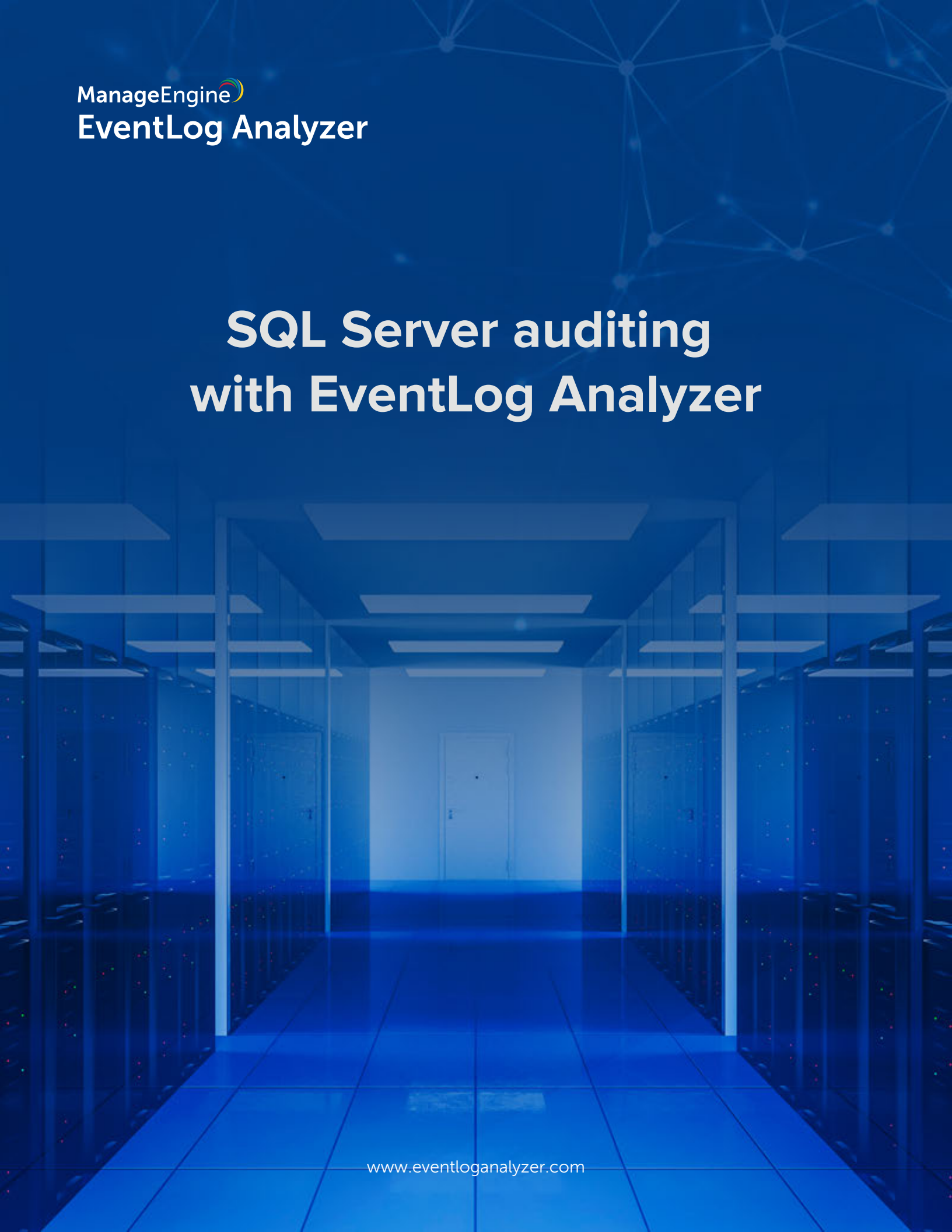
ManageEngine
EventLog Analyzer

SQL Server auditing with EventLog Analyzer



www.eventloganalyzer.com

Introduction

Databases are the most important element of an organization's network, as they store and process the company's critical business data. This data is of high value to cybercriminals, who are coming up with new methods of targeting it every day. On top of this, the average volume of data being processed by organizations is growing.

Managing vast amounts of data and securing it from attacks is a daunting task that can reveal poor security practices. This is why database integrity, auditing, and security are prime topics of concern in many organizations.

The importance of database auditing

Your databases are susceptible to both external and internal attacks. Attackers are adept at finding weak spots which allow them to find their way to your network and databases. Auditing activities happening on your database can help you ensure everything is running smoothly on your servers and detect threats that could potentially lead to data loss. Auditing helps you pick out events such as:

- **Erroneous changes:** If there is no stringent change management process in place, a multitude of erroneous changes could occur in your database and disrupt data integrity. For example, if multiple users have write access to a database, important data may get overwritten with the wrong values. When such invalid changes are made to a critical column like bank account numbers, it could have disastrous effects.

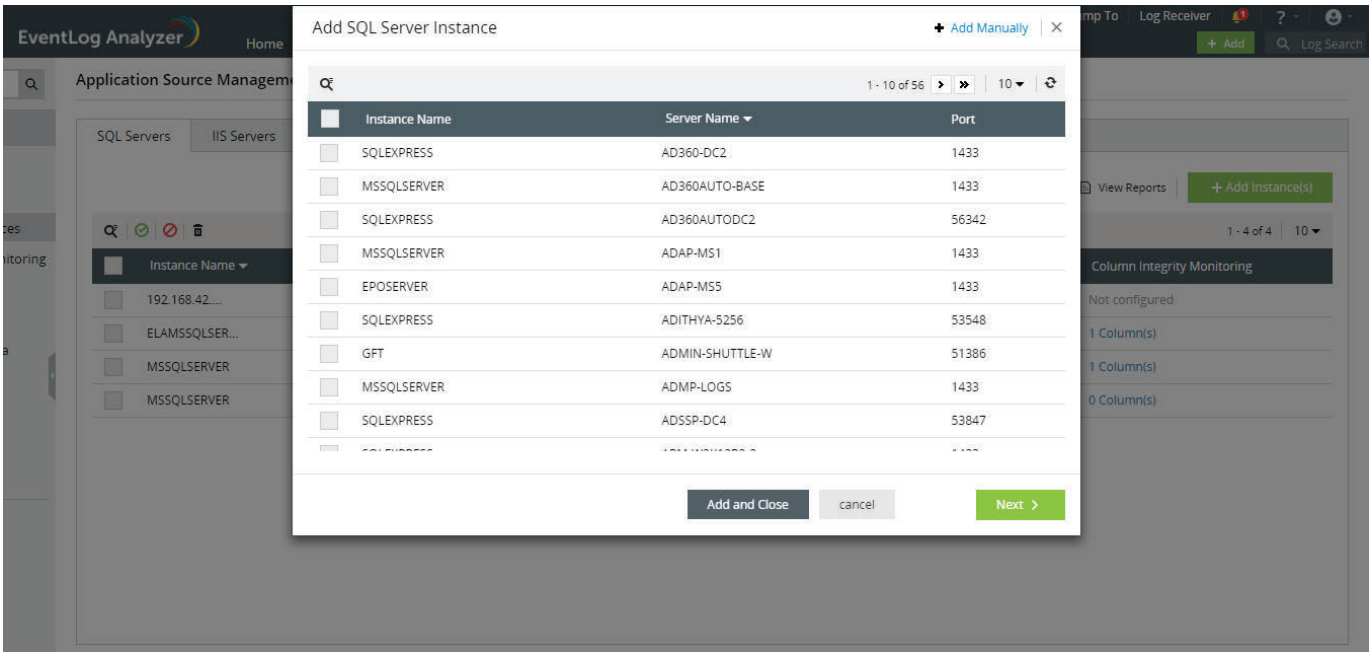
- **Unauthorized activity:** When permissions and user accounts are not properly managed, users may gain elevated rights and unauthorized access to sensitive data, which they'll be able to modify. Also, external attackers might try to access confidential data with stolen credentials. The user accounts they use may not have enough privileges to access the data, resulting in unauthorized user access attempts. You need to monitor all such events to block attacks at the earliest stage.

- **Suspicious logon activity:** User accounts with weak passwords can easily be compromised. Attackers can easily gain control of such accounts by hacking in using brute force or other password cracking methods. If these accounts are privileged and have elevated access, hackers get free rein over highly confidential data.

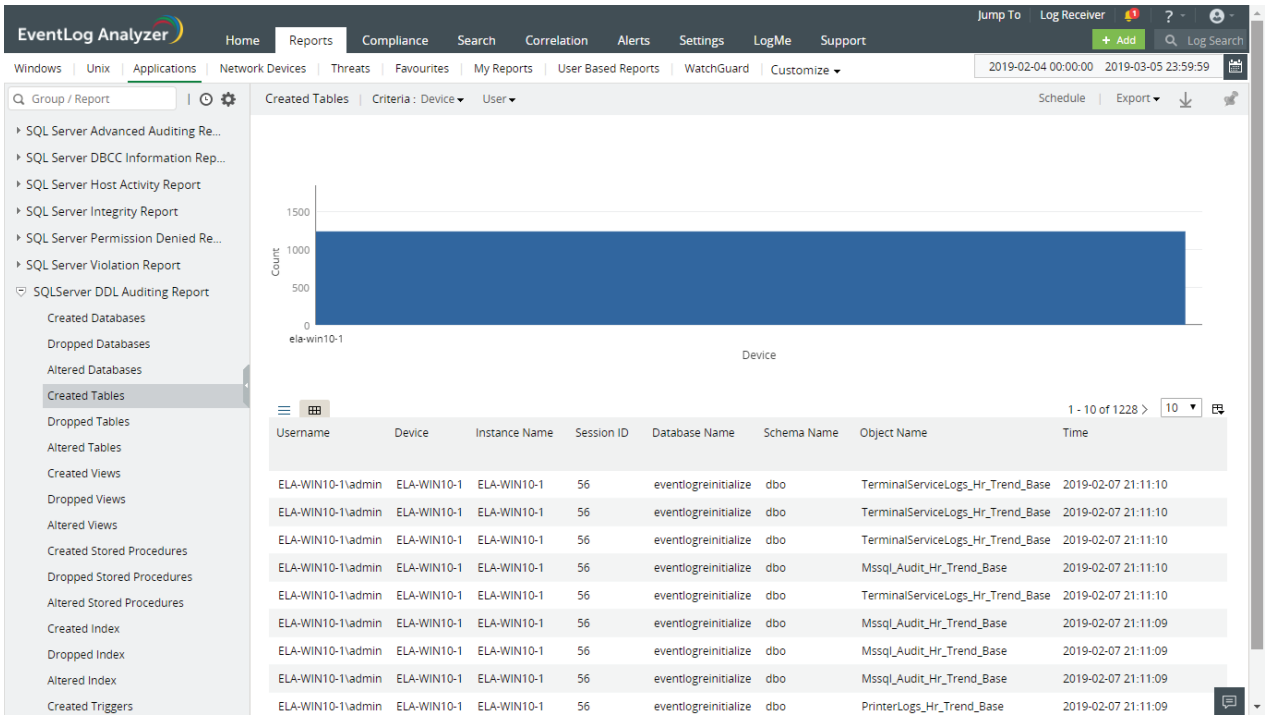
- **Inconsistent updates:** Failure to apply updates and patches released by your database vendor can make your server vulnerable to viruses and other attacks.
  Inconsistent backups: Without a good backup policy in place, you can lose a lot of data if your server goes down for any reason.

Highlights of SQL Server auditing with EventLog Analyzer

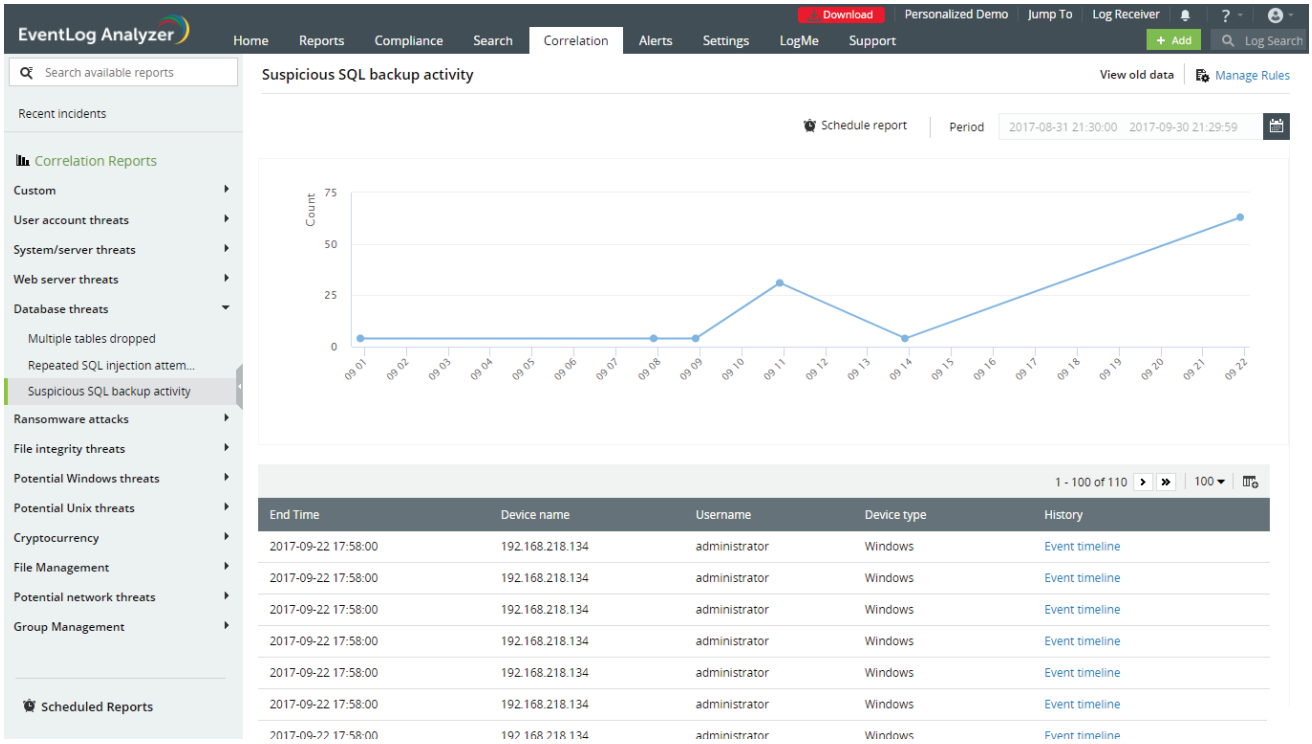
EventLog Analyzer is a log management, auditing, and IT compliance management solution that analyzes database logs with ease. This tool provides extensive reports and alerts for Microsoft SQL Server that help you enhance your security posture. EventLog Analyzer offers a number of features, including:



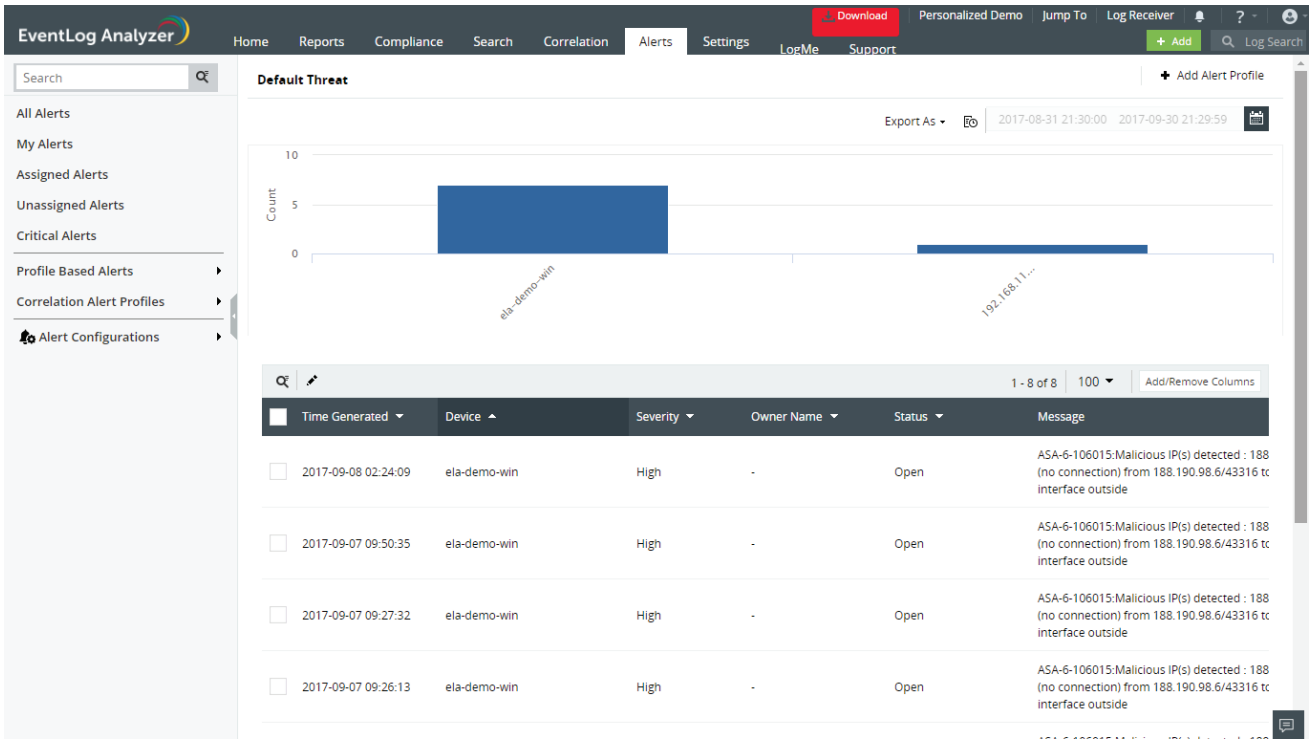
- **Autodiscovery of SQL Server instances:** Automatically discover all the SQL Server instances in your network so you can start auditing them right away.



- **In-depth auditing reports and alerts:** Get detailed information about:
  - **DDL and DML activity:** Understand how your databases and tables are being used and modified.
  - **SQL Server activity:** Track SQL Server startups and shutdowns, and track changes made to user accounts and server-level objects like audit and audit specification objects.
  - **Low-level database activity:** Delve deeper into database activity with advanced auditing reports about database processes, security changes, connected applications, and more.
  - **Column integrity:** Protect critical columns within your databases from being tampered with or modified erroneously. Track changes made to data values and maintain overall data integrity.



- **Event correlation:** Gain more context around events on SQL servers with event correlation. This feature correlates events occurring across SQL Server and other applications and devices to discover suspicious patterns of activity. For example, the predefined Suspicious SQL Server Backup rule identifies potential brute force hacks of your Windows machines followed by a SQL backup event.



Threat intelligence: Receive notifications based on the latest threat feeds and identify known malicious actors trying to interact with your database.

Database auditing scenarios

EventLog Analyzer provides over 120 predefined reports and alerts for Microsoft SQL Server. Some of the most commonly used reports and what they can do are listed below:

Report/alert name	Category	Use case
Dropped databases	DDL auditing	**Detect anomalous or mass data removal:** Ensure that critical data isn't lost forever by launching immediate recovery efforts.
Selected tables	DML auditing	**Track database accesses:** Understand what data is being accessed and by whom.
User account altered	Account management	**Manage database users:** Prevent unauthorized accounts from gaining access to sensitive data.
Top logons based on user	Server auditing	**Discover server logon trends:** Identify the most active users, and detect potentially compromised accounts in cases of abnormally high activity.

Suspicious SQL server backup	Security	**Detect suspicious backup activity:** Get notified of unauthorized database backups.
Column modified	Column integrity monitoring	**Maintain data integrity:** Track changes made to the values of sensitive database columns.
Connected applications	Advanced auditing	**Track dependent applications:** Audit all applications that interface with your database, and ensure no unauthorized

With its comprehensive auditing and alerting capabilities, EventLog Analyzer serves as the perfect tool to monitor activity, gain insights, and discover and prevent breach attempts on your SQL server.