



Cyber Unified Defense Platform

Platform Capabilities Overview

Prepared by DADavisDesigns: Cyber Defenders

Enterprise-Grade Network Security Monitoring for Small & Mid-Sized Organizations

Executive Summary

Most small and mid-sized organizations — including local government offices — face the same security challenge as large enterprises: an ever-growing set of endpoints, files, and network traffic that needs constant monitoring. Unlike large enterprises, they typically don't have a 24/7 Security Operations Center (SOC) or the six-figure budget that comes with one.

Cyber Unified Defense Platform (CUDP) closes that gap. It is a single, self-hosted platform that brings enterprise-level Endpoint Detection & Response (EDR), File Integrity Monitoring (FIM), Data Loss Prevention (DLP), Threat Intelligence, Email Security, and Network Monitoring together in one dashboard — built and priced for organizations with 5 to 15 endpoints, not 5,000.

The sections below walk through each capability using a simple format: the problem it solves, how CUDP solves it, and the practical benefit to your organization.

Endpoint Detection & Response (EDR)

Problem: Malicious or unauthorized software can run on a laptop or server for days or weeks before anyone notices — by then, damage is already done.

Solution: CUDP's lightweight endpoint agent continuously watches running processes, installed software, and file activity on every protected device, comparing behavior against known-bad signatures and ransomware behavioral patterns in real time.

Benefit: Threats are caught and flagged within minutes of appearing, not discovered weeks later during an audit.

- Real-time process and file monitoring on Windows and Linux endpoints
- Ransomware behavioral detection (not just signature matching)
- Hash-based blocking of known-malicious files across the entire fleet
- Full remote file scanning without requiring risky administrative network shares

File Integrity Monitoring (FIM)

Problem: Sensitive files (configs, credentials, financial records) can be modified, deleted, or accessed without anyone knowing until it's too late.

Solution: CUDP watches designated files and folders for unauthorized changes, deletions, or access, and generates an alert the moment something unexpected happens.

Benefit: You get an audit trail and early warning system for tampering — critical for compliance and incident response.

- Configurable watch paths per endpoint, including user home directories
- Severity-based alerting (medium, high, critical) so real threats aren't buried in noise
- Built-in noise suppression for routine OS activity, so alerts stay meaningful

Data Loss Prevention (DLP)

Problem: Sensitive data — SSNs, credit card numbers, credentials — can leave an organization through email, USB drives, or cloud uploads without any visibility into it happening.

Solution: CUDP scans file and data movement for sensitive data patterns and flags matches before they become a breach, without requiring a separate DLP product.

Benefit: Reduces the risk of accidental or malicious data exfiltration, and gives you evidence for compliance reporting if an incident does occur.

- Pattern-based detection tuned to avoid false positives on legitimate business files

Threat Intelligence & IOC Sweeping

Problem: New phishing domains, malicious IPs, and compromised files appear constantly — a static antivirus definition list can't keep up.

Solution: CUDP continuously sweeps endpoint activity (browser history, network connections, file hashes) against live threat intelligence feeds, flagging matches to known-malicious indicators of compromise (IOCs).

Benefit: You're protected against today's threats, not last year's — without manually researching every new domain or IP.

- Automatic matching against known phishing domains, malicious IPs, and malware hashes
- Custom Watchlist for tracking specific hashes, URLs/domains, IPs, or process names your organization cares about
- One-click actions to whitelist, blacklist, or escalate any flagged indicator

Intro to SOAR (Security Orchestration, Automation & Response)

Problem: Most small-business security tools only alert — a human has to read every finding and manually decide what to do, which means real threats sit open while someone gets to them.

Solution: CUDP doesn't just detect threats, it acts on them automatically. When a domain is confirmed malicious, DNS Sinkholing blocks it at the network level in real time, no manual step required. When a Trust Rule confirms an indicator as bad, matching alerts are automatically resolved and tracked, so an analyst never has to click through the same threat twice.

Benefit: Faster containment and less manual triage — the platform is already working in the background instead of just handing you a queue of alerts.

- Automated, real-time domain blocking via DNS Sinkholing when a threat is confirmed
- Automatic alert resolution and tracking when Trust Rules confirm an indicator as malicious
- Not full enterprise-scale orchestration, but a genuine step beyond alert-only tools for organizations with 5–15 endpoints

Email Security Monitoring

Problem: Phishing remains the #1 entry point for breaches, and most small organizations have no visibility into what's actually landing in employee inboxes.

Solution: CUDP monitors email traffic for threat indicators and gives you a dashboard view of total email volume, threat types, and trends over time.

Benefit: Leadership gets a clear, non-technical view of email risk without needing to read raw logs.

- Threat-type breakdown and volume trending on the Executive Dashboard
- Automated phishing and malicious-content detection with SPF, DKIM, and DMARC review
- Mailbox auto-forward and rule-tampering detection (Microsoft 365 and Google Workspace), catching a common post-compromise persistence technique attackers use to silently exfiltrate mail

Network Monitoring

Problem: You can't secure what you can't see — many organizations don't have an accurate picture of every device connected to their network.

Solution: CUDP continuously discovers and inventories devices on the network, tracks DNS and traffic activity, and flags unauthorized or unknown devices.

Benefit: Full visibility into everything on your network, with the ability to investigate and act on suspicious connections immediately.

- Automatic device discovery and inventory

- DNS and traffic pattern monitoring
- One-click domain blacklisting for known-bad destinations

DNS Sinkholing & Host-Level Enforcement

Problem: Detecting a malicious domain doesn't stop a device from actually reaching it — an alert alone leaves the connection open until a person manually intervenes.

Solution: CUDP actively blocks malicious domains at the DNS level, per-endpoint or fleet-wide, automatically syncing from live Threat Intel feeds. Per-endpoint enforcement status is tracked so you can confirm coverage across the fleet at a glance.

Benefit: Known-bad destinations are blocked outright, not just flagged — real containment instead of detection alone.

- Automatic sync of blocklists from Threat Intel feeds
- Per-endpoint and fleet-wide enforcement
- Per-endpoint enforcement status tracking

Multi-Factor Authentication (MFA)

Problem: Stolen or weak passwords remain one of the most common ways attackers gain initial access to a network.

Solution: CUDP includes built-in Time-based One-Time Password (TOTP) multi-factor authentication for dashboard access, compatible with standard authenticator apps.

Benefit: Even if a password is compromised, unauthorized access to the security dashboard itself is blocked.

Executive Dashboard & Reporting

Problem: Security data is only useful if the people making decisions can actually understand it — most SIEM tools are built for analysts, not decision-makers.

Solution: CUDP's Executive Dashboard translates raw security data into a clear security score, trend charts, and a weekly summary report.

Benefit: Leadership and non-technical stakeholders can see, at a glance, whether the organization's security posture is improving or declining.

- Weekly automated Executive Report
- At-a-glance organizational Security Score

Simple Deployment & Automatic Updates

Problem: Security tools that are difficult to deploy or maintain often end up out of date, which defeats the purpose of having them.

Solution: CUDP endpoints are deployed with a single branded install command generated from the dashboard, and agents self-update automatically — no manual reinstalls, no per-machine maintenance visits.

Benefit: Lower ongoing administrative burden, and confidence that every endpoint is always running the latest protection.

- One-click "Deploy Agent Link" generation for new endpoints
- Fully automated agent self-update pipeline

Part 2 — A Closer Look: Selected Detailed Capabilities

Part 1 covered CUDP's capabilities at a high level. The features below are a closer look at some of the specific tools inside the platform that give day-to-day, hands-on control over detection and response.

File Scanner (Endpoint Security Scan)

The File Scanner lets you request an on-demand, in-depth analysis of any file on any protected endpoint — Windows or Linux — directly from the dashboard, without needing physical or remote-desktop access to the machine.

- **Remote retrieval** — Files are pulled securely through the endpoint's own agent connection, so no administrative network shares or stored credentials are required.
- **Hash & signature analysis** — Every scanned file is hashed (MD5/SHA-256) and checked against known-malicious hash lists and file-type signatures.
- **Ransomware behavioral classification** — Files are evaluated for ransomware-like characteristics, not just matched against a static blacklist.
- **DLP content inspection** — File contents are checked for sensitive data patterns (e.g., SSNs, credentials) as part of the same scan.
- **Linux path resolution** — Handles symbolic links, Snap package paths, and PATH-based executables so Linux scans resolve the real file being analyzed, not a broken shortcut.
- **Graceful fallback** — If a full file can't be retrieved, the scanner still returns path, size, and metadata rather than failing silently.

Watchlist

The Watchlist is a running list of specific indicators your organization wants CUDP to actively track across every endpoint. Any activity matching a Watchlist entry generates an alert, even if it wouldn't otherwise trigger one.

- **Hash** — Track a specific file by its cryptographic hash — useful for a known-bad file identified during an investigation.
- **URL / Domain** — Track a specific website or domain (e.g., a phishing site reported by an employee).
- **IP** — Track a specific IP address, such as one associated with a prior incident.
- **Process Name** — Track a specific running process name across all endpoints.

Each Watchlist entry can be added directly from an existing alert with a single click, turning a one-time detection into ongoing, fleet-wide monitoring.

Threat Lookup

Threat Lookup is an on-demand research tool built into the dashboard: enter a hash, IP address, or domain and instantly check it against live threat intelligence sources — no need to leave CUDP or use a separate external tool. This is useful for quickly validating whether something unfamiliar showing up in logs is actually a known threat before deciding how to respond.

Network Tools

The LAN Monitor includes a set of hands-on tools for investigating and controlling network activity:

- **Device Discovery & Inventory** — Automatically identifies every device on the network, including manufacturer identification, so unknown or unauthorized devices stand out.

- **DNS & Traffic Monitoring** — Tracks DNS lookups and traffic patterns per device to spot unusual destinations or volume.
- **Block Domain** — Blacklist a malicious or unwanted domain directly from an alert or investigation, network-wide.
- **Investigate IP** — Pivot directly from any flagged connection into a deeper investigation of that IP's activity across the network.

Available Reports

- **Weekly Executive Report** — An automated, plain-language summary of security posture, alerts, and trends delivered on a recurring schedule — built for leadership, not analysts.
- **Executive Dashboard Trend Charts** — Historical alert volume and security score trending, viewable at any time.
- **Alert & Incident Detail Export** — Full detail on any individual alert — timestamps, endpoint, evidence, and actions taken — available for compliance or audit documentation.

Why Cyber Unified Defense Platform

- Enterprise-grade EDR, FIM, DLP, and Threat Intelligence in one platform — no need to license and integrate five separate tools
- Self-hosted — your security data stays on your own infrastructure, not a third-party cloud
- Built specifically for organizations with 5–15 endpoints, priced and scaled accordingly
- Simple deployment and automatic updates minimize ongoing IT overhead
- Clear, executive-level reporting so security posture is understandable to non-technical stakeholders

Next Steps

Cyber Unified Defense Platform is available for a 30-day evaluation trial with full platform access. For a more detailed understanding of the full capabilities of Cyber Unified Defense Platform, we recommend taking the 30-day trial into your own environment to see its benefits firsthand. For questions or to begin a trial, contact DADavisDesigns: Cyber Defenders at support@dadavisdesignsllc.com.