Kaseya

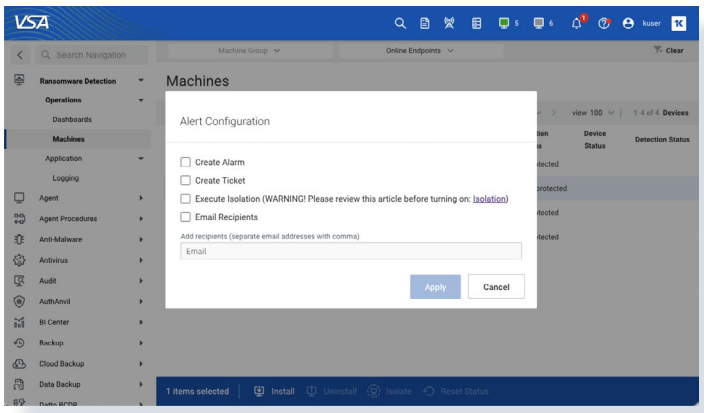
VSA™

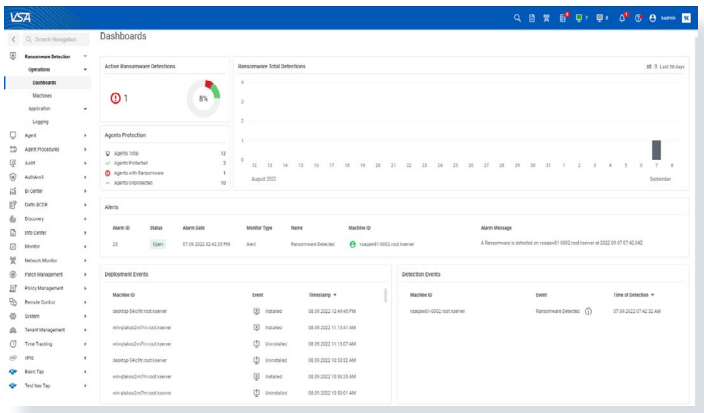
Ransomware Detection

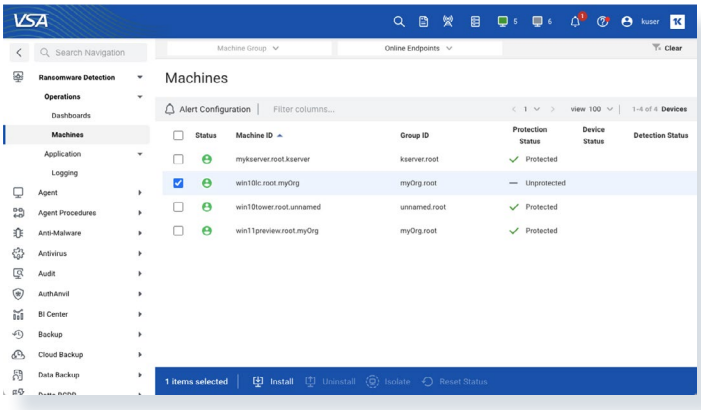
An Increasing Threat

In 2021 there were 31,000 ransomware attacks per day on small and medium businesses (SMBs). In 2022, there is forecasted to be between 68,000 and 73,000 ransomware attacks per day. The average ransomware attack is up to $1,800,000 USD and the time to takes to recover can take up to 287 days. The impact of a ransomware attack is at best budget destroying and more likely business destroying. What's worse, the downtime after an attack can cost up to 50 times more than the ransom itself. Simply put, our community is under attack.

There are countless tools that you can use to reduce downtime for your clients and protect their businesses from security threats. Remote monitoring and management (RMM) platforms have always played an important role for managed service providers (MSPs) in reducing downtime and protecting businesses from security threats through real time monitoring and patching to keep managed devices secure from known vulnerabilities.







Kaseya

DATA SHEET

Kaseya

VSA™

Ransomware Detection

Reduce the Risk of Ransomware

VSA is a secure and fully-featured cloud platform enabling MSPs to remotely monitor, manage and support every endpoint under contract. VSA now provides an extra layer of security with native Ransomware Detection. VSA monitors for the existence of cryptoransomware on endpoints using behavioral analysis of files, and alerts you when a device is infected. Once detected, VSA attempts to stop the ransomware process, and isolates the device to prevent the ransomware from spreading. VSA Ransomware Detection offers MSPs these benefits:

- **Monitor for ransomware at scale.** VSA's powerful policy-driven approach allows you to easily monitor targeted devices and specify what the monitor looks for prior to creating an alert (e.g. locations, extensions, priority of alerts).
- **Receive immediate notification when ransomware is detected.** Instead of waiting for a user to report the issue, VSA will automatically notify technicians the moment files start being encrypted by ransomware. Additionally, integrations with key MSP tools, such as PSA, ensure the right resources can be notified and tickets created immediately.
- **Prevent the spread of ransomware through network isolation.** Once ransomware is detected, VSA will attempt to kill the ransomware process and can automatically isolate the affected device from the network.
- **Remediate issues remotely.** Devices automatically isolated from the network still maintain contact with VSA, allowing technicians to take effective action to resolve the issue.
- **Recover with Kaseya Continuity products.** When VSA is integrated with Unitrends, Spanning, Datto continuity and disaster recovery (BCDR) products, technicians can quickly recover from the ransomware outbreak by restoring the impacted endpoint to a previous state.

VSA Ransomware Detection Requirements:

- An active VSA RMM subscription or trial
- Devices must be Managed (and not On Demand)
- Users will require the relevant permissions to add this monitor to a device or as part of a policy
- Use of the new VSA RMM UI
- Supported devices: currently supported Windows OS devices

To learn more about VSA RMM, please visit:
https://www.kaseya.com/products/vsa/

20102022

Kaseya
DATA SHEET