CyberGuardian XDR

User Guide

Business / Professional Plan • up to 10 devices
Version 2.0 • 2026

cyberguardian.bg
cgs.xdr@gmail.com

SECTION 1 — QUICK START

Follow these steps in order for every new installation. It takes approximately 15–20 minutes. Do not skip any steps.

Before You Begin

Make sure you have:

- **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+
RAM	4 GB	8 GB+
Free Disk Space	500 MB	1 GB+
Display	1280 × 800	1920 × 1080
Internet Connection	Required	Required
Permissions	Administrator	Administrator

⚠ IMPORTANT
Microsoft WebView2 is required by the application. The installer will install it automatically if not already 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_2.0.2_x64-setup.exe
4. Save the file to an easily accessible location (e.g. Desktop)

⚠ IMPORTANT
Only download from the official website cyberguardian.bg. Do not install files received by email or from third parties.

Step 2 — Installation

> ⚠ **IMPORTANT**
> You must run the installer as administrator. Without administrator rights the installation will fail.

2 Install CyberGuardian XDR

1. Locate the downloaded file CyberGuardian XDR_2.0.2_x64-setup.exe
2. Right-click the file
3. Select "Run as administrator"
4. If Windows shows a SmartScreen warning:
   → Click "More info"
   → Click "Run anyway"
5. Follow the installer instructions
6. Wait for installation to complete (approximately 1–2 minutes)
7. CyberGuardian XDR launches automatically after installation

Step 3 — Obtaining and Activating Your License

When you first launch the application, the activation window opens:

3A If you don't have a license key — purchase a plan

1. In the activation window click "Don't have a license key? Buy Now"
2. The plans page opens — choose the plan that suits you:
   - Home — €89/yr. — up to 3 devices
   - Business — €379/yr. — up to 5 devices
   - Professional — €669/yr. — up to 10 devices ★ Recommended
3. Click on your selected plan
4. Complete the payment details and finish the purchase
5. You will receive a license key by email in the format:
   CG-XXXX-XXXX-XXXX-XXXX-XXXXXXXX
6. Save the key in a secure location

3B Activate your license key

1. Enter the license key in the "License Key" field
2. Click "Activate License"
3. Upon successful activation the main Dashboard loads

ℹ Can't find your license key?

Check your "Spam" / "Junk" folder.
If the key has not arrived within 10 minutes of purchase,
contact us at: cgs.xdr@gmail.com

Step 4 — Settings

4 Fill in your details in Settings

1. From the left menu open "Settings"
2. Fill in your organization details (Company Name, Contact)
3. In the "Email Accounts" section add an email for scanning:
   - Select the email type (Gmail, Outlook, Yahoo or Custom IMAP)
   - Enter email address and App Password (NOT your main password)
   - Enable two-factor verification when prompted
4. Save settings

i NIS2 — Mandatory or Optional?
MANDATORY: For organizations subject to NIS2 / Cybersecurity Act obligations. Without completed details the system cannot generate valid regulatory reports as required by NIS2 Directive and applicable cybersecurity legislation.
OPTIONAL: For organizations without NIS2 registration obligations. You may skip this and return later.

i What is an App Password?
An App Password is a special password generated by Gmail/Outlook for applications. It is NOT your main email password. Generate it from your email account settings:
Gmail: Account → Security → 2-Step Verification → App Passwords
Outlook: Account → Security → Advanced Security → App Passwords

Step 5 — Activating the Windows Service

This is the most critical step. Without it the machine is NOT fully protected.

5 Install and start the Windows Service

1. From the left menu open "Process Protection"
2. Click "Install Service" → approve in the UAC prompt
3. Wait 5 seconds
4. Click "Start Service"
5. You should see: ☑ Service Installed and ☑ Service Running

— Additional Protection (recommended) —

6. Click "Enable Self-Healing" — automatic recovery in case of a crash
7. Click "Maximum Protection" — enables all protection mechanisms

⚠ IMPORTANT

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

✓ SUCCESS

On success you will see "☑ Service Installed" and "☑ Service Running". From this point CyberGuardian XDR protects the machine even when the application is closed.

Step 6 — Enable Blocking (Detection Overview)

6 Enable active threat blocking

1. From the left menu open "Detection Overview"
2. Find and click the "Enable Blocking" button
3. Status should become: "Blocking: Active" ☑

ℹ Why is this important?
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 this always active.

Step 7 — Real-Time Protection

7 Start file system protection

1. From the left menu open "Protection"
2. Click "Protection Status" to activate monitoring
3. Optionally configure "Watch Paths" — directories to monitor
4. Select a Sensitivity Profile:
   - Low Sensitivity — minimal false positives
   - Medium Sensitivity — recommended for most organizations
   - High Sensitivity — maximum protection

Step 8 — Initial Scan

8 Run all three scan types

1. From the left menu open "Scan"
2. Click "Quick Scan" → wait (~2 minutes)
3. Click "Standard Scan" → wait (~10 minutes)
4. Click "Deep Scan" → wait (~30+ minutes)
5. Review results in Scan History

ℹ Tip
Run a Deep Scan when installing on each new machine. It scans the full file system and detects hidden threats.
Run it outside business hours — it does not significantly impact performance.

Step 9 — File Integrity Monitoring

9 Generate and verify the Integrity Manifest

1. From the left menu open "Integrity"
2. Click "Generate Manifest" — the system creates SHA-256 checksums
3. Wait for the operation to complete
4. Click "Verify All Files"
5. Status should show "HEALTHY" ☑

Step 10 — Tamper Protection

10 Enable tamper protection

1. From the left menu open "Tamper Protection"
2. Click "Start Watchdog" — starts the process watchdog
3. Click "Verify" — verifies configuration files
4. Click "Config" — review settings
5. Click "Enable Protection" — activates full tamper protection
6. Status should show "System Protected" (green) ☑

Step 11 — Honeypots

11 Verify the honeypot traps

1. From the left menu open "Honeypots"
2. You will see 9 active honeypot traps showing "Live"
3. The traps run automatically — no setup is required
4. Optionally click "Verify traps" to confirm all are active

ℹ What are Honeypots?
Honeypots are fake "traps" — simulated network services.
When an attacker probes them, the system detects and logs their methods.
They run automatically and are a key part of CyberGuardian's active defense.

Final Verification — Is everything set up correctly?

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 shows "System Protected"
- ☐ All 9 Honeypots are active (Deception + Honeypots)
- ☐ Email account added in Settings
- ☐ Quick Scan, Standard Scan and Deep Scan completed

✓ SUCCESS
Congratulations! The machine is fully protected by CyberGuardian XDR.

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 view the threat details
2. Check the risk level — see the table below
3. Check the "FP Risk" indicator (above 50% = likely false positive)
4. Go to the affected machine → open "Incidents" for the full history

Threat Levels and Recommended Actions

Level		Recommended Action
🔴	CRITICAL	Immediate action required! Do NOT turn off the machine — contact support.
🟠	HIGH	Check the machine within 1 hour. Contact your IT team.
🟡	MEDIUM	Review by end of day. Check the Incidents page for details.
⚪	LOW	Monitor. Check FP Risk indicator — likely a false positive.

CRITICAL Threat — What to do

● CRITICAL — System Response

CyberGuardian XDR automatically blocks the threat. You only need to:

1. Open Incidents → review the details
2. Follow the AI Response Playbook
3. If in doubt contact us immediately: cgs.xdr@gmail.com

Machine Status — Managed Devices

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

Machine Statuses

Status		Meaning
🟢	Online	Machine is active and fully protected
🔴	Offline	Machine is powered 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

If the system flags a legitimate program as a threat, add it to FP Control:

! Adding a trusted process

1. From the left menu open "FP Control"
2. Identify the false positive in the incidents list
3. Click "Add Trusted Process"
4. Enter the exact process name (e.g. "myapp.exe")
5. Save — the process will no longer generate false positives

⚠ IMPORTANT
Only add programs you are 100% certain about. Do not add "svchost.exe", "explorer.exe" or other system processes — attackers use these names as cover.

Regular Maintenance

We recommend regular checks of the following indicators.

Daily Check (5 minutes)

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

Weekly Check

- ☐ Integrity → Verify All Files → status "HEALTHY"
- ☐ Tamper Protection → status "System Protected"
- ☐ Honeypots → all active
- ☐ Email Scanner → review detected phishing emails
- ☐ NIS2 Compliance → check compliance score

Subscription & Renewal

Plan	Devices	Price	Per Month	Renewal
Home	3	€89 / yr.	≈ €7.42	Automatic
Business	5	€379 / yr.	≈ €31.58	Automatic
Professional ★	10	€669 / yr.	≈ €55.75	Automatic
Enterprise	10+	Contact us	—	Manual

- **Automatic renewal:** you receive an email reminder 30 days before expiry.
- **Removing a machine:** Managed Devices → find the machine → click "Remove".

Frequently Asked Questions (FAQ)

Q: A machine shows Offline but it is powered on. What should I do?

A: Go to Process Protection → check "Service Running". If not active → click "Start Service". Wait 2 minutes and check again in Managed Devices.

Q: I see a threat but I'm not sure if it's real.

A: Click ⚠ and check the "FP Risk" indicator. Above 50% = likely 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 using your license key and complete all steps in Section 1. If the device limit is reached — contact us for an upgrade.

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

A: Managed Devices → find the machine → click "Remove". This frees up one license slot.

Q: I'm getting many false positives. What should I do?

A: Go to FP Control → add the legitimate programs to Trusted Processes. You may also lower the Sensitivity Profile from High to Medium in the Protection page.

For Organizations with an IT Administrator

In some cases an organization may have an IT specialist who manages the installation of all machines centrally — with one admin machine and the rest as endpoints.

In this case the installation process is different and requires a special configuration.

i Contact Us

If your organization has an IT administrator and you require centralized deployment across multiple machines, please contact us for additional instructions and a configuration key:

● cgs.xdr@gmail.com

cyberguardian.bg

Contact & Support

ℹ Get in Touch

- Email: cgs.xdr@gmail.com
- Website: cyberguardian.bg

Business hours: Monday – Friday, 09:00 – 18:00 (EET)
For critical incidents email cgs.xdr@gmail.com
Expect a response within 2 hours for critical cases.