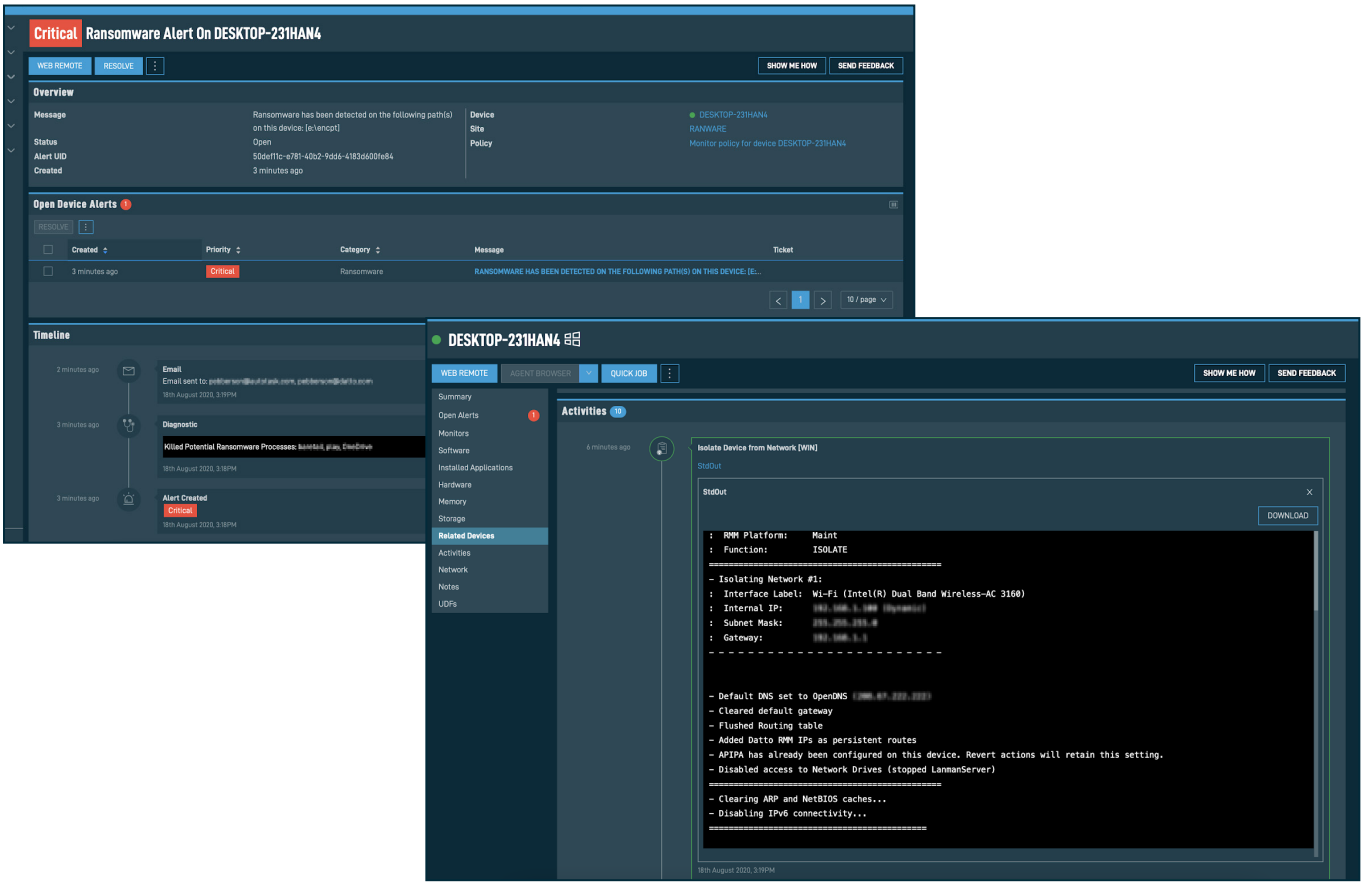
datto | BUSINESS MANAGEMENT

# Datto RMM Ransomware-Erkennung

## Eine zunehmende Bedrohung

**Im Jahr 2021 werden Ransomware-Angriffe Schätzungen zufolge Schäden in einer Höhe von 20 Milliarden Dollar anrichten, was 57 Mal höher ist als der Wert des Jahres 2015[1]. Die Erholung von einem solchen Angriff wird im Schnitt 287 Tage in Anspruch nehmen[2].** Das Lösegeld, das bei einem Angriff gefordert wird, liegt bei durchschnittlich 5.600 Dollar. Viel schlimmer aber ist: Die Ausfallzeit nach einem solchen Angriff kann bis zu 50 Mal mehr kosten als das Lösegeld selbst[3].

Es gibt unzählige Tools, die Sie nutzen können, um die Ausfallzeiten für Ihre Kunden zu verkürzen und ihre Unternehmen vor sicherheitstechnischen Bedrohungen zu schützen. Remote Monitoring & Management-Plattformen (RMM) haben für Managed Service Provider (MSPs) immer eine große Rolle gespielt, wenn es darum ging, mit Hilfe von Echtzeit-Monitoring und Patching Ausfallzeiten zu minimieren und Unternehmen vor sicherheitstechnischen Bedrohungen zu schützen, indem man die bekannten Schwachstellen der Geräte absichert.



## Reduzieren Sie das Ransomware-Risiko

Datto RMM ist eine sichere und voll ausgestattete Cloud-Plattform, die MSPs in die Lage versetzt, jede unter Vertrag genommene Endstelle aus der Ferne zu überwachen, zu verwalten und zu unterstützen. Darüber hinaus bietet Datto RMM jetzt auch noch ein zusätzliches Sicherheitsnetz: eine native Ransomware-Erkennung. Um dies zu ermöglichen, führt Datto RMM Verhaltensanalysen von Dateien durch und untersucht die Endstellen so auf das Vorhandensein von Krypto-Ransomware. Ist ein Gerät infiziert, sendet das Programm eine Meldung. Anschließend versucht Datto RMM, den Ransomware-Prozess zu stoppen, und isoliert das Gerät, um eine Ausbreitung der Schadsoftware zu verhindern. Dies sind die Vorteile, die die Ransomware-Erkennung von Datto RMM den MSPs bieten kann:

- **Passgenaue Überwachung auf Ransomware** Der starke, auf Richtlinien basierende Ansatz von Datto RMM ermöglicht es Ihnen, die anvisierten Geräte mühelos zu überwachen und zu spezifizieren, worauf die Überwachung achten soll, bevor sie eine Meldung generiert (z. B. Orte, Erweiterungen, Priorisierung von Meldungen).
- **Sofortige Benachrichtigung, wenn Ransomware erkannt wurde.** Statt darauf zu warten, dass der Nutzer ein Problem meldet, können Sie sofort aktiv werden, denn Datto RMM wird die Techniker automatisch in dem Moment informieren, in dem Dateien von Ransomware angegriffen werden. Die Integration in wichtige MSP-Tools, wie etwas PSA, sorgt außerdem dafür, dass die richtigen Ressourcen angefordert und auf der Stelle Tickets erstellt werden.
- **Verhinderung der Ausbreitung von Ransomware durch Netzwerkisolierung.** Wenn Ransomware erkannt wurde, wird Datto RMM versuchen, den Ransomware-Prozess zu unterdrücken. Dazu kann es das betroffene Gerät automatisch vom Rest des Netzwerks isolieren.
- **Fehlerbehebung aus der Ferne.** Die automatisch vom Netzwerk getrennten Geräte bleiben in Kontakt mit Datto RMM, sodass die Techniker effektiv Maßnahmen ergreifen können, um das Problem zu lösen.
- **Wiederherstellung mit Continuity-Produkten von Datto** Wenn Datto RMM in Business Continuity und Disaster Recovery-Produkte (BCDR) von Datto integriert ist, können die Techniker die Wiederherstellung nach dem Ransomware-Angriff blitzschnell durchführen, indem sie die betroffene Endstelle auf einen vorherigen Zustand zurücksetzen.

## Anforderungen für die Datto RMM Ransomware-Erkennung:

- Ein aktives Datto RMM-Abo oder Datto RMM auf Probe
- Die Geräte müssen verwaltet werden (nicht On-Demand)
- Die Nutzer benötigen die entsprechenden Genehmigungen, um die Überwachung zu einem Gerät oder einer Richtlinie hinzufügen zu können
- Nutzung der neuen Benutzeroberfläche von Datto RMM
- Unterstützte Geräte: aktuell unterstützte Geräte mit Windows-Betriebssystem

**Mehr über Datto RMM erfahren Sie auf**
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]Global State of the Channel Ransomware Report von Datto

datto

**Hauptsitz des Unternehmens**
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
USA
partners@datto.com
www.datto.com
888,294.6312

**Weltweite Standorte**
USA: 888,294.6312
Kanada: 877,811.0577
EMEA: +44 (0) 118 402 9606
Australien: +61 (02) 9696 8190
Singapur: +65-31586291

©2020 Datto, Inc. Alle Rechte vorbehalten.
Aktualisiert im Dezember 2020