ManageEngine
EventLog Analyzer

Privileged user activity monitoring and auditing

www.eventloganalyzer.com

Introduction

Of all the user accounts in your organization, privileged user accounts have the most bearing on your network security due to their administrative power. Your organization's sensitive data stores, critical servers, and other important network devices are only as secure as the accounts entrusted with their care.

These accounts—belonging to your organization's database administrators, system administrators, and other network administrators—are prime targets for external attackers looking to gain full control over your network resources. But external threats aren't the only problem organizations need to worry about. Administrators may exhibit malicious intent by abusing their privileges, or they may act carelessly with their credentials or systems.

To add to this, multiple compliance policies such as PCI DSS and SOX mandate the thorough auditing of privileged user activity. This makes privileged user activity monitoring not just a preference, but a necessity. This guide explains the best practices for privileged user monitoring, as well as how EventLog Analyzer can be used to report on all your privileged users' activities and alert you about any suspicious activity.

Privileged user monitoring best practices

1. Perform a regular inventory of critical assets and privileged accounts.

In mid to large-size networks, it's important to keep track of newly added critical systems and applications along with the privileged accounts associated with them. Track newly created users= and permission changes to know which accounts' rights have been elevated. This awareness helps you maintain complete visibility and control over your network so that no privileged activity gets missed.

2. Enforce strong privileged account security practices.

Given that privileged accounts are likely targets for attackers, it helps to enforce tight security protocols around them, like password complexity requirements, unique accounts for each user, clearly-defined access policies, and more. You can also track password changes and logon activity to identify any hacking attempts, anomalies in account usage, possible account sharing, and more.

3. Provide only necessary permissions.

Even privileged users can have too many privileges. A user may be given write access to a sensitive folder when they only need to read it, or they may be given access to an entire database when they only need to work with selected records. When critical resources are accessible by several unnecessary users, it only increases the chances of a breach. This is why privileged users must only be provided the rights they require.

4. Maintain a separation of duties between privileged users and those auditing them.

The tools and processes used to monitor your privileged users should not be managed by the privileged users themselves. Your monitoring solution's administrators should be independent of the remaining network administrators. This separation of duties helps ensure that privileged users cannot tamper with their audit trails or reports. Entrust your monitoring and security auditing activities to your security operations center (SOC).

5. Report on all privileged activities.

It isn't necessary to monitor all the actions of regular employees, but it is important to track all privileged user activities. Any action taken by a privileged user, like a logon failure or configuration change, could be an indicator of an ongoing attack, however innocent it may seem. Maintaining detailed reports will prove useful during compliance audits or forensic investigations.

Auditing privileged user activity with EventLog Analyzer: Important reports

EventLog Analyzer is a comprehensive auditing solution that lets you centrally monitor all your network devices, servers, and applications. The solution helps you constantly monitor your privileged users and provides you with detailed audit trails and reports; it also alerts you in case any suspicious activity is detected.

Some key report types include:

Logon activity monitoring: Auditing logons helps you understand when and how administrators log on to your network, so you can catch anomalies like possible account sharing, hacking attempts, or irregular logon times.

> **Reports:** Unix Logons | Unix Logoffs | Unix Failed Logons | Router Logons | Router Failed Logons | Firewall Logons | Firewall Failed Logons | Session Activity Monitoring Reports

User account changes: Monitoring user account changes helps you stay on top of the various privileged accounts in your network as well as the various changes made to account settings.

> **Reports:** Unix Added User Accounts | Unix Deleted User Accounts | Unix Groups Added | Unix Groups Deleted | Password Changes | Failed Password Changes | Special Groups Assigned to New Logon | Symantec Endpoint Admins Added | Nessus Admin Discovery Report | Nessus Elevated Admin Privilege Failures

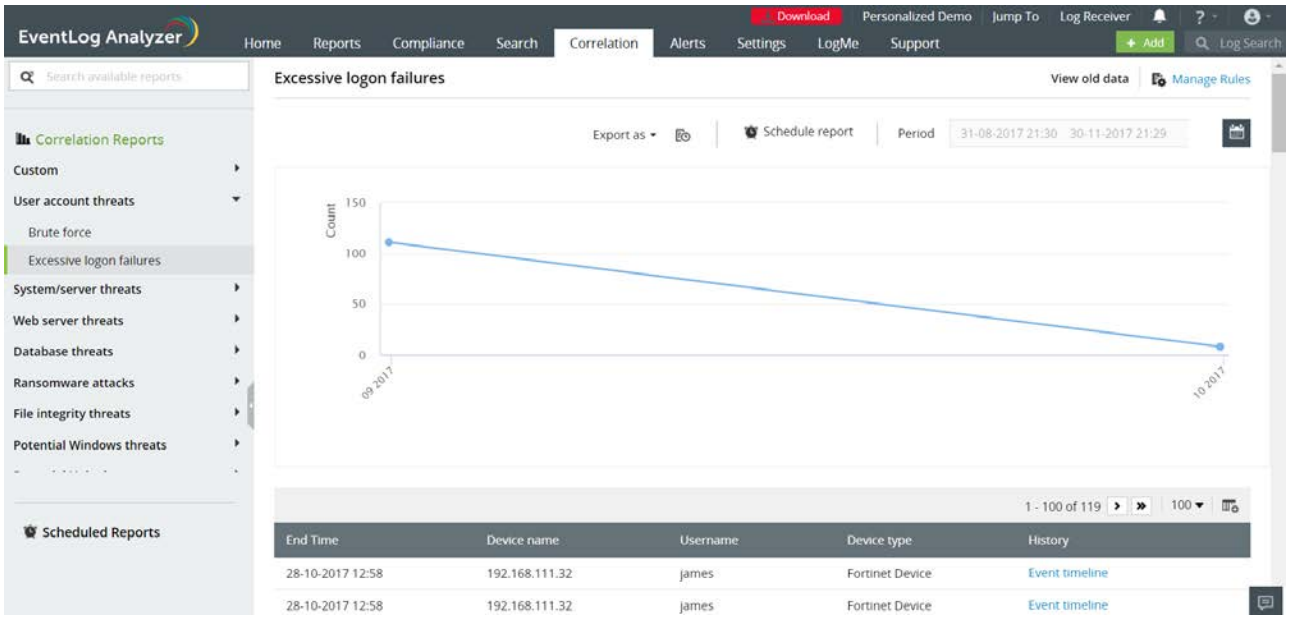
System and configuration changes: Tracking important configuration changes made by privileged accounts is essential as a single change could create a security loophole that allows a hacker to gain access to your network.

> **Reports:** Software Installed | Failed Software Installations Due To Privilege Mismatches | Windows Updates Installed | Registry Changes | Windows Backup and Restore | Firewall Rule Added | Firewall Rule Deleted | Firewall Settings Changes | Router Configuration Changes | Router Commands Executed

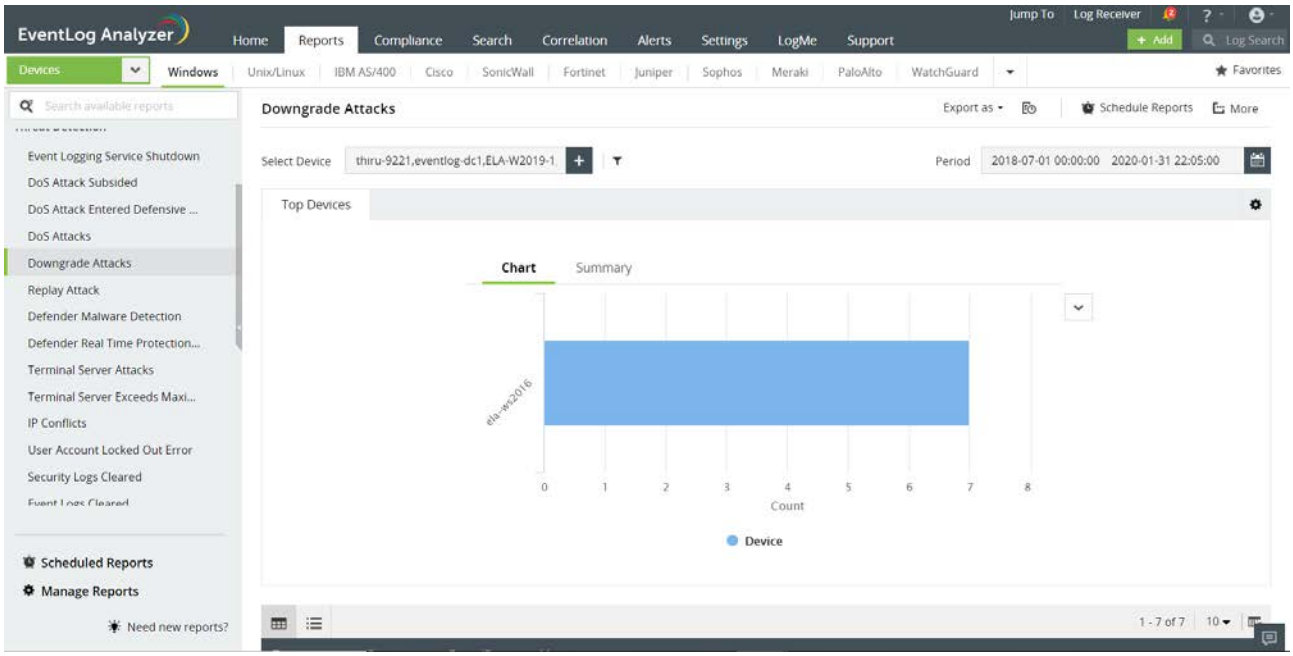
Sensitive data access: Auditing privileged activity on critical database and file servers helps you protect sensitive business data from unauthorized access.

> **Reports:** DDL Audit Reports | Privilege Abuses | Admin Authority Changes | Permission Changes | Owner Changes | Database Backup Report | Database Permission Denied | Access Violation | File Permission Changes

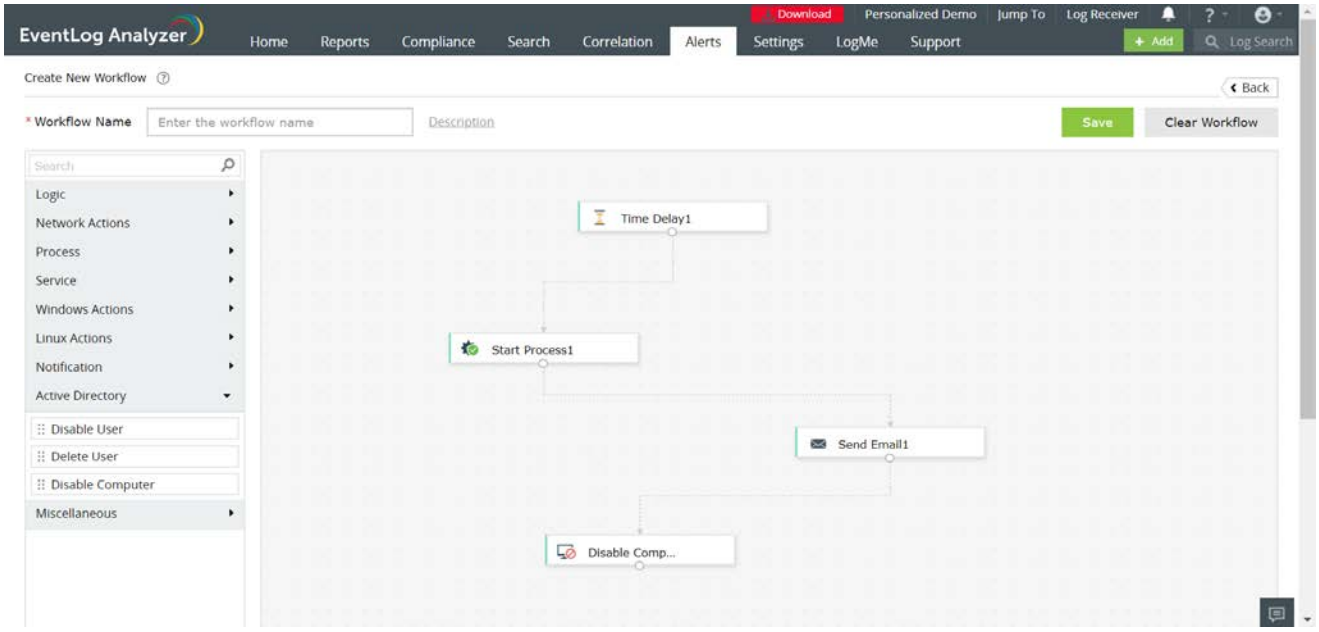
Highlights of EventLog Analyzer



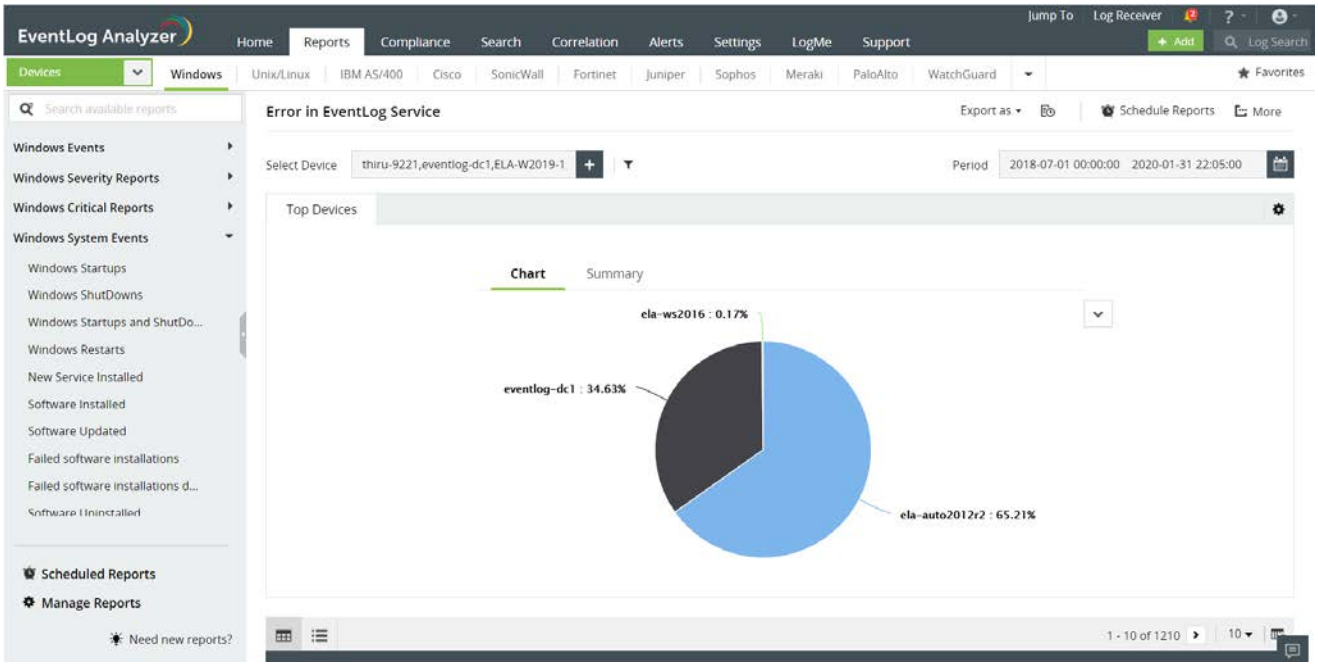
Advanced Event Correlation: The advanced correlation engine contains over thirty predefined attack rules, including those for ransomware, brute force, and more. You can correlate logs from multiple log sources and create rules to suit your business environment.



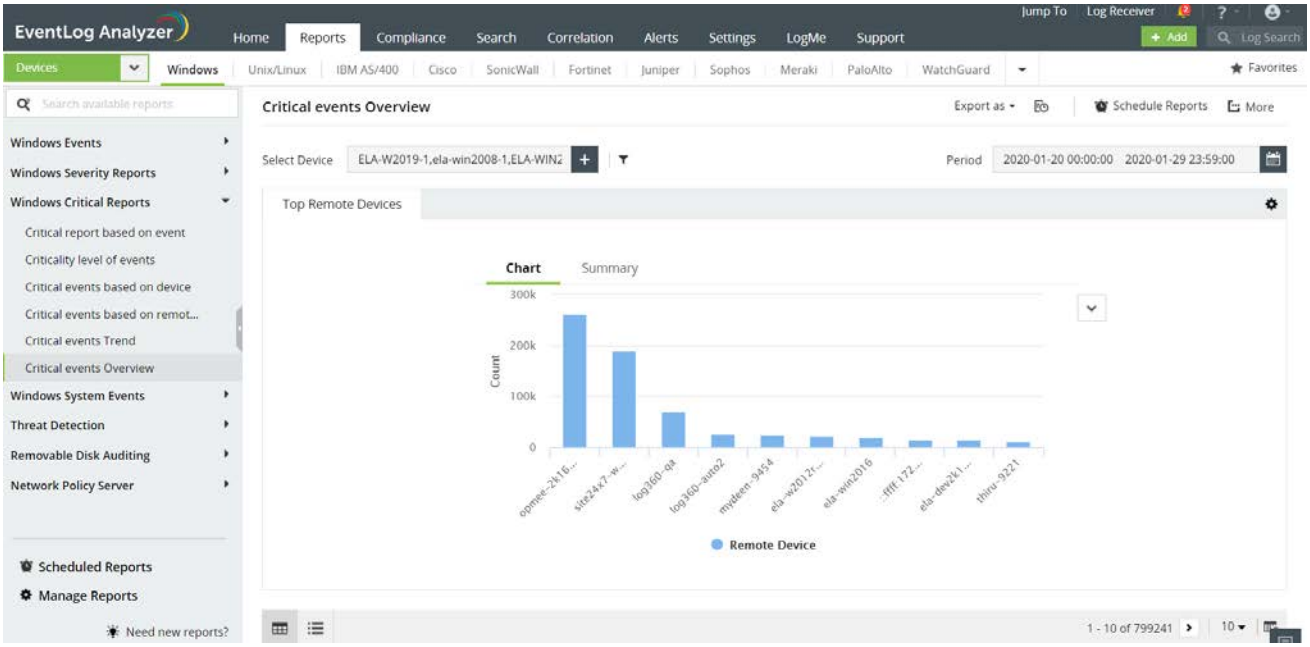
Dynamic Threat Intelligence: The advanced threat intelligence platform comes with a built-in STIX/TAXII feed processor. You can get real-time alerts for suspicious inbound and outbound traffic from malicious domains and callback servers. Additionally, the advanced threat analytics add-on provides deeper insights on the malicious source including details on the reputation score of the IP, history on when it was flagged as malicious, geo location of the threat origination, and more.



Built-in incident management console: Track the response and resolution process of incidents by automatically creating tickets from alerts and assigning them to the right administrator based on the device or device group that generated the alert. Keep track of incident tickets with the built-in ticketing option, or raise tickets in external help desk tools - ServiceDesk Plus and ServiceNow. You can also choose from the multiple built-in workflows that automatically responds to incidents, like disabling compromised computers and locking hacked or malicious user accounts.



Comprehensive log management: Collects, analyzes, correlates, searches, and archives log data from over 700 log sources. Includes a custom log parser to analyze any human-readable log format.

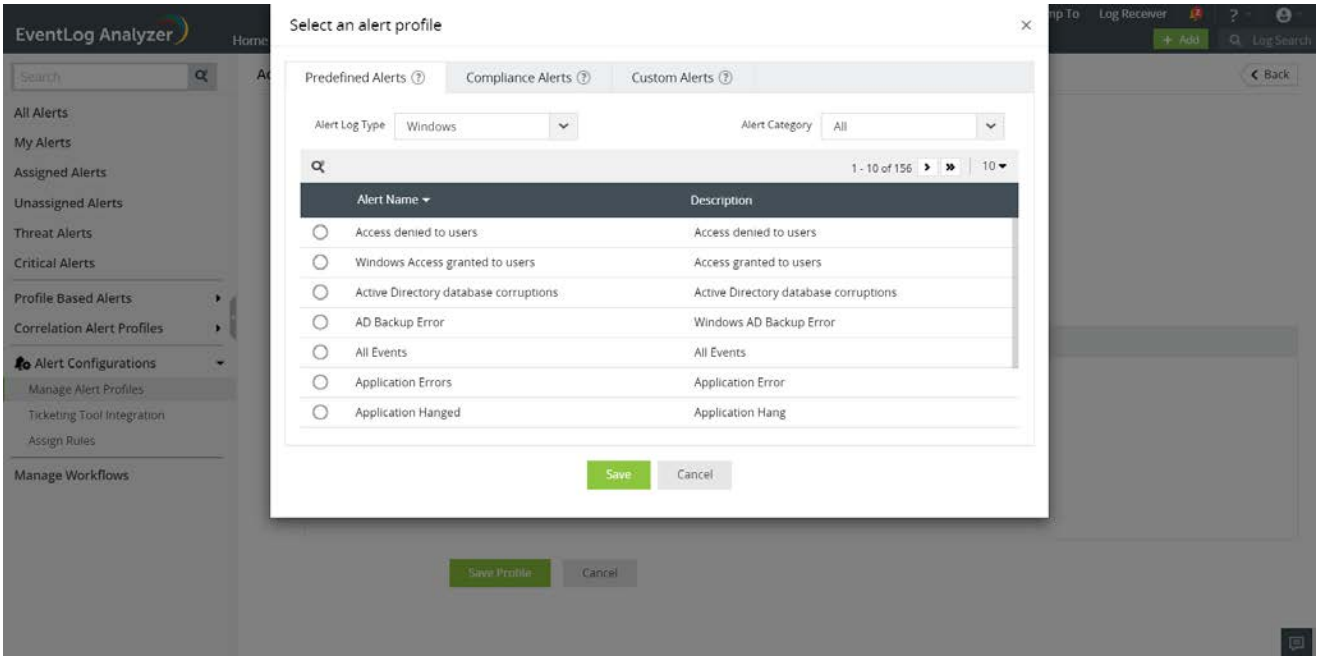


In-depth audit reports: Access intuitive reports which can be easily exported or scheduled. These reports include

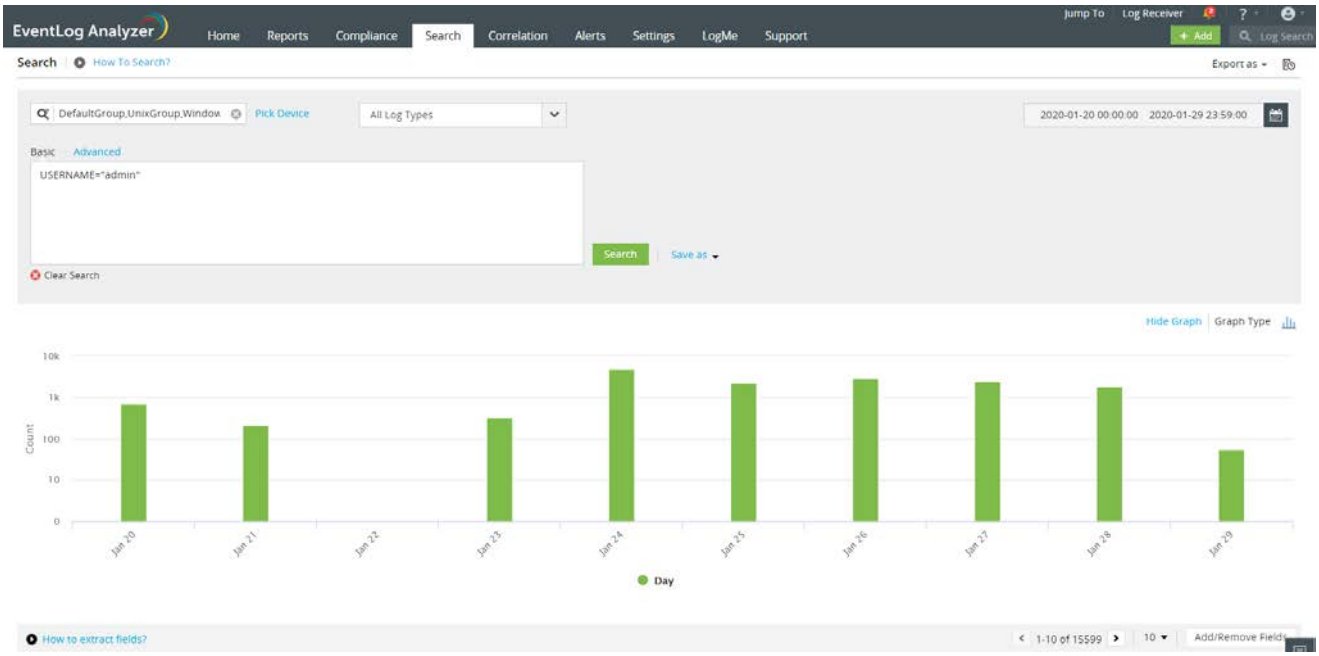
> **Independent privileged user activity reports:** Get individual reports for various privileged activities, such as configuration changes, software installations, sensitive data accesses and changes, and more.

> **Consolidated reports:** Get a consolidated view of all privileged user actions in your Windows network in the User Activity Overview report. The graph can also be broken down by user in the User Based Report.

> **Compliance reports:** Generate predefined reports for various compliance policies, including SOX and PCI DSS, which mandate the thorough auditing of privileged user activity



Security alerts: Receive notification about any anomalous or suspicious activity from privileged users in your network. Get alerts for independent events or multiple events correlated across your network. You can also get threat feed-based alerts and identify communication between privileged users and known malicious entities.



Forensic investigations: Use the advanced search engine to investigate security incidents and discover their root cause. You can save the search results as reports and use them to present any findings.

Privileged user accounts hold a lot of power over your network. With EventLog Analyzer, you can ensure they are used responsibly and are secured against attacks

ManageEngine
EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

$ Get Quote Download