

Datto EDR: Purpose-built for modern IT teams by cybersecurity experts

Datto EDR was never built to be ordinary.

It started at the highest level, developed by veterans of the U.S. Air Force Cyber Emergency Response Team (AFCERT) after their military service, who leveraged their elite expertise to hunt down the latest advanced threats. Then, it quickly proved itself inside Fortune 500 giants. However, the most important evolution was turning this elite-level protection into a solution built for MSPs and mid -market businesses. With patented threat-hunting technology and a relentless focus on detection and response, Datto EDR is getting smarter and stronger with every release.

Here's a glimpse of how it all unfolded – and where it's heading.

2014



Born from the battlefield

Infocyte is founded by AFCERT veterans with deep experience in national cyberthreat response and incident forensics.

Patents granted

- ✓ <u>US10929536B2</u>: Techniques for post-breach detection and analysis
- ✓ <u>US11610001B2</u>: Host-based threat hunting via memory and behavioral analysis

2015 -2021



Tested in the big leagues

Infocyte becomes a trusted tool in high-stakes environments.

- ✓ Fortune 500 law firms, banks and energy companies Deployed across thousands of endpoints
- - Proven to detect and neutralize advanced post-breach activity

2022



The Datto era begins

Datto's acquisition of Infocyte transformed EDR into a solution purpose-built for MSPs and mid-market businesses.

- ✓ Scales to 300K+ protected endpoints in the first year
- ✓ Launches Ransomware Rollback a feature that enables file recovery even when backups or VSS are compromised

2023



Major platform enhancements

Added detection, role-based access and multitenant management features, plus gave the UX and policy management a complete overhaul.

- ✓ More granular detection rules and customizable suppression settings
- ✓ New user roles: Admin vs. analyst for better access control
- ✓ Improved alert visibility across multitenant environments Advanced search filters and an updated alert view
- Easier group policy assignments and override settings

2024



Unified protection arrives

Datto AV is now part of a single-agent stack alongside Datto EDR, with built-in suppression rule management. New features include:

- ✓ Deploy and manage AV directly from the EDR console ✓ Initial AV policy, exclusion and status support inside the EDR UI
- ✓ More granular rule application per org/location Ability to track suppressed alert matches historically
- EDR launches customizable automated threat responses

2025



Evolving again

new protections and a smoother admin experience. Highlights include:

Datto continues to push security and usability forward with powerful

Security updates ✓ Full AV support rolls out for MacOS endpoints

- ✓ Adds web protection through DNS-based URL filtering
- ✓ Tamper protection prevents unauthorized users from disabling EDR or AV components
- Major UI and workflow upgrades

✓ Dark mode, redesigned alerts table and unsaved changes prompts ✓ Persistent uninstall jobs (6-month lifespan)

- RMM device link accessible even when offline



Coming



The next chapter brings Al-driven enhancements that make Datto EDR even faster, smarter and more adaptive.

Built with AI in mind

Nothing gets past it unless you allow it. - Corey Mason, Network Services Manager, **United Systems and Software**

Datto EDR is like a boa constrictor.

Want endpoint protection that keeps you secure without

slowing you down?

©2025 Datto, Inc. All rights reserved.