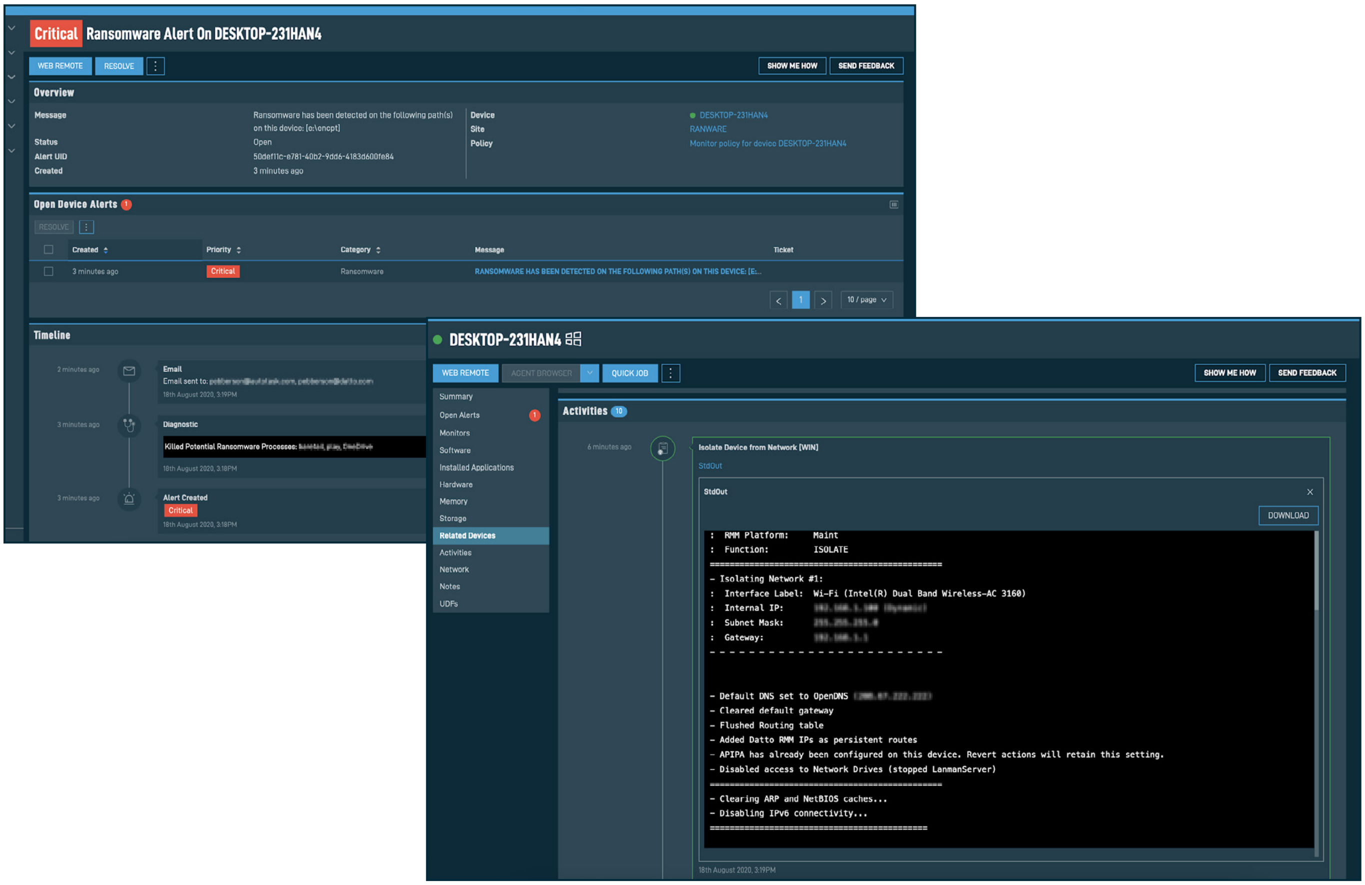
datto | BUSINESS MANAGEMENT

# Datto RMM Ransomware Detection

## An increasing threat

**Having the right cybersecurity tools in place is more important than ever. Year-over-year ransomware attacks have increased by 92.7%[1] with the average ransom demanded during an attack being roughly $5,600.** What's worse, the downtime after an attack can cost up to 50 times more than the ransom itself[2].

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



Critical Ransomware Alert On DESKTOP-231HAN4

Overview

Message: Ransomware has been detected on the following path(s) on this device: [c:\encpt]
Status: Open
Alert UID: 50def11c-e781-40b2-9dd6-4183d600fe84
Created: 3 minutes ago
Device: DESKTOP-231HAN4
Site: RANWARE
Policy: Monitor policy for device DESKTOP-231HAN4

Open Device Alerts 1

| Created | Priority | Category | Message | Ticket |
|---|---|---|---|---|
| 3 minutes ago | Critical | Ransomware | RANSOMWARE HAS BEEN DETECTED ON THE FOLLOWING PATH(S) ON THIS DEVICE: [E:... | |

Timeline

2 minutes ago — Email
Email sent to: [redacted]
18th August 2020, 3:19PM

3 minutes ago — Diagnostic
Killed Potential Ransomware Processes: [redacted]
18th August 2020, 3:18PM

3 minutes ago — Alert Created
Critical
18th August 2020, 3:18PM

DESKTOP-231HAN4

Activities 10

6 minutes ago — Isolate Device from Network [WIN]
StdOut

StdOut

```
:  RMM Platform:     Maint
:  Function:         ISOLATE
===============================================
- Isolating Network #1:
:  Interface Label:  Wi-Fi (Intel(R) Dual Band Wireless-AC 3160)
:  Internal IP:      [redacted]
:  Subnet Mask:      [redacted]
:  Gateway:          [redacted]
- - - - - - - - - - - - - - - - - - - - - - - -



- Default DNS set to OpenDNS [redacted]
- Cleared default gateway
- Flushed Routing table
- Added Datto RMM IPs as persistent routes
- APIPA has already been configured on this device. Revert actions will retain this setting.
- Disabled access to Network Drives (stopped LanmanServer)
===============================================
- Clearing ARP and NetBIOS caches...
- Disabling IPv6 connectivity...
============================================
```

18th August 2020, 3:19PM

## Reduce the risk of ransomware

Datto RMM is a secure and fully-featured cloud platform enabling a businesses IT operations team to remotely monitor, manage and support every endpoint under contract. Datto RMM 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 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 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 continuity products.** When Datto RMM is integrated with 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 supports Windows OS devices

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

[1] https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021

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

**Corporate Headquarters**
Kaseya Miami
701 Brickell Avenue
Suite 400
Miami, FL 33131
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 |

Updated February 2023