ManageEngine
Log360

CASE STUDY

# Strengthening cybersecurity: How Log360 helps SafeRack strengthen its network security

## About the organization

**SafeRack** is a company that specializes in providing safety solutions for various industries, such as oil and gas, aviation, rail, and chemical. The company was founded in 2003 and is headquartered in Andrews, South Carolina. SafeRack provides a wide range of products, including gangways, loading racks, safety cages, safety gates, and fall protection systems. These products are designed to improve safety and efficiency in the workplace, and are often customized to meet the specific needs of each customer.

In addition to its products, SafeRack also offers a range of services including site surveys, product installation, and training for employees. The company has a team of experienced engineers and safety experts who work closely with customers to ensure that their safety needs are met.

## Challenges

SafeRack must constantly guard its security perimeter because it often shares its network resources with third parties such as suppliers and other vendors. This causes the perimeter to expand, leading to more attack opportunities. Securing important data, like intellectual property and sensitive customer information, from adversaries required a solution that would help SafeRack proactively hunt for threats, investigate them, and resolve them.

Loy Dsouza, system administrator at SafeRack, also said that the company faced challenges in detecting identity-based security threats, such as account compromises, privilege misuse, anomalous authentications, and suspicious sensitive data modifications.

## Solutions

SafeRack was looking for a solution that could help it proactively hunt for threats, tackle identity-based security threats, monitor and audit its network devices and applications, and also stay ahead in compliance management. ManageEngine Log360, a unified SIEM solution with integrated DLP and CASB capabilities, was able to meet all the company's requirements. "Log360 has become an integral part of our cybersecurity operation," said Desouza. Using Log360, SafeRack was able to:

- Swiftly audit and analyze security data points from different sources across the network with the intuitive and interactive graphical dashboard.
- Immediately spot and automatically block malicious traffic in the network with the advanced threat analytics module.
- Detect insider threats and user-based attacks more easily than ever before with user and entity behavior analytics.
- Sift through voluminous log data and conduct forensic analysis effectively with the search console.
- Receive audit-ready compliance reports and violation alerts that made compliance audits a breeze with the integrated compliance management component.

"Specifically, SafeRack was able to detect privilege abuse and effectively manage privileged accounts from being compromised," said Desouza.

## Other significant features of Log360

**Security orchestration, automation, and response:** Compile all security data from different platforms such as 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, all in a single console. Expedite threat resolution by automating your response to detected incidents using workflow options.

**User and entity behavior analytics:** Collect and analyze the data of users, machines, and other entities in a network, like event logs and packet capture data. Continuous monitoring and analysis of data from different sources will help to detect anomalies easily and instantly.

**Active Directory change auditing:** Monitor and audit critical Active Directory changes in real time. 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.

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