netwrix

Top 5 SQL Database Incidents You Need Visibility into

www.netwrix.com | **Toll-free**: 888-638-9749

Table of Contents

#1: Table and Record Deletions 2

#2: Role and Privilege Escalation 3

#3: Failed Logons 4

#4: Account Changes 5

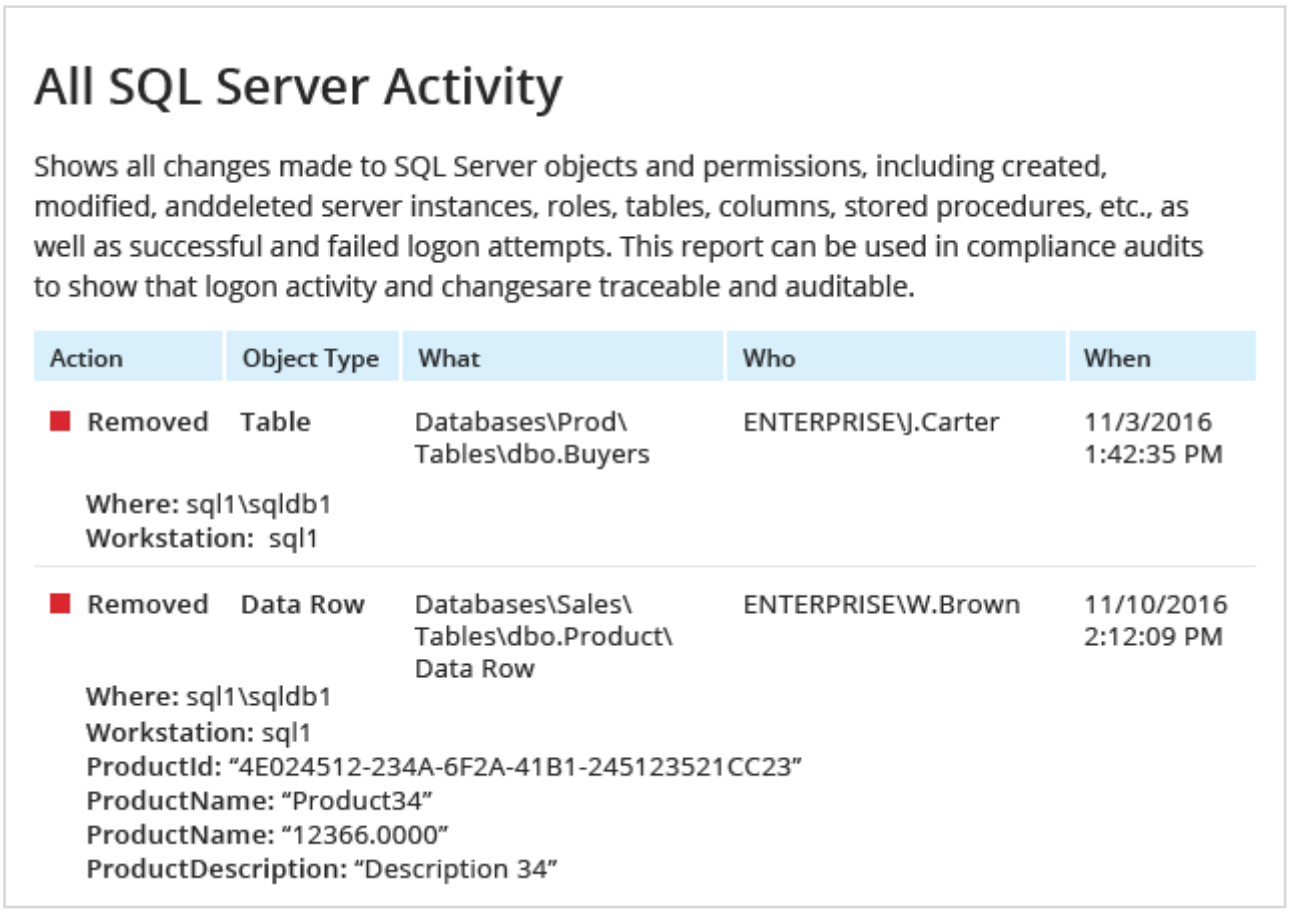
#5: Trigger and Constraint Changes 6

About Netwrix Auditor 7

#1: Table and Record Deletions

Because SQL database tables store important information used by critical enterprise applications, unauthorized or inappropriate deletion of data can lead to downtime and business losses. You need to know quickly if someone deletes a table or any table elements, either maliciously or by mistake. Netwrix Auditor reports on dropped tables and removed records, providing answers to the following questions:

- **Who** removed a table or record from any of your SQL databases?
- **What is the name** of each removed object?
- **From which workstation** was each deletion made?
- **Where** was the object stored before it was deleted?
- **When** was each deletion made?



All SQL Server Activity

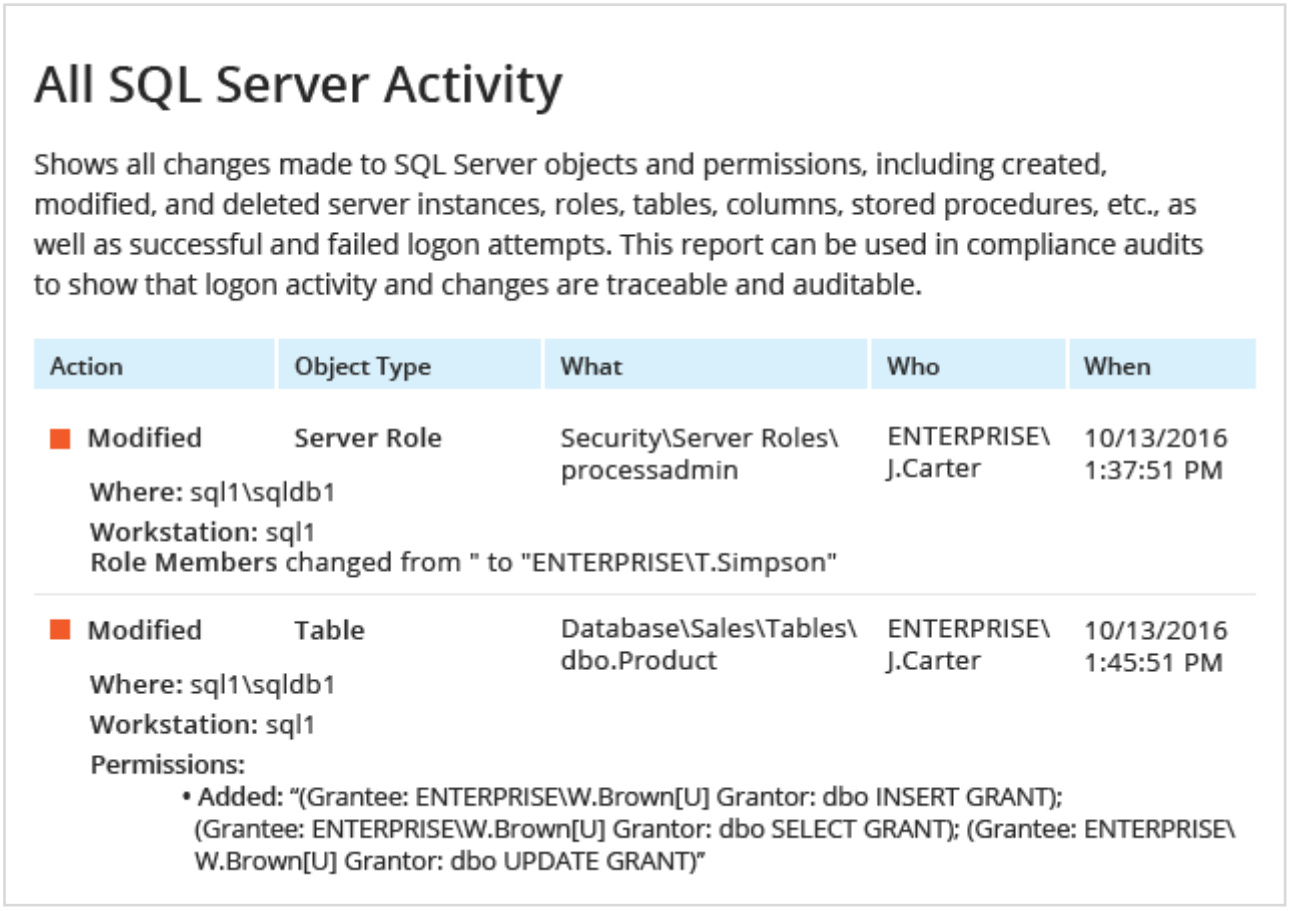
Shows all changes made to SQL Server objects and permissions, including created, modified, anddeleted server instances, roles, tables, columns, stored procedures, etc., as well as successful and failed logon attempts. This report can be used in compliance audits to show that logon activity and changesare traceable and auditable.

Action	Object Type	What	Who	When
Removed	Table	Databases\Prod\ Tables\dbo.Buyers	ENTERPRISE\J.Carter	11/3/2016 1:42:35 PM
Where: sql1\sqldb1 Workstation: sql1				
Removed	Data Row	Databases\Sales\ Tables\dbo.Product\ Data Row	ENTERPRISE\W.Brown	11/10/2016 2:12:09 PM
Where: sql1\sqldb1 Workstation: sql1 ProductId: "4E024512-234A-6F2A-41B1-245123521CC23" ProductName: "Product34" ProductName: "12366.0000" ProductDescription: "Description 34"				

#2: Role and Privilege Escalation

Users' database roles control which types of SQL statement they can run and whether they have administrative rights to manipulate the database. Security best practices require granting users only the minimum privileges needed to accomplish their work. Netwrix Auditor helps control unwarranted role assignments and modifications, and provides answers to the following questions:

- **Who** made a privilege or role assignment?
- **Which user account** received a new role or privilege?
- **From which workstation** was each change made?
- **When** did each modification occur?



All SQL Server Activity

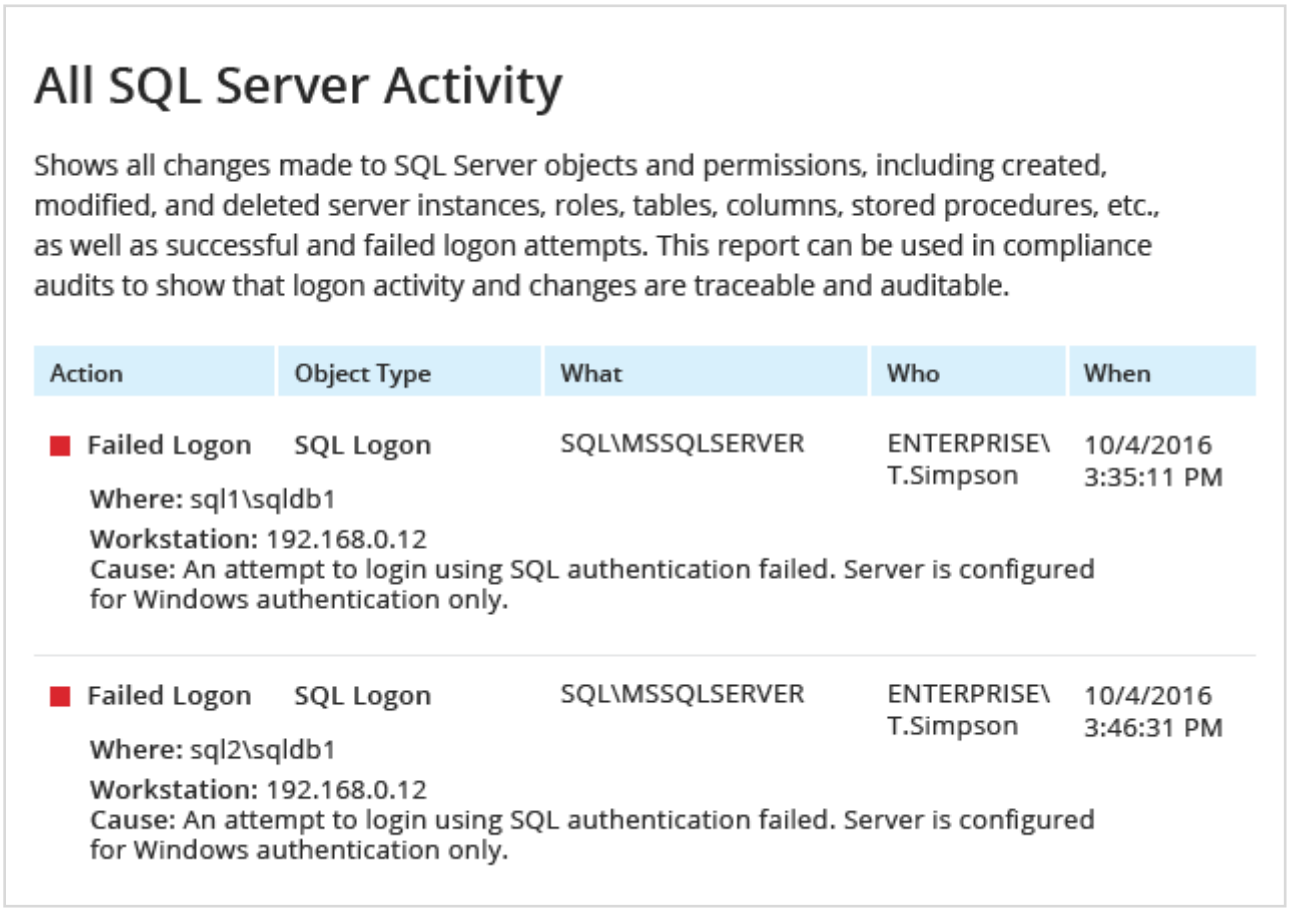
Shows all changes made to SQL Server objects and permissions, including created, modified, and deleted server instances, roles, tables, columns, stored procedures, etc., as well as successful and failed logon attempts. This report can be used in compliance audits to show that logon activity and changes are traceable and auditable.

Action	Object Type	What	Who	When
Modified	Server Role	Security\Server Roles\ processadmin	ENTERPRISE\ J.Carter	10/13/2016 1:37:51 PM
Where: sql1\sqldb1 **Workstation:** sql1 **Role Members** changed from '' to "ENTERPRISE\T.Simpson"				
Modified	Table	Database\Sales\Tables\ dbo.Product	ENTERPRISE\ J.Carter	10/13/2016 1:45:51 PM
Where: sql1\sqldb1 **Workstation:** sql1 **Permissions:** • **Added:** "(Grantee: ENTERPRISE\W.Brown[U] Grantor: dbo INSERT GRANT); (Grantee: ENTERPRISE\W.Brown[U] Grantor: dbo SELECT GRANT); (Grantee: ENTERPRISE\W.Brown[U] Grantor: dbo UPDATE GRANT)"				

#3: Failed Logons

Multiple failed attempts to log on to your SQL databases can be the first sign of an attack. Netwrix Auditor shows details about every failed logon attempt and helps answer the following questions:

- **Which users** failed to connect to a SQL Server instance?
- **How many** logons were attempted by each user?
- **From which workstation** was each logon attempt made?
- **What was the cause** of each failed logon?
- **When** was each failed logon attempted



All SQL Server Activity

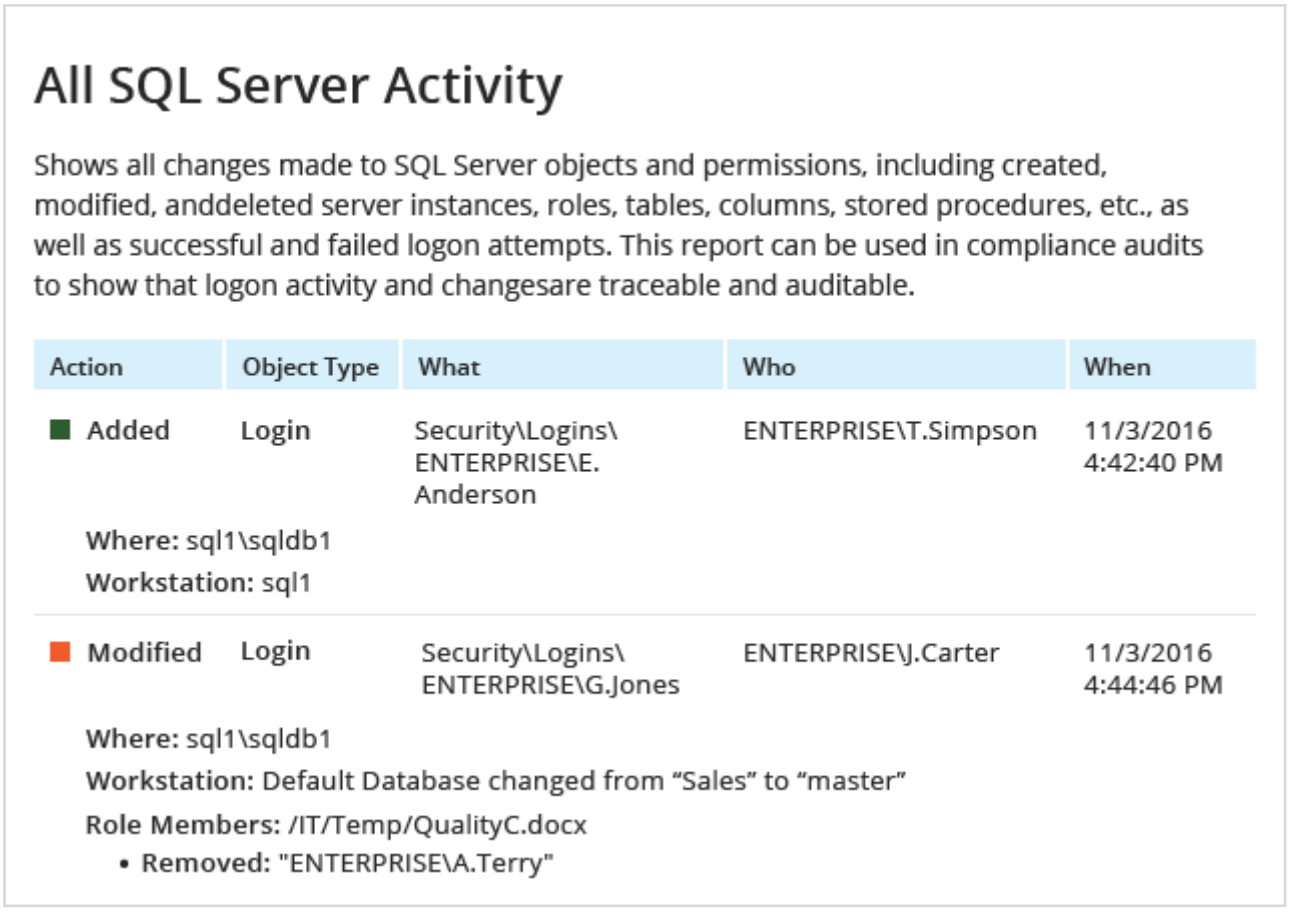
Shows all changes made to SQL Server objects and permissions, including created, modified, and deleted server instances, roles, tables, columns, stored procedures, etc., as well as successful and failed logon attempts. This report can be used in compliance audits to show that logon activity and changes are traceable and auditable.

Action	Object Type	What	Who	When
Failed Logon	SQL Logon	SQL\MSSQLSERVER	ENTERPRISE\ T.Simpson	10/4/2016 3:35:11 PM
Where: sql1\sqldb1 **Workstation:** 192.168.0.12 **Cause:** An attempt to login using SQL authentication failed. Server is configured for Windows authentication only.				
Failed Logon	SQL Logon	SQL\MSSQLSERVER	ENTERPRISE\ T.Simpson	10/4/2016 3:46:31 PM
Where: sql2\sqldb1 **Workstation:** 192.168.0.12 **Cause:** An attempt to login using SQL authentication failed. Server is configured for Windows authentication only.				

#4: Account Changes

Complete visibility into changes made to your SQL Server accounts is necessary for timely detection of attacks and prevention of data breaches. Netwrix Auditor gives you control over user account changes and provides detailed answers to the following questions:

- **Who** made user account changes?
- **Which user accounts** were affected?
- **What changes** were made to each user account?
- **From which workstation** was each change made?
- **When** was each change made?



All SQL Server Activity

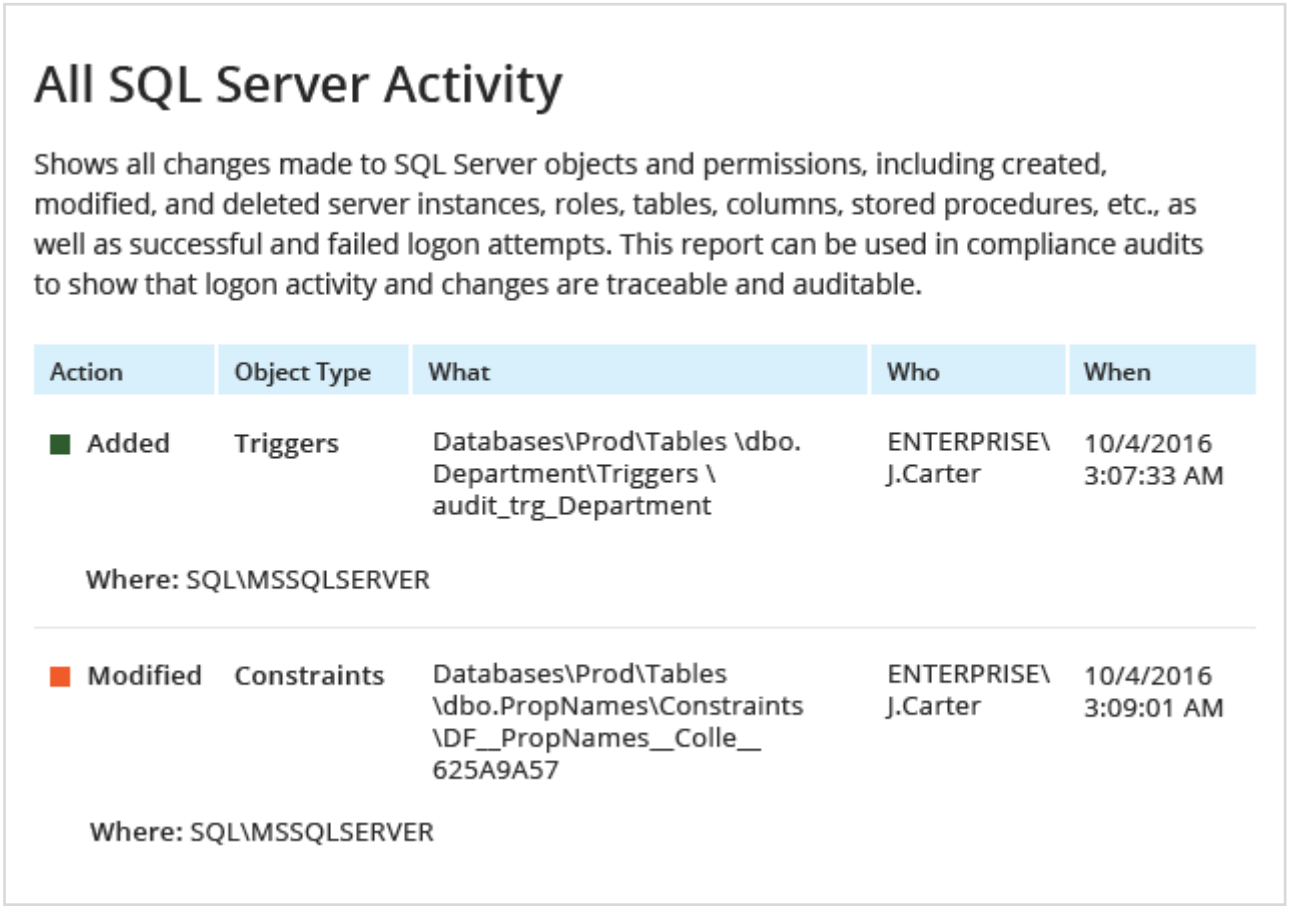
Shows all changes made to SQL Server objects and permissions, including created, modified, anddeleted server instances, roles, tables, columns, stored procedures, etc., as well as successful and failed logon attempts. This report can be used in compliance audits to show that logon activity and changesare traceable and auditable.

Action	Object Type	What	Who	When
Added	Login	Security\Logins\ ENTERPRISE\E. Anderson	ENTERPRISE\T.Simpson	11/3/2016 4:42:40 PM
Where: sql1\sqldb1 Workstation: sql1				
Modified	Login	Security\Logins\ ENTERPRISE\G.Jones	ENTERPRISE\J.Carter	11/3/2016 4:44:46 PM
Where: sql1\sqldb1 Workstation: Default Database changed from "Sales" to "master" Role Members: /IT/Temp/QualityC.docx • Removed: "ENTERPRISE\A.Terry"				

#5: Trigger and Constraint Changes

To maintain the integrity of the information stored in your SQL databases, you need control over all changes made to database triggers and constraints. Netwrix Auditor tracks every change to the procedural code and answers the following questions:

- **What triggers or constraints** were added, modified or deleted?
- **Who changed** a trigger or a constraint?
- **What action** did each user perform?
- **On which server** was each change made?
- **When** did each change take place?



All SQL Server Activity

Shows all changes made to SQL Server objects and permissions, including created, modified, and deleted server instances, roles, tables, columns, stored procedures, etc., as well as successful and failed logon attempts. This report can be used in compliance audits to show that logon activity and changes are traceable and auditable.

Action	Object Type	What	Who	When
Added	Triggers	Databases\Prod\Tables \dbo. Department\Triggers \ audit_trg_Department	ENTERPRISE\ J.Carter	10/4/2016 3:07:33 AM
Where: SQL\MSSQLSERVER				
Modified	Constraints	Databases\Prod\Tables \dbo.PropNames\Constraints \DF__PropNames__Colle__ 625A9A57	ENTERPRISE\ J.Carter	10/4/2016 3:09:01 AM
Where: SQL\MSSQLSERVER				

About Netwrix Auditor

Netwrix Auditor is a **visibility and governance platform** that enables control over changes, configurations and access in hybrid cloud IT environments to protect data regardless of its location. The unified platform provides security analytics for detecting anomalies in user behavior and investigating threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, Dell data storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with a RESTful API, Netwrix Auditor provides **endless integration, auditing and reporting capabilities** for security and compliance.

Unlike other vendors, Netwrix focuses exclusively on providing complete visibility and governance for hybrid cloud security. The sharp focus enables us to offer much more robust functionality than legacy change auditing solutions. Netwrix Auditor has been already honored with more than **100 awards** and recognized by almost **160,000 IT departments** worldwide.

Deploy Netwrix Auditor Wherever You Need It

Free 20-Day Trial for On-Premises Deployment: netwrix.com/freetrial

Free Virtual Appliance for Hyper-V and VMware Hypervisors: netwrix.com/go/appliance

netwrix.com/social

6160 Warren Parkway, Suite 100, Frisco, TX, US 75034

Toll-free: 888-638-9749

Int'l: +1 (949) 407 -5125

EMEA: +44 (0) 203 -318-0261