ManageEngine
Log360

DATASHEET

Securing cloud resources

Secure your cloud infrastructure using Log360

The hurdle

Advances in cloud storage technologies have changed the way organizations handle data and conduct business. The widespread adoption of cloud infrastructures has presented substantial opportunities for growth. At the same time, it has made organizations more vulnerable to malware infections, data leakage, and other cybersecurity threats. Many organizations do not have the security tools they need to ensure their cloud data is protected and compliance requirements are met.

The solution

Log360 is a one-stop solution for all your cloud security challenges. It allows you to efficiently monitor, report on, and audit your public cloud infrastructure. It also serves as a comprehensive log collection tool that allows you to aggregate, search, analyze, and audit events happening across your IT environment. Read on to learn mor

Highlights of Log360's cloud capabilities

- ### Secure data on the cloud

A data breach in your cloud infrastructure can lead to potential identity theft, as sensitive customer information can be sold elsewhere. On top of this, failure to meet compliance requirements can result in huge fines along with legal action.

Log360 offers complete visibility to help you secure sensitive data residing in your infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) infrastructures. This visibility comes in the form of comprehensive reports, an easy and powerful search mechanism to perform log forensic analysis, customizable alert profiles, and much more. With complete visibility on your sensitive data, you can track, analyze, and respond to events happening in your cloud environments that may compromise your data.

Lets look at an example where Log360 helps monitor data exfiltration in your Salesforce deployment. Imagine Bob, a malicious insider, logs in after working hours and accesses critical account reports. Bob then proceeds to export more reports than usual and logs out. Log360 reports and alerts on both the unusual login activity and the suspicious report export activity. With an alert rule configured for unusual logins followed by report exports, you'll know right away when any data exfiltration attempts occur in your Salesforce environment.

- ### Detecting cloud security threats using machine learning

Tracking the behavior of each user and entity in a network is an integral part of identifying security anomalies in the cloud. Actions from users and entities often mean nothing when evaluated individually. However, when these actions are pieced together, they tell a cohesive story and provide meaningful security context. For instance, an unsuccessful login attempt may have been caused by a typo in the password, but numerous login failures followed by a successful login could indicate a brute-force attack.

One of the best ways to defend against both internal and external attacks is to leverage user and entity behavior analytics (UEBA) to continuously monitor user and device activity on your cloud infrastructure. UEBA engines learn about each user and create a baseline of regular activities for each user and entity. Any activity that deviates from this baseline gets flagged as a time, count, or pattern anomaly. The IT administrator can then investigate the issue and take the necessary steps to mitigate the risk. Powered by machine learning, UEBA solutions grow more effective the longer they're in use.

Cloud resource access monitoring using security analytics

Cloud platforms allow you to store data, create virtual machines (VMs), host web applications, and manage accounts on their server, however, hosting a large amount of data on the cloud comes with its risks. For security and privacy reasons, continuously monitoring these resources in your cloud environment is crucial.

Log360 provides centralized log management capabilities that allow organizations to store, search, monitor, analyze, and alert on log data and events on cloud platforms. It ingests log data from different systems, applications, and VMs, and analyzes it in real time. It then provides comprehensive reports including information like:

- When an event occurred.
- Which user was responsible for the event.
- The source IP address of the request.
- The geographic region in which the event took place.
- The request parameters involved.
- And more.

On top of this, Log360 provides insightful trend reports on events such as failed logons, denied connections, successful authorizations, and allowed traffic.

Other key features of Log360

Support for multiple cloud platforms

Log360 supports multiple platforms such as Amazon Web Services (AWS), Azure, Salesforce, and Google Cloud Platform. Even if you have a cloud infrastructure distributed across multiple platforms, Log360 allows you to monitor all of them from a single interface.

Forensic analysis

Once a threat is detected, Log360 helps you in conducting an extensive forensic analysis. Searching through an enormous amount of log data requires little effort when using Log360's advanced search capability. Options such as wildcard, Boolean, phrase, range, and grouped searches let you drill down to the required logs with just a few clicks.

Comprehensive reports

Log360 provides complete visibility into your cloud infrastructure by offering a wide range of predefined reports. The events shown in reports can be drilled down to the raw log level so you can view the actual log information. You can also configure reports to be generated and emailed at specified intervals. These reports can also be exported in PDF, CSV, XLS, and HTML formats for audit purposes.

Incident management and alerting

Log360 helps security teams detect and mitigate security threats at an early stage. Its incident management console allows you to detect, categorize, analyze, and resolve a security incident as soon as it occurs. Its alerting module can be configured to send real-time notifications through email or SMS whenever an event of interest occurs.

- **Out-of-the-box compliance audit reports**

Following the shift of businesses to the cloud environment, many compliance mandates require organizations to deploy security information and event management (SIEM) tools with dedicated cloud monitoring features. Log360's cloud monitoring component helps you keep your business running smoothly and secure and protect your cloud environment. It also comes with prebuilt compliance reports for several mandates, including PCI DSS, SOX, HIPAA, FISMA, GLBA, ISO 27001, and the GDPR. You can construct custom templates for internal requirements as well.

- **Real-time correlation engine**

Log360 helps you identify attack patterns accurately by correlating different logs from various sources. It comes with over 30 predefined correlation rules to detect several common attacks. You can customize existing attack rules or build new ones from scratch with the flexible rule builder interface.

- **Augmented threat intelligence**

STIX/TAXII protocols provide globally applicable standards for identifying and sharing threat information. Log360 processes STIX/TAXII-based feeds to alert you in real-time when globally blacklisted IPs and URLs interact with your network.

Supported log sources

The following log sources are supported by Log360.

Support for multiple cloud platforms

Cloud platforms

Amazon Web Server (AWS)
Salesforce
Google Cloud
Azure
Azure AD

Other log sources

- Applications
  SQL and Oracle databases, IIS and Apache web servers, and more.

- File servers
  Windows, NetApp filers, EMC file servers, Synology NAS servers, Hitachi NAS servers, and file server clusters.

- Network perimeter devices
  Routers, switches, firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and more.

- Virtual platforms
  Microsoft Hyper-V and VMware.
- Linux/Unix servers and devices
- Windows servers and workstations