ManageEngine
Log360

INDUSTRY SOLUTION BRIEF

FINANCIAL SERVICES

Mitigate insider threats and identify compromised credentials swiftly.

www.manageengine.com/log360

Table of content

Introduction

The cost of cyberattacks is highest in the banking industry, reaching $18.3 million annually per company, according to Accenture. The financial services sector is adapting to the ever-changing technological environment by embracing innovations such as artificial intelligence (AI), big data analytics, machine learning (ML), and so on. While these technologies are proving to be beneficial to the workforce and the customers, each innovation opens a new door to the cyber attackers.

The industry is plagued with data breaches, from malware attacks to credential and identity thefts. Moreover, the increasing number of third-party financial transactions has opened a Pandora's box of new attack vectors.

ManageEngine Log360 helps banks and other financial organizations stay ahead of cyberattacks. The solution addresses cybersecurity challenges by detecting advanced threats, such as credential dumping, insider threats, and more. The solution also helps organizations comply with regulatory mandates associated with the financial sector such as the Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standards (PCI DSS), the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), and others.

How Log360 helps address challenges in financial sector

The financial and banking sector is prone to cyberattacks because that's where the money is. According to Hands On Banking, there are 27 million victims of identity theft every year in the United States.

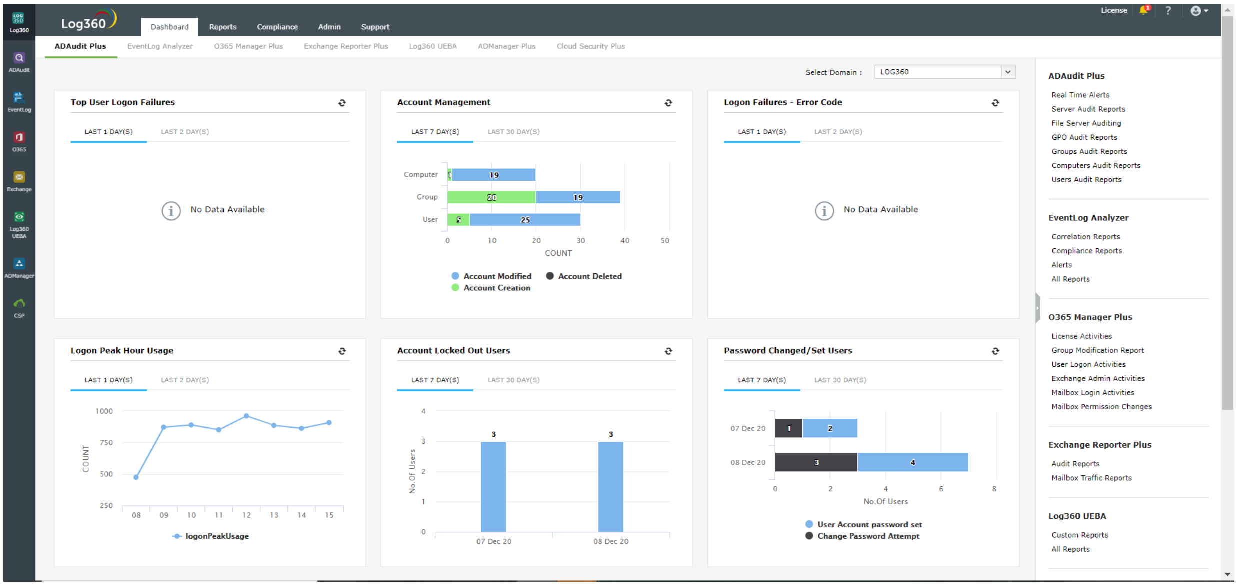
For financial services organizations managing numerous devices connected to the network is a herculean task, especially with working remotely being the new normal. The Vizon malware outbreak in Brazil, a remote overlay attack which involves displaying a fake full-screen image over the victim's browser window, demonstrates why a solution capable of monitoring the network and mitigating threats is imperative.

This is where Log360, the one-stop SIEM solution comes in. The solution helps identify and mitigate potential cyberattacks such as malware deployment, remote code execution, and DOS by providing real-time alerts and out-of-the-box reports.

- The solution is empowered with threat intelligence which can spot ransomware attacks, credential thefts, and other malicious activities using machine-learning, and user and entity behavior analytics (UEBA).

- Log360's data security component helps to monitor and discover configuration changes to applications and devices, ensuring the security of sensitive data.

- With Log360's search engine, you can gain useful insights by diving deep into the security instances, and conducting a forensic analysis to determine the impact of the attack.



Identify and mitigate threats at an early stage

The financial industry is facing several forms of cyberattacks such as distributed denial-of-service (DDoS), malware, spear phishing, etc. To successfully mitigate the impact of these attacks, organizations need to monitor their IT infrastructure closely. While this might sound easy for small or medium organizations, for a large organizations, monitoring the network devices and activities is a time-consuming and cumbersome activity.

Log360 automates the process of log monitoring and threat detection. The solution can:

- Monitor logs from all the devices connected to the network.
- Track and detect anomalous activities in the server.
- Satisfy compliance requirements of banking and other financial institutions by monitoring Active Directory and network devices.
- Generate reports by collecting, parsing, and analyzing logs or creating custom reports based on requirement.
- Protect the network from known attacks by leveraging the threat intelligence capability and correlating information from various threat feeds.

For instance, an employee tries to access a malicious IP address using the organization's network device. This may have serious consequences based on the nature of the website.

With Log360, you will receive instant alerts through email and SMS when malicious IP sources interact with your network. The solution verifies the integrity of the website and alerts the administrator.

Detecting and mitigating DDoS attacks: A DDoS attack is the fastest growing threat to financial sector, according to isBuzz news. DDoS attacks are usually carried out using techniques such as flooding, including network SYN floods. This tactic involves overwhelming the server with massive amounts of SYN requests.

Log data contains invaluable information about events occurring in your network. Monitoring and auditing log data in your network is a must, and can go a long way in detecting and mitigating DoS attacks.

Log360 monitors network devices, such as firewall, IDS/IPS, etc., and instantly detects DDoS attacks. Its real-time alerting capability helps detect threats early so you can more efficiently mitigate the impact of an attack.

Complying with regulatory mandates

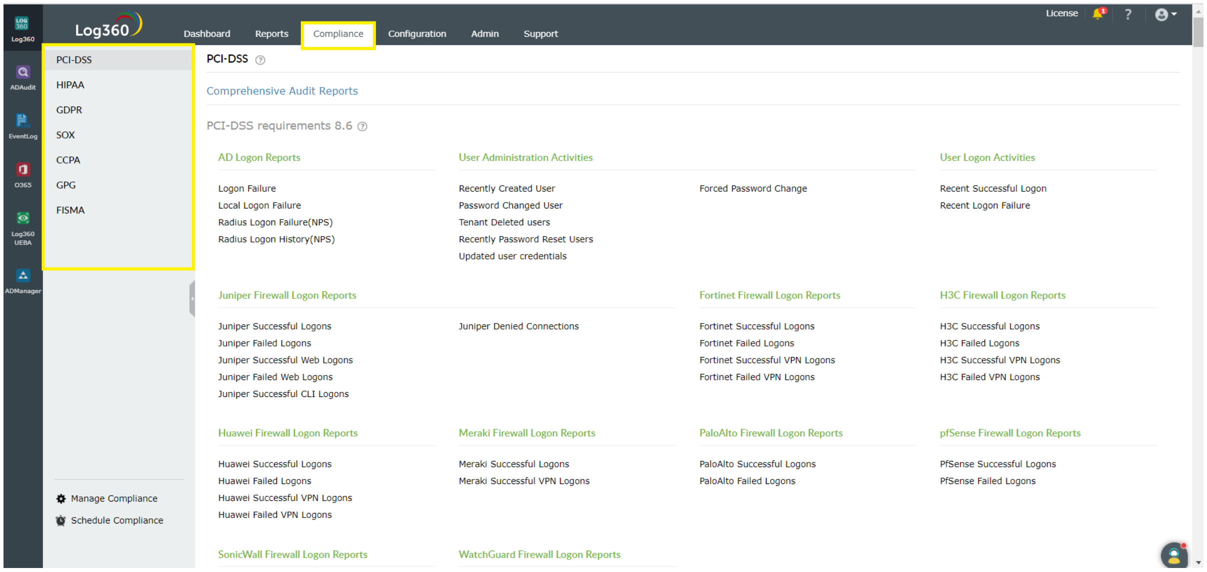
Due to the financial sector's complex nature, complying with federal, state, and local laws can be a monumental challenge. Cybersecurity further complicates the issue.

PCI DSS is one of the most enforced compliance regulations. It is a set of security standards that protects the cardholder information from security breaches, and ensures protection of information against thefts from within the organization and also from external brute forces.

For instance, section 10 and 11 of PCI DSS mandates event log collection, continuous log monitoring, and analysis.

Log360 helps you keep track of your network activities by continuously monitoring and collecting logs. It also provides exhaustive compliance reports, ensuring your organization is audit-ready.

Log360 helps IT security admins meet PCI DSS requirements by monitoring and auditing access to critical data. This solution tracks and identifies suspicious insider activity as well. It provides out-of-the-box reports with exhaustive information on data access, user activity, user logon and logoff activity, and more. Log360 also generates real-time email or SMS alerts that help instantly mitigate any compliance violations.



PCI-DSS

Comprehensive Audit Reports

PCI-DSS requirements 8.6

AD Logon Reports
Logon Failure
Local Logon Failure
Radius Logon Failure(NPS)
Radius Logon History(NPS)

User Administration Activities
Recently Created User
Password Changed User
Tenant Deleted users
Recently Password Reset Users
Updated user credentials
Forced Password Change

User Logon Activities
Recent Successful Logon
Recent Logon Failure

Juniper Firewall Logon Reports
Juniper Successful Logons
Juniper Failed Logons
Juniper Successful Web Logons
Juniper Failed Web Logons
Juniper Successful CLI Logons
Juniper Denied Connections

Fortinet Firewall Logon Reports
Fortinet Successful Logons
Fortinet Failed Logons
Fortinet Successful VPN Logons
Fortinet Failed VPN Logons

H3C Firewall Logon Reports
H3C Successful Logons
H3C Failed Logons
H3C Successful VPN Logons
H3C Failed VPN Logons

Huawei Firewall Logon Reports
Huawei Successful Logons
Huawei Failed Logons
Huawei Successful VPN Logons
Huawei Failed VPN Logons

Meraki Firewall Logon Reports
Meraki Successful Logons
Meraki Successful VPN Logons

PaloAlto Firewall Logon Reports
PaloAlto Successful Logons
PaloAlto Failed Logons

pfSense Firewall Logon Reports
PfSense Successful Logons
PfSense Failed Logons

SonicWall Firewall Logon Reports

WatchGuard Firewall Logon Reports

What next?

Explore Log360 by yourself

Download

Get expert's assistance for leveraging the solution

Schedule Demo

Get a personalized pricing quote

Get Quote

ManageEngine
Log360

ManageEngine Log360, a comprehensive SIEM solution, helps enterprises to thwart attacks, monitor security events, and comply with regulatory mandates.

The solution bundles a log management component for better visibility into network activity, and an incident management module that helps quickly detect, analyze, prioritize, and resolve security incidents. Log360 features an innovative ML-driven user and entity behavior analytics add-on that baselines normal user behaviors and detects anomalous user activities, as well as a threat intelligence platform that brings in dynamic threat feeds for security monitoring.

Log360 helps ensure organizations combat and proactively mitigate internal and external security attacks with effective log management and in-depth AD auditing.

For more information about Log360, visit manageengine.com

$ Get Quote

⤓ Download