ManageEngine
Log360

CASE STUDY

PaperSolve Effectively Monitors Network Devices using Log360

Company: **PaperSolve** | Industry: **IT** | Country: **USA**

About the Organization

Established in the year 1986 as Stardate Computer Systems, PaperSolve is a managed IT services and software development company based in New York. The company not only provides IT solutions and services to small and medium-sized businesses, but also deals with document imaging and cloud hosting.

PaperSolve specializes in resolving any discrepancies that may arise within an organization by providing a complete suite of services comprising technology consulting, data recovery options, remote monitoring, and more.

> *ManageEngine Log360 seems to be doing everything that we need it to do.*

Michael Russo
Systems engineer, PaperSolve

Challenges

The IT team at PaperSolve consists of five people, including Michael Russo who works in the managed services department. The organization was looking for a solution to help them overcome the following issues:

1. Being a managed service provider, PaperSolve collects logs from different types of devices in its client network to track events and spot threats. Though most firewall and other network device vendors provide log analysis capabilities, these metrics are available in silos. There is no central view of all security events to facilitate rapid threat detection and response.

2. The tool that PaperSolve previously employed didn't provide sufficient insights on account lockouts. This was one of the vital requirements for PaperSolve as it dealt with a number of users with account lockout issues.

The Solution

Deploying ManageEngine Log360 has helped PaperSolve's network administrators efficiently manage the IT infrastructure of their clients in the following ways:

- **Automated account lockout alerts:** Real-time alerts are sent to IT administrators in the event of account lockouts, along with details such as locked-out time, source IP, device name, and more. This helps with tracking the source of authentication failure and troubleshooting.

  Russo mentioned, "Before ManageEngine, I don't think [account unlock activity] was really automated at all. We use Log360 for analyzing account lockouts. It helps us unlock user accounts and provide reports on where the issue came from."

- **Network device monitoring:** Provides better visibility into network events by monitoring devices such as firewalls, routers, switches, and intrusion detection and prevention systems. The logs from these devices are parsed and correlated to identify attack patterns and alert security professionals.

In addition, PaperSolve values ManageEngine's technical support in terms of sorting out issues and providing timely upgrades. "They've [the customer support team] worked with me, and we've sorted out all the issues that we've ever had. It's very good," said Russo.

Other Highlights of Log360

Log360 is a one-stop solution for all log management and network security needs. It offers:

- **Advanced threat analytics:** Log360 has the ability to correlate events with dynamically updated threat feeds, and alerts you in real-time upon any malicious intrusion attempts. Further, the solution's advanced threat analytics feature provides more information about the security threat, including the geolocation of the threat's origin, the threat category, the reputation score of the source, and more.

- **Behavior analytics:** Log360 utilizes machine learning to analyze logs from heterogeneous devices and detects any deviation from normal behavior. By assigning risk scores and generating intuitive reports, Log360 provides IT administrators with actionable insights to defend their network from both internal and external attacks.
  Satisfy compliance requirements: Log360 audits every change made within the organization's network and provides hundreds of audit-ready report templates to fulfill compliance mandates for regulations including PCI DSS, GDPR, FISMA, SOX, HIPAA, and more.

- **Customization:** We believe that security information and event management (SIEM) isn't a one-size-fits-all approach. Therefore, along with offering built-in reports, Log360 allows IT administrators to generate and schedule custom reports. The report and alert builder are highly intuitive and easy to use. With these reports, you can generate any report or alert required for your internal security needs.

Impact

PaperSolve is glad it switched to ManageEngine Log360 as its SIEM tool. PaperSolve now gets a comprehensive picture of its clients' IT infrastructures, enabling it to drill down on issues and provide optimal solutions.

Offering his feedback about Log360, Russo remarked, "ManageEngine Log360 seems to be doing everything that we need it to do."