ManageEngine Log360 | CASE STUDY

4 ways Buyers Products **mitigates threats using Log360**

Company: **Buyers Products** | Industry: **Manufacturing** | Location: **USA**

About Buyers Products Company

Established in 1946, Buyers Products Company has grown to become a leading American manufacturer of equipment for the work truck industry. Buyers Products' mission is to produce the highest quality products, at the best value, in a turnaround time second to none in the industry.

Buyers Products leads the industry in value and velocity for custom manufacturing. The company's manufacturing operations utilize large aluminum, steel, and stainless steel in its standard product line, which allows it to bid competitively and deliver quickly on custom orders.Buyers Products delivers hundreds of custom projects every year—from diamond-tread, aluminum meter boxes, to custom stainless steel spreaders.

Business challenges

Buyers Products previously was challenged in three main areas: security, regulatory requirements, and authorized access.

- Buyers Products handles a significant amount of sensitive data, including customer information, financial data, and operational details. Being a manufacturing company, data breaches can occur through external attacks or insider attacks, leading to the compromise of sensitive information.
- Another challenge that they needed to resolve was meeting necessary compliances, such as those for file storage and data protection.
- Buyers Products also collects and stores various types of data, such as product specifications, and operational data. Protecting this data from unauthorized access, data breaches, or accidental exposure is critical to maintaining customer trust, complying with data protection regulations (such as the GDPR and CCPA), and avoiding legal and financial consequences.

The solution: Log360

Buyers Products was looking for a solution to monitor logs efficiently, ensure it stays compliance ready, and effectively thwart cyberattacks. It decided to go with ManageEngine Log360 to improve its overall cyber security posture after carefully evaluating other SIEM solutions in the market.

According to Christian Eagan, Buyers Products' Network Security Specialist, "The product has most of what we need predefined."

Log360 provides Buyers Products with:

- **Real-time event log monitoring, analysis, and correlation.** Log360 collects and analyzes log data from a variety of sources, including network devices, servers, applications, and databases.
- **Detection and notifications of potential security issues.** By continually monitoring log data, Log360 detects suspicious user actions and unauthorized access attempts. With the alarms this solution generates, Buyers Products can respond quickly to potential threats and mitigate them before they cause substantial damage.
- **An ML-based user behavior monitoring console.** Log360 tracks user activities, especially those with privileged access. This ensures Buyers Products can detect and mitigate insider threats.
- **Built-in compliance reports and audit capabilities.** This enables Buyers Products to comply with its internal policies as well as regulatory requirements. By utilizing Log360 to analyze log data, the organization can efficiently create compliance reports, and carrying out audits.

How Buyers Products efficiently detects threats with Log360

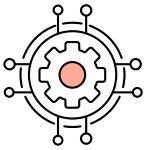
The company's ability to detect and respond to security events has greatly improved since deploying Log360. By utilizing Log360's threat hunting capabilities, Buyers Products is able to string isolated security events together to identify indicators of an attack. With quick, accurate alerts, they can take a proactive stance to prevent damage to its network data and resources.

File integrity monitoring constantly checked files for unauthorized changes, maintaining the integrity and security of important system files, configuration files, and sensitive data.

Eagan also highlighted the ease in setting up the product. "I could find all the information for deploy and utilizing Log360 in their documentation," he pointed out.

Other significant features of Log360

Log360 incorporates technologies and capabilities to automate responses to security incidents, detect unusual user and entity behaviors, and track Active Directory modifications in real time.



Security orchestration, automation, and response (SOAR): This is security technology that compiles all security data from different platforms into a single console, including Exchange Server, Microsoft 365, Infrastructure as a Service solutions, Platform as a Service solutions, Software as a Service solutions, on-premises network devices, servers, and applications. SOAR expedites threat resolution by automating your response to detected incidents using workflow options.

User and entity behavior analytics (UEBA): This technology enables the collection and analysis of the data from users, machines, and other entities in a network, like event logs and packet capture data. Continuous monitoring and analysis of data from different sources helps detect anomalies easily and instantly.

Active Directory change auditing: This capability enables the monitoring and auditing of critical Active Directory changes in real time. You can utilize detailed information on Active Directory objects, track suspicious user behavior, monitor critical changes to groups and OUs, and more to proactively mitigate security threats.

Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download