ManageEngine
ADAudit Plus

Overview of ADAudit Plus

ManageEngine ADAudit Plus is a unified platform for Active Directory (AD), Entra ID, Windows Server, workstation, and file server auditing, security, and compliance.

Top 10 capabilities of ADAudit Plus	3 compelling reasons to choose ADAudit Plus
• Real-time change notifications • User logon monitoring • Account lockout analysis • Privileged user monitoring • File change auditing • File integrity monitoring • UBA-driven anomaly detection • Attack surface analysis • AD backups, recovery, and change rollbacks • Compliance reporting	• ADAudit Plus has been named a Gartner® Peer Insights™ Customers' Choice for SIEM for 4 years in a row. • You can go from downloading ADAudit Plus to receiving audit-ready reports and security alerts in around 30 minutes, without professional help. • ADAudit Plus is licensed per server, so even with a growing number of users each year, you can continue to ingest log data without additional costs.

For more information on the top 10 capabilities of ADAudit Plus, check out this data sheet.

Market drivers

Auditing is essential for addressing security, operational, and compliance needs in a Windows Server environment. However, limitations in native Windows auditing tools, such as the need for expertise, time-intensive processes, and missing capabilities, necessitate the use of third-party auditing tools like ADAudit Plus.

Centralized auditing:

Event logs that contain audit data are not replicated, so manually reviewing logs on each computer is impractical. While Windows Event Forwarding enables log aggregation, setting it up involves technical complexity. ADAudit Plus simplifies the process by aggregating logs from all computers into a central console.

Threat mitigation:

Windows Task Scheduler can send alerts about specific event IDs but cannot detect unusual patterns like multiple failed logons followed by a successful one—a telltale sign of a brute-force attack. ADAudit Plus leverages correlation and machine learning to detect such patterns in real time.

Compliance reporting:

Windows event logs often lack complete context. For example, AD attribute changes are split across events, needing manual correlation. PowerShell can help but isn't practical for real-time auditing at scale. ADAudit Plus provides a consolidated audit trail of all changes and helps organizations meet compliance requirements.

For more information on how ADAudit Plus helps organizations overcome the limitations of native Windows auditing tools, check out this e-book.

Profiling evaluators

Evaluators can be broadly classified into:

- **IT administrators and auditors:**
  As the end users of ADAudit Plus, they will be more receptive to how we address common pain points that they face. Their concerns involve addressing the auditing, security, and compliance challenges that they face in their day-to-day work as well as the ease with which the tool can solve them.

- **Security managers:**
  They are CIOs, management information system managers, and IT and operations leads, or they hold similar managerial positions. Their primary interests are usually business benefits, our reputation among clients, recognitions by independent analysts, and the ROI.

- **Technical evaluators:**
  Their primary interests are the back-end workings of the tool, deployment, and other technical specifications of the product.

Pitching ADAudit Plus to prospects

Here are some key points you can present to different prospects:

Administrators and IT auditors	Security managers	Technical evaluators
Get instant alerts about changes, including who performed what **change**, when, and from where in your IT environment. Continuously track user **logon** activity and audit everything from logon failures to the logon history. Receive alerts about **lockouts** and analyze the reason by tracking down the source of the authentication failures. Audit **file** access attempts, permission changes, and more across Windows and NAS file servers. Detect over 25 AD attacks and GPO, Azure, AWS, and GCP misconfigurations using the **Attack Surface Analyzer**. Spot anomalous logon, file, user management, and process activities using **UBA**. **Back up** and restore AD objects like users, computers, groups, organizational units, and GPOs. Also, undo changes made to AD objects. Get audit-ready **compliance** reports for SOX, the GDPR, and other IT mandates.	ADAudit Plus provides a **single pane of glass** for AD, Entra ID, Windows Server, workstation, and file server auditing, security, and compliance. ADAudit Plus has been named a Gartner Peer Insights Customers' Choice for SIEM for 4 years in a row. This recognition cements our place as a standout among IT auditing solutions on the market. ADAudit Plus is trusted by over **10,000 organizations** across verticals like healthcare, education, government, retail, and banking. ADAudit Plus is **licensed per server,** unlike other IT auditors that are licensed per user. With per-server licensing, even with a growing number of users each year, you can continue to ingest log data without additional costs. You can save around $4,226 by automating IT audit report generation with ADAudit Plus. You can check this for yourself using this ROI calculator.	ADAudit Plus is **easy** to deploy and operate, and we provide training courses that will help you set up and get the most out of the tool. ADAudit Plus provides both **agent**-based and agentless log collection modes. Audit data can be compressed, **archived**, and retained for as long as you need. Audit data can be forwarded to syslog servers and other **SIEM** solutions like Splunk, making SIEM processes more efficient and cost-effective. Users can be granted varying levels of access to ADAudit Plus to ensure **role-based access**.
Conversation starters		
Do you find it difficult to trace the root cause of frequent account **lockouts** or failed logons in your AD environment?	Are you confident that your current auditing **setup** can detect and respond to insider threats or misconfigurations before they escalate?	Have you had challenges in deploying or **scaling** auditing tools across hybrid environments with AD, Entra ID, and file servers?

Are you currently receiving real-time alerts for **critical changes** happening in AD or on file servers? How confident are you about spotting anomalous **user behavior** before it turns into a serious security threat?	How are you ensuring your **IT team** complies with regulations without overwhelming them with manual reporting work? Do your clients or **auditors** ask about how your organization monitors privileged access or critical changes?	How **customizable** and granular is your current auditing setup when it comes to filtering alerts or scheduling reports? Do you currently have a way to **back up AD** and roll back unintended changes without relying on complex scripts?

Tackling comparisons

ADAudit Plus' top three competitors, Quest, Netwrix, and Lepide, are licensed on a per-user basis. So, the more users an organization adds, the more it pays. This means that even without an increase in the number of data sources, costs will likely increase each year. However, ADAudit Plus is licensed on a per-server basis, which ensures that an organization can ingest data from all sources and still remain within its budget over the years.

Competitor	Additional capabilities provided by ADAudit Plus
Quest Change Auditor	• Risky configuration detection for GPOs, Azure, AWS, and GCP • Support for additional NAS systems, including Synology devices, Hitachi solutions, Huawei devices, Amazon FSx for Windows File Server, Amazon FSx for NetApp ONTAP, QNAP devices, and Azure Files • Agentless log collection • Incident response
Netwrix Auditor	• Risky configuration detection for GPOs, Azure, AWS, and GCP • Windows Local Administrator Password Solution auditing • PowerShell auditing • AD Certificate Services (AD CS) auditing • Support for additional NAS systems, including Hitachi solutions, Huawei devices, Amazon FSx for Windows File Server, QNAP devices, and Azure Files
Lepide Auditor	• User idle and active hours tracking • AD Federation Services and AD CS auditing • LDAP authentication auditing • PowerShell auditing