trackd

Automating Vulnerability Remediation without the Fear of Disruption.

The top two reasons vulnerability remediation teams give for patch delays are:

- **Resource constraints**
- **Fear of breaking something**

trackd is addressing both issues with a single platform.

The Vulnerability Remediation Reality

Less than 2% of patches are rolled back, meaning at least 98% are strong candidates for automation that would require little human involvement.

But remediation teams are justifiably reluctant to leverage auto-patching: that 2% can do a lot of damage if the wrong guess is made.

How Does trackd Help?

The trackd platform collects patching experience data across all users, anonymizes it, and shares it with all other users in real-time. So, trackd users can see how many times a given patch was applied, and more importantly, how often it caused a disruption.

trackd Enables Data-Driven Remediation Decision-Making

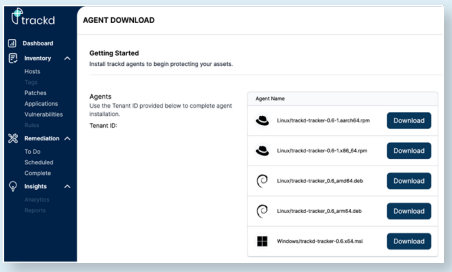
Armed with this real-world (and real-time) insight, remediation teams can maximize auto-patching with confidence, freeing precious resources for the 2% of patches that are best handled manually.

We're taking the guesswork out of vulnerability remediation.

How Does the trackd Platform Work?

1 Install our lightweight agent

The trackd agent can be installed on any of our supported operating systems to securely register a device to your isolated tenant environment.



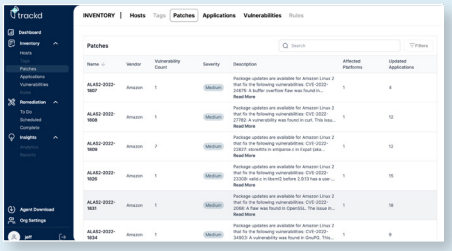
2 Metadata is collected by our agent

As soon as the trackd agent is installed, it starts collecting metadata about the operating system and applications installed on the system.

3 Data is reported to the trackd platform

Our correlation engines:

- Ensure the most accurate and up-to-date understanding of what vulnerabilities affect that device.
- Determine if patches are available to remediate them.
- Check for any reported or detected distruption data previously observed by other operators using trackd.



4 Patches are delivered and analyzed

When patch delivery is orchestrated using the trackd platform, each agent collects general system state information and patch installation performance telemetry during its job execution.

5 Data is reported back in real-time

Upon completion, this data is reported back to the platform to provide real-time situational awareness of overall remediation progress and any detected distruptions to your environment.

6 Remediation telemetry is aggregated

Additionally, any remediation telemetry helpful in illuminating a patch's potential tobe disruptive to others is anonymized and aggregated to be presented to the collective usres of trackd in the web application.

7 More data. More confidence. Shorter MTTR.

As more patches are applied, data collected, and insights shared, vulnerability remediation teams will have confidence in accelerating their patching cadence to eliminate vulnerabilities in their organizations before malicious cyber actors are able to exploit them.