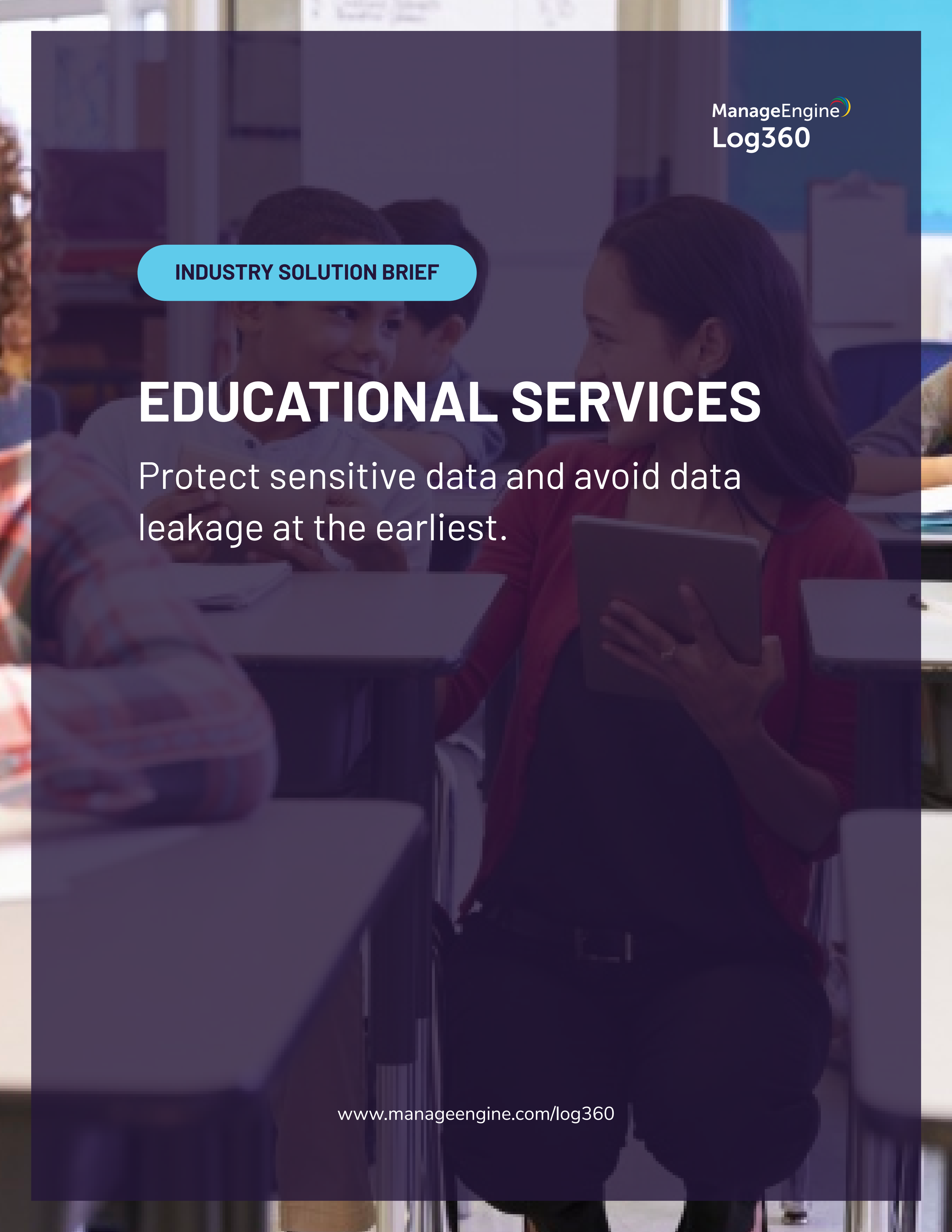


ManageEngine
Log360

INDUSTRY SOLUTION BRIEF

EDUCATIONAL SERVICES

Protect sensitive data and avoid data leakage at the earliest.

www.manageengine.com/log360

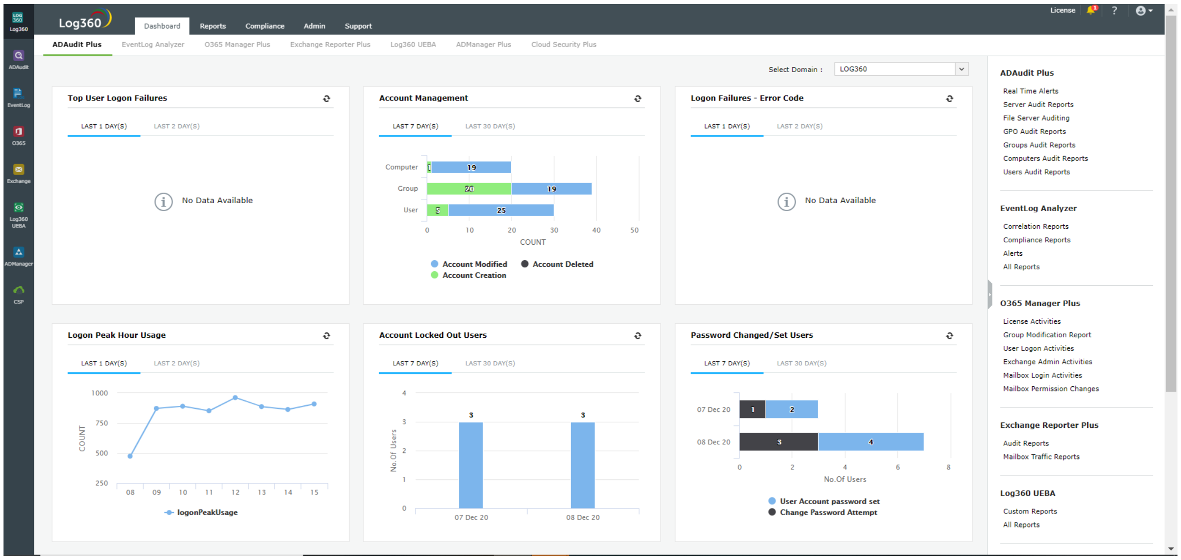
Table of content

Introduction

According to BusinessLine, cyber criminals are increasingly targeting the educational sector as students have been attending online classes since the beginning of this pandemic. Cyber attacks ranging from malware installations to compromised credentials have enabled cyber attackers to exploit the industry.

With educational institutions embracing novel learning pathways, such as distance learning, bring your own device (BYOD), learning applications, etc., the perimeter of their networks has extended, making network monitoring a difficult task.

ManageEngine Log360 helps educational institutions monitor their networks efficiently by collecting, parsing, and analyzing logs collected from different network endpoints, such as firewalls, IDS/IPS, routers, servers, and more. The one-stop SIEM solution is also capable of detecting and mitigating threats, and helping institutions stay compliant with regulatory mandates.



Challenges faced by educational institutions and how Log360 can help

The ever-changing technology has largely contributed to the development of the education sector. Students can now learn anything from any part of the world with just a smart device and internet.

While this has eased the process of learning, educational institutions are facing the challenge of ensuring that their network security isn't compromised. Moreover, as students use their own devices to attend the online classes, it has radically increased the number of entities in the network required to be monitored.

With Log360, though, network monitoring becomes easy. From collecting logs in the network to archiving those logs after a designated period, this tool can automate the complete process. The solution also generates real-time alerts, and exhaustive reports to help IT administrators keep attackers at bay.

Log360 helps organizations develop strategic plans to thwart threats proactively. The solution combines the power of rule-based threat detection and automated behavioral analytics, empowered by machine-learning and artificial intelligence.

The solution deploys a powerful log search engine that helps you drill down into security events, and conduct a quick but in-depth forensic analysis to identify attack patterns and prevent attacks in future.

Detecting and mitigating external and internal attacks

Distributed denial-of-service (DDoS) attacks and data thefts are the most commonly observed cyberattacks in the education industry, according to swivelsecure. DDoS attacks disrupt the smooth functioning of educational institutions by making the resources unavailable to the intended users. This impacts their productivity as well.

Data thefts are much more serious attacks that can result in the loss of sensitive user information from the institutions' databases. Attackers can then sell this information to third parties, or extort money from the institutions.

Log360 detects DDoS attacks by constantly monitoring network devices and providing out-of-the-box reports on network activities, such as logon, database modifications, unauthorized access, policy changes, and more.

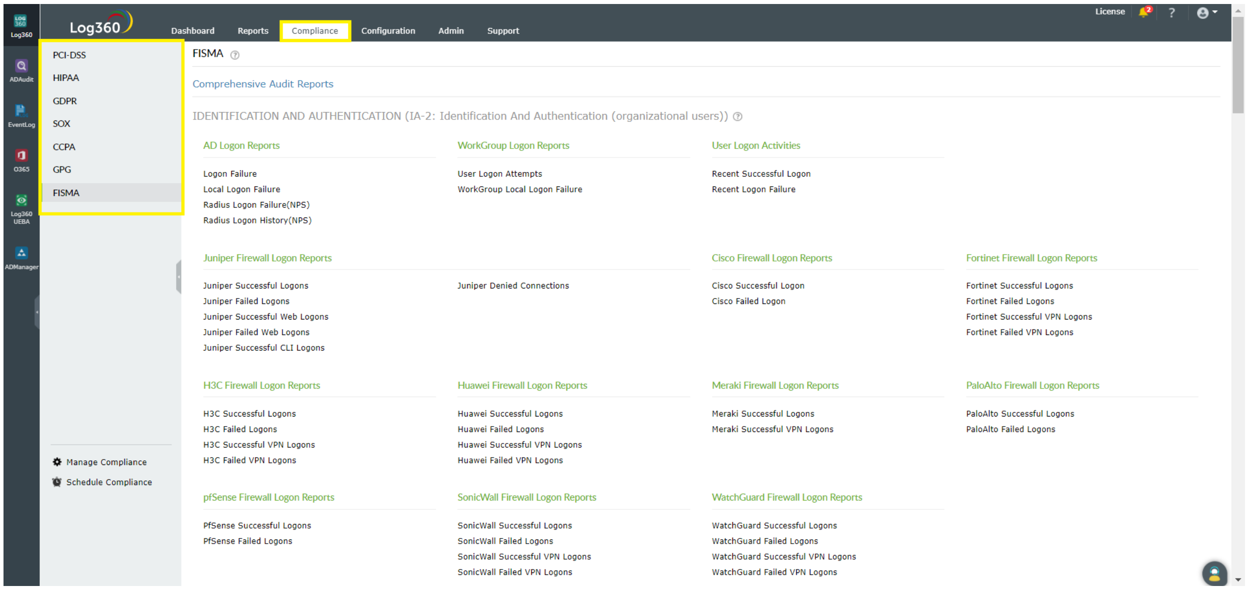
Insider threats present the biggest threat to educational institutions, according to Lepide. For instance, a user serving his notice period in the organization, logs in at a wee hour of the day and accesses certain sensitive files from the database. These logs can be used to drill down into the incident, root out, and gain visibility about the malicious activities carried out by the user.

Log360 can send real-time alerts via SMS or email, and generates reports based on the logs collected from the network. These logs can be used to drill down into the incident and understand the malicious activities carried out by the user.

Meeting regulatory mandates with Log360

Educational institutions are expected to meet several regulatory mandates, such as the Federal Information Security Management Act (FISMA), the Family Educational Rights and Privacy Act (FERPA), the Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standards (PCI DSS), and others. Log360 comes with audit-ready report templates and compliance violation alerts, enabling organizations to stay compliant all the time.

The solution monitors the database constantly, identifying potential data breaches or thefts. It provides out-of-the-box reports with exhaustive information on logon activities, user activities, privilege changes, configuration changes, database access, and more.



FISMA

Comprehensive Audit Reports

IDENTIFICATION AND AUTHENTICATION (IA-2: Identification And Authentication (organizational users))

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

WorkGroup Logon Reports
- User Logon Attempts
- WorkGroup Local Logon Failure

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

Cisco Firewall Logon Reports
- Cisco Successful Logon
- Cisco Failed Logon

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
- SonicWall Successful Logons
- SonicWall Failed Logons
- SonicWall Successful VPN Logons
- SonicWall Failed VPN Logons

WatchGuard Firewall Logon Reports
- WatchGuard Successful Logons
- WatchGuard Failed Logons
- WatchGuard Successful VPN Logons
- WatchGuard Failed VPN Logons

For instance, the Audit and Accountability requirement of FISMA mandates continuous monitoring of access and activities performed on the files and folders (objects) that store confidential government data. Log360 provides reports on objects accessed, created, modified, or deleted by each user, making it easy for IT admins to identify unauthorized access or operations performed on objects.

User activity monitoring

Log360 is also capable of monitoring user activities and providing exhaustive individual user reports. It monitors all users in real time, and provides exhaustive reports with a complete audit trail of all user activities that occurred from the moment a user logs in and logs out.

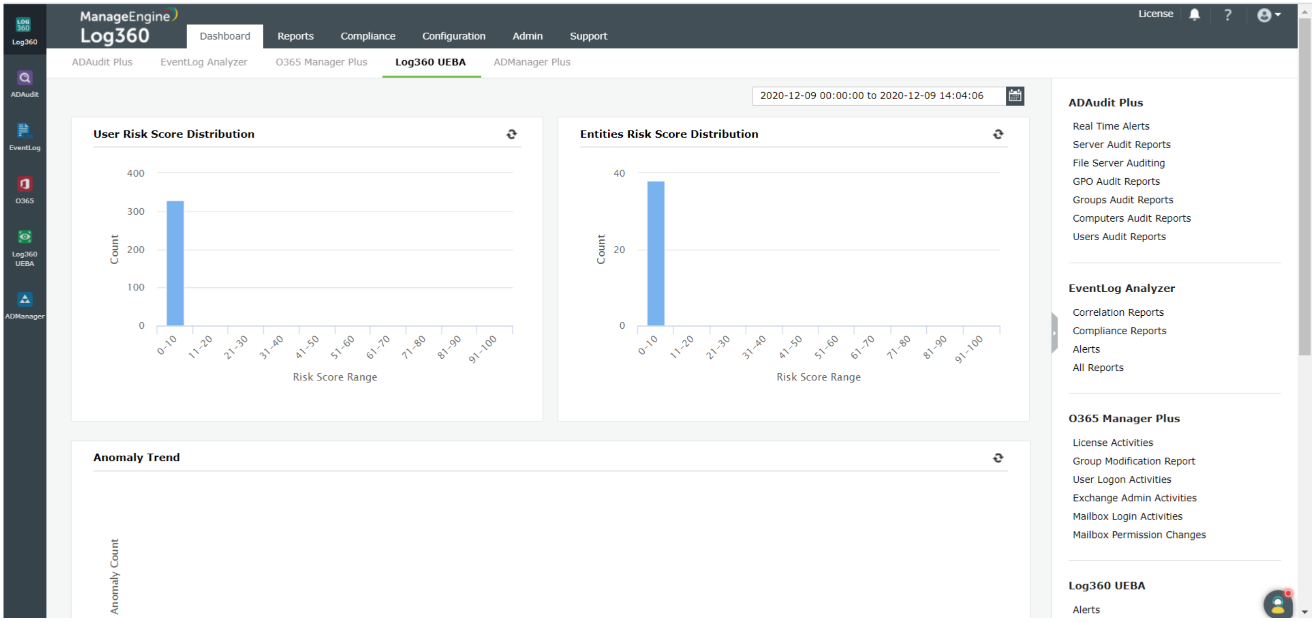
The solution comes bundled with a user and entity behavior analytics (UEBA) component that uses advanced techniques such as machine learning and artificial intelligence to analyze and detect anomalous user behavior. It assigns a risk score to each user based on the nature of activities and this can be used as an assessment of the user behavior. The dashboard gives real-time insights on user activities, which will be used to mitigate risk at the earliest.

Combating against 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 excess user privileges, employing UEBA, updating antivirus and firewalls, and more.

Log360 can help you monitor changes to user privileges, thus identifying potential insider attacks. The solution has a powerful UEBA component to help you identify anomalies and attack patterns. It also monitors your endpoints, alerting the administrators in real-time.



Database monitoring

According to The National Law Review, data breaches are becoming more common in the education sector. Some of the observed reasons include human error, cyberattacks, and malicious insider activities.

Log360 is capable of performing database auditing which identifies changes to the database. The solution also provides reports on unauthorized access, which identifies and mitigates data theft quickly and efficiently. This simplified and automated database monitoring capability enables database administrators to monitor and instantly identify the root cause of any operational issues, and detect unauthorized access to confidential data in real time.

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