Kaseya VSA Security & Compliance Overview

A System You Can Trust

Kaseya is used by thousands of companies within high-security environments which are subject to compliance requirements such as HIPAA and PCI. Kaseya has incorporated communications encryption, strong access control and authentication features which enable customers to meet security and compliance requirements.

Secure Agent Technology

The Kaseya Platform architecture is central to providing maximum security. Each managed computer has a small software agent installed. The agent securely receives configurations, schedules, and instructions from the Kaseya Server. The Kaseya Agent performs all necessary management functions as if the technician were sitting right in front of the remote computer.

Since the Kaseya Agent will not accept any inbound connections, it is impossible for a third-party application to attack the agent from the network. All communication from the Kaseya Agent originates from the agent outbound to the Kaseya Server. As an additional measure, Kaseya Agents can also securely 'bind' to a single Kaseya system protecting against any kind of Internet based spoofing attack.

Encryption

Data communications are encrypted to provide security, privacy and compliance with HIPAA, PCI and other standards. Specifically, the following encryption methods are utilized:

Agent Communications – Communication between the Kaseya Server and Agents is encrypted using AES-256.

Remote Control – Kaseya remote control sessions to end-user machines/servers is encrypted using Transport Layer Security (TLS).
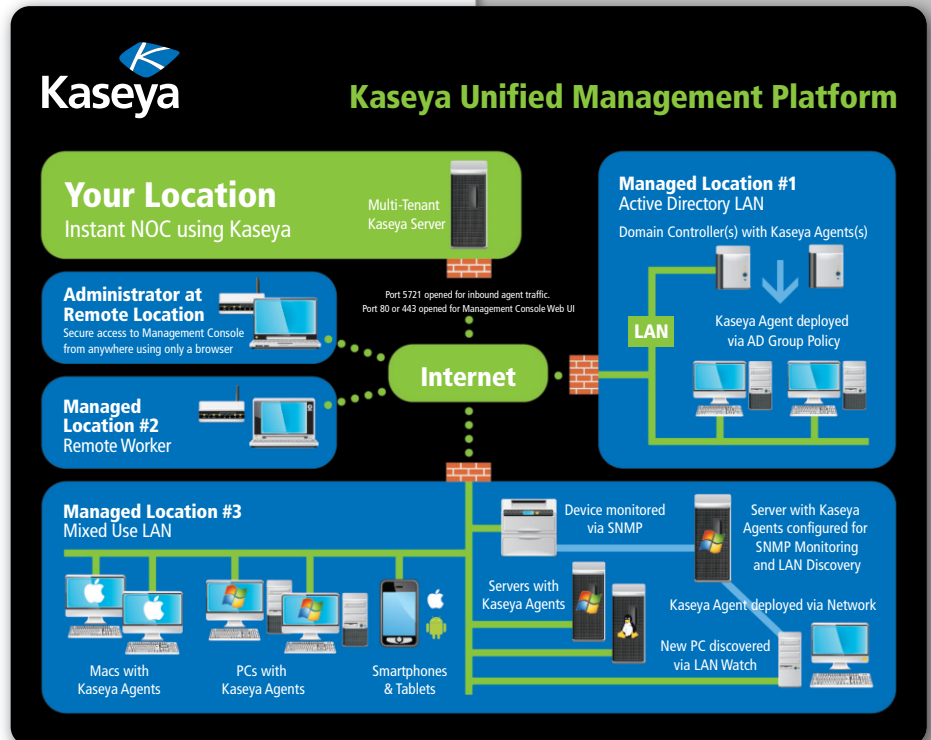
Web Access – Access to the user and admin web interface is encrypted using industry standard TLS.

Access Control

Kaseya provides strong access control features to ensure compliance with HIPAA and PCI. The technician's ability to control and manage machines is limited by both role and scope. Each technician is granted one or more scoping rights to have visibility to only the devices they are allowed to see. Each technician is also assigned one or more roles thereby enabling specific functionality in the system. Each function is highly controlled, limiting technicians to only the functionality and devices to which they should have access.

Secure Access

Administrators and technicians access the Kaseya server through a Web interface after a secure logon process. They can either authenticate against the Kaseya system itself alone, use the integrated Active Directory authentication, or use two-factor authentication to satisfy high security requirements. The system never sends passwords over the network. Each technician is the only one who knows his or her password. The Kaseya server combines passwords with unique randomly generated challenges

Kaseya Unified Management Platform

Your Location
Instant NOC using Kaseya

Multi-Tenant Kaseya Server

Administrator at Remote Location
Secure access to Management Console from anywhere using only a browser

Port 5721 opened for inbound agent traffic.
Port 80 or 443 opened for Management Console Web UI

Managed Location #2
Remote Worker

Internet

Managed Location #1
Active Directory LAN

Domain Controller(s) with Kaseya Agents(s)

LAN

Kaseya Agent deployed via AD Group Policy

Managed Location #3
Mixed Use LAN

Device monitored via SNMP

Server with Kaseya Agents configured for SNMP Monitoring and LAN Discovery

Servers with Kaseya Agents

Kaseya Agent deployed via Network

New PC discovered via LAN Watch

Macs with Kaseya Agents

PCs with Kaseya Agents

Smartphones & Tablets

Kaseya®
THE IT MANAGEMENT CLOUD COMPANY™

for each attempt, hashed with SHA-256. This challenge process protects against a man-in-the-middle attack.

Strong Authentication

In many highly sensitive situations, username and password protection is not enough. Kaseya supports powerful yet simple to use Two Factor Authentication to add an extra layer of security. The two form authentication support is not limited to credentials into the Kaseya System, but also includes authentication for endpoints, cloud systems, and other related systems.

System Logging

Each time a technician remote administers, performs an action, or otherwise manages a system, it is logged in the system log. Administrators can review the actions of each technician on time periods as they were performed on different machines. In addition to technician operations, automation actions, such as those performed by the policy engine, are also logged thereby showing a complete view of all management activities performed on each managed system.

End User Privacy

To help resolve privacy concerns, Kaseya offers an optional system tray application which allows the end user to "disable" or "enable" remote control to the system. When the end user disables remote control, all screen recording, remote control, chat, or other kinds of potential intrusions by the technicians are disabled.

Kaseya Agent Encryption

Your Location
Instant NOC using Kaseya

Multi-Tenant Kaseya Server

Internet

Managed Computer
Running Kaseya Agent Process

Communication Encryption Steps

1. An Agent initiates communication to the KServer by sending its name/GUID as identification.

2. The KServer responds by sending a random number challenge back to the Agent. (The use of a different random number with each checkin session prevents playback/ man-in-the-middle vulnerabilities.)

3. The Agent computes a SHA-256 value over a combination of the current password and random number.

4. The Agent sends the resultant hash value to the server.

5. The KServer computes the SHA-256 hash of the same combination its copy of the random number with its copy of the current password for the particular Agent.

6. The hash values are compared and if they match, then the Agent session has been authenticated.

7. All subsequent messages, containing commands and responses, between the KServer and Agent are encrypted using AES-256.

About Kaseya

Kaseya is the leading provider of cloud-based IT management software. Kaseya solutions allow Managed Service Providers (MSPs) and IT organizations to efficiently manage IT in order to drive IT service and business success. Offered as both an industry-leading cloud solution and on-premise software, Kaseya solutions empower MSPs and mid-sized enterprises to command all of IT centrally, manage remote and distributed environments with ease, and automate across IT management functions. Kaseya solutions are in use by more than 10,000 customers worldwide in a wide variety of industries, including retail, manufacturing, healthcare, education, government, media, technology, finance, and more. Kaseya is privately held with a presence in over 20 countries. To learn more, please visit **www.kaseya.com**

Kaseya®

THE IT MANAGEMENT CLOUD COMPANY™