ManageEngine
Log360

CASE STUDY

How Log360 transformed **Savana's security landscape**

Company: **Savana, Inc.** | Industry: **Finance** | Location: **United States**

About Savana

Savana, Inc. is a technology company that offers a digital delivery platform for financial institutions that aims to streamline and enhance customer engagement through digital channels. With Savana, banks can own and manage their processes and channel experiences holistically, from core to customer, to maximize operational efficiency, enhance the customer experience, and greatly reduce the complexities and risks of launching and operating a new bank or transforming a legacy ecosystem.

Challenges

As Savana operates in the digital delivery platform industry, it faces a range of challenges that are unique to this rapidly evolving sector. Some of the key challenges include account compromise, failed logons or failed authentication, network security, cyberattacks, and compliance audits.

Network security: As a digital delivery platform, it is paramount for Savana to maintain a secure network infrastructure to protect highly sensitive financial data. The company must also protect its network from unauthorized access, data breaches, and malware attacks.

Cyberattacks: As the threat landscape continues to evolve, Savana faces the challenge of defending itself against various forms of cyberattacks, including phishing, ransomware, and distributed denial-of-service (DDoS) attacks. These attacks can disrupt the platform's availability, compromise data security, and disrupt business operations.

Compliance audits: In the digital delivery platform industry, compliance with industry standards and regulations is crucial to maintain trust and credibility. Savana must navigate through complex compliance requirements such as data protection regulations (e.g., the GDPR, CCPA), industry-specific standards (e.g., PCI DSS, SOX), and privacy regulations.

The Solution: Log360

To tackle these challenges, Savana successfully implemented ManageEngine's unified SIEM solution, Log360. After using the product for few months, Log360 proved to be highly effective in providing tailored solutions to address the unique needs of Savana's digital delivery platform. The following key features of Log360 played a crucial role in mitigating the challenges faced by the organization:

Detecting and mitigating threats: Savana leveraged Log360's event correlation engine to identify and respond to security threats. By analyzing log data from various sources, the IT team could pinpoint suspicious behaviors and take swift action to mitigate risks.

Searching specific logs or events: Log360's search option empowered Savana to quickly retrieve specific logs or events, facilitating efficient forensic analysis and investigations. This capability saved valuable time and resources by enabling swift identification and resolution of security incidents.

Enhancing network security: Log360 empowered Savana to fortify its network defenses. With real-time monitoring and alerts, the IT team could identify and block malicious IP addresses, domains, and URLs, bolstering the company's network security against external threats.

By leveraging the customizability of Log360, Steven Ivankin, senior security engineer at Savana, was able to fine-tune alerts and customize searches according to his specific requirements. This flexibility enhanced the effectiveness of Log360 in meeting Savana's unique security needs.

Impact

Ivankin reported that although the organization had not encountered any significant threats, account lockouts were a recurring issue. With Log360's AD auditing component, his team was able to identify the source of these lockouts. The tool provided detailed insights into the origin of the lockouts, enabling the security team to take immediate action and resolve the issue promptly.

Ivankin added that Log360 has become an integral part of Savana's cybersecurity infrastructure. With its comprehensive features and user-friendly interface, Log360 has seamlessly integrated into the organization's security operations.