ManageEngine
EventLog Analyzer MSSP

Managing multiple clients, made easy!

A web-based log **management solution** to scale your MSSP business across borders.

Table of Contents

Challenge: The evolving need for great MSSPs

As the complexity of cyberattacks increase, more businesses now realize the importance of having a team, either internal or external, to manage security operations and ensure business continuity. As a result, we can witness many traditional IT services and consulting providers entering the MSSP market, either through acquisitions or partnerships. With the MSSP space becoming crowded, here are five capabilities that customers expect from their MSSP partner:

1. Ability to scale with the customer

With the increased adoption of the cloud, more organizations around the world are growing rapidly. As a MSSP, you should be able to support your client's business during this stage. Your customers need you to be there for them, and proactively implement the security tools that support their anticipated growth.

However, scaling doesn't necessarily always mean upwards. As the number of customers you support varies, you need security tools that can easily enable you to scale up or down. It's best to develop a strategic plan for scalability before the issue arises. This allows you to dynamically adapt to risks and scale to secure thousands of customer devices all at once.

2. Ability to share threat feed intel

One way to mitigate risks in this evolving threat landscape is to have a shared intel on the latest threats. This can be accomplished by using STIX/TAXII threat feeds to gather real-time intel on malicious URLs, IPs, files, and more. Threat intelligence lets you stop attack attempts promptly, as well as triage security alerts and reduce false positives.

A significant benefit is that you can leverage the threat intel acquired from one customer to check for similar patterns in other customer environments. This provides a competitive advantage over other security service providers that don't offer this service. A security tool that can integrate with open-source and commercial threat feeds can save time spent on preliminary threat hunting practices.

3. Ability to quickly respond to security incidents

Many enterprises are turning to MSSPs to proactively detect and respond to security incidents on a daily basis. To combat evolving threats and complex incidents, you need to be able to coordinate with your customers during incident response activities.

Every minute of inactivity during an incident gives the hacker an upper hand to inflect damage. Once a threat is identified, MSSPs need to escalate the event to the organization and develop counter measures. Integrating with the client's processes, and automating alerts and response measures can reduce false positives during a large-scale attack.

4. Ability to provide a great support experience

Cybersecurity has become one of the largest costs for organizations, complicated by the industry's talent crunch. Acquiring the best talent and developing a robust in-house team is becoming increasingly difficult. That where MSSPs come in.

Business turn to security service providers for the security expertise and the 24x7x365 support they can provide. MSSPs are also expected to have:

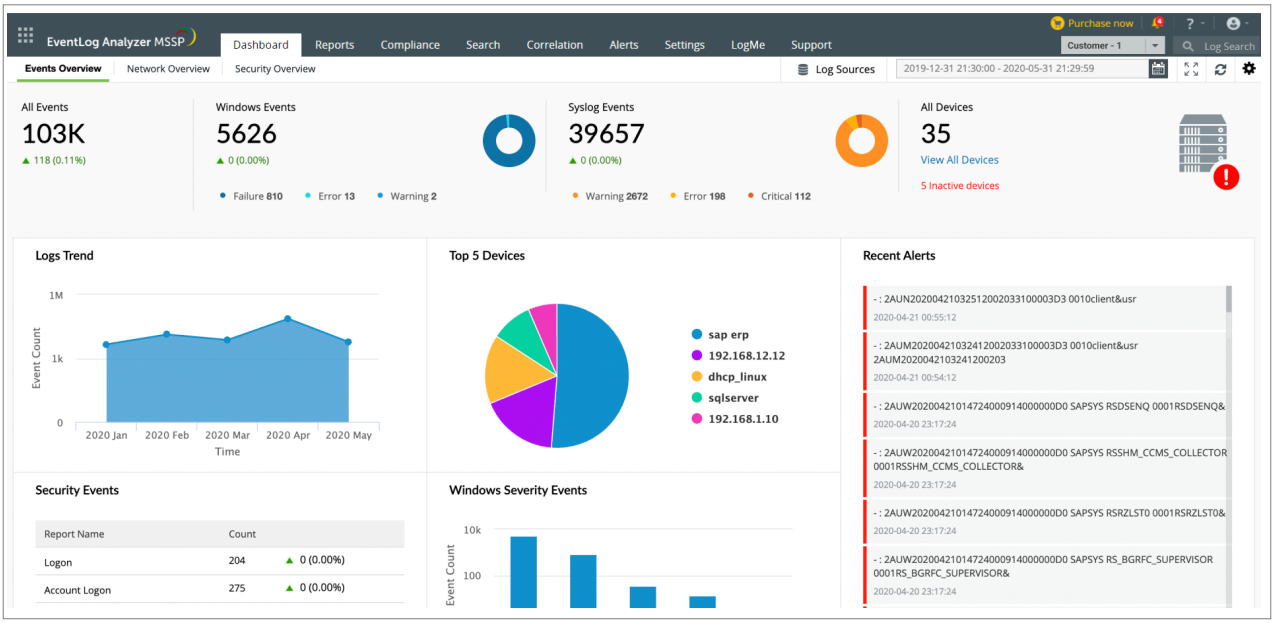
- Skilled and certified security staff who can give personalized response plans and security roadmaps based on the client's unique needs
- Local IT technicians who can arrive on-site to resolve issues
- A good relationship with software vendors so tools can be customized to quickly resolve security issues

5. Ability to demonstrate a strong internal security infrastructure

As more organizations start relying on MSSPs to control of their security operations, you are required to strengthen your internal security as well. This is essential as more MSSPs are becoming the primary target of ransomware attacks, and hackers strive to find a vulnerability that can be exploited and used to gain access to your client's network.

Implementing security best practices will protect your data and your client's data. This includes restricting access to which SOC analysts can view which customer's data, securely storing all your customer data, adhering to your client's privacy and security compliance regulations, and implementing multi-factor authentication.

Solution: A centralized multi-client log management tool



As an organization's security service expectations grow, MSSPs also need to strengthen their security arsenal with the best-in-class tools to help meet the needs of their customers. That's why ManageEngine EventLog Analyzer MSSP is a must-have solution in your security strategy.

EventLog Analyzer MSSP is the ideal platform for security service providers to provide visibility into what's happening in each of customer's environment. The solution is especially helpful for monitoring large client networks of thousands of log sources spread across multiple geographic regions. It follows a distributed architecture with multiple managed servers being controlled by a single, central admin server.

You can use the tool to gather insights from the detected security events and defend against potential attacks using sophisticated threat response techniques. Integration with Webroot BrightCloud® Threat Intelligence Services delivers real-time, accurate threat feeds on malicious URLs, IPs, files, and more. With this solution, you can monitor outbound traffic and send real-time alerts when any communication takes place with malicious or block listed IPs.

EventLog Analyzer benefits

Comprehensive log collection

Auto-discover log sources and add them for monitoring. Use centralized, secure log collection with either agentless or agent-based methods.

Real-time event log correlation

Discover security incidents by correlating events across your network. Includes more than 30 predefined correlation rules and a custom correlation rule builder.

Secure log archival

Retain network log data for as long as needed. Archives are secured using time stamping and hashing techniques.

Efficient log forensics

Perform high-speed log search using flexible search options. Discover the root cause of attacks, and perform forensic investigations.

Streamlined incident management

Use the built-in ticketing system to assign incidents as tickets, track their status, and speed up the incident resolution process.

EventLog Analyzer MSSP deployment: Simple rules of thumb

EventLog Analyzer MSSP is an on-premise application that needs to be installed in your client's servers. However, when you need to monitor cloud infrastructures, you can use agents to pull the necessary log data for analysis.

Some MSSP models involve taking customer data from their source for storing and processing them in the MSSP's environment. While this can ensure that they have control of all the data, it poses many risks when they face an attack, making it easier for attackers to gain access to the data of multiple customers. To minimize this risk, EventLog Analyzer MSSP enables discrete data management by storing them in separate client environments, while providing SOCs the visibility into their entire network.

How do you implement EventLog Analyzer?

The MSSP edition of EventLog Analyzer involves deploying one admin server and many managed servers. The managed servers can be installed at different client locations (one per LAN environment) and connected to the central admin server.

Managed server

The managed server is the installation of EventLog Analyzer that collects logs from sources present in your client location. This information is then relayed onto the single central admin server.

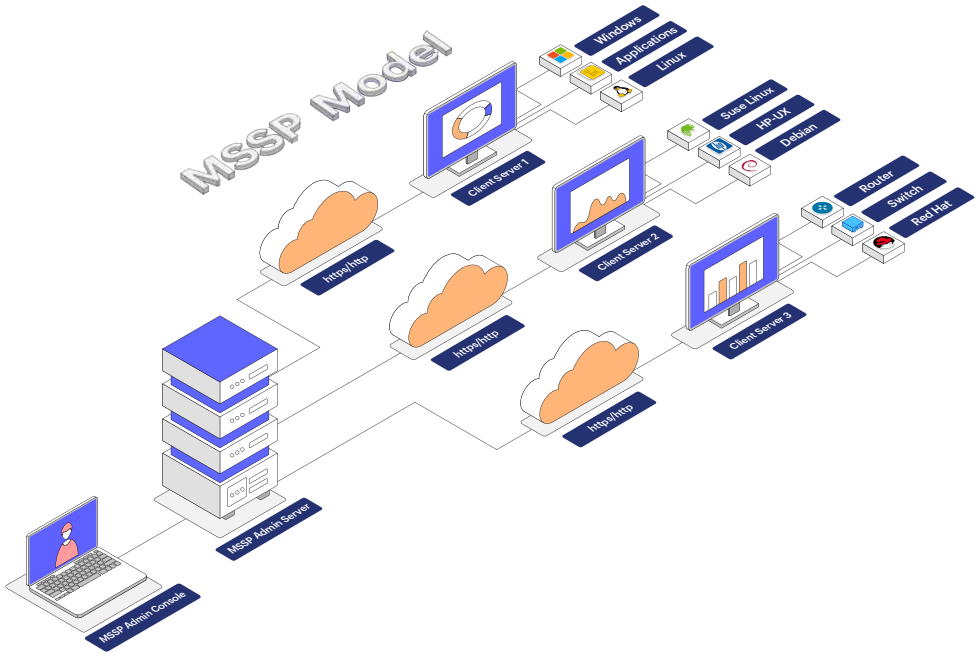
Admin server

The admin server is the installation of EventLog Analyzer which aggregates information from all the other managed servers installed across the globe. The admin server acts as a single central console and displays reports, alerts, and other log information from all the managed servers.

MSSPs need to install the EventLog Analyzer premium editions in both their own environment and that of their client's. Once the alerts, incident response measures and threat intelligence features are set up in each customer's instances, they will be able to get total visibility from the centralized admin server console.

Note:

A single admin server is designed to manage up to 50 managed servers.



Each node at the customer's side represents a complete standalone deployment with its own alerts, high availability, incident response, and data protection capabilities. The logs collected by the managed server are stored only in the managed server database. You can't store the logs in the admin server. However, you can forward the logs to the admin server to archive them. As an MSSP, architecting the software this way will solve the following goals for you:

1. Ensure client data is secure by keeping them in their respective environments.
2. Customize the product and security strategies specific to each customer's industry or use case.
3. Gain a central view into what's happening in each customer's network and respond to threats immediately.
4. Prevent performance issues by servicing each customer's deployments separately without affecting the other ones.
5. Every industry or business needs to follow a specific compliance law. You can set alerts for the respective compliance report and notify your customers when their is a violation.

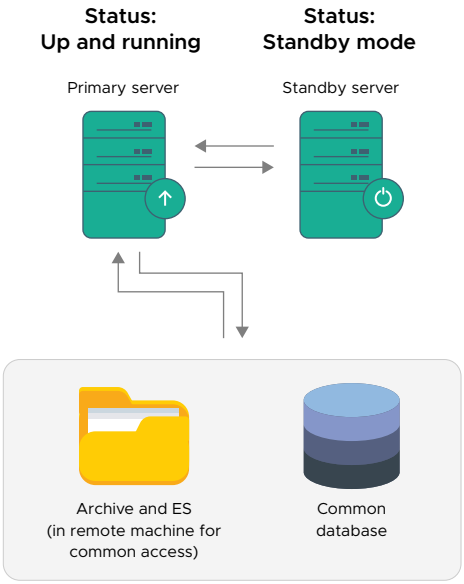
High availability architecture and disaster recovery measures

The EventLog Analyzer MSSP server is a critical component from the perspective of an organization's network security. In the unlikely event of a major glitch in your environment which causes the EventLog Analyzer MSSP server to go down, log processing and analysis would come to a halt. This stoppage might turn out to be a gateway for security breaches. Such breaches can cause not just huge financial losses and non-compliance penalties but also loss of credibility and reputation. To avert such disasters, EventLog Analyzer MSSP has a backup mechanism.

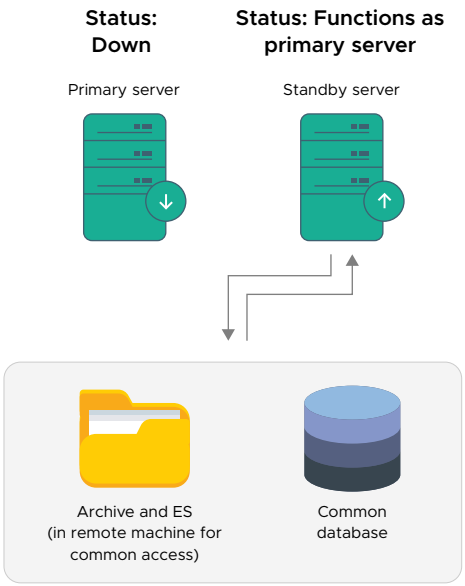
As a disaster recovery measure, EventLog Analyzer MSSP offers a high availability feature. It allows for every EventLog Analyzer server, both admin and managed, to be configured with a standby server. This standby server would continuously monitor the primary server. In case the primary server fails, the standby server would immediately step in and start performing all the duties of the primary one without any lapse.

How the High Availability feature works

EventLog Analyzer's high availability setup includes two separate installations. One of them acts as a primary server while the other acts as a standby server. Both the installations would point to the same database. And the archived log data and Elasticsearch data will be available in the common network share.



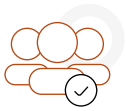
By default, the primary server will deliver all the required services. The standby server will also be started but it will remain in the standby mode. But it will continuously keep monitoring the primary server's status. Whenever the primary server fails, the standby server will kick in and take up the role of the primary server. It will start collecting the logs to prevent any data loss and continue to perform all the functions of the primary server until the actual primary server is brought back into service.



Other security features of EventLog Analyzer MSSP

Secure web communication:

EventLog Analyzer MSSP is a web-based solution with a web client that can be accessed from anywhere in the network. Enabling HTTPS protocol ensures that all web communication is secure.



Role-based access control:

RBAC enables you to compartmentalize your data among the product's technicians. Three access levels are provided: administrator, operator, and guest, in order to limit user access and control to specific features and device information. This way, you can ensure that data is accessed only by authorized personnel.

Audit EventLog Analyzer technician actions:

The solution provides a built-in option to generate the audit trail of all user actions performed in the product. This allows you to ensure accountability within the solution itself.

Session termination after idle time:

You can set up a session expiry time and if the session is idle for more than 30 minutes (which is the minimum time), then the session will be terminated. Users can change the default setting of 30 minutes for session expiry to 10 minutes.

Archive encryption:

Archived data is secured using the AES 256 encryption mechanism.

Tamper detection in archived data:

EventLog Analyzer MSSP has an option to detect tampered log archives. When you enable the Archive Integrity option, the solution shows the status of the archived file as Tampered if it's mishandled. It does this by using time-stamping techniques.

EventLog Analyzer MSSP's file integrity monitoring feature can be implemented on the archived log files to get instant notifications for changes made to the archived log data.

Why you should have EventLog Analyzer MSSP at the core of your services

ManageEngine EventLog Analyzer MSSP is committed to providing a reliable log management solution for security service providers around the globe. With thousands of customers trusting EventLog Analyzer for their internal security needs, it is the ideal solution to build your business on.

Our vision is to empower every organization with the right tools to help them get deeper visibility into security events, accelerate threat detection and response, and enhance their network security posture.

Our value proposition

- Transparent pricing model for organizations of all sizes—based on the number of nodes and add-on security features you choose
- Exceptional 24x7 support experience, and onsite and online training to help you make the best use of the tool
- Support for over 750 log sources and a custom log parser to meet the logging requirements of your customers
- Security hardening features to fortify your organization's internal security—MFA, secure data transmission, and more
- Robust log analytics and automated incident response capabilities to full harness the investments in your skilled manpower

Awards and testimonials

ManageEngine Log360 recognized as a gold winner of the Cybersecurity Excellence Awards 2022

ManageEngine recognized as a 2021 Gartner Peer Insights Customers' Choice for SIEM

Gartner

Recognized in 2021 Gartner Magic Quadrant for SIEM for the fifth time

ManageEngine
EventLog Analyzer MSSP

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. It also offers out-of-the-box compliance reports and alerts that help organizations meet stringent IT regulatory mandates' requirements with ease.

$ Get Quote Download