



Cyber Unified Defense Platform

Official Release Roadmap

What's committed, what's in testing, and where the product is headed

Version 5.41.0

Published August 23, 2026

DADavisDesigns: Cyber Defenders

Cyber Unified Defense Platform — Official Release Roadmap

A Note on This Roadmap

Cyber Unified Defense Platform is under active, continuous development. This roadmap reflects the current direction as of this release and is intended to give evaluators a clear picture of where the product is going — not a binding release date commitment. Items may move between sections as priorities and trial feedback shape the plan.

Draft for review

The items below are drafted from currently open, known items in the codebase. They are a starting point — confirm, edit, or reprioritize before this is distributed as a public-facing document.

Coming in the Official Release

Committed items planned for the transition from trial/evaluation build to official release:

- Fully automated server/tray auto-start — wired directly into the installer so no manual, elevated scheduled-task setup is required after installation.
- Hash Watchlist coverage extended to File Integrity Monitoring (FIM) and File Scanner — currently, watchlist matching runs only against the hourly System32 integrity scan.
- Branded installer polish — resolving the placeholder application icon shown by the agent installer on some systems.
- Expanded proactive alerting for licensing and platform health, building on the license-expiration alerts introduced this release.

Enhancements in Testing

Features under active evaluation, not yet committed to a specific release:

- DNS Sinkholing & Host-Level Enforcement (in development, dev lab testing) — extends Blacklist rules to actively block malicious domain resolution via DNS sinkholing, with optional host-level firewall enforcement on the endpoint. Today, Blacklisting only escalates severity; this closes the gap toward real containment.
- Direct mail-gateway integration — deeper, message-level link and attachment analysis via provider APIs (Microsoft Graph, Gmail API, Exchange EWS), beyond current inbox polling.
- Broader automated response actions — optional auto-containment for confirmed high-confidence threats, rather than alert-and-review only.
- Additional SIEM/EDR data source integrations, expanding beyond the platform's native agent telemetry.
- Deeper patch compliance reporting, including trend-over-time views alongside current-state snapshots.

An Invitation for Trial Feedback

If you are evaluating Cyber Unified Defense Platform during this trial period, your feedback directly shapes which of the items above get prioritized — and surfaces the ones that are not on this list yet. If something in your environment feels like it is missing, awkward, or would change your decision to adopt the platform, that is exactly the kind of feedback this roadmap is built from.

Contact: support@dadaavisdesignsllc.com