ManageEngine
Log360

USE CASE

Fraud detection and prevention

Fraud detection and prevention

Today, sensitive data access and financial transactions are guarded by digital identities; when these identities are forged, the underlying transaction or data becomes compromised. From the banking and healthcare sectors to insurance companies, fraud plagues multiple industries in the form of malicious account creation, account takeovers, malicious insiders, spoofing, imposter user behavior, and more. It's essential for a security operations center (SOC) to implement an advanced defense mechanism that combines traditional rule-based and new-age machine learning (ML)-based behavioral analytics to detect and prevent fraudulent activities.

How Log360 helps detect and combat fraud

ManageEngine Log360, a comprehensive security information and event management (SIEM) solution, utilizes both rule-based and machine learning capabilities to spot fraudulent activities. Here's how they work to detect and prevent fraud in your network.

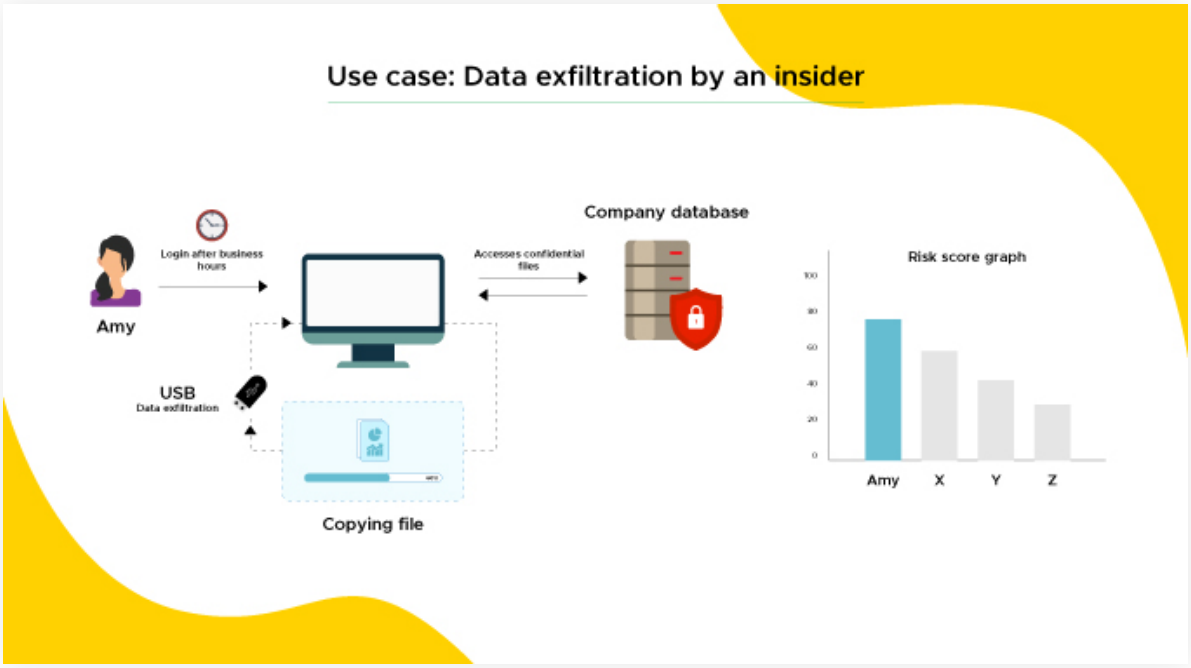
Leveraging a real-time correlation engine to detect fraud events

Log360 has a powerful built-in correlation engine that connects disparate events to detect malicious activity. With a range of prebuilt rules, Log360 can alert you when any fraudulent activities are detected, including brute-force attempts, unauthorized group membership modifications, excessive virtual private network (VPN) logon failures, account creations, and more.

ML-driven, behavior-based fraud detection

Log360 seamlessly combines traditional SIEM mechanics with machine learning to detect and prevent fraud with its user and entity behavior analytics (UEBA) add-on.

Consider a scenario where a user logs in after their typical working hours, accesses a sensitive folder that doesn't concern their job, and copies data onto an external device. All of these actions are legitimate, but in this case, are being performed with malicious intent. Log360 UEBA works by analyzing large volumes of log data and establishing baseline activity for every user and entity in your network. It alerts you when deviations from those baselines occur by tagging them as anomalies.



High-privilege user account monitoring and risk profiling

Log360 is capable of closely monitoring privileged accounts and their actions, and displays the information on multiple security dashboards in real time. Apart from account changes, permission changes, and user-based profile monitoring, Log360 creates risk profiles using UEBA.

Consider a scenario where a user account is remotely compromised by a hacker. The hacker then elevates the user account privileges and legitimately accesses sensitive data. With risk scoring for even low-risk activity, Log360 ensures you see these attacks coming, and alerts you so you can mitigate them in time.

Continuous security and compliance monitoring

Log360 provides complete visibility into your network with numerous security dashboards to monitor user account changes, database changes, permission changes, and much more. It also provides dedicated dashboards that help you monitor and demonstrate adherence to compliance regulations. With Log360, you're always audit-ready.

Fraud detection and prevention in the cloud

Log360 provides comprehensive security dashboards that offer insights into your Amazon Web Services (AWS), Azure, and Salesforce cloud environments. With a wide range of reports on everything from failed logon attempts to creation of instances, you get complete visibility into your cloud environments.

Incident response and remediation

With incident timelines that provide detailed records of what, when, and how, Log360 facilitates quick investigation of security incidents. The security team can then take action as per the company security policy. Log360 also provides multiple real-time dashboards that have informative widgets such as anomalous trends, anomalies based on categories, and overview of risk scores. These capabilities ensure you're better equipped to detect and prevent fraud in time with Log360.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a Customers' Choice for SIEM

Check out why

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in Gartner's Magic Quadrant for Security Information and Event Management, 2020.

Get the report

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/logmanagement/ and follow the LinkedIn page for regular updates.

ManageEngine Log360

$ Get Quote

Download