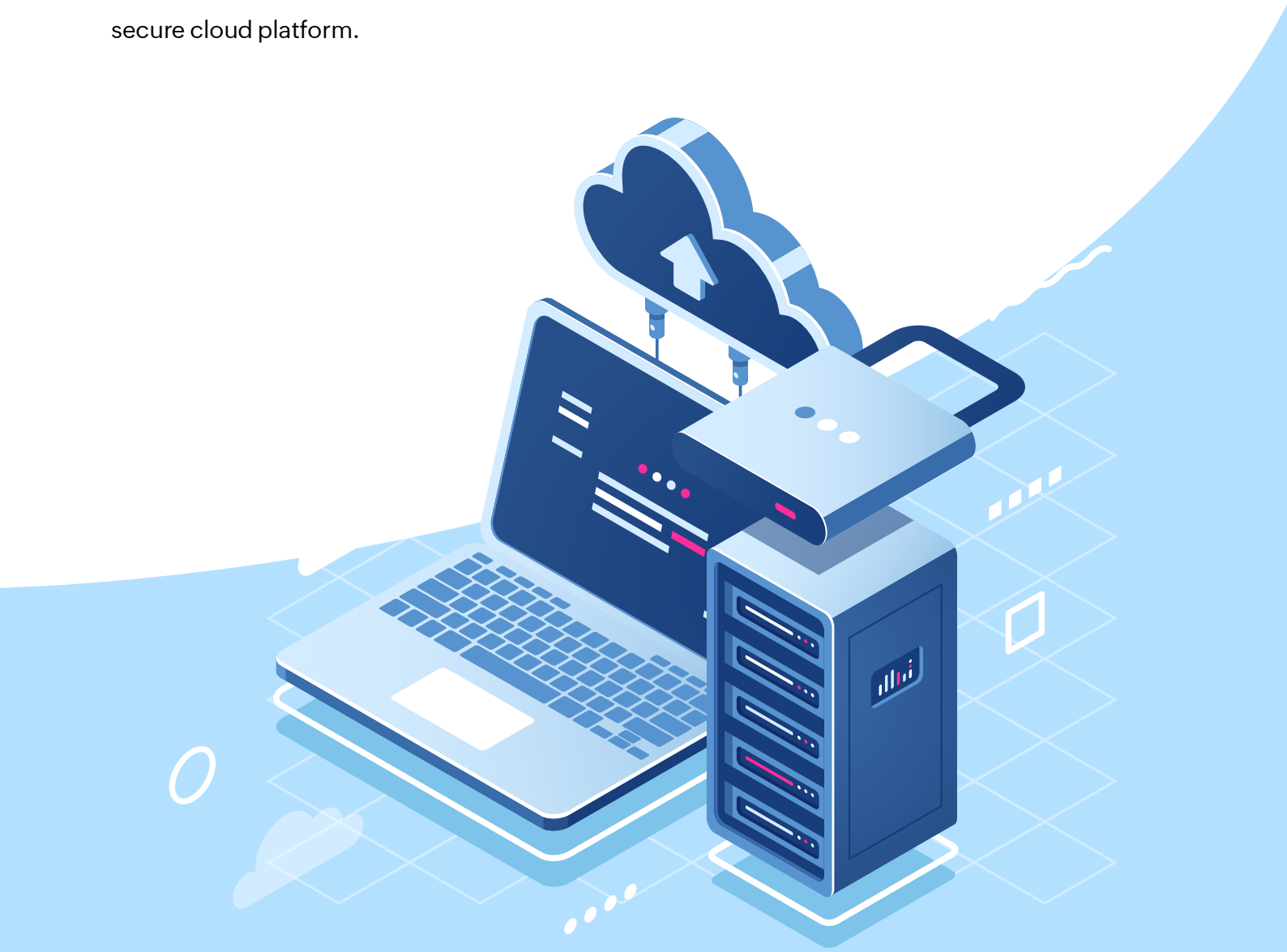
ManageEngine
Log360 Cloud

Benefits and architecture of Log360 Cloud

The importance of secure log storage

Logs are what security teams turn to when investigating security incidents and breaches. Attackers often try to access, modify or delete log records in order to cover their tracks. It is important to ensure that the logs collected from the network are securely stored and haven't been tampered with. This is why several compliance regulations require organizations to implement measures to ensure the integrity and reliability of log archives as part of their log management process. Managing logs, however, poses challenges to security teams, resulting in insecure storage, high costs and inefficiencies. These challenges can be overcome by storing logs on a secure cloud platform.



Benefits of cloud storage

Security:

While there is no guarantee in cybersecurity, storing logs on the cloud does provide added security measures compared to on-premises storage. Learn more about the security features of Zoho Corporation's cloud platform here.

Storage and cost optimization:

Storing logs on the cloud tends to be significantly cheaper, helping IT teams save on disk space costs. Security teams need to pay only for the storage space they need on the cloud.

Accessibility:

Log data can be securely accessed from anywhere by authorized technicians without any hassles.

Scalability:

As networks grow, so does the volume of log data that needs to be managed. It is far simpler for security teams to scale up on the cloud, without worrying about infrastructure considerations.

ManageEngine
Log360 Cloud

ManageEngine's Log360 Cloud is a cloud-based solution that allows organizations to securely manage and store logs. The solution makes use of an agent to upload the logs to the cloud.

- The built-in search engine allows security teams to run queries and retrieve information they need in a given scenario.
- Audit reports can be generated to review key security events happening in the network.
- The log sources supported are Windows/Linux machines, firewalls and more

Architecture

Log360 Cloud uses the Zoho Logs service developed by parent company, Zoho Corporation, to index the logs. A UD server (Uploads Downloads server), which is also a service from Zoho, is used to ensure smooth upload of data from the agent to Zoho Logs.

Agent-based approach

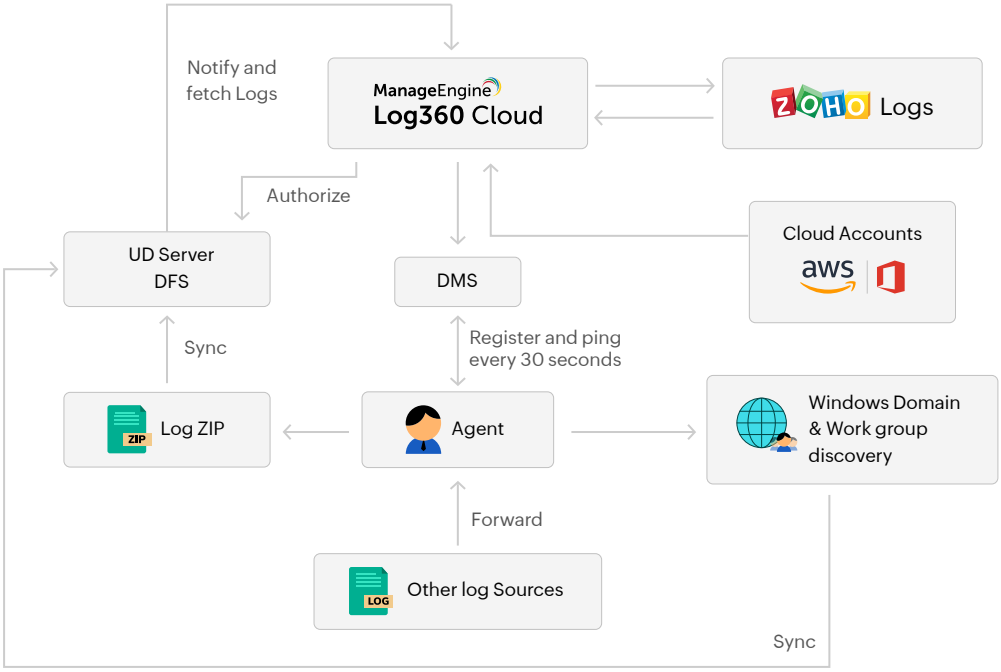
- The Log360 Cloud agent needs to be installed on any machine for communication with Log360 Cloud. The access key obtained while signing up needs to be entered while installing the agent.
- The agent automatically discovers Windows Domain and Workgroup devices. Other log sources can forward their data to the machine in which the agent is installed.
- The host details are sent to the UD server, which has it's own DFS (distributed file system), and the details are updated in Log360 Cloud's database.
- A messaging service, called DMS, is used to communicate changes made in Log360 Cloud's GUI to the agent. Every agent needs to register with the DMS. The agent subsequently pings the DMS every 30 seconds to check for new communications.
- The log data received from the log sources is zipped every 5 minutes and sent to the UD server, which requests Log360 Cloud for authorization.
- Once the license and storage space is checked, the request is authorized and the data is written to the DFS. A notification is subsequently sent to Zoho Logs.
- Then, Zoho Logs fetches the data and indexes the logs for generating reports and performing searches.

Agent-less approach

- Integrate multiple cloud accounts (e.g., AWS, M365) into Log360 Cloud.
- Configure specific data sources (e.g., Cloud Trail, S3, M365) for log collection within each cloud account.
- Log360 Cloud automatically collects logs from the defined data sources at regular 10-minute intervals.

- The collected logs undergo storage and license checks.

- Once validated, logs are written to a Distributed File System (DFS) and forwarded to ZohoLogs for further analysis and management.



Pricing

The pricing for the solution is based on the storage space required by the organization. The basic plan costs $300/year, for up to 75 GB of storage and 90 days of storage retention.

More details about pricing can be found here.