Kaseya was designed and built with security as the fundamental building block to its core architecture. In fact, the name itself, Kaseya, stems from an American Indian word meaning “to secure and protect”, inspired by its founders who brought over 50 years of experience designing and architecting secure systems for the likes of government and financial institutions. With millions of systems under management today, Kaseya has a proven track record of the highest levels of security available in a management platform and uniquely combines ease-of-use with high security. At Kaseya, we start and end with security as the cornerstone of everything we do.

Certified 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.

Firewall Friendly

Kaseya just works with your existing, unmodified, network infrastructure. Since all communications are outbound from the client endpoints, Kaseya does not need any inbound ports opened. This lets the Kaseya system work across the internet or any network to remotely manage machines without the need for open ports at the remote site, removing susceptibility to inbound port probes or new network attacks at remote sites.

Network Topology

If a computer can see the internet, Kaseya supports it. Kaseya’s agent connects back to the central Kaseya server in any network topology, including several layers of NAT, easily without any special configuration or permissions. With Kaseya, you do not need to introduce a secret back door in order to support centralized management.

Encryption

Kaseya protects against man-in-the-middle attacks by encrypting all communications between the agent and server with FIPS certified 256-bit AES using a key that rolls every time the server tasks the agent, often multiple times per day. Since there are no plain text data packets passing over the network, there is nothing available for an attacker to exploit.
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 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. By teaming with a market-leading security software provider, 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.

For more information click here.

Roles and Scopes

Technician’s ability to control and manage are 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 thereby limiting technicians to only the functionality and devices they should have access to.

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 end user concerns of “big brother” watching over them, 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 Platform Hotfixing

For self hosted customers, The Kaseya Server itself is further protected by Kaseya Hotfixing. As soon as new patches and fixes are released, the Kaseya Server automatically detects they are needed and applies all security patches automatically based on your policies. Hotfixes are delivered securely with a digital signature and cannot be spoofed.

The Kaseya Hotfixing allows for security fixes to be pushed out globally in a very short period of time thus minimizing the impact of security holes or zero day attacks.
Certifications and Compliance

Kaseya’s strong dedication to security is more than just a mere talking point, the commitment is verified and certified through standards bodies and third party verification organizations of those standards.

Federal Information Processing Standard (FIPS)

Kaseya has achieved third party certification of Federal Information Processing Standard (FIPS) compliance. The FIPS standard was developed by the United States federal government for use in all non-military government agencies and contractors. Many FIPS pronouncements are modified versions of standards used in the technical communities, such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE), and the International Organization for Standardization (ISO).

Common Criteria

Similar to the FIPS certification, which originates from the USA, Kaseya has also achieved third party certification of EAL2+ Common Criteria. The Common Criteria for Information Technology Security Evaluation or Common Criteria certification brings independent validation of Kaseya systems including the use of industry recognized security standards originating from the international computing community. Common Criteria is a globally recognized set of guidelines (ISO 15408), which defines a common framework for evaluating security features and capabilities of information technology security products. The Common Criteria Mutual Recognition Agreement (CCRA) is a pact that was designed to allow all evaluations to be recognized by all participating countries, regardless of where the evaluation was completed. There are currently 26 countries involved in the CCRA, with many others that follow unofficially. Many organizations around the world mandate Common Criteria certification for all information technology systems.

Platform Vulnerability Testing

Kaseya performs recurring third party vulnerability testing of the entire Kaseya Platform. Third party vendors who specialize in penetration and vulnerability testing attack the Kaseya System in order to ensure the highest levels of security using the latest tools and techniques employed by today’s hackers and cybercriminals. If new problems are discovered, they are quickly pushed out to all environments using Kaseya Hotfixing.

PCI, HIPAA, and other compliance

Kaseya customers include a wide range of organizations where information security is far more valuable than the hardware itself. Kaseya enables and supports a number of different compliance standards including PCI compliance and HIPAA compliance.

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

©2014 Kaseya. All rights reserved. Kaseya and the Kaseya logo are among the trademarks or registered trademarks owned by or licensed to Kaseya Limited. All other marks are the property of their respective owners.