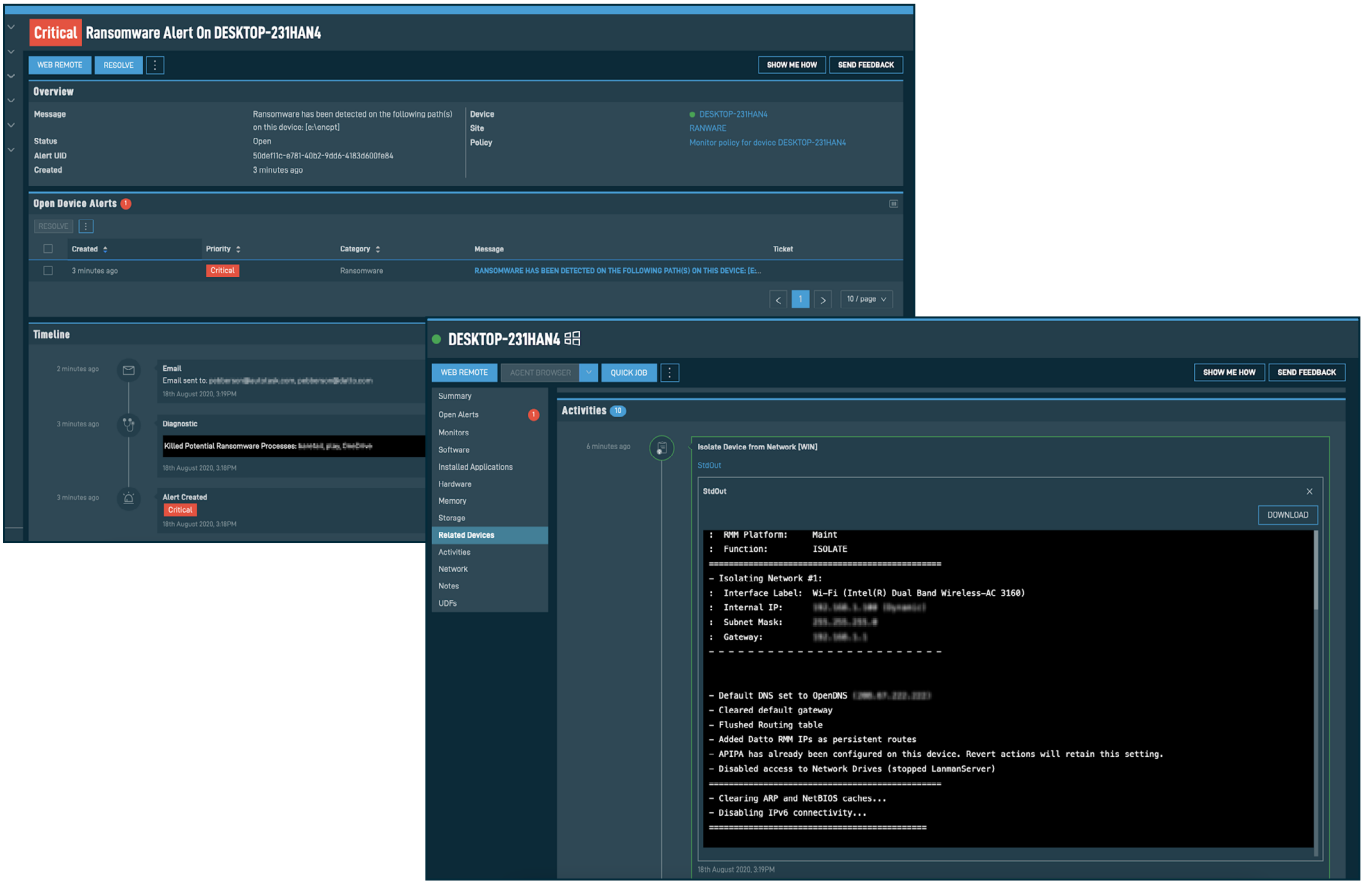
datto | BUSINESS MANAGEMENT

Datto RMM Ransomware Detection

An Increasing Threat

By 2021, ransomware attacks are anticipated to cause £15 billion in damage, which is 57 times higher than in 2015[1], and on average, it can take 287 days to recover from an attack[2]. The ransom demanded during an attack is roughly £4,100. What's worse, the downtime after an attack can cost up to 50 times more than the ransom itself[3].

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.



Reduce the Risk of Ransomware

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

- **Monitor for ransomware at scale.** Datto RMM'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, Datto RMM 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, Datto RMM 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 Datto RMM, allowing technicians to take effective action to resolve the issue.
- **Recover with Datto Continuity products.** When Datto RMM is integrated with Datto business continuity and disaster recovery (BCDR) products, technicians can quickly recover from the ransomware outbreak by restoring the impacted endpoint to a previous state.

Datto RMM Ransomware Detection Requirements:

- An active Datto 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 Datto RMM UI
- Supported devices: currently supported Windows OS devices

To learn more about Datto RMM, please visit www.datto.com/products/rmm.

[1]https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

[2]blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019

[3]Datto's Global State of the Channel Ransomware Report

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291