts at absolutely no cost.

The following freeware tools can save you a lot of time and make your network more efficient – at absolutely no cost. Some of these tools have advanced commercial versions with additional features, but none of them will expire and stop working when you urgently need them.

1. Change Notifier for Active Directory
Tracks changes to Active Directory (AD) users, group memberships, OUs, permissions, and provides visibility into what's happening inside your AD.
Free Download

2. Change Notifier for Group Policy
Tracks every change made to your group policy objects (GPOs), including GPO links, audit policy, password policy, and software deployment changes, and fills major gaps found in native auditing tools.
Free Download

3. Account Lockout Examiner
Alerts on account lockouts, helps troubleshoot these events, and analyzes their potential causes. The accounts can be unlocked via Netwrix Account Lockout Examiner console or mobile device.
Free Download

4. Change Notifier for Exchange
Reports on what's happening inside your Exchange servers, and tracks both configuration and permission changes with "before" and "after" values.
Free Download

5. Password Expiration Notifier
Automatically reminds your users to change their passwords before they expire so you can avoid password reset calls. It works nicely for users who don't log on interactively and never receive standard password change reminders at logon time (e.g., VPN users).
Free Download

6. Change Notifier for File Servers
Tracks changes to files and shares permissions, detects deleted and newly-created files, and reports on file-access attempts. This freeware tool strengthens security of your Windowsbased file servers.
Free Download

7. Password Manager
Allows users to reset forgotten passwords and unlock their accounts through a convenient, web-based, self-service portal and integration with the standard Windows logon produre. The tool supports up to 100 users.
Free Download

8. Change Notifier for SQL Server
Detects changes made to your SQL Server configurations, including database creation and deletion, changes to database users, roles, and schemas. It also reports "before" and "after" values for every change, and sends daily reports showing all changes made.
Free Download

9. Change Notifier for VMware
Allows you to control changes in your virtual environments. It notifies you about changes to VMware virtual machine settings, creation and deletion of virtual machines. It also sends daily reports of all changes made in the past 24 hours with "before" and "after" values.
Free Download

10. Change Notifier for Windows Server
Alerts you about changes made to your Windows Server configurations, including installed software and hardware, services and scheduled tasks. It sends summary reports listing changes of the last 24 hours with "before" and "after" values.
Free Download

JOHN BAGLEY
Award-winning professional writer and independent consultant

How to Detect Who Deleted a File on Your SharePoint

Native Auditing vs. Netwrix Auditor for Active Directory

The deletion of a file on your SharePoint by outsiders or internal users could result in the loss of sensitive data. That's why the timely detection of file deletions on SharePoint minimizes hassles for users and reduces file restoration times, while providing an early warning of possible breaches.

Native Auditing

1.

Navigate to Site Settings → Site Collection Administration → Site collection features → Choose "Reporting" → Press "Activate".

2.

Navigate to Site Settings → Site Collection Administration → Site collection audit settings → Mark "Deleting or restoring items" → Click "OK".

3.

Navigate to Site Settings → Site Collection Administration → Audit log reports → Deletions → Open the generated report in Microsoft Excel.

Netwrix Auditor for SharePoint

1.

Navigate to "Managed Objects" → "SharePoint Server" and click "Run" to collect data.

2.

You can schedule automatic data gathering by navigating to "Managed Objects" → SharePoint Server → SharePoint → Click "Configure Delivery" and set the appropriate time so you don't need to gather data manually every time.

3.

Open the received e-mail after collecting is complete. You can also view SharePoint changes by navigating to Netwrix Auditor Managed Objects → SharePoint Server → SharePoint → Reports → All Changes → and select "All SharePoint content changes by user" report → Define "From:" and "To:" dates, click "view report".

Quick Reference Guide

SQL Server Auditing

How to enable logging of important SQL Server events via trace procedure

Trace Creation

- Run **MS SQL Management Studio** > Connect to database you want to audit > New Query > Copy the following script into new query box:

```
DECLARE @RC int, @TraceID int, @on BIT
EXEC @rc = sp_trace_create @TraceID output, 2,
N'C:\pathname\file'
SELECT RC = @RC, TraceID = @TraceID
-- Follow Common SQL trace event list and common sql trace
-- tables to define which events and tables you want to capture
SELECT @on = 1
EXEC sp_trace_setevent @TraceID, 111, 1, @on
-- (111-Event Audit Add/Drop Role, 1-TextData table column)
EXEC sp_trace_setevent @TraceID, 111, 11, @on
EXEC sp_trace_setevent @TraceID, 111, 14, @on
EXEC @RC = sp_trace_setstatus @TraceID, 1
GO
```

- Define file trace location and hit “Execute” to start a new trace

Trace Management

- Execute this query to stop the trace:

```
sp_trace_setstatus @traceid = 2, @status = 0
```

- Execute this query to delete the trace:

```
sp_trace_setstatus @traceid = 2, @status = 2
```

- Execute this query in order to import the trace into database table:

```
USE DBname
SELECT * INTO tablename FROM ::fn_trace_gettable
('C:\pathname\file.trc' , DEFAULT)
GO
```

- Execute this query in order to view trace data:

```
SELECT TOP 1000 [TextData] , [HostName] , [LoginName] ,
[StartTime] , [EndTime] , [ServerName] , [EventClass]
FROM [DBname]. [dbo]. [tablename]
```

- Inspect “TextData” table for events like: *CREATE LOGIN, ALTER SERVER ROLE, DROP LOGIN* etc...

Common SQL Trace Events

- 12 – SQL:BatchCompleted
- 13 – SQL:BatchStarting
- 105 – Audit Login GDR Event
- 109 – Audit Add DB User Event
- 110 – Audit Add Member to DB Role Event
- 111 – Audit Add/Drop Role
- 113 – Audit Statement Permission
- 128 – Audit Database Management Event
- 131 – Audit Schema Object Management Event
- 176 – Audit Server Object Management Event
- 177 – Audit Server Principal Management Event

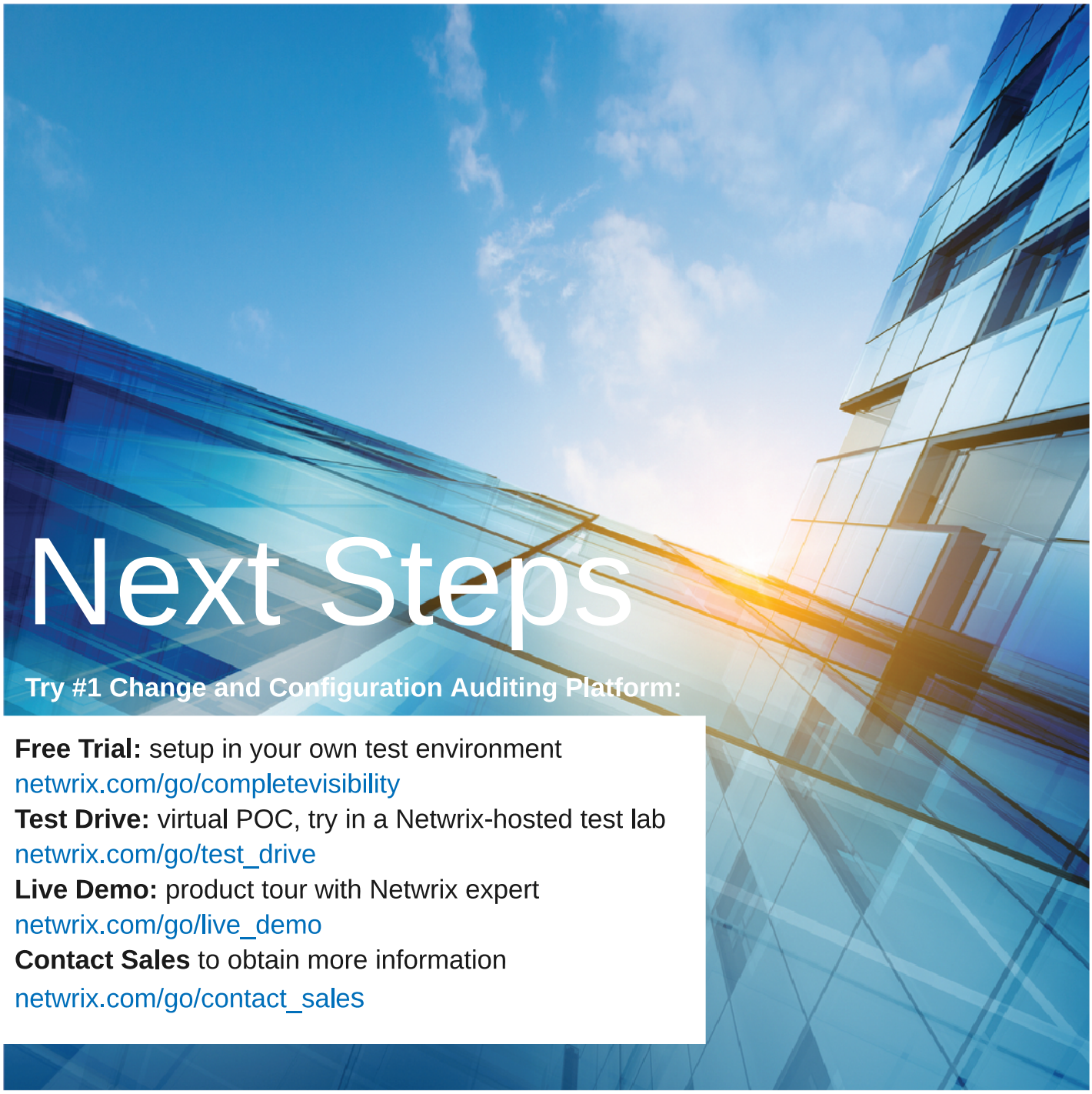
Common SQL Trace Table Columns

- 1 – TextData
- 6 – NTUserName
- 11 – LoginName
- 14 – StartTime
- 15 – EndTime
- 26 – ServerName
- 35 – DatabaseName

You can fid full events and tables list here: url2open.com/sqltrace

For Detailed SQL Server Auditing, Try Netwrix Auditor - netwrix.com/go/ss-trial

- **Change auditing**: detection, reporting and alerting on all confiuration changes across your entire IT infrastructure with Who, What, When, Where details and Before/After values.
- **More than 200 predefied reports and dashboards** with fitering, grouping, sorting, export (PDF, XLS etc.), email subscriptions, drill-down, access via web, granular permissions and ability to create custom reports.
- **Long-Term Archiving:** scalable two-tiered storage (fie-based + SQL database) holding consolidated audit data for up to and beyond 10 years.
- **Unifid platform** to audit the entire IT infrastructure, as opposed to multiple hard-to-integrate standalone tools from other vendors.



Next Steps

Try #1 Change and Configuration Auditing Platform:

Free Trial: setup in your own test environment
netwrix.com/go/completevisibility
Test Drive: virtual POC, try in a Netwrix-hosted test lab
netwrix.com/go/test_drive
Live Demo: product tour with Netwrix expert
netwrix.com/go/live_demo
Contact Sales to obtain more information
netwrix.com/go/contact_sales

netwrix.com | netwrix.com/social

Corporate Headquarters: 8001 Irvine Center Drive, Suite 820 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749
EMEA: +44 (0) 203-318-02

netwrix
#1 for change auditing