PRODUCT DATASHEET · 2026

CodeRed Server Agent

AGENT SOFTWARE v1.0.0

Modular Endpoint Monitoring & Security Agent

CodeRed Server Agent puts a light, modular sensor on every host. It collects system and application logs, watches critical files for tampering, inventories what is installed and running, hunts for rootkits and brute force, maps packages to CVEs, and audits the box against CIS benchmarks, then reports it all back to your CodeRed Manager.

One interactive CLI drives everything. An operator scans the host, picks the logs worth watching, and toggles the modules the environment needs. The agent restarts itself, and you edit no config files by hand, on Linux, macOS or Windows.

⬡ 7 Modules · Linux · macOS · Windows · CLI-Managed

Configured in minutes

A guided console scans the endpoint, recommends the logs and modules that matter, and applies the change. The operator never touches raw XML.

One agent, three platforms

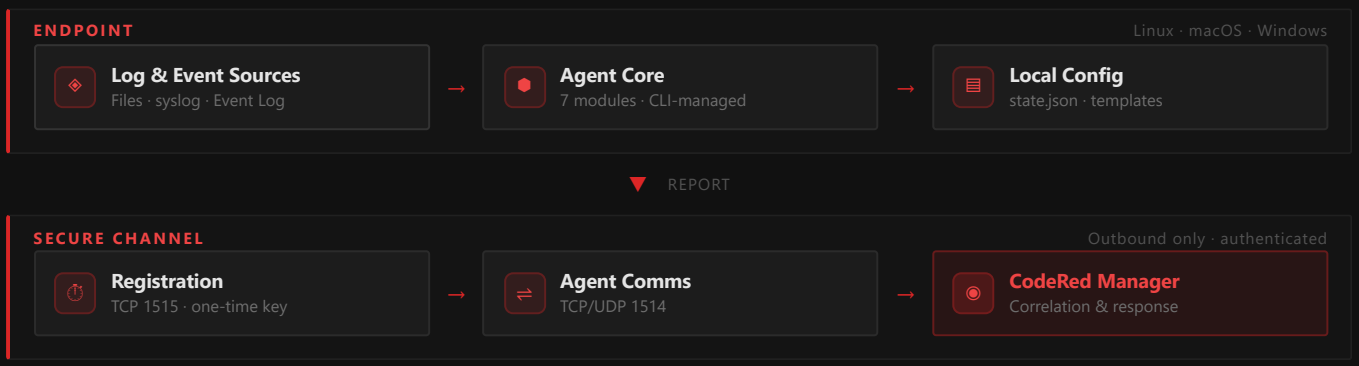
Separate, platform-native builds for Linux, macOS and Windows share one CLI and one module model, so operations look the same everywhere.

PLATFORM OVERVIEW

Endpoint Telemetry, Reported to Your Manager

Each agent runs seven independent modules and streams the results over an authenticated channel to the CodeRed Manager, where they are correlated with the rest of your estate. The agent is installed with a single command and managed entirely from its own console.

System Architecture



Capabilities

log-collection	System, application and security log collection
fim	File integrity monitoring with SHA-256 checksums
inventory	Hardware, OS, packages, processes, open ports
threat	Rootkit scanning, brute force, MITRE ATT&CK
vuln	CVE mapping for installed packages (NVD feed)
compliance	CIS Benchmark and custom SCA policy checks
active-response	Auto-block IPs, kill processes, quarantine files

Deployment Model

ONE-COMMAND INSTALL

A single bootstrap detects the platform, installs the matching build, sets the manager address, normalises log formats and starts the service. macOS auto-selects the Apple Silicon or Intel package.

OUTBOUND ONLY

The agent opens no listening port. It connects out to the manager on TCP 1514/1515 and reuses its registration key on every restart.

PLATFORM-NATIVE BUILDS

Linux, macOS and Windows each get their own scripts and templates, so every OS uses the correct log formats, paths and service model. The builds are not interchangeable.

MODULES

Seven Modules, Enabled On Demand

Each module runs on its own. Turn on only what a host needs: a web server calls for different coverage than a domain controller. Toggle the rest from the console as the role of the box changes, and the agent applies each change and restarts itself.

Required

Log Collection

codered-agent enable log-collection

Collects logs from system files and application sources. Use the scan wizard to manage which paths are included.

Optional

Vulnerability Detection

codered-agent enable vuln

Maps installed packages against the NVD CVE database. Supports apt, yum, dnf and Windows Update.

Recommended

File Integrity Monitoring

codered-agent enable fim

Watches /etc, /bin, /sbin for unauthorised change using SHA-256 checksums, flagging create, modify and delete events.

Optional

Compliance & Auditing

codered-agent enable compliance

Runs CIS Benchmark SCA checks; custom YAML policies drop into /etc/codered/sca/.

Recommended

System Inventory

codered-agent enable inventory

Snapshots installed packages, running processes, open ports and network interfaces every hour.

Optional

Active Response

codered-agent enable active-response

Executes firewall drops and process kills on alert. Blocked IPs auto-unblock after 5 minutes by default.

Recommended

Threat Detection

codered-agent enable threat

Rootkit and hidden-process scanning, plus rules for SSH/web brute force, ATT&CK techniques and privilege escalation.

> *Enable Active Response last.*
>
> Test its rules in your environment before switching it on. A misconfigured response can block legitimate traffic, including your own management connections.

Recommended Modules by Environment

ENVIRONMENT	RECOMMENDED MODULES
General server	Log Collection, FIM, Inventory, Threat Detection
Web server	The above + Vulnerability Detection
PCI / compliance	The above + Compliance & Auditing
High-security / SOC	All modules, including Active Response

LOG DISCOVERY

The Agent Finds the Logs Worth Watching

The discovery engine detects the OS, enumerates running services and installed packages, then scores every log source by security relevance. High and Medium sources are pre-selected; the operator confirms, and selections are written straight into the agent config.

Service Detection → Log Source Scan → Priority Scoring → Config Injection → Auto-Restart

Linux queries systemctl and dpkg/rpm and checks 28+ known paths under /var/log. Windows queries sc and wmic and verifies 12 Event Log channels via wevtutil, plus IIS logs under C:\inetpub.

Linux Log Catalogue

PATH	PRIORITY
/var/log/auth.log	High
/var/log/secure	High
/var/log/syslog	High
/var/log/kern.log	High
/var/log/audit/audit.log	High
/var/log/ufw.log	High
nginx / apache access	Medium
mysql / postgresql / mongodb	Medium
fail2ban · dpkg · cron	Medium
/var/log/mail.log	Low

Windows Event Channels

CHANNEL	PRIORITY
Security	High
System	High
PowerShell/Operational	High
Sysmon/Operational	High
Windows Defender/Operational	High
TerminalServices (RDP)	High
Firewall/Operational	High
Application	Medium
TaskScheduler · WMI · DNSClient	Medium
Bits-Client · IIS logs	Medium

— *Re-scan whenever the host changes.*

Install a new database or web server and re-run the scan, and the agent replaces the previous discovery config with your new selection. On Windows, install Sysmon first to unlock the highest-fidelity process, network and registry telemetry.

MANAGEMENT & SPECIFICATIONS

One Console. Every Platform.

Interactive Console

Run codered-agent with no arguments

1 · Scan Log Directories	Discover logs and choose what to monitor
2 · Module Setup	Enable / disable monitoring modules
3 · Agent Status	Service status and active modules
4 · Agent Settings	Set manager IP, test connection, restart
5 · Uninstall Agent	Fully remove the agent from the host

Direct Subcommands

For scripting and automation, no menu:

`scan` `setup` `status` `settings` `restart`

`enable <module>` `disable <module>` `uninstall`

Manager Connectivity

Agent comms	TCP/UDP 1514 (outbound to manager)
Registration	TCP 1515 (outbound, one-time enrolment)
Direction	Outbound only, no inbound listener

Platform Requirements

Linux	Ubuntu 20.04+, Debian 11+, RHEL/CentOS 8+, Fedora, Oracle 7/8/9; Python 3.6+; root
Windows	Server 2016+ / Windows 10+; PowerShell 5.0+; Python 3.6+ (auto-installed); Administrator
macOS	Monterey 12+; Apple Silicon or Intel (auto-detected); Python 3.6+; root
Manager	Reachable CodeRed Manager on TCP 1514/1515

Install Targets

Linux / macOS CLI	/usr/local/bin/codered-agent
Windows CLI	C:\Program Files\CodeRed\Agent\
Config (Linux/macOS)	/etc/codered/ · agent config under ossec
Module templates	Per-OS: linux / macos / windows

SAFE INSTALLATION

Installers download over TLS and run locally instead of piping to a shell, so interactive prompts and antivirus behave. On Linux and macOS you set the manager IP on the install line; on Windows you download the script first, then run it.

Coverage on Every Host, Set Up in Minutes.

One command to install, one console to run it. Roll the agent out across Linux, macOS and Windows and report it all to a single manager.

Get In Touch

Email
business@coderedcyber.ai

Website
https://coderedcyber.ai

Provintell Technologies Sdn. Bhd.
Powered by CodeRed Cyber

See It Running

Deploy the agent on a test host and watch logs, integrity events and threat detections flow into your manager within minutes of enrolment.

BOOK A TECHNICAL WALKTHROUGH
https://coderedcyber.ai

Deploys Alongside

The Server Agent is one component of the CodeRed platform. Its endpoint telemetry joins the same picture built from network and log sources.

CodeRed AI Log Manager

Universal log acquisition and SIEM forwarding, with AI-generated connectors for any source. Covered in its own datasheet.

CodeRed NDR Sensor

Passive network detection and response across ~75 ATT&CK techniques. Covered in its own datasheet.

Why Teams Choose It

- ✓ Seven modules, enabled per host
- ✓ Linux, macOS and Windows from one CLI
- ✓ Guided log discovery, no XML by hand
- ✓ Outbound-only, key-based enrolment
- ✓ Reports into the CodeRed platform