ManageEngine
Log360

CASE STUDY

Log360 helps Direct Transact detect hacking attempts

About Direct Transact

Direct Transact is a Software as a Service finance company based out of South Africa. The company helps banks and other businesses that want to launch financial products solve any legacy issues and deploy cost-effective banking and payment systems. Direct Transact also helps companies with technical and compliance advice and provides financial operational support that businesses need to run their payment and banking solutions efficiently.

The challenge:

Finding a comprehensive SIEM solution for all its security needs

Direct Transact needed a solution that could help ensure data security by keeping the network safe from mishaps arising from inadvertent security breaches and also help comply with regulatory mandates. The organization also needed help in spotting ongoing attack attempts from hackers. Though this may sound simple, finding a security information and event management (SIEM) solution that caters to all these security needs is no easy task.

The solution:

ManageEngine Log360 for advanced threat detection and mitigation

When the other SIEM solutions Direct Transact evaluated didn't meet its security and monitoring needs, it decided to give ManageEngine Log360 a shot. The solution's capabilities in monitoring and auditing network devices, detecting and mitigating cyberattacks and threats, and actively helping comply with regulatory mandates convinced the company to continue using Log360 after the 30-day, free trial.

When asked about the security challenges faced by the company, Arthur Spickett, an ICT systems engineer at Direct Transact, mentioned that failed logons and authentication and port scans from malicious sources were the main security threats it faces. With regard to the hacking attempts, he said, "An active hacking attempt was picked up by the network team and the evidence needed was pulled from Log360." He added that, unlike the previous solutions, Log360 helped Direct Transact resolve all its security needs and has become an integral part of the organization's cybersecurity operations.

Key features of Log360

- Monitor and audit critical Active Directory (AD) changes in real time
- Automatically collect, analyze, archive, and report on logs from Windows and Linux/Unix machines, IIS and Apache web servers, SQL and Oracle databases, and perimeter security devices
- Report on critical events in Azure AD, Exchange Online, and Microsoft Exchange Server in real time
- Gain a holistic view of activities in Amazon Web Services and Azure cloud infrastructures

About Log360

ManageEngine Log360, an integrated solution that combines ADAudit Plus and EventLog Analyzer into a single console, is the one-stop solution for all log management and network security challenges. This solution offers real-time log collection, analysis, monitoring, correlation, and archiving capabilities that help protect confidential data, thwart internal security threats, and combat external attacks. Log360 comes with over 1,200 predefined reports and alert criteria to help enterprises meet their most pressing security, auditing, and compliance demands.

For more information about Log360, visit manageengine.com/log-management.

$ Get Quote Download