CYBERTECTION LLC

Training Center

GuardBot AI Security Suite

Comprehensive User & Training Guide

Beginner to Advanced | CYB 100

2026 Edition

Platforms: Windows | macOS | iOS | Android | Linux

cybertection.net

support@cybertection-guardbot.com | (410) 701-2931

Table of Contents

Module 1: Introduction to GuardBot AI Security

Welcome to the official Cybertection GuardBot AI Security Suite training guide. This document serves as both a comprehensive user manual and a training curriculum for students at the Cybertection Training Center. Whether you are a new user setting up GuardBot for the first time or a cybersecurity trainee learning how AI-powered security tools work under the hood, this guide will take you from beginner fundamentals to advanced configuration and threat analysis.

1.1 What is GuardBot?

GuardBot is an AI-powered cybersecurity platform developed by Cybertection LLC that provides comprehensive digital protection across every major operating system. Unlike traditional antivirus software that relies solely on signature-based detection, GuardBot combines artificial intelligence, behavioral analysis, real-time monitoring, and VPN encryption into a single unified security suite.

GuardBot is not a black-box solution that hides its activity behind a progress bar. It is designed as an interactive Security Command Center that gives users full transparency into what is happening on their system. Every scan, every detection, every network connection is logged and visible in the live info console, giving you the knowledge and control that traditional antivirus products withhold.

Core Capabilities

- AI-Driven Antivirus Engine: Uses machine learning models trained on millions of malware samples to identify and block threats in real-time, including zero-day malware that has never been seen before.
- Secure Global VPN (WebGuard): Built on the WireGuard protocol, providing military-grade encryption for all internet traffic. Masks your IP address and protects your data on any network.
- Deepfake Detection Scanner: AI-powered image and video analysis that identifies manipulated media, protecting against deepfake fraud and misinformation.
- Real-Time Threat Monitoring: Continuous background scanning that watches for suspicious process behavior, unauthorized network connections, and file system anomalies.
- Ransomware Protection: Behavioral detection that identifies encryption activity and file-locking patterns characteristic of ransomware attacks, stopping them before damage occurs.
- Network Honeypot: Deploys decoy services that attract and identify network-based attacks, providing early warning of intrusion attempts.
- Wireless Network Analysis: Scans and evaluates the security of Wi-Fi networks, identifying vulnerabilities and unauthorized devices.
- Password Manager and Breach Monitor: Secure password storage with dark web monitoring to alert you if your credentials appear in data breaches.
- File Encryption: Military-grade encryption for sensitive files and folders, protecting data even if your device is compromised or stolen.

1.2 Platform Availability

GuardBot is available on every major platform, providing consistent protection regardless of which devices you use:

Platform	App Name	Distribution	Key Features
Windows	GuardBot AI Security	Microsoft Store, Direct Download	Full suite: AV, VPN, AI scans, firewall
macOS	GuardBot Security	Apple App Store	Full suite: AV, VPN, deepfake scan
iOS	GuardBot Security	Apple App Store	VPN, deepfake scan, network tools
Android	GuardBot AI Security	Google Play Store	Full suite: AV, VPN, AI scans, tools
Linux	Cybertection GuardBot	Snapcraft	VPN, AV, firewall, real-time monitor
Fire OS	GuardBot Security	Amazon Appstore	AV, VPN, security tools

> **Note:** *iOS and macOS share the same codebase (Universal Purchase). Buying on one Apple platform gives you access on both.*

1.3 Subscription Tiers

GuardBot offers three subscription tiers designed to provide security at every budget level:

Free Tier

The free tier gives every user access to basic security tools at no cost. This includes URL safety checking, basic system information, and limited security assessments. The free tier is designed to let you experience GuardBot before committing to a subscription.

Basic Security

The Basic Security tier unlocks the core protection suite including AI-driven malware scanning, deepfake detection, full system scans, and the complete tools menu. Basic Security is ideal for users who want comprehensive threat detection without VPN services.

- Monthly: $4.99/month
- Yearly: $52.99/year (save over 10%)

Premium Security (Full Protection)

Premium Security includes everything in Basic plus the WebGuard VPN with global server access, priority support, and all advanced features. This is the complete GuardBot experience with no limitations.

- Monthly: $12.99/month
- Yearly: $150.00/year
- Free Trial: 7-day free trial available for new users

Subscriptions can be purchased through the Apple App Store (iOS/macOS), Google Play Store (Android), or the Cybertection website (cybertection.net) for Windows and Linux. All subscriptions sync across platforms through your Cybertection account via Firebase authentication.

1.4 What Makes GuardBot Different

The cybersecurity market is crowded with products from Norton, Bitdefender, Malwarebytes, and others. GuardBot differentiates itself in several important ways:

Full Transparency

Traditional antivirus products hide their operations behind simple progress bars and status icons. GuardBot provides a live information log that shows exactly what the engine is doing in real-time. Every file scanned, every threat detected, every network connection analyzed is visible to you. This transparency is not just a feature; it is a philosophy. We believe users have the right to understand what their security software is doing.

Interactive Security Command Center

GuardBot is not a passive shield. It is designed as an interactive command center where you control every aspect of your security. You choose which scans to run, which shields to enable, which folders to monitor, and which network connections to allow. Advanced users can customize every parameter while beginners can rely on intelligent defaults.

AI Behavioral Analysis

While competitors rely primarily on signature databases (known malware fingerprints), GuardBot's AI engine analyzes behavior. It takes a baseline of your normal system activity and watches for deviations. When Microsoft Word suddenly tries to launch PowerShell, or an unknown process begins encrypting files, or a program allocates executable memory, GuardBot's AI recognizes these as threat indicators and responds immediately, even if the specific malware has never been seen before.

Cross-Platform Consistency

Most security companies offer different products for different platforms with inconsistent features and interfaces. GuardBot provides a unified experience across Windows, macOS, iOS, Android, and Linux. Your subscription works everywhere, your settings sync across devices, and the cyberpunk-themed interface is recognizable on every platform.

Built by Security Professionals

Cybertection LLC is a cybersecurity company first, not a marketing company that happens to sell security software. GuardBot is built by people who understand threats, network security, and malware analysis at a deep technical level. The same team that builds GuardBot also runs the Cybertection Training Center, teaching the next generation of cybersecurity professionals.

Module 2: Installation and Setup

This module walks you through downloading, installing, and configuring GuardBot on every supported platform. By the end of this module, you will have GuardBot running with optimal settings on all your devices.

2.1 Creating Your Cybertection Account

Before installing GuardBot on any device, you need a Cybertection account. This account syncs your subscription, settings, and device registrations across all platforms.

1. Visit cybertection-guardbot.com or open the GuardBot app on any platform.
2. Click Sign Up or Create Account.
3. Enter your email address and create a strong password (minimum 12 characters recommended).
4. Verify your email address by clicking the link sent to your inbox.
5. Complete your profile setup.

> **Note:** *Your Cybertection account supports up to 6 devices simultaneously. You can manage your registered devices from the app settings on any platform.*

2.2 Windows Installation

Microsoft Store Installation (Recommended)

6. Open the Microsoft Store on your Windows PC.
7. Search for "Cybertection GuardBot AI Security" or visit the direct link from cybertection-guardbot.com/windows.
8. Click Get/Install to download and install the application.
9. Launch GuardBot from your Start menu or desktop shortcut.
10. Sign in with your Cybertection account credentials.
11. The dashboard will appear showing your security status and available features.

Direct Download Installation

12. Visit cybertection-guardbot.com/windows and click the Download button.
13. Run the downloaded installer (.exe file). Windows SmartScreen may display a warning; click "More info" then "Run anyway" as the application is code-signed by Cybertection LLC.
14. Follow the installation wizard prompts.
15. Launch GuardBot and sign in with your account.

Windows System Requirements

- Operating System: Windows 10 version 1903 or later, Windows 11
- Processor: 1 GHz or faster, 64-bit compatible
- RAM: 4 GB minimum (8 GB recommended)
- Storage: 500 MB available disk space

- Network: Internet connection required for updates and VPN

2.3 macOS Installation

16. Open the Mac App Store.
17. Search for "GuardBot Security" by Cybertection LLC.
18. Click Get/Install. You may need to authenticate with your Apple ID.
19. Once installed, open GuardBot from your Applications folder or Launchpad.
20. Sign in with your Cybertection account.
21. Grant necessary permissions when prompted (Network Extensions for VPN, Notifications).

> **Tip:** *If you purchased GuardBot on iOS, you already own it on macOS through Apple's Universal Purchase. Just download it from the Mac App Store at no additional cost.*

2.4 iOS Installation

22. Open the App Store on your iPhone or iPad.
23. Search for "GuardBot Security" by Cybertection LLC.
24. Tap Get/Install and authenticate with Face ID, Touch ID, or your Apple ID password.
25. Open GuardBot and sign in with your Cybertection account.
26. When prompted, allow VPN configuration (required for WebGuard VPN).
27. Enable notifications to receive real-time threat alerts.

2.5 Android Installation

28. Open the Google Play Store.
29. Search for "Cybertection GuardBot AI Security" or scan the QR code from cybertection.net.
30. Tap Install and wait for the download to complete.
31. Open GuardBot and sign in with your Cybertection account.
32. Grant requested permissions (storage access for scanning, network access for VPN, notification access for alerts).
33. The dashboard will display your security status.

2.6 Linux Installation

GuardBot for Linux is distributed via Snapcraft, making it available on Ubuntu, Debian, Fedora, Arch, and many other distributions.

```
sudo snap install cybertection-guardbot
```

After installation, launch GuardBot from your application menu or terminal:

```
cybertection-guardbot
```

Sign in with your Cybertection account and the cyberpunk GUI will appear with all available security modules.

2.7 Initial Configuration

After installing GuardBot on any platform, complete these initial configuration steps for optimal protection:

34. Update Threat Definitions: GuardBot will automatically download the latest threat intelligence database on first launch. Allow this process to complete before running your first scan.
35. Run a Full System Scan: Perform a comprehensive scan to establish a security baseline for your device. This first scan may take 30-60 minutes depending on your system.
36. Enable Real-Time Protection: Turn on real-time monitoring to protect high-risk folders like Downloads and Desktop. GuardBot will scan new files the instant they appear.
37. Enable GuardBot AI: Activate the AI behavioral analysis engine. It will take a baseline snapshot of your normal system activity and begin monitoring for anomalies.
38. Configure VPN (Premium): If you have a Premium subscription, connect to the VPN and select your preferred server location.
39. Set Up Notifications: Configure alert preferences for threat detection, scan completion, and VPN connection status.

Module 3: The GuardBot Dashboard

The GuardBot dashboard is your Security Command Center. It provides at-a-glance status of all protection modules and quick access to every feature. This module explains every element of the dashboard and how to interpret the information presented.

3.1 Dashboard Layout

The dashboard is organized into logical sections for clarity and rapid access. Understanding the layout helps you navigate GuardBot efficiently and respond to threats quickly.

Security Status Indicator

The main status indicator at the top of the dashboard shows your overall protection level using a color-coded system:

- Green (Protected): All enabled security modules are active and functioning correctly. Threat definitions are up to date. No threats detected.
- Yellow (Warning): One or more security modules are disabled or require attention. This could indicate outdated threat definitions, a pending scan, or a module that needs re-enabling.
- Red (At Risk): Critical protection is disabled or a threat has been detected that requires immediate action. Take action immediately by reviewing the alert details and following recommended steps.

Main Action Panels

The top sections of the dashboard contain the primary scanning and protection controls. Each panel represents a major feature category:

- Scan Center: Access to Quick Scan, Full Scan, Custom Scan, and Scheduled Scan options.
- Real-Time Shields: Controls for enabling and disabling real-time protection modules including GuardBot AI, Ransomware Protection, and Network Honeypot.
- WebGuard VPN: VPN connection controls, server selection, and connection status (Premium only).
- Tools: Additional security utilities including Deepfake Scanner, URL Checker, Network Analyzer, Password Manager, and File Encryption.

Live Info Log

The text console at the bottom of the dashboard is a live feed of the antivirus engine’s activities. It provides transparent, real-time updates about scans, threat intelligence updates, network monitoring events, and other background tasks. This is what makes GuardBot unique—you can see exactly what your security software is doing at every moment.

Log entries are color-coded by severity: white for informational messages, yellow for warnings, and red for threat detections. You can filter, search, and export log data for analysis.

3.2 Scan Center

The Scan Center provides multiple scanning options to match different use cases and time constraints:

Quick Scan

A rapid scan that checks the most common threat locations: running processes, startup items, browser extensions, temporary files, and recently downloaded files. Quick Scans typically complete in 2-5 minutes and are ideal for daily use.

Full System Scan

The most thorough scanning option. A Full System Scan meticulously checks every single file on all connected drives. This includes system files, application files, user documents, hidden files, and archived content. Full Scans may take 30-90 minutes depending on the number of files and system speed. Recommended weekly.

Custom Scan

Allows you to select specific files, folders, or drives to scan. Useful when you want to check a specific download, USB drive, or folder without scanning the entire system.

Scheduled Scan

Configure automatic scans that run at specified times without manual intervention. You can schedule Quick Scans daily and Full Scans weekly. Scheduled scans run in the background and notify you of results when complete.

3.3 Remediation Center

When GuardBot detects a threat, it is logged in the Remediation Center. This is your threat management hub where you can review detected threats, take action (quarantine, delete, or whitelist), view threat details, and track remediation history.

Each detected threat displays the file name and path, threat type and severity rating, detection method (signature, AI behavioral, heuristic), recommended action, and detailed analysis explaining why the file was flagged. You always have the final say in how each threat is handled. GuardBot provides recommendations but never takes irreversible action without your confirmation.

Module 4: GuardBot AI Threat Intelligence Engine

This module takes a deep dive into the technology that powers GuardBot's AI-driven threat detection. Understanding how the AI engine works will help you configure it optimally and interpret its findings accurately. This is where Cybertection truly enters the next generation of security.

4.1 How the AI Engine Works

The GuardBot AI engine is not just scanning files; it is scanning behavior. Traditional antivirus relies on signature databases—lists of known malware fingerprints. If a piece of malware is not in the database, it passes undetected. GuardBot's AI takes a fundamentally different approach.

When you enable the AI engine, it takes a baseline snapshot of your normal system activity. From then on, it actively watches for deviations from that baseline. This behavioral approach catches threats that do not have a file to scan, including fileless malware, living-off-the-land attacks, and zero-day exploits.

What the AI Monitors

- Suspicious Process Chains: Is a trusted program like Microsoft Word suddenly trying to open PowerShell or the Command Prompt? The AI knows this is a classic tactic for fileless malware and will alert you immediately.
- Anomalous Memory Allocation: The AI watches for programs trying to allocate memory with executable permissions, a key indicator of an attempt to inject malicious code directly into your system's RAM.
- Unusual Network Patterns: The AI learns which applications normally access the network, what servers they connect to, and how much data they transfer. When an application suddenly begins communicating with an unknown server or transferring unusual amounts of data, the AI flags it for review.
- File System Behavior: The AI monitors file creation, modification, and deletion patterns. Rapid encryption of files (ransomware behavior), mass file deletion, or unauthorized modification of system files triggers immediate alerts.
- Registry and Configuration Changes: On Windows, the AI watches for unauthorized modifications to the system registry, startup entries, and critical configuration files that could indicate persistence mechanisms.
- Privilege Escalation Attempts: The AI detects when processes attempt to gain elevated permissions beyond what they should normally require.

4.2 Enabling and Configuring the AI

40. Navigate to the GuardBot AI panel in the dashboard.
41. Click the Enable AI button. The status label will turn green and read "AI Status: Enabled."
42. The AI will spend 5-15 minutes building a baseline of your normal system activity. During this time, use your computer normally so the baseline accurately reflects your typical usage patterns.
43. Once the baseline is established, the AI begins active monitoring.

> **Tip:** *Build your baseline during a normal work session. If you enable the AI during unusual activity (like running a system update), the baseline may not accurately represent your typical usage.*

AI Sensitivity Levels

GuardBot's AI engine supports configurable sensitivity levels to balance detection accuracy with false positive rates:

- Low Sensitivity: Only alerts on high-confidence detections. Fewer false positives but may miss subtle threats. Recommended for servers and production environments.
- Medium Sensitivity (Default): Balanced detection that catches most threats with a manageable false positive rate. Recommended for most users.
- High Sensitivity: Maximum detection capability. Will catch the subtlest anomalies but may generate more false positives. Recommended for high-security environments and security professionals.

4.3 Machine Learning Models

GuardBot uses multiple machine learning models working in parallel, each specialized for different types of threat detection:

Static Analysis Model

This model analyzes file characteristics without executing them. It examines file structure, entropy levels, embedded strings, import tables, and other static attributes to determine the likelihood that a file is malicious. The model was trained on millions of known malware and benign samples and achieves over 95% accuracy on previously unseen files.

Dynamic Behavioral Model

The behavioral model monitors running processes and their actions in real-time. It builds a graph of process relationships, API calls, and system interactions to identify malicious behavior patterns. This model is particularly effective against fileless malware, polymorphic threats, and zero-day exploits that evade signature-based detection.

Network Anomaly Model

This model analyzes network traffic patterns to identify command-and-control (C2) communications, data exfiltration attempts, and other malicious network activity. It uses unsupervised learning to establish baseline network behavior and detects deviations that indicate compromise.

Model Updates

GuardBot's AI models are updated regularly through Firebase Remote Config, allowing model improvements to be deployed without requiring app updates. When new threat patterns emerge, Cybertection's security team retrains the models and pushes updates to all GuardBot installations automatically.

4.4 VirusTotal Integration

For advanced users, GuardBot supports integration with VirusTotal, a service that aggregates results from over 70 antivirus engines. When you provide your own VirusTotal API key,

GuardBot can submit suspicious files for multi-engine analysis, providing an additional layer of verification.

To configure VirusTotal integration, navigate to Settings, enter your VirusTotal API key (free keys available at virustotal.com), and enable the integration. Suspicious files will be automatically submitted for cross-referencing against 70+ antivirus engines.

> **Important:** *VirusTotal is a cloud service. Files submitted to VirusTotal may be shared with the security community. Do not submit files containing sensitive personal or business data.*

Module 5: WebGuard VPN

The WebGuard VPN is GuardBot's built-in virtual private network service, providing encrypted internet connectivity and IP address privacy. This module covers VPN technology, the WireGuard protocol, server selection, and advanced VPN configuration.

5.1 What is a VPN?

A Virtual Private Network (VPN) creates an encrypted tunnel between your device and a VPN server. All your internet traffic passes through this tunnel, making it unreadable to anyone who might intercept it—including your internet service provider (ISP), hackers on public Wi-Fi, and government surveillance.

When you connect to the VPN, your real IP address is hidden and replaced with the IP address of the VPN server. This provides anonymity online and prevents websites, advertisers, and other third parties from tracking your real location and identity.

5.2 WireGuard Protocol

GuardBot's VPN is built on WireGuard, a modern VPN protocol that represents a significant advancement over older protocols like OpenVPN and IPSec:

- Speed: WireGuard's lightweight codebase (approximately 4,000 lines of code compared to OpenVPN's 100,000+) provides significantly faster connection speeds and lower latency.
- Security: Uses state-of-the-art cryptography including Curve25519 for key exchange, ChaCha20 for encryption, Poly1305 for authentication, and BLAKE2s for hashing.
- Simplicity: The small codebase is easier to audit for security vulnerabilities, reducing the attack surface compared to larger, more complex VPN protocols.
- Battery Efficiency: WireGuard's efficient design uses less CPU and battery power, making it ideal for mobile devices.
- Roaming: Seamlessly handles network transitions (e.g., switching from Wi-Fi to cellular) without dropping the VPN connection.

5.3 Connecting to the VPN

44. Open GuardBot and navigate to the WebGuard VPN panel.
45. Select a server location from the available options. GuardBot automatically suggests the fastest server based on your location.
46. Tap or click the Connect button. The VPN will establish a secure tunnel within seconds.
47. The VPN status indicator will turn green, showing your new IP address and the connected server location.
48. All internet traffic is now encrypted and routed through the VPN server.

To disconnect, simply tap or click the Disconnect button. Your internet traffic will return to its normal, unencrypted path.

5.4 Server Infrastructure

Cybertection operates VPN servers on Google Cloud Platform infrastructure, providing reliable, high-speed connectivity with enterprise-grade security:

- Geographic Distribution: Servers are deployed across multiple regions to provide fast connections regardless of your location.
- No-Log Policy: Cybertection does not log your VPN activity, browsing history, or connection timestamps. Your privacy is absolute.
- Dedicated IP Addresses: Each VPN server has dedicated IP addresses that are not shared with other services, reducing the risk of IP blacklisting.
- Auto-Provisioning: When you connect to the VPN, your WireGuard configuration is automatically provisioned through our secure Peer API. No manual configuration is required.
- Platform-Specific Interfaces: Each platform (Windows, macOS, iOS, Android, Linux) connects to dedicated WireGuard interfaces on the server, ensuring optimized performance and isolation.

5.5 Advanced VPN Features

Kill Switch

The Kill Switch is a critical privacy feature that blocks all internet traffic if the VPN connection drops unexpectedly. This prevents your real IP address from being exposed during brief disconnections. Enable the Kill Switch in VPN Settings for maximum privacy protection.

Split Tunneling

Split tunneling allows you to choose which applications use the VPN and which connect directly to the internet. This is useful for applications that require your real IP address (like banking apps) or for reducing VPN bandwidth usage while still protecting sensitive traffic.

DNS Leak Protection

DNS leaks can expose your browsing activity even when connected to a VPN. GuardBot automatically routes DNS queries through the VPN tunnel and uses secure DNS servers to prevent leakage. The DNS Leak Protection feature is enabled by default and should remain active for optimal privacy.

> **Note:** *The WebGuard VPN requires a Premium subscription. Basic and Free tier users can upgrade at any time through the app or cybertection.net/pricing-plans/list.*

Module 6: Real-Time Protection Shields

GuardBot's real-time shields provide continuous, proactive protection without requiring manual scans. Each shield monitors a specific aspect of your system's security and can be independently enabled or disabled. This module explains each shield, how it works, and when to use it.

6.1 Accessing Real-Time Shields

To access the shields, navigate to the Tools menu in GuardBot and tap Real-Time Monitor Shields. You will see a menu of available shields, each with its own detail page and enable/disable toggle. When a shield is enabled, it integrates into GuardBot's scanning engine and runs continuously in the background.

6.2 GuardBot AI Shield

The GuardBot AI Shield is the primary real-time protection module. When enabled, it provides continuous behavioral monitoring of all system activity using the AI engine described in Module 4.

What It Does

- Monitors all running processes for suspicious behavior patterns.
- Detects fileless malware that operates entirely in memory without creating files on disk.
- Identifies suspicious process chains (e.g., Office documents launching command shells).
- Watches for anomalous memory allocation patterns indicative of code injection.
- Analyzes network traffic for communication with known malicious servers.
- Provides real-time alerts with detailed explanations of detected anomalies.

When to Enable

The AI Shield should be enabled at all times for maximum protection. The only reason to disable it temporarily would be during resource-intensive tasks like video rendering or gaming, as the behavioral monitoring uses some system resources.

6.3 Ransomware Protection Shield

Ransomware is one of the most devastating cyber threats, encrypting your files and demanding payment for the decryption key. GuardBot's Ransomware Protection Shield specifically targets this threat category.

What It Does

- Monitors the filesystem for rapid encryption activity—the hallmark of ransomware in action.
- Watches for mass file renaming with new extensions (e.g., .encrypted, .locked, .ransom).
- Detects processes attempting to access and modify large numbers of files in rapid succession.
- Monitors for deletion of Volume Shadow Copies (a common ransomware tactic to prevent recovery).

- Identifies known ransomware signatures and behavioral patterns.
- Automatically blocks suspicious encryption activity and quarantines the responsible process.

When to Enable

Ransomware Protection should always be enabled. It operates with minimal system overhead and provides critical protection against one of the most common and destructive threat types.

> **Important:** *If you are a developer or IT professional who regularly works with encryption tools, file archivers, or batch file operations, you may need to whitelist your legitimate tools to prevent false positives.*

6.4 Network Honeypot

A honeypot is a decoy system designed to attract and identify attackers. GuardBot's Network Honeypot deploys virtual decoy services that appear to be legitimate but are actually traps that detect network-based attacks.

What It Does

- Creates virtual network services that mimic common targets (file shares, web servers, database ports).
- Monitors for connection attempts to these decoy services, which indicate scanning or attack activity.
- Logs the source IP, techniques used, and timing of attack attempts.
- Generates alerts when suspicious network activity is directed at your system.
- Provides early warning of network intrusion attempts before attackers reach real services.

When to Enable

Enable the Network Honeypot when connected to networks you do not fully trust, such as public Wi-Fi, shared networks, or when you suspect your network may be compromised. On your home network, it provides an additional layer of detection that complements your router's firewall.

6.5 Real-Time File Monitor

The Real-Time File Monitor watches a specified folder and all its subfolders for any new or modified files and scans them the instant they appear.

What It Does

- Monitors a user-selected directory (typically Downloads or Desktop) for new files.
- Automatically scans any new or modified file the moment it appears in the monitored folder.
- Catches malicious files before they have a chance to execute.
- Provides immediate notification if a threat is detected in a new file.

How to Configure

49. Click Enable Real-Time in the scan panel.
50. A dialog will ask you to select a directory to monitor.
51. Choose a high-risk folder like Downloads.
52. Protection is now active. To stop, click Disable Real-Time.

> **Tip:** *Monitor your Downloads folder as a priority. This is where most malicious files first appear on your system, whether from email attachments, browser downloads, or file transfers.*

6.6 Network Connection Monitor

The Network Connection Monitor acts as a gatekeeper for your computer's internet connections. It watches for new or unknown programs attempting to send or receive data.

- Monitors all outbound network connections in real-time.
- Identifies programs making network connections and displays their status.
- Alerts you when an unknown or suspicious program attempts to connect to the internet.
- Allows you to block individual connections or whitelist trusted applications.
- Logs all network activity for later analysis.

Module 7: Security Tools Suite

Beyond scanning and real-time protection, GuardBot includes a comprehensive suite of security tools for specialized tasks. Each tool is accessible from the Tools menu and provides focused functionality for specific security needs.

7.1 Deepfake Detection Scanner

Deepfake technology has advanced rapidly, making it increasingly difficult to distinguish manipulated media from authentic content. GuardBot's Deepfake Detection Scanner uses AI-powered image and video analysis to identify manipulated media.

How It Works

The deepfake detection model analyzes images and video frames for telltale signs of manipulation including inconsistent lighting and shadows, facial boundary artifacts, eye reflection inconsistencies, temporal coherence issues in video (frame-to-frame inconsistencies), compression artifacts typical of AI-generated content, and anatomical anomalies in facial features.

How to Use

53. Navigate to Tools and select Deepfake Scanner.
54. Upload an image or video file for analysis.
55. The AI model will analyze the media and return a confidence score indicating the likelihood of manipulation.
56. Review the detailed analysis showing which artifacts were detected and where.

> **Note:** *Deepfake detection is available on Basic and Premium tiers.*

7.2 URL Safety Checker

The URL Safety Checker allows you to verify whether a website is safe before visiting it. Enter any URL and GuardBot will analyze it for known phishing domains, malware distribution sites, suspicious redirects, certificate issues, and reputation scores from multiple threat intelligence sources.

7.3 Wireless Network Analyzer

The Wireless Network Analyzer evaluates the security of your current Wi-Fi network and nearby networks:

- Encryption analysis: Identifies the encryption protocol used (WPA3, WPA2, WEP, Open) and warns about weak configurations.
- Rogue access point detection: Identifies suspicious access points that may be attempting to intercept traffic.
- Signal strength mapping: Shows the strength and quality of nearby wireless networks.
- Connected device listing: Displays all devices connected to your current network.
- Vulnerability assessment: Identifies known vulnerabilities in your router's firmware and configuration.

7.4 Password Manager

GuardBot includes a built-in password manager that securely stores your credentials using AES-256 encryption:

- Secure vault: Store usernames, passwords, notes, and other sensitive information in an encrypted vault.
- Password generator: Create strong, unique passwords with configurable length and complexity.
- Breach monitoring: Checks your stored credentials against known data breach databases and alerts you if any are compromised.
- Auto-fill: Automatically fills login credentials on supported platforms.
- Cross-platform sync: Your password vault syncs across all devices through your Cybertection account.

7.5 File Encryption

The File Encryption tool provides military-grade encryption for individual files and folders:

- AES-256 encryption: Industry-standard encryption that would take billions of years to crack with current technology.
- Easy interface: Select files or folders, set a password, and encrypt. Decryption is equally simple.
- Secure deletion: After encrypting, the original unencrypted file can be securely deleted so it cannot be recovered.
- Multiple file support: Encrypt individual files, multiple files, or entire folder structures.

7.6 Integrated Firewall (Windows/Linux)

On Windows and Linux platforms, GuardBot provides an integrated firewall management interface:

- Visual firewall rules: View and manage firewall rules through GuardBot’s intuitive interface rather than command-line tools.
- Application-based rules: Create rules based on applications rather than ports and IP addresses.
- Quick block: Instantly block any application from accessing the network.
- UFW integration (Linux): Manage and automate your Uncomplicated Firewall settings directly through the GuardBot interface.
- Emergency stop: Instantly disable all network connections with a single click if you suspect a system breach.

Module 8: Advanced Configuration

This module covers advanced GuardBot configuration for power users, system administrators, and security professionals who want to customize every aspect of their protection.

8.1 Custom Scan Profiles

Create custom scan profiles that target specific file types, locations, or threat categories:

- File type filters: Scan only executables, scripts, documents, or archives.
- Exclusion lists: Exclude trusted directories, files, or file types from scans to improve performance.
- Heuristic sensitivity: Adjust the aggressiveness of heuristic analysis on a per-profile basis.
- Schedule profiles: Assign different scan profiles to different schedules (e.g., quick scan daily, full scan weekly, custom scan of sensitive directories twice daily).

8.2 Enterprise Deployment

For organizations deploying GuardBot across multiple devices, Cybertection offers enterprise management capabilities:

- Centralized management: Manage all GuardBot installations from a central dashboard through the Cybertection admin portal.
- Policy deployment: Push scan schedules, shield configurations, and exclusion lists to all devices simultaneously.
- Threat reporting: Aggregate threat data from all devices for organizational security visibility.
- Compliance monitoring: Monitor endpoint protection status across the organization for compliance purposes.
- Group policies: Create device groups with different protection profiles based on department, risk level, or user role.

8.3 API Integration

GuardBot's backend API allows advanced users to integrate with other security tools and workflows:

- Subscription verification: The Flask API at api.cybertectionllc.com provides endpoints for subscription validation, device management, and user authentication.
- Firebase integration: GuardBot uses Firebase Authentication and Firestore for real-time data synchronization across devices.
- Webhook support: Receive notifications through webhooks when threats are detected or protection status changes.
- RESTful endpoints: All API interactions follow REST conventions with JSON payloads and token-based authentication.

8.4 Troubleshooting

Common issues and their resolutions:

VPN Connection Issues

- Cannot connect: Verify your internet connection is active, check that your subscription includes VPN (Premium tier), and ensure no other VPN applications are running simultaneously.
- Slow speeds: Try connecting to a different server closer to your location. Disconnect and reconnect to obtain a fresh connection. Check if your ISP is throttling VPN traffic.
- Frequent disconnections: Enable the Kill Switch and check your network stability. On mobile devices, ensure battery optimization is not killing the VPN process.

Scan Performance

- Scans running slowly: Close unnecessary applications to free system resources. Consider using Quick Scan instead of Full Scan for routine checks. Add large, trusted directories to the exclusion list.
- High CPU usage during scans: Adjust the scan intensity in settings. Schedule scans during off-peak hours.

False Positives

- Legitimate file flagged as threat: Add the file or directory to the whitelist. Report the false positive through the app to help improve detection accuracy. If using High sensitivity, consider reducing to Medium.

Getting Support

If you encounter issues not covered here, support is available through multiple channels:

- In-App Support: Use the Help button in GuardBot to access the support portal.
- Online Manual: Visit cybertection-guardbot.com for comprehensive documentation and tutorials.
- Email: support@cybertection-guardbot.com
- Phone: (410) 701-2931
- Help Center: cybertection.net/general-5
- Bug Reports: cybertection.net/report

8.5 Device Management

GuardBot supports up to 6 devices per account. Managing your device registrations ensures all your devices stay protected and you can maximize your subscription value.

Viewing Registered Devices

Navigate to Settings and select Device Management to see all devices registered to your account. Each device entry shows the device name and platform, operating system version, registration date, last active time, and current protection status.

Adding a New Device

Simply install GuardBot on the new device and sign in with your Cybertection account. The device is automatically registered and begins syncing your subscription and settings. If you have reached the 6-device limit, remove an existing device before adding a new one.

Removing a Device

Go to Device Management, select the device you want to remove, and confirm. The device will lose access to premium features immediately. You can also remotely deregister devices from any other device signed into your account.

8.6 Platform-Specific Tips

Windows Optimization

- Exclude development IDE folders from real-time scanning to improve build performance (add to exclusion list in scan settings).
- Use the integrated firewall management to create application-specific rules that complement Windows Defender Firewall.
- Schedule Full Scans during lunch breaks or after hours to avoid performance impact during productive hours.
- Enable the Emergency Stop feature in your system tray for quick access during potential security incidents.

macOS Optimization

- Grant GuardBot Full Disk Access in System Settings > Privacy & Security for the most thorough scanning capability.
- Allow the Network Extension when prompted during VPN setup. This is required for WireGuard VPN functionality.
- macOS Gatekeeper works alongside GuardBot—both can run simultaneously without conflict.
- Use the keyboard shortcut to quickly toggle VPN on/off when switching between trusted and untrusted networks.

iOS Optimization

- Enable VPN On Demand to automatically connect to the VPN when leaving trusted Wi-Fi networks.
- Allow notifications for immediate alerts about detected threats and VPN status changes.
- iOS sandbox restrictions limit some features compared to macOS. The VPN and deepfake scanner are the primary protection tools on iOS.
- Keep the app updated through the App Store to receive the latest threat intelligence and AI model updates.

Android Optimization

- Disable battery optimization for GuardBot to ensure real-time shields run continuously without being killed by the system.
- Grant all requested permissions during setup for full functionality (storage for scanning, network for VPN/monitoring).

- Enable the persistent notification to keep GuardBot running in the foreground.
- Use the home screen widget for quick access to VPN toggle and security status.

Linux Optimization

- If using Snap, GuardBot may need classic confinement for full system access. Follow setup instructions for your distribution.
- The UFW firewall integration allows you to manage firewall rules through GuardBot's GUI instead of the command line.
- For headless servers, GuardBot can be configured through command-line options and configuration files.
- GuardBot's WireGuard VPN integration on Linux uses the native kernel WireGuard module for maximum performance.

Module 9: Understanding Threats

To get the most from GuardBot, it helps to understand the threats it protects against. This module provides an educational overview of common cyber threats, how they work, and how GuardBot detects and prevents them. This knowledge makes you a more informed user and helps you interpret GuardBot's alerts accurately.

9.1 Malware Types

- Viruses: Self-replicating programs that attach to legitimate files and spread when those files are shared or executed. GuardBot detects viruses through both signature matching and behavioral analysis.
- Worms: Self-propagating malware that spreads across networks without requiring user interaction. GuardBot's network monitoring detects worm propagation patterns.
- Trojans: Malware disguised as legitimate software that performs malicious actions when executed. GuardBot's AI behavioral analysis detects trojans by identifying discrepancies between expected and actual behavior.
- Ransomware: Encrypts your files and demands payment for the decryption key. GuardBot's Ransomware Protection Shield specifically monitors for encryption behavior patterns.
- Spyware: Secretly monitors your activity, captures keystrokes, and steals personal information. GuardBot detects spyware through both signature matching and by identifying unauthorized data collection behavior.
- Adware: Unwanted software that displays advertisements and may track your browsing habits. GuardBot identifies adware through both signature databases and behavioral analysis.
- Rootkits: Malware designed to hide deep within the operating system, making it invisible to traditional security tools. GuardBot's deep scanning capabilities check system-level components for rootkit signatures.
- Fileless Malware: Malware that operates entirely in memory without creating files on disk. This is where GuardBot's AI behavioral analysis excels, detecting malicious behavior regardless of whether a file exists.
- Cryptominers: Malware that hijacks your system's processing power to mine cryptocurrency. GuardBot detects cryptominers through unusual CPU usage patterns and known mining server connections.

9.2 Network Threats

- Phishing: Fraudulent emails, messages, or websites designed to trick you into revealing sensitive information. GuardBot's URL Checker and network monitoring help identify phishing attempts.
- Man-in-the-Middle (MITM) Attacks: Attackers intercept communication between you and a server to steal data or inject malicious content. The WebGuard VPN prevents MITM attacks by encrypting all traffic.
- DNS Spoofing: Attackers redirect DNS queries to malicious servers. GuardBot's VPN includes DNS leak protection and uses secure DNS servers.

- Wi-Fi Attacks: Evil twin access points, deauthentication attacks, and other wireless threats. GuardBot's Wireless Network Analyzer identifies these threats.
- DDoS Attacks: Overwhelming a target with traffic to make it unavailable. While primarily a server-side concern, GuardBot monitors for botnet participation on your devices.

9.3 Social Engineering

Social engineering attacks target the human element rather than technical vulnerabilities:

- Phishing emails: Emails that appear to be from legitimate organizations requesting credentials or personal information.
- Pretexting: Creating a fabricated scenario to obtain information or access.
- Baiting: Leaving infected USB drives or offering free downloads that contain malware.
- Deepfakes: AI-generated audio or video impersonating real people. GuardBot's Deepfake Detection Scanner helps identify manipulated media.

While GuardBot's technical controls catch many social engineering attempts, the most effective defense is awareness and education. The Cybertection Training Center offers courses specifically on recognizing and responding to social engineering attacks.

9.4 Reading GuardBot's Threat Reports

When GuardBot detects a threat, the report includes:

- Threat name and classification: The specific malware family or threat category identified.
- Severity rating: Critical, High, Medium, or Low based on the potential impact and exploitability.
- Detection method: Whether the threat was identified by signature matching, AI behavioral analysis, heuristic analysis, or network monitoring.
- File details: The file name, path, size, hash values, and any associated processes.
- Recommended action: Quarantine, delete, or whitelist with an explanation of why each option is appropriate.
- Technical details: For advanced users, detailed technical information about why the file was flagged, including specific behaviors, signatures, or anomalies detected.

9.5 Emerging Threats

The cybersecurity landscape is constantly evolving. Here are the key emerging threats that GuardBot is designed to protect against, and that every user should be aware of:

AI-Powered Attacks

Attackers are increasingly using artificial intelligence to create more convincing phishing emails, generate deepfake audio and video for social engineering, automate vulnerability discovery, and evade traditional security tools. GuardBot's AI engine is specifically designed to counter AI-powered threats by detecting behavioral anomalies that even sophisticated AI-generated attacks produce.

Supply Chain Attacks

Supply chain attacks compromise software before it reaches the end user. By infecting popular libraries, development tools, or update mechanisms, attackers can distribute malware to millions of systems simultaneously. The SolarWinds attack of 2020 demonstrated the devastating potential of supply chain compromises. GuardBot's behavioral analysis can detect the anomalous activity that occurs when compromised software activates its malicious payload, even when the software itself appears legitimate and is signed by a trusted vendor.

IoT Vulnerabilities

As homes and businesses connect more devices to the internet (smart TVs, cameras, thermostats, appliances), the attack surface expands dramatically. Many IoT devices have weak security, default passwords, and infrequent updates. GuardBot's network monitoring and Wi-Fi analyzer help identify vulnerable IoT devices on your network and detect suspicious traffic patterns that indicate compromise.

Ransomware-as-a-Service (RaaS)

Ransomware has evolved from isolated attacks to a full criminal industry. Ransomware-as-a-Service platforms allow anyone with criminal intent to launch sophisticated ransomware attacks without technical expertise. This has led to a massive increase in ransomware attacks targeting organizations of all sizes. GuardBot's dedicated Ransomware Protection Shield is specifically engineered to detect and stop ransomware before it can encrypt your files, regardless of the specific ransomware variant.

9.6 Best Practices for Digital Security

While GuardBot provides comprehensive technical protection, good security habits are your first line of defense:

Password Hygiene

- Use unique, strong passwords for every account. Never reuse passwords across services.
- Use GuardBot's built-in password manager to generate and store complex passwords securely.
- Enable multi-factor authentication (MFA) on every service that supports it, especially email, banking, and social media.
- Never share passwords via email, text, or chat.
- Change passwords immediately if you receive a breach notification from GuardBot's breach monitoring.

Safe Browsing

- Always verify URLs before entering credentials. Look for HTTPS and check the domain name carefully.
- Use GuardBot's URL Safety Checker before visiting unfamiliar websites.
- Be skeptical of emails and messages containing links, even from known contacts.
- Keep your browsers updated to the latest version.
- Use the WebGuard VPN when connecting to public Wi-Fi networks.

Device Security

- Keep your operating system and all applications updated. Enable automatic updates when possible.
- Enable full-disk encryption on all devices (BitLocker on Windows, FileVault on macOS, LUKS on Linux).
- Set a strong PIN or biometric lock on all mobile devices.
- Enable Find My Device features on all platforms in case of loss or theft.
- Regularly review app permissions and remove unnecessary access grants.

Data Protection

- Use GuardBot's file encryption to protect sensitive documents stored on your devices.
- Back up important data regularly using the 3-2-1 rule: three copies, two media types, one offsite.
- Be cautious about what personal information you share online.
- Review privacy settings on all social media accounts and limit public access to personal information.

Network Security

- Change the default password on your Wi-Fi router and use WPA3 encryption if available (WPA2 minimum).
- Disable WPS (Wi-Fi Protected Setup) on your router as it can be easily brute-forced.
- Create a separate guest network for visitors and IoT devices to isolate them from your primary network.
- Regularly use GuardBot's Wireless Network Analyzer to check for unauthorized devices.
- Consider using GuardBot's VPN for all internet activity, not just on public networks.

Module 10: Practical Exercises and Capstone Project

This final module puts your knowledge into practice with hands-on exercises and a comprehensive capstone project. These exercises are designed for students in the Cybertection Training Center and advanced users who want to deepen their understanding of GuardBot.

10.1 Lab Exercises

Exercise 1: Full System Security Assessment

57. Install GuardBot on your primary device (or a virtual machine for training purposes).
58. Run a Full System Scan and document all findings including detected threats, warnings, and informational items.
59. Enable all real-time shields and monitor the Live Info Log for 24 hours.
60. Document any alerts, their severity, and the actions you took.
61. Write a one-page security assessment of your system based on GuardBot's findings.

Exercise 2: VPN Security Testing

62. Connect to the WebGuard VPN and verify your IP address has changed using an IP lookup service.
63. Test for DNS leaks using an online DNS leak test tool.
64. Measure connection speeds with and without the VPN to understand the performance impact.
65. Test the Kill Switch by simulating a VPN disconnection and verifying that internet traffic is blocked.
66. Connect to three different server locations and compare speeds and latency.

Exercise 3: Threat Detection Validation

67. Download the EICAR test file (a harmless file recognized as a test virus by all antivirus engines) from eicar.org.
68. Observe how GuardBot's Real-Time File Monitor detects the test file immediately upon download.
69. Review the threat report and understand each section.
70. Practice quarantining and restoring the test file.
71. Test with GuardBot AI enabled and note any additional behavioral analysis information.

Exercise 4: Wireless Network Assessment

72. Use GuardBot's Wireless Network Analyzer to scan your current Wi-Fi network.
73. Document the encryption protocol, signal strength, and connected devices.
74. Identify any security weaknesses or recommendations provided by GuardBot.
75. Compare the findings with a manual assessment using command-line tools.
76. Write a brief wireless security report with recommendations for improvement.

Exercise 5: Deepfake Detection

77. Find sample deepfake and authentic images/videos from publicly available deepfake detection datasets.
78. Submit each sample to GuardBot's Deepfake Detection Scanner.
79. Document the confidence scores and analysis for each sample.
80. Evaluate the accuracy of GuardBot's detection compared to known labels.
81. Write a brief analysis of the scanner's strengths and limitations.

10.2 Capstone Project: Complete Security Audit

For the capstone project, you will perform a complete security audit of a test environment using GuardBot as your primary tool. This project demonstrates your ability to use GuardBot effectively and interpret its findings professionally.

Project Requirements

82. Environment Setup: Set up a test environment with a virtual machine running Windows or Linux. Install GuardBot and complete initial configuration.
83. Baseline Assessment: Run a Full System Scan and document the initial security posture. Enable all available shields and record the baseline configuration.
84. Threat Simulation: Download and execute safe test files (EICAR, test malware samples from controlled sources) to validate detection capabilities. Document GuardBot's response to each test.
85. VPN Assessment: Test VPN connectivity, perform leak tests, and measure performance. Document findings and compare against security best practices.
86. Network Assessment: Use the Wireless Network Analyzer and Network Connection Monitor to assess the network security posture. Document findings.
87. Shield Effectiveness Report: Analyze the effectiveness of each real-time shield by reviewing 48 hours of monitoring data. Document alert frequency, types, and actions taken.
88. Security Report: Compile a professional security assessment report including executive summary, methodology, detailed findings with severity ratings, and recommendations for improvement.
89. Presentation: Present your findings in a 15-minute briefing to the class, demonstrating your ability to communicate security concepts effectively.

10.3 Continuing Your Journey

Completing this course gives you a strong foundation in using GuardBot and understanding the threats it protects against. To continue developing your cybersecurity skills:

- Cybertection Training Center courses: Take additional courses in penetration testing, SOC 2 compliance, cloud security, and more at cybertection.net/training-center.
- Cybertection CTF Challenge: Test your skills against our Capture the Flag challenges at cybertection.net/cybertection-ctf-challenge.
- Join the Cybertection community: Connect with other learners and professionals through our Discord server and LinkedIn page.
- Consider certifications: Use your knowledge as a foundation for industry certifications like CompTIA Security+, CEH, or OSCP.

- Internship opportunities: Outstanding students may be invited to join Cybertection LLC as interns, working directly on GuardBot development and security operations.

10.4 Download Links and Resources

Platform	Download Location	Type
Windows	Microsoft Store or cybertection-guardbot.com/windows	Free Download
macOS	Apple App Store	Free Download
iOS	Apple App Store	Free Download
Android	Google Play Store	Free Download
Linux	snap install cybertection-guardbot	Free Download
Fire OS	Amazon Appstore	Free Download
Subscriptions	cybertection.net/pricing-plans/list	Basic / Premium
App Manual	cybertection-guardbot.com	Free
Training Center	cybertection.net/training-center	Free

Appendix A: GuardBot Feature Reference by Platform

This appendix provides a complete feature comparison across all supported platforms. Use this reference to understand which capabilities are available on each device.

Feature	Windows	macOS	iOS	Android	Linux
AI Malware Scan	✓	✓	✓	✓	✓
Full System Scan	✓	✓	Limited	✓	✓
Quick Scan	✓	✓	✓	✓	✓
Custom Scan	✓	✓	—	✓	✓
WebGuard VPN	✓	✓	✓	✓	✓
Deepfake Scanner	✓	✓	✓	✓	—
Real-Time File Monitor	✓	✓	—	✓	✓
Ransomware Protection	✓	✓	—	✓	✓
Network Honeypot	✓	✓	—	✓	✓
Network Monitor	✓	✓	✓	✓	✓
Wi-Fi Analyzer	✓	✓	✓	✓	✓
URL Safety Checker	✓	✓	✓	✓	✓
Password Manager	✓	✓	✓	✓	✓
File Encryption	✓	✓	—	✓	✓
Integrated Firewall	✓	—	—	—	✓ (UFW)
VirusTotal Integration	✓	✓	—	✓	✓
Emergency Stop	✓	✓	—	✓	✓

> **Note:** *iOS has platform restrictions imposed by Apple's App Store sandbox. Some features like full filesystem scanning, real-time file monitoring, and integrated firewall are not available on iOS due to these restrictions. macOS has fewer restrictions and supports most features.*

Appendix B: Subscription Tier Comparison

This appendix provides a detailed comparison of what is included in each GuardBot subscription tier.

Feature	Free	Basic ($4.99/mo)	Premium ($12.99/mo)
URL Safety Checker	✓	✓	✓
System Info	✓	✓	✓
Basic Security Assessment	✓	✓	✓
AI Malware Scanning	—	✓	✓
Deepfake Detection	—	✓	✓
Full System Scan	—	✓	✓
Custom Scan	—	✓	✓
Real-Time Shields	—	✓	✓
Ransomware Protection	—	✓	✓
Network Honeypot	—	✓	✓
Tools Menu (all tools)	—	✓	✓
Password Manager	—	✓	✓
File Encryption	—	✓	✓
WebGuard VPN	—	—	✓
VPN Kill Switch	—	—	✓
Split Tunneling	—	—	✓
Priority Support	—	—	✓

All tiers support up to 6 devices per account. Subscriptions purchased on any platform (Apple App Store, Google Play, or cybertection.net) sync across all devices through your Cybertection account.

Appendix C: Comparison with Competitors

This appendix compares GuardBot with leading cybersecurity products to help you understand how GuardBot's features and approach differ from industry competitors.

Feature Comparison

Feature	GuardBot	Norton	Bitdefender	Malwarebytes	McAfee
AI Behavioral Analysis	✓	✓	✓	Partial	✓
Built-in VPN	✓	✓	✓	Add-on	✓
Deepfake Detection	✓	—	—	—	—
Real-Time Live Log	✓	—	—	—	—
Network Honeypot	✓	—	—	—	—
Open Transparency	✓	—	—	—	—
Cyberpunk UI	✓	—	—	—	—
6 Platforms	✓	4	4	4	4
Ransomware Shield	✓	✓	✓	✓	✓
File Encryption	✓	—	✓	—	✓
VirusTotal Integration	✓	—	—	—	—
Integrated Firewall Mgmt	✓	✓	✓	—	✓

Philosophy Comparison

The most important difference between GuardBot and traditional antivirus products is not a feature list—it is a fundamental difference in philosophy.

Traditional Antivirus: Black Box Approach

Major antivirus companies like Norton, Bitdefender, and Malwarebytes are designed as "black box" solutions for the average consumer. You turn them on and they work in the background. You see a simplified dashboard with a green checkmark or a red warning. Scan results show a list of threats that were blocked. But the real-time process is hidden behind a progress bar, and you have limited visibility into what the software is actually doing at any given moment.

This approach works for users who want zero-friction protection and do not care about the technical details. But it leaves power users, developers, IT professionals, and security enthusiasts in the dark. You cannot learn from a tool you cannot see.

GuardBot: Interactive Command Center

GuardBot takes the opposite approach. Every action the security engine takes is visible in the live info log. You can see exactly which files are being scanned, which processes are being monitored, which network connections are being analyzed, and why specific decisions were made. When a threat is detected, the report explains not just what was found but how it was detected and what specific behaviors or signatures triggered the alert.

This transparency serves two purposes. First, it gives advanced users the information they need to make informed security decisions. Second, it is educational—by watching GuardBot work, you learn how cybersecurity operates at a practical level. This is why GuardBot is the primary tool used in Cybertection Training Center courses.

Cross-Platform Coverage

Most competitors offer their products on Windows, macOS, iOS, and Android—four platforms. GuardBot supports six platforms: Windows, macOS, iOS, Android, Linux, and Fire OS. For users who work across multiple ecosystems, including Linux servers and development environments, GuardBot provides consistent protection everywhere.

Pricing Advantage

GuardBot's Premium plan at $12.99/month covers all six platforms with up to six devices. Competitors like Norton 360 Deluxe charge $49.99/year for five devices, Bitdefender Total Security is $49.99/year for five devices, and Malwarebytes Premium is $59.99/year for five devices (VPN is additional). GuardBot's yearly Premium plan at $150/year includes the full VPN—a feature that competitors either charge extra for or limit in bandwidth.

Appendix D: Glossary of Cybersecurity Terms

This glossary defines key terms used throughout this guide and in GuardBot's interface.

- AES-256: Advanced Encryption Standard with a 256-bit key length. One of the strongest encryption algorithms available, used by GuardBot for file encryption and VPN data protection.
- API Key: A unique identifier used to authenticate requests to a service. GuardBot uses API keys for VirusTotal integration and backend communication.
- Behavioral Analysis: A detection technique that identifies malware based on what it does rather than what it looks like. GuardBot's AI engine specializes in behavioral analysis.
- Botnet: A network of compromised computers controlled remotely by an attacker, often used for DDoS attacks or spam distribution.
- Brute Force: An attack that tries every possible password combination to gain access. GuardBot's password manager generates strong passwords resistant to brute force attacks.
- C2 (Command and Control): Infrastructure used by attackers to communicate with malware on compromised systems. GuardBot's network monitoring detects C2 communication patterns.
- ChaCha20: A stream cipher used by WireGuard for encryption. Provides excellent performance on devices without hardware AES acceleration.
- Cryptominer: Malware that uses your system's resources to mine cryptocurrency without your knowledge or consent.
- Curve25519: An elliptic curve used for key exchange in the WireGuard protocol. Provides strong security with efficient computation.
- Deepfake: AI-generated or AI-manipulated media (images, video, audio) designed to deceive. GuardBot includes dedicated deepfake detection capabilities.
- DDoS (Distributed Denial of Service): An attack that overwhelms a target with traffic from multiple sources, making it unavailable to legitimate users.
- DNS (Domain Name System): The system that translates human-readable domain names to IP addresses. DNS leaks can expose your browsing activity.
- EDR (Endpoint Detection and Response): A security solution that monitors endpoint devices for threats and provides automated response capabilities.
- EICAR Test File: A standardized test file recognized as a simulated virus by all antivirus products. Used to verify that antivirus software is functioning correctly.
- Encryption: The process of converting readable data into an unreadable format that can only be decrypted with the correct key.
- Entropy: A measure of randomness in data. High entropy can indicate encrypted or compressed content, which may be associated with malware or ransomware activity.
- Evil Twin: A rogue Wi-Fi access point that mimics a legitimate network to intercept user traffic and credentials.
- Fileless Malware: Malware that operates entirely in system memory without writing files to disk, making it harder to detect with traditional file-based scanning.
- Firebase: Google's application development platform used by GuardBot for user authentication, subscription management, and data synchronization.

- Firewall: A network security system that monitors and controls network traffic based on predetermined security rules.
- GCP (Google Cloud Platform): Google's cloud computing platform used by Cybertection for VPN server infrastructure and backend services.
- Heuristic Analysis: A detection method that uses rules and algorithms to identify potentially malicious behavior, even in previously unknown files.
- Honeypot: A decoy system designed to attract attackers and detect intrusion attempts. GuardBot includes a network honeypot feature.
- IP Address: A numerical label assigned to each device connected to a network. The VPN masks your real IP address with the server's address.
- Kill Switch: A VPN feature that blocks all internet traffic if the VPN connection drops, preventing your real IP from being exposed.
- MITM (Man-in-the-Middle): An attack where an attacker intercepts communication between two parties without their knowledge.
- MFA (Multi-Factor Authentication): An authentication method requiring two or more verification factors to gain access to an account.
- Phishing: A social engineering attack that uses fraudulent communications to trick recipients into revealing sensitive information or installing malware.
- Poly1305: A cryptographic message authentication code (MAC) used by WireGuard to verify data integrity.
- Quarantine: The process of isolating a detected threat in a secure location where it cannot execute or spread.
- Ransomware: Malware that encrypts files and demands payment for the decryption key.
- Rootkit: Malware designed to hide deep within the operating system, providing persistent access while evading detection.
- Signature-Based Detection: A detection method that compares files against a database of known malware signatures (fingerprints).
- SIEM: Security Information and Event Management system that collects and analyzes security log data from across an organization.
- Split Tunneling: A VPN feature that allows some traffic to go through the VPN while other traffic connects directly to the internet.
- Spyware: Software that secretly collects information about a user's activities without their knowledge or consent.
- TLS (Transport Layer Security): A cryptographic protocol that provides secure communication over a network, used for HTTPS websites.
- Trojan: Malware disguised as legitimate software that performs malicious actions when executed.
- VPN (Virtual Private Network): A technology that creates an encrypted tunnel for internet traffic, providing privacy and security.
- WireGuard: A modern VPN protocol known for its simplicity, speed, and security. Used by GuardBot's WebGuard VPN.
- Zero-Day: A vulnerability that is unknown to the software vendor and has no available patch, making it particularly dangerous.

Appendix E: Frequently Asked Questions

General Questions

Q: Is GuardBot free to use?

A: GuardBot offers a free tier with basic security features. The Basic tier ($4.99/month) unlocks malware scanning, deepfake detection, and all tools. The Premium tier ($12.99/month) adds the WebGuard VPN and priority support.

Q: How many devices can I protect with one account?

A: All GuardBot subscription tiers support up to 6 devices per account. Your subscription syncs across all platforms through your Cybertection account.

Q: Does GuardBot slow down my computer?

A: GuardBot is designed for minimal system impact. The AI engine runs efficiently in the background, and you can adjust scan scheduling and shield sensitivity to balance protection with performance.

Q: Can I use GuardBot alongside another antivirus?

A: While GuardBot can coexist with other security software, running multiple real-time protection engines simultaneously may cause conflicts and performance issues. We recommend using GuardBot as your primary security solution.

VPN Questions

Q: Does the VPN keep logs of my activity?

A: No. Cybertection maintains a strict no-log policy. We do not log your VPN activity, browsing history, DNS queries, or connection timestamps.

Q: Will the VPN slow down my internet?

A: WireGuard is one of the fastest VPN protocols available. Most users experience minimal speed reduction. Connecting to a server close to your physical location minimizes latency.

Q: Can I use the VPN for streaming?

A: Yes. GuardBot's VPN provides the bandwidth needed for HD and 4K streaming. Server selection allows you to connect from different geographic locations.

Technical Questions

Q: How often are threat definitions updated?

A: Threat intelligence databases are updated multiple times daily. AI model updates are pushed through Firebase Remote Config as needed.

Q: What is the EICAR test file and how do I use it?

A: The EICAR test file is a harmless standardized file that all antivirus products recognize as a test virus. Download it from eicar.org to verify GuardBot's real-time detection is working. GuardBot should detect and alert on it immediately.

Q: How do I report a false positive?

A: In the Remediation Center, select the flagged item and choose Report False Positive. You can also report through cybertection.net/report or email support@cybertection-guardbot.com.

Q: What happens to my subscription if I switch devices?

A: Your subscription is tied to your Cybertection account, not your device. Sign in on any supported device and your subscription activates automatically. You can manage your registered devices in app settings.

Account and Billing

Q: How do I cancel my subscription?

A: Cancel through the platform where you purchased: Apple App Store subscription settings, Google Play subscription settings, or your account on cybertection.net. Your access continues until the end of the current billing period.

Q: Can I get a refund?

A: Refund policies follow the respective platform's guidelines (Apple, Google, or Wix). Contact support@cybertection-guardbot.com for billing questions.

Q: How do I upgrade from Basic to Premium?

A: Open GuardBot, navigate to Settings or Subscription, and select Upgrade to Premium. You can also upgrade at cybertection.net/pricing-plans/list. The upgrade takes effect immediately.

Training Center Questions

Q: Is the Cybertection Training Center free?

A: Yes. The Cybertection Training Center is a free, 6-week internship-style program. All courses, materials, and mentorship are provided at no cost. We believe cybersecurity education should be accessible to everyone regardless of financial situation.

Q: Do I need a degree to enroll?

A: No. Cybertection does not require degrees, certifications, or formal credentials. We look for passion, aptitude, and willingness to learn. If you are motivated to learn cybersecurity, you are welcome in our program.

Q: How are Training Center classes conducted?

A: Classes are 100% online and remote through Discord for live instruction and Google Meet for recorded sessions. Most classes are weekday evenings at 6:00 PM Eastern Time.

Q: Can Training Center graduates join Cybertection LLC?

A: Yes. Outstanding students who demonstrate strong skills and dedication may be offered internship or team member positions at Cybertection LLC.

Q: What other courses does the Training Center offer?

A: The Training Center offers courses covering Introduction to Cybersecurity, Advanced Threat Detection, VPN Technology, Secure Application Development, Cloud Security with GCP, Mobile App Security, Penetration Testing, Web Application Testing with Burp Suite, and SOC 2 Audit compliance. See the full catalog at cybertection.cc.

Cybertection LLC | cybertection.net
Kent Island, Maryland | (410) 701-2931 | support@cybertection-guardbot.com