ManageEngine
Log360

INDUSTRY SOLUTION BRIEF

HEALTHCARE

Protect patient privacy, identify your cybersecurity risks, and improve your IT performance.

www.manageengine.com/log360

Table of content

Introduction

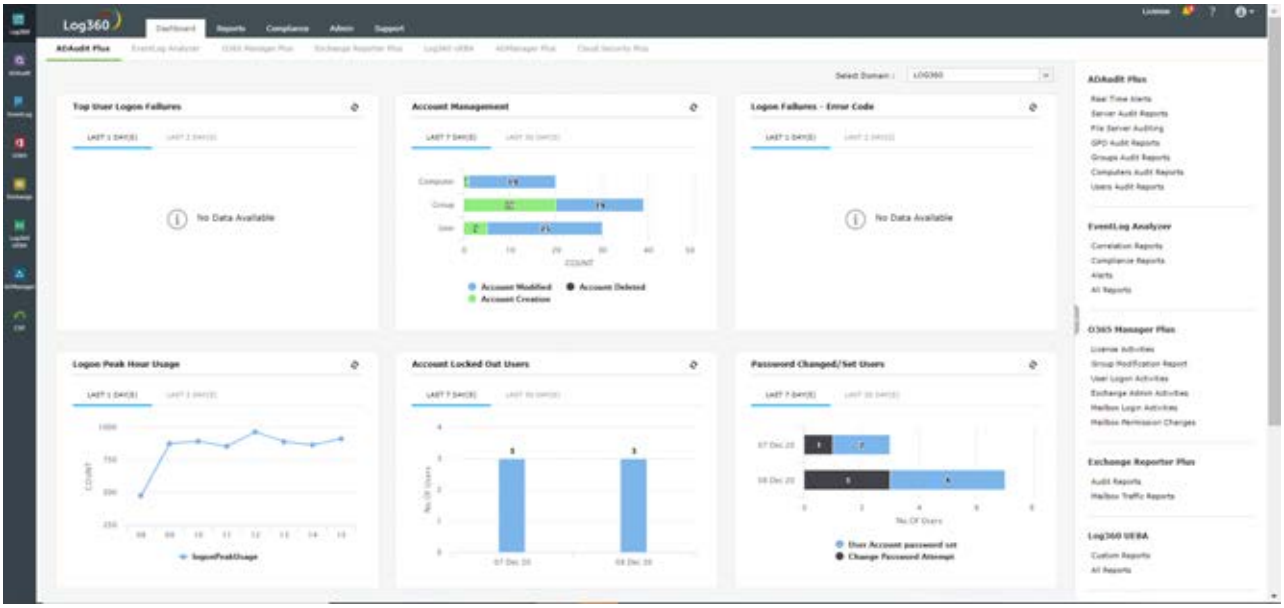
According to Securit, healthcare continues to be the industry most frequently exposed to cyberattacks. The healthcare sector already offers critical services, and improving treatment and patient care, along with embracing new technologies such as the Internet of Things (IoT), digital therapeutics, and artificial intelligence (AI), has increased the complexity of safeguarding protected health information (PHI) from cybercriminals and threat actors.

This industry is plagued by multitudes of cyber issues, ranging from malware attacks that compromise the integrity of the systems to distributed denial of service (DDoS) attacks that prevent the facilities from providing adequate services to patients.

Helping healthcare institutions stay protected and ahead of cyberattacks, Log360 is a one-stop solution that can detect, respond, and mitigate threats and attacks; secure sensitive data; and help organizations comply with regulatory mandates.

- The solution combines the power of configurable, rule-based threat detection and automated machine language-based behavioral analytics to spot ransomware attacks, DDoS attacks, credential thefts, account compromise, and other malicious acts.
- Log360's data security component helps discover sensitive PHI across devices and applications in networks, and protects them by monitoring changes to configurations and conducting thorough user activity auditing.
- Log360's rapid and precise log search engine facilitates quick and in-depth forensic analysis to track attack patterns and prevent the attack from happening again in the future.

With Log360, complying with HIPAA is easier than ever, as the solution comes with an audit-ready reporting template and compliance violation alerts.



Secure PHI from data breaches

Data breaches are widely observed in the healthcare sector, and can be attributed to different types of incidents, such as credential-stealing malware, insider threats, or a lost device. Many healthcare IT security teams find it difficult to manage the huge amount of data collected every day. Moreover, the volume of data also inhibits the identification of threats at an early stage.

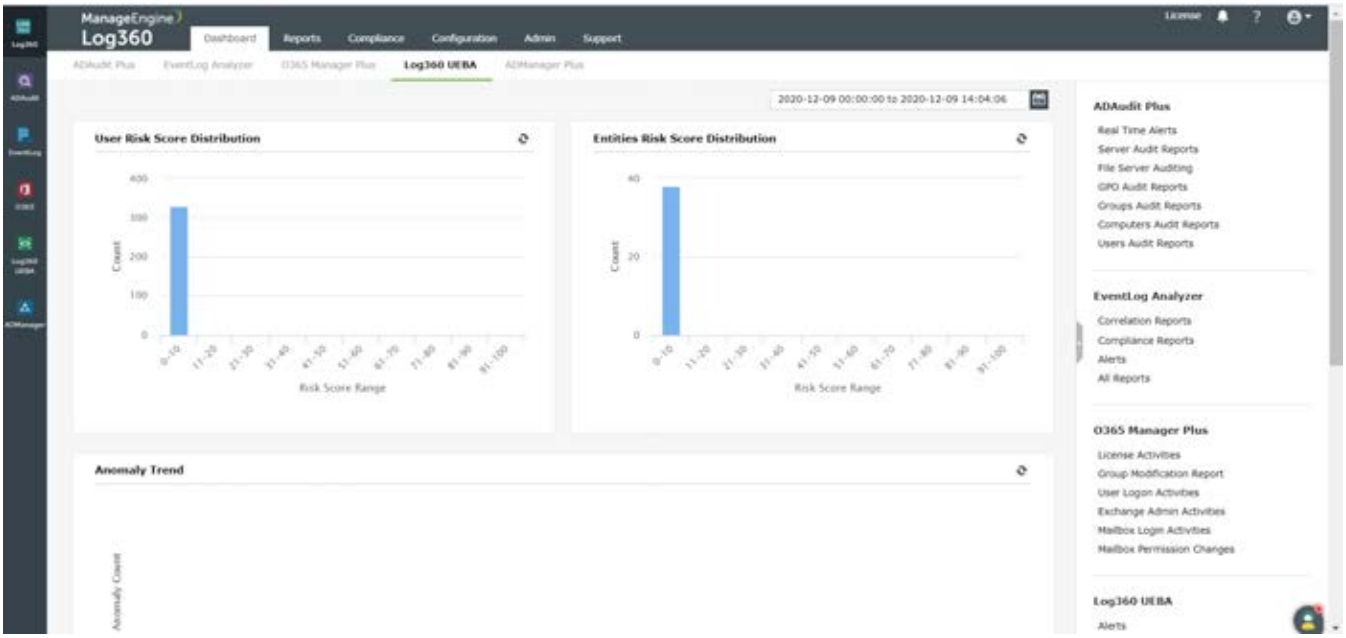
Log360 helps protect sensitive patient information from potential breaches. Wherever the data is stored, be it in files and folders or on a database, the solution ensures complete protection.

The data security component of Log360 is equipped with a personally identifiable information (PII) scanner, which can locate PII to help comply with HIPAA. The solution can also scan for sensitive data from over 50 file types, including email, text, or compressed.

It doesn't stop with just detection. Log360 monitors activities and operations being performed on this data to detect unauthorized access, permission changes, and more.

Detecting data security threats: Log360's powerful correlation engine enables admins to set correlation rules to identify threats as soon as they're detected. Detect data security threats such as ransomware attacks, compromised credentials, insider threats, and more with the solution's rule-based correlation engine.

Further, Log360 is also empowered with machine learning-based user and entity behavior analytics (UEBA), which can analyze user behavior, identify anomaly patterns, and generate real-time alerts. It also provides useful insights to the security team by assigning a risk score to every user action. This will help analyze individual user activities periodically, and initiate actions against users with higher risk scores.



Dealing with ransomware

Ransomware attacks on healthcare service providers rose 350 percent in the last quarter of 2019, according to a report from healthitsecuritycom. Ransomware typically tries to make its way into an enterprise's network via phishing websites or emails. For example, say an unsuspecting user opens an attachment. The ransomware launches itself, infects their system, and encrypts their files and folders, or even their entire hard drive. It then demands a ransom amount to be paid in Bitcoin within a deadline, after which the data is permanently encrypted. Hackers use Bitcoin because it is a digital cryptocurrency that ensures their identity cannot be traced.

The biggest problem with ransomware is the dual nature of the malware it uses for the attack. The malware not only encrypts data, but is also a worm that can spread across the network, affecting all the systems in an enterprise. This lateral movement is carried out by exploiting reported or unreported vulnerabilities. For instance, WannaCry and Petya ransomware use the EternalBlue exploit in Windows to quickly spread across an enterprise's network.

Another common method used by attackers to extract information from users is social engineering. This is a technique that exploits human error to gain sensitive information, privileged access, or other valuables.

Log360 provides an incident timeline on malicious software installations, helping identify and mitigate ransomware attacks before they take hold across the network. It also helps detect unauthorized use of sensitive data in real time.

Log360 also improves overall operational efficiency with automated workflows that can retaliate against cyberattacks.

Combating advanced persistent threats

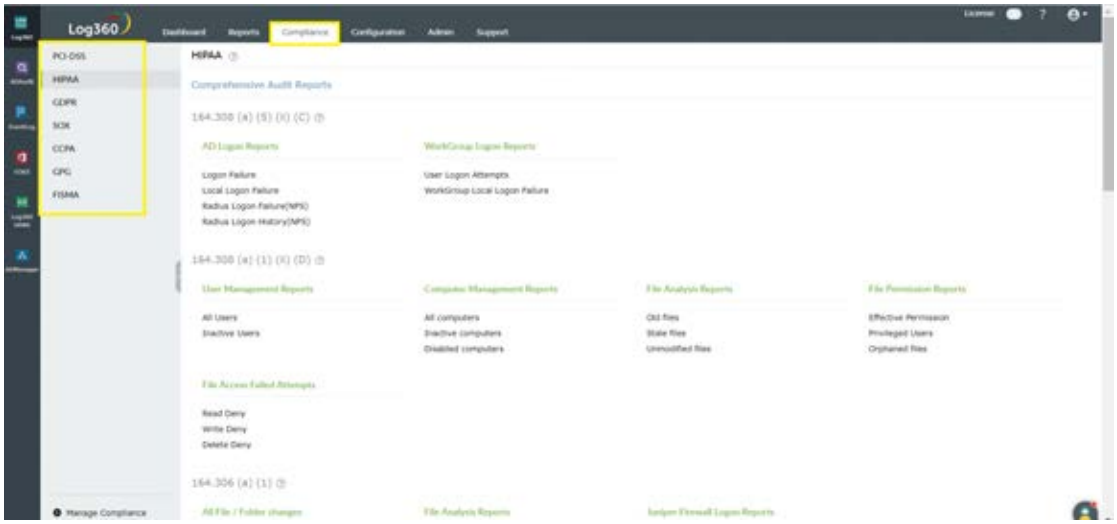
An advanced persistent threat (APT) is a sophisticated cyberattack where threat actors enter the network by exploiting a system's vulnerabilities, and remain undetected for a significant time. This cyber espionage attack is designed to extricate valuable data, and avoid detection for as long as possible. An APT attack can be prevented by analyzing and revoking user privileges, employing UEBA, updating antivirus and firewalls, etc.

Log360 monitors changes to user privileges, helping identify potential insider attacks. The solution has a powerful UEBA component that can help identify anomalies and attack patterns. This one-stop solution also monitors endpoints, alerting administrators about any anomalies in real time.

Meeting compliance requirements

When it comes to data protection in healthcare, the Health Insurance Portability and Accountability Act (HIPAA) is one of the most common compliance standards. Apart from this, healthcare providers must also adhere to local data privacy laws, government regulations, and so on. Managing and tracking compliance requirements is a challenging and time-consuming process.

By harnessing hundreds of compliance reports, which can be used to fulfill audit and regulatory requirements, and the ability to search and retrieve historical logs in minutes, Log360 significantly reduces the burden of compliance monitoring, making organizations audit-ready.



How Log360 helps organizations comply with HIPAA mandates

HIPAA mandates the security of a patient's health information from any unauthorized use or access. HIPAA requires that all health care organizations dealing with sensitive patient data establish a security management process to protect patients' confidential data from attempted unauthorized access, use, disclosure, or interference. For this reason, IT security administrators must collect and analyze log data across the network and extract meaningful information on data access in the form of reports.

Log360 helps IT security admins meet HIPAA requirements by monitoring and auditing access to critical data, and also identifies and tracks suspicious insider activity. 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.

For instance, section 164.308 (a) (5) (ii) (C) mandates organizations to have a procedure for monitoring login attempts and reporting discrepancies. Reports such as AD Logon Reports, WorkGroup Logon Reports, etc. help monitor logon events and provide insights on such events.

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