



Cyber Unified Defense Platform

Release Notes

Version 5.41.0 — what's new, what's fixed, and what to know before upgrading

Version 5.41.0

Published August 23, 2026

DADavisDesigns: Cyber Defenders

New Features

- One-command agent install links — generate a token-based install link for Windows (iwr | iex) or Linux (curl | bash) directly from the dashboard, so deploying to a new endpoint no longer requires copying installer files by hand.
- Proactive license expiration alerts — an email and in-app banner now warn an administrator once a trial license is within 7 days of expiring, instead of the platform simply going read-only with no notice.
- System file integrity ingestion — hourly System32 change reports from the agent are now received and checked against the Hash Watchlist, with a critical alert on any match.
- Critical severity tier — email threat scoring now supports a Critical tier above High, for messages with a very strong combination of indicators.
- Medium severity is now included in the Top Threat Type calculation on the Email Security Monitor, with Critical and High still taking priority over Medium regardless of count.
- Azure Trusted Signing wired into both build scripts, so server and agent installers are digitally signed as part of every build.
- EULA scroll-to-accept flow added to the first-run license agreement screen.
- Knowledge Base module added, seeded with 8 default cybersecurity runbooks that auto-populate on fresh installs.
- Email alert on-call override system — a per-recipient "always notify" flag ensures on-call staff receive every alert regardless of their normal severity filter.
- Full DNS Sinkholing shipped — hosts-file enforcement, auto-sync from Threat Intel feeds, and per-endpoint status badges showing confirmed enforcement.
- FIM and DLP default watch paths expanded to include user home directories.
- Branded Windows agent install page, matching the main site header with a token-gated installer route.
- New Getting Started Guide, Administrator Guide, Release Notes, and Roadmap — the documentation set you are reading now.

Bug Fixes

- Fixed repeated HTTP 429 errors from the GeoIP lookup service by adding server-side response caching, so the same IP is not re-queried on every dashboard refresh.
- Fixed Email Security event counts not matching what was actually displayed in the table — clean messages were being counted toward totals shown to the user but filtered out of the visible list, making the numbers look wrong.
- Added pagination ("Load More") to both the Phishing Analysis and Behavioral Events tables, and to the shared Total Emails view — previously capped at the first 100 results with no way to see the rest.
- Consolidated the "Total Emails" view so the Phishing and Behavioral tabs share a single listing instead of maintaining two separate, occasionally inconsistent copies of the same data.
- Fixed character encoding corruption ("mojibake") in email notification templates, weekly reports, and dashboard labels, where emoji and punctuation had been double-encoded at the source.
- Fixed the Weekly Executive Report donut chart, where summary text (e.g. "100% Resolved") could overflow past the ring instead of staying inside it.
- Fixed alignment in the Weekly Executive Report's "This Week at a Glance" stat grid, where the two average-time boxes did not line up under the three count boxes above them.
- Replaced the black-background application logo with a transparent-background version across the dashboard and all email templates.

- Added the missing `/api/agent/sys32-hashes` and `/api/health` endpoints, which the agent was already calling but the server had no handler for.
- Resolved a confirmed Kaspersky false positive triggered by a PyArmor obfuscation heuristic; false positive submissions were also completed with AVG, Arctic Wolf, and VIPRE/WithSecure.
- Fixed the build pipeline so version numbers are injected before obfuscation instead of after, preventing stale version numbers from being baked into shipped bytecode.
- Fixed server installer upgrade path: backups now use `.NET ZipFile`, and stale nested PyArmor folders are cleaned up automatically during upgrade.
- Fixed a legacy Linux agent issue where systemd services were not running as root, which blocked system-level enforcement actions.
- Fixed the agent self-update pipeline, which had a path constant mismatch preventing some agents from picking up new builds.
- Fixed a DNS Sinkholing reflection flood bug where agents were logging their own sinkholed domains as real traffic, generating false alerts and bad Threat Intel hit records; resolved via a shared sinkhole-reflection check applied at every ingestion point.
- Redesigned Sinkhole auto-sync to pull from PhishTank only with a 300-domains-per-run cap, after an earlier feed source caused an oversized single-run import.
- Fixed a Threat Intelligence display gap where domains already flagged as active indicators of compromise could still show as "Clean" elsewhere in the platform.
- Fixed a timezone bug where new indicator-of-compromise timestamps were recorded in UTC instead of matching server local time.
- Fixed a word-boundary matching bug in vulnerability scan scoring that could produce false positive CVE matches on partial software name matches.

Known Issues

- The server/tray auto-start scheduled task is not yet fully automated by the installer and may require a manual, elevated task setup step in some environments.
- The Hash Watchlist is currently checked by the System32 integrity scan only. File Integrity Monitoring (FIM) and the File Scanner do not yet cross-check discovered hashes against the watchlist.
- The agent installer's desktop icon may display as a blank/generic icon instead of the branded shield on some systems. This is cosmetic only and does not affect functionality.
- A benign warning ("name 'local_ip' is not defined") may appear in internet-activity logging under specific conditions; it does not affect data collection or alerting.
- The IOC Library search currently covers only the most recently loaded 500 rows rather than the full table; a fix is planned.
- DNS Sinkholing auto-sync remains paused pending a redesign following a fleet-wide false-alert incident; sinkholing enforcement itself is unaffected.

Upgrade Notes

- Server-side Python files (`app.py`, `config.py`, `license_manager.py`, `file_scanner.py`, and `database.py`) are distributed obfuscated and must always be rebuilt together in a single pass — mixing files from different builds will cause the server to fail to start.

- If upgrading from a version prior to 5.36.0, deploy the new transparent shield logo asset (shield-icon-transparent.png) to the server's static/img folder alongside the updated application files, or the previous black-background logo will continue to display.
- No database schema changes require manual migration in this release; new tables are created automatically on first use.

Recommended

Confirm a current backup exists before upgrading a production server. See the Administrator Guide's Backup & Restore section for the recommended procedure.

Version History

Version	Date	Highlights
5.41.0	August 2026	Full DNS Sinkholing (hosts-file enforcement, auto-sync, status badges), Knowledge Base module with default runbooks, on-call alert override, Azure Trusted Signing, EULA scroll-to-accept, multiple AV false-positive resolutions, agent self-update and Linux systemd fixes, sinkhole reflection-flood and auto-sync redesign, Threat Intel display and timezone fixes, KEV scan word-boundary fix.
5.36.0	July 15, 2026	Email Security overhaul, GeoIP caching, license alerts, documentation set, cosmetic and encoding fixes.
5.x	June – July 2026	Stability and installer hardening: server path migration, watchdog scheduled tasks, DB lock fixes, MFA/TOTP, 30-day trial licensing, EULA flow.
Earlier 5.x / 1.4.x agent	Q2 2026	Ransomware behavioral detection, Hash Watchlist, async File Scanner, software inventory, Executive Dashboard and Reports, FIM noise suppression, WAL mode.