



CyberGuardian XDR

User Guide

Business / Professional plan • up to 10 machines

Version 2.0.5 • September 2026

cyberguardian.bg

support@cyberguardian.bg

SECTION 1 — QUICK START

Follow the steps in order for every new installation. It takes about 15–20 minutes. Do not skip steps.

Before you begin

Make sure you have:

- An internet connection — required for activation
- Administrator rights on the Windows machine
- Windows 10 or Windows 11 (64-bit)

System requirements

Component	Minimum	Recommended
Operating system	Windows 10 (64-bit)	Windows 11 (64-bit)
Processor	Dual-core 2.0 GHz	Quad-core 2.5 GHz+
Memory	4 GB	8 GB+
Free disk space	500 MB	1 GB+
Display	1280 × 800	1920 × 1080
Internet	Required	Required
Rights	Administrator	Administrator

IMPORTANT

The application requires Microsoft WebView2. The installer installs it automatically if it is not present on the machine.

Step 1 — Download the installer

1 Download the installation file

1. Go to cyberguardian.bg
2. Click the “Download” button
3. Download the file: CyberGuardian.XDR_<version>_x64-setup.exe (for example CyberGuardian.XDR_2.0.5_x64-setup.exe)
4. Save the file somewhere easy to find (for example the Desktop)

IMPORTANT

Download only from the official website cyberguardian.bg. Do not install files received by e-mail or from third parties.

Step 2 — Installation

IMPORTANT

The installer requires administrator rights. Without them the installation will fail.

2 Install CyberGuardian XDR

1. Locate the downloaded file CyberGuardian.XDR_<version>_x64-setup.exe
2. Right-click the file and choose “Run as administrator”
3. In the Windows permission prompt (UAC), check the publisher: it must read “Verified publisher: CyberGuardian Security EOOD”
4. If Windows shows a SmartScreen warning: click “More info” → check that the publisher is CyberGuardian Security EOOD → “Run anyway”
5. Follow the installer and wait for it to finish (about 1–2 minutes)
6. The installer itself installs and starts the protection Windows service — you do not need to do anything else
7. Open CyberGuardian XDR (automatically after installation, or from the desktop icon)

SECURITY

All CyberGuardian XDR files are digitally signed by CyberGuardian Security EOOD. If the publisher is different or shows “Unknown publisher” — do NOT install the file and contact us.

Step 3 — Obtain and activate the licence

On first start the activation window opens:

3A If you do not have a licence key — buy a plan

1. In the activation window click “Don't have a license key? Buy Now”
2. The plans page opens — choose the right one: Home — €199/year (up to 3 devices), Business — €299/year (up to 5 devices), Professional — €499/year (up to 10 devices, recommended)
3. Click the chosen plan, fill in the payment details and complete the purchase
4. You receive a licence key by e-mail in the format CG-XXXX-XXXX-XXXX-XXXX-XXXXXXXX
5. Keep the key in a safe place

3B Activate the licence key

1. Enter the licence key in the “License Key” field
2. Click “Activate License”
3. After successful activation the main Dashboard loads

Can't find your licence key?

Check the “Spam” / “Junk” folder of your e-mail. If the key has not arrived within 10 minutes of purchase, contact us at support@cyberguardian.bg

Step 4 — Settings**4 Fill in the Settings**

1. Open “Settings” from the left menu
2. Enter your organisation's details (Company Name, Contact)
3. In “Email Accounts” add an e-mail account to scan: choose the type (Gmail, Outlook, Yahoo or Custom IMAP), enter the e-mail address and an App Password (NOT your main password), enable two-factor verification when asked
4. Save the settings

NIS2 — mandatory or optional?

MANDATORY: for organisations in scope of NIS2 / the Bulgarian Cybersecurity Act. Without these details the system cannot generate valid regulatory reports under the NIS2 Directive and the Cybersecurity Act (State Gazette No. 17 / 13.02.2026).

OPTIONAL: for organisations without a NIS2 registration obligation. You can skip this and come back later.

What is an App Password?

An App Password is a special password generated by Gmail/Outlook for applications. It is NOT your main password. You generate it in your e-mail account settings:

Gmail: Account → Security → 2-Step Verification → App Passwords

Outlook: Account → Security → Advanced security → App Passwords

Step 5 — Check the Windows Service

The protection service runs 24/7 — even when the application is closed.

5 Check that the service is running

1. Open “Process Protection” from the left menu
2. You should see “Service Installed” and “Service Running” — from version 2.0.5 the installer enables them automatically
3. Only if either is missing: click “Install Service” (allow it in the UAC prompt), wait 5 seconds and click “Start Service”
4. Optional: “Maximum Protection” — enables all protection mechanisms

IMPORTANT

Without the Service installed and running, the machine does NOT appear in Managed Devices and is NOT fully protected.

SUCCESS

With “Service Installed” and “Service Running”, CyberGuardian XDR protects the machine even when the application is closed.

Step 6 — Enable blocking (Detection Overview)

6 Turn on active threat blocking

1. Open “Detection Overview” from the left menu
2. Find and click the “Enable Blocking” button
3. The status should become: “Blocking: Active”

Why does it matter?

Without Enable Blocking the system only DETECTS threats but does not block them. With Enable Blocking the system automatically BLOCKS threats in real time. We recommend keeping it enabled at all times.

Step 7 — Real-Time Protection

7 Start file system protection

1. Open “Protection” from the left menu
2. Check “Protection Status” — it must be ACTIVE
3. In “Additional Paths” add extra folders to monitor (separated by semicolons). Downloads and Desktop are always protected.
4. In “Settings” set the “Threat Threshold” (default 75) — files scoring at or above this threshold are quarantined automatically. Enable “Auto-Quarantine”.
5. The “What I Am Protecting Right Now” section shows in real time: Folders Watched, Fingerprints On This PC (known hashes) and Engine (scanning engine status).

How does protection work?

Protection is read directly from the machine through the CyberGuardianXDR service (SYSTEM, 24/7) — these are the real folders the engine monitors, not a saved setting. A file with a known, unchanged hash (fingerprint) is not scanned again — this saves resources.

Step 8 — Initial scan

8 Run the three scan types

1. Open “Scan” from the left menu
2. Click “Quick Scan” → wait (about 2 minutes)
3. Click “Standard Scan” → wait (about 10 minutes)
4. Click “Deep Scan” → wait (30+ minutes)
5. Review the results in Scan History

Tip

Run a Deep Scan when installing every new machine — it scans the entire file system and finds hidden threats. Run it outside working hours.

Step 9 — File Integrity Monitoring

9 Verify the integrity of critical files

1. Open “Integrity” from the left menu
2. Click “Verify This Device” — the system compares the SHA-256 fingerprints of critical system files against the baseline
3. Review the result: Monitored, Intact, Modified, Missing, Locked, Critical
4. In “Fleet — All Machines” you see all machines centrally: Health (HEALTHY), Files OK, Issues and Last Check
5. Optional: “Add File” to monitor an extra file, or “Export Report (PDF)” for a report

What is File Integrity Monitoring?

FIM creates a SHA-256 fingerprint (baseline) of critical files and checks whether they have been changed, are missing or are compromised. HEALTHY means all monitored files are intact.

Step 10 — Tamper Protection

10 Check tamper protection

1. Open “Tamper Protection” from the left menu
2. Review the “Fleet Lead Protection Score” (0–100) — an overall self-protection score for the fleet
3. You see counters for: Machines, Protected, Critical and Canary Traps (ransomware decoys)
4. Each device reports its state after boot and then every 6 hours. Until the first report the status is “UNKNOWN”.
5. Optional: “Export Report” for a protection report

How does Tamper Protection work?

Tamper Protection is self-protection against process termination, configuration tampering and ransomware. Canary Traps are hidden decoy files: on an encryption attempt (T1486) the system detects and stops the attacking process.

Step 11 — Honeypots

11 Check the honeypot traps

1. Open “Honeypots” from the left menu
2. You will see 9 active honeypot traps with status “Live”
3. The traps work automatically — no configuration is required
4. Optional: “Verify traps” to check that all are active

What are Honeypots?

Honeypots are fake “decoys” — simulated network services. When an attacker touches them, the system detects it and records the attacker's methods. They work automatically.

Final check — is everything in order?

After completing all steps, check the Dashboard and confirm:

- ☐ Detection Rate shows 100%
- ☐ Protection status is “Active”
- ☐ Service Installed and Service Running are active (Process Protection)
- ☐ Enable Blocking is active (Detection Overview)
- ☐ Integrity status is “HEALTHY”
- ☐ Tamper Protection has reported the device status
- ☐ All 9 Honeypots are active
- ☐ An e-mail account is added in Settings
- ☐ Quick Scan, Standard Scan and Deep Scan have been run

SUCCESS

Congratulations! The machine is fully protected by CyberGuardian XDR.

SECTION 2 — DAILY OPERATION

When a threat is detected

When the system detects a threat you will see an orange triangle with a number. Follow these steps:

1. Click the triangle to see the threat details
2. Check the risk level — see the table below
3. Check the “FP Risk” indicator (above 50% = probable false positive)
4. Open “Incidents” on the affected machine for the full history

Level	Recommended action
CRITICAL	Act immediately! Isolate the machine from the network. Do not power it off.
HIGH	Check the machine within 1 hour. Contact IT.
MEDIUM	Check by the end of the day. Review the Incidents page.
LOW	Monitor. Check FP Risk — probably a false positive.

CRITICAL — system response

On a CRITICAL threat CyberGuardian XDR blocks the threat automatically. All you need to do: open Incidents → review the details → follow the AI Response Playbook. If in doubt, contact us: support@cyberguardian.bg

Machine status — Managed Devices

For organisations with 2 or more machines — all are visible centrally in Managed Devices. Repeat Steps 1–11 on each machine.

Status	Meaning
Online	The machine is active and fully protected
Offline	The machine is switched off or the agent is not running
0 Threats	No threats detected
3 Threats	3 threats detected — click for details

False positives — legitimate programs flagged as threats

! Add a trusted process

1. Open “FP Control” from the left menu
2. Identify the false positive in the incident list
3. Click “Add Trusted Process”
4. Enter the exact process name (for example “myapp.exe”)
5. Save — the process will no longer generate false positives

IMPORTANT

Only add programs you are 100% sure about. Do not add “svchost.exe”, “explorer.exe” or other system processes — attackers use these names to hide.

Updating the program

CyberGuardian XDR updates automatically over the internet — new versions are digitally signed and verified before they are installed.

1. Open “Software Updates”

2. Click “Check for Updates”
3. If a new version is available you will see “New Update Available” with a description of the changes
4. Click “Download & Install” → confirm
5. The program updates and restarts itself. The protection service keeps running.

Corporate installations (MSI)

If the program was installed by an IT administrator using the MSI package, you will see a message that updates are managed by your IT administrator. This is normal — the IT department controls the versions.

Removing the program

1. Open Windows Settings → Apps → Installed apps
2. Find CyberGuardian XDR → Uninstall
3. Leave “Delete the application data” UNchecked if you plan to reinstall — the licence and settings are kept
4. The uninstaller itself stops the protection and removes the Windows service
5. To free the licence slot: Managed Devices → find the machine → “Remove”

Version 2.0.4 and older

With older versions the uninstaller does not start while protection is running. Update to the latest version first (Software Updates), then uninstall.

Regular maintenance

Daily check (5 minutes)

- ☐ Dashboard → Detection Rate = 100%
- ☐ Dashboard → Protection = Active
- ☐ Managed Devices → all machines are Online
- ☐ Managed Devices → Threats = 0 for every machine
- ☐ Incidents → no new High Confidence incidents

Weekly check

- ☐ Integrity → Verify This Device → status “HEALTHY”
- ☐ Tamper Protection → the device has reported its status
- ☐ Honeypots → all active
- ☐ Email Scanner → review detected phishing e-mails
- ☐ NIS2 Compliance → check the compliance score
- ☐ Software Updates → check for a new version

Subscription and renewal

Plan	Devices	Price	Per month	Renewal
Home	3	€199 / year	≈ €16.58	Automatic
Business	5	€299 / year	≈ €24.92	Automatic
Professional	10	€499 / year	≈ €41.58	Automatic
Enterprise	10+	On request	—	Manual

- Automatic renewal: you receive a reminder e-mail 30 days before expiry.
- Removing a machine: Managed Devices → find the machine → “Remove”.

Frequently asked questions (FAQ)

Q: The machine shows Offline but it is switched on. What should I do?

A: Process Protection → check “Service Running”. If it is not active → “Start Service”. Wait 2 minutes and check Managed Devices.

Q: I see a threat but don't know whether it is real.

A: Click the triangle and check “FP Risk”. Above 50% = probable false positive. Below 20% = real threat. If in doubt, contact us.

Q: How do I add a new machine?

A: Install CyberGuardian XDR on the new machine with your licence key and complete the steps in Section 1. If you have reached the limit, contact us for an upgrade.

Q: How do I remove a machine from the licence?

A: Managed Devices → find the machine → “Remove”. One licence slot is freed.

Q: I get many false positives. What should I do?

A: FP Control → add the legitimate programs to Trusted Processes. You can also lower the Threat Threshold on the Protection page.

Q: How do I know I have the latest version?

A: Software Updates → “Check for Updates”. If it says “You're Up to Date!”, you have the latest version.

For organisations with an IT administrator

For organisations with 10 or more machines that want centralised installation through Group Policy (GPO), there is a separate Enterprise package: an MSI installer plus an automatic deployment script.

- Download: cyberguardian.bg → “Enterprise MSI + GPO script” button
- Detailed instructions are in the Enterprise Installation and Management Guide
- Enterprise licence key: support@cyberguardian.bg

Contact and support

- E-mail: support@cyberguardian.bg
- Website: cyberguardian.bg
- Working hours: Monday – Friday, 09:00 – 18:00 (EET)
- For a critical incident write to support@cyberguardian.bg — expect a reply within 2 hours.

CyberGuardian XDR is a product of CyberGuardian Security EOOD, Bulgaria. All rights reserved © 2026 CyberGuardian Security EOOD.