ManageEngine Log360

CASE STUDY

Florida school district solves network visibility and compliance woes with Log360

Organization: Monroe County School District | Industry: Education | Country: USA

About Keysschools

Keysschools, also known as the Monroe County School District, is a public school district located in Monroe County, Florida. The administrative offices of the district are situated in Key West, while the school sites are spread throughout the Florida Keys from Key West to Key Largo. The district provides educational services for students from prekindergarten to the 12th grade, as well as adult learners enrolled in adult education programs.

The Monroe County School Board oversees the district's general management and appoints a superintendent of schools to head the district's administrative departments. The district's territory covers the entire county and serves over 11,000 students and teachers in the upper, middle, and lower Keys region.

Apart from traditional K-12 education, Keysschools provides adult education programs and vocational training. The district's goal is to empower all students to become responsible and contributing global citizens, with a focus on adapting to an ever-changing and diverse world.

Keysschools IT system administrators: Responsibilities and management

The IT department of the school district centrally manages the security backbone, network monitoring, and other technical aspects of the entire school district, which consists of multiple public schools with thousands of students and staff members. The IT department is managed by two system administrators, Andrew Hish and Tony Garcia, who oversee the day-to-day operations of the network infrastructure and system security.

Daily activities of school district's IT system administrators

Hish's responsibilities primarily involve monitoring the servers, reviewing security events, and ensuring that all software is patched and updated. He starts the day by checking server activity. Hish reviews security events that might have occurred overnight when no one was present. He also keeps an eye on any permission escalations or antivirus issues that might occur. Additionally, Hish handles backups to ensure that data is secure in case of a failure.

On the other hand, Garcia starts the day by conducting a network-level infrastructure check and reviewing security at various levels, including Active Directory and the firewall. He is responsible for looking for any new attacks and exploits, and responding to them accordingly. Garcia also ensures that the school district is protected against any attacks by importing and applying any indicators of compromise, or indicators of attack.

On the whole, the school district's IT department ensures that the network infrastructure is secure, and the system administrators take proactive measures to protect against attacks, ensuring the safety and privacy of students and staff members.

School district challenged by visibility and compliance audits

The primary business requirement for the school district was to have a logging and a SIEM solution in place for auditing purposes. This solution would also need to provide a robust platform for generating comprehensive reports during periodic audits. Although the district had wanted to implement a SIEM solution for some time, they had not found a solution that was manageable, given the number of users and schools in the district and the complexity in configuring the solution.

"In the years I've been here, we've never felt that we could put one up because they tend to be behemoths and beasts," Hish stated.

Another significant challenge the district faced was the lack of visibility into user activities and permissions. As Hish explained, the district needed to know "who's accessing what, who's looking at what, what file permissions are being changed." The administration never had good visibility into these activities because Microsoft's native tools are complex, difficult to work with, and time-consuming.

Garcia added that "Active Directory was a big beast too," and that the district had no way of knowing who was deleting or adding things. This lack of visibility was a significant concern for the district, especially because it conducted its own security tests over the last three years. It determined it needed a SIEM solution to get the full story of what was happening in its network.

SIEM solution chosen after thorough evaluation process

For the Keysschools' IT department, the decision to implement a SIEM solution was driven by its need for an audit tool and better visibility into its network activities. The admins evaluated other logging solutions, but none provided the output required, or it required a dedicated person to manage the solution on premises.

Specifically, they were looking at implementing SIEM over other logging solutions. Unlike traditional logging solutions, SIEMs are designed to help organizations detect and respond to security incidents in real time, and provide forensic analysis capabilities. SIEMs also help identify and mitigate insider threats, which traditional logging solutions are unable to do.

Reasons for choosing Log360: Enhanced visibility, simplicity, and auditability

The IT department of the school district assessed various logging solutions before opting for ManageEngine Log360. Log360 fulfilled the department's primary business requirement for auditing solutions, and obtaining enhanced visibility into its network activities.

In contrast to other solutions evaluated, Log360 is quick and easy to audit. During the evaluation, administrators Hish and Garcia set up and run the solution within 20 minutes, an impressive feat.

The simplicity of SIEM implementation was essential as the IT team had previously encountered difficulties implementing these solutions due to their complexity. The ease of implementing Log360 by availing the Custom Onboarding service was a significant advantage for them.

Even though the demo was not precisely customized to the department's network environment, it still allowed the department to gain a comprehensive overview of what was actually happening in its server farm and network. Garcia mentioned that he liked the logical flow of the products offered by ManageEngine, including ADAudit Plus, ADManager Plus, and Endpoint Central, which made a lot more sense than other solutions he had evaluated as it aligned well with his daily routine.

Seamless integration with existing infrastructure

The integration of the Log360 SIEM solution was essential to provide the IT team with complete visibility into its servers and network. The solution enabled the team to track access and changes to file permissions, which had previously been a challenge due to the limitations of Microsoft's tools. Log360 integrated seamlessly with the school district's existing infrastructure, including ADAudit Plus, ADManager Plus, and Endpoint Central. The administrators felt Log360 was easy to integrate and required minimal resources to manage when compared to the other products evaluated.

Impact of Log360 on the school network

Log360 has significantly enhanced the IT system administrators' day-to-day activities by providing them with improved visibility and control over their IT infrastructure, as well as making their jobs easier through time savings and other benefits. Before implementing Log360, the IT system administrators had challenges with knowing what was happening in their IT infrastructure, which made it difficult to identify potential security threats.

> *With Log360, we can get a quick snapshot of what's happening in our network, in our environment, and we can jump right to what's needed.*
>
> **Andrew Hish,** IT system administrator,
> Monroe County School District

The IT department can quickly identify anomalies and address them efficiently. One specific example of how Log360 helped the IT system administrators address security incidents was when they were alerted to unusual logins in their network.

"We noticed that someone was trying to log in multiple times from the same account. This was suspicious because it was outside of the usual login patterns, and the login attempts were happening during odd hours when we knew the user was not supposed to be accessing the system," Hish observed.

Log360 detected an unusual pattern of login attempts from an admin account. This helped the IT system administrators investigate the issue and determine the root cause. In this case, it turned out to be an application trying to use admin credentials and the issue was resolved. Had this been a cyberattack attempt, Log360's advanced threat detection capabilities would have efficiently identified and alerted the IT administrators, ensuring the network's security. Its comprehensive monitoring and analysis features play a crucial role in distinguishing between genuine and malicious activities, safeguarding the system from potential breaches.

Log360 has helped to improve the overall security posture of the school district.

> *The solution has made us much more secure because now we can see everything that's happening.*
>
> **Tony Garcia,** IT system administrator,
> Monroe County School District

By implementing Log360, the school district's IT team was also able to meet audit requirements and provide a full story of what is actually happening in their server farm and network.

Final thoughts on Log360, support, and ManageEngine

The IT system administrators also expressed satisfaction with the support and Custom Onboarding implementation teams.

Hish appreciated the solution's easy of use.

> *It’s definitely easily digestible. I told my director, Log360 is a system admin tool built by system admins. I don’t have to go through several PowerShell scripts, or multiple interfaces to get what I need out of it. It's right there at my fingertips. It's definitely easy.*
>
> **Andrew Hish,** IT system administrator,
> Monroe County School District

Garcia observed, "We had a really good experience with the implementation team. They were very knowledgeable and helped us get the solution up and running quickly."

Furthermore, the IT system administrators were pleased with the support they received during the implementation process. He compared the rollout process to other products, stating that it was incredible and did not require an entire team of scientists or PhDs to manage. They were able to customize the solution to meet their logging and SIEM requirements quickly and efficiently.

Additionally, the IT system administrators were happy with ManageEngine. They were able to conduct network-level infrastructure and security checks at multiple levels, including endpoints, firewalls, applications, and other devices, using ManageEngine's Active Directory and SIEM offerings.

> *They are flexible and they'll work with you, and they will break things down and explain things for each product... They want to answer your questions and it's a good process to go through.*
>
> **Andrew Hish,** IT system administrator,
> Monroe County School District

In summary, implementing Log360 has brought numerous benefits to the Monroe County School District. The primary goal of implementing the solution was to comply with audits, and it has provided the district with visibility into server farms, networks, file and user activities, and Active Directory. As a result, the district has gained a better understanding of what is happening in its system and improved its security. Furthermore, the solution has helped the district prevent potential penalties or loss of funding resulting from non-compliance. These audit, security, and compliance benefits show that other educational organizations can also enhance its system security by implementing Log360.

Ratings

Log360 post-implementation, ease of use

difficult 1 2 3 4 5 6 7 8 9 **10** *easy*

How likely would you be to recommend Log360 to others?

less likely 1 2 3 4 5 6 7 8 9 **10** *most likely*

About Custom Onboarding

Custom Onboarding is a ManageEngine service that provides solution implementation to clients upon request. This service includes the installation and customized configuration of the ManageEngine solutions. It enables clients to seamlessly begin work without worrying about the complexities of installation, deployment, and product use. Every client environment is unique and requires additional support beyond the basic installation and standard features. With Custom Onboarding, clients have the option to engage a team of product experts to manage the installation, implementation, customization and training based on the business needs.

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. It combines threat intelligence, machine learning-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks, and 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/log-management/