RANSOMWARE DETECTION Pulseway

Pulseway Ransomware Detection

Automated Peace of Mind

Your customers are increasingly worried about Ransomware

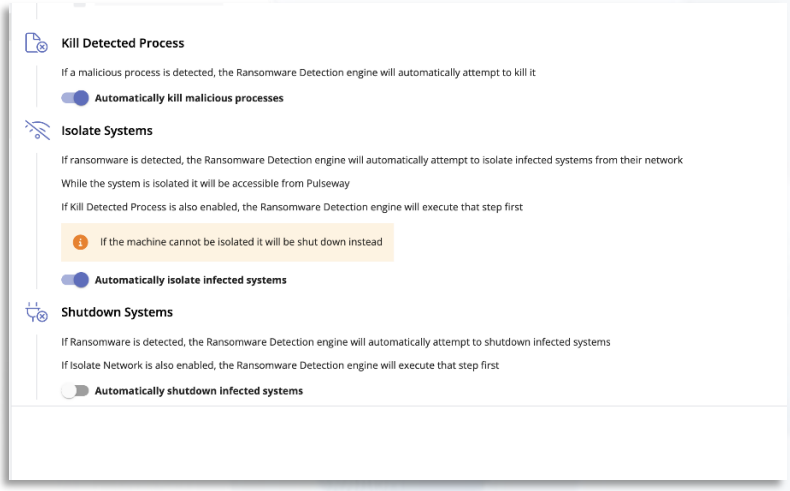
Can you identify an attack before it has any major impact?

The trouble with Ransomware is that you usually don't know it's there until it is too late. This makes life difficult for MSPs.

It's time to shift the balance with Pulseway Ransomware Detection (PRD).

Pulseway Ransomware Detection: Automated Peace of Mind

Integrated with the Pulseway RMM, Pulseway Ransomware Detection scans your customers' networks for suspicious file behavior. You can define ransom detection policies that determine what automated actions should be performed when suspicious activity is detected. In addition to defining alert severity, you can also automatically kill malicious processes, isolate infected machines and shut down infected systems.



Ransomware attacks tend to happen when there is no one watching

Most recent ransomware attacks took place over weekends and holidays so they can spread and inflict maximum damage before anyone notices.

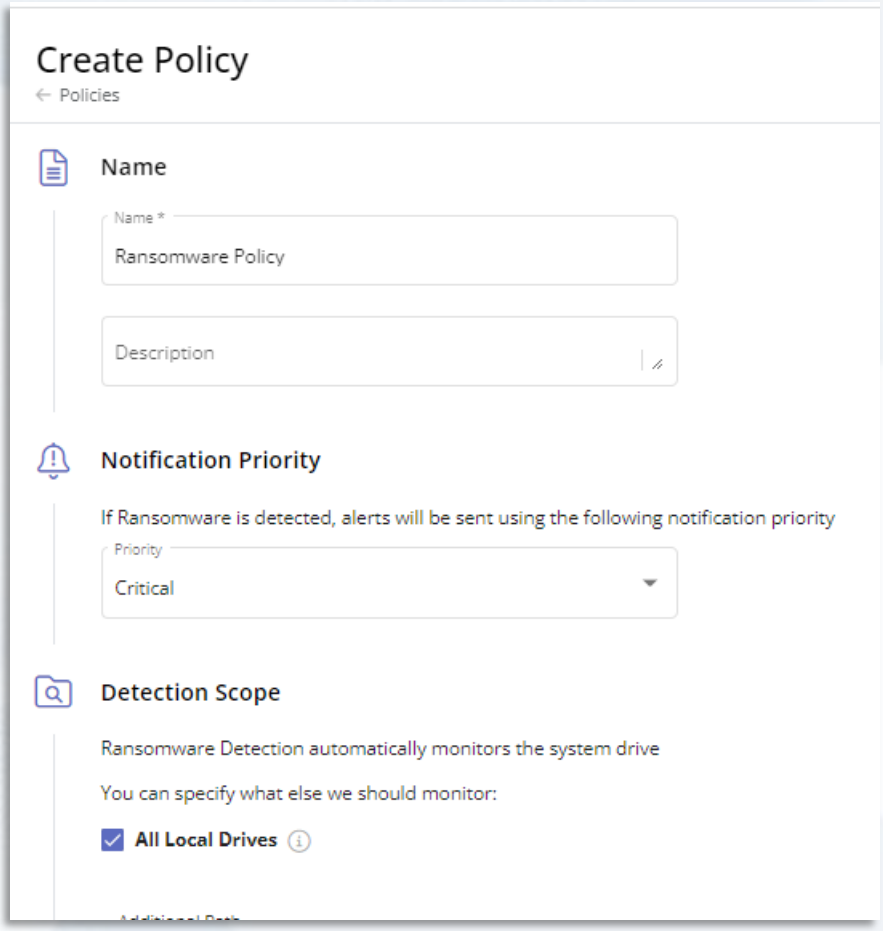
Pulseway Ransomware Detection stays alert 24x7 and automatically stops ransomware spreading.

Pulseway

Automated Response

Easy to use policies allow you to define exactly how to respond when Ransomware is detected. You can:

- Kill malicious processes (ON by default)
  - Kill the processes identified as the cause of the suspicious activity
- Isolate infected machines (ON by default)
  - You can still access isolated machines via Pulseway for investigation
- Shutdown infected machines (OFF by default)
  - For total protection



Targeted Protection

Ransomware Detection automatically monitors the system drive. You can also choose to monitor all local drives or choose specific paths to include or exclude. You can also exclude specific file types.

How Ransomware Detection Works

Ransomware is constantly evolving with over 1200 variants being created **every day.** Instead of looking for specific variants, Pulseway Ransomware Detection works by identifying the suspicious file activity typically associated with Ransomware attacks.

It detects patterns of change in specific file types, that typically indicates Ransomware:

- In-place file content overwrite with random data.
- Overwriting content of ONLY the file types that ransomware commonly targets.
- Excludes file types commonly ignored by ransomware.
- Preserve all the original file modified timestamps, including overwritten files

Supported Platforms

Pulseway Ransomware Protection supports Windows 8 & above and Windows server 2012 & above

Ransomware by numbers

There is a Ransomware attack every **11** seconds

The average cost of downtime after an attack is **$53,000**

82% of Ransomware attacks were on companies with less than 1000 employees

40% of small businesses lost valuable data after an attack

Offer enhanced monitoring services with Pulseway Ransomware Detection.

Try it today!

Pulseway