



CyberGuardian XDR

Ръководство за потребителя

Business / Professional план • до 10 машини

Версия 2.0.5 • септември 2026

cyberguardian.bg

support@cyberguardian.bg

РАЗДЕЛ 1 — БЪРЗ СТАРТ

Следвайте стъпките по ред при всяка нова инсталация. Отнема около 15–20 минути. Не прескачайте стъпки.

Преди да започнете

Уверете се, че разполагате с:

- Интернет връзка — задължителна за активация
- Администраторски права на Windows машината
- Windows 10 или Windows 11 (64-bit)

Системни изисквания

Компонент	Минимум	Препоръчително
Операционна система	Windows 10 (64-bit)	Windows 11 (64-bit)
Процесор	Dual-core 2.0 GHz	Quad-core 2.5 GHz+
Оперативна памет	4 GB	8 GB+
Свободно място	500 MB	1 GB+
Монитор	1280 × 800	1920 × 1080
Интернет	Задължителна	Задължителна
Права	Администратор	Администратор

ВАЖНО

Microsoft WebView2 се изисква от приложението. Инсталаторът го инсталира автоматично, ако не е наличен на машината.

Стъпка 1 — Изтегляне на инсталатора

1 Изтеглете инсталационния файл

1. Отидете на cyberguardian.bg
2. Кликнете на бутона „Download“
3. Изтеглете файла: CyberGuardian.XDR_<версия>_x64-setup.exe (например CyberGuardian.XDR_2.0.5_x64-setup.exe)
4. Запазете файла на лесно достъпно място (например Работен плот)

ВАЖНО

Изтегляйте само от официалния сайт cyberguardian.bg. Не инсталирайте файлове, получени по имейл или от трети страни.

Стъпка 2 — Инсталация

ВАЖНО

Инсталаторът изисква администраторски права. Без тях инсталацията ще се провали.

2 Инсталирайте CyberGuardian XDR

1. Намерете изтегления файл CyberGuardian.XDR_<версия>_x64-setup.exe
2. Кликнете с десен бутон върху файла и изберете „Изпълни като администратор“ (Run as administrator)
3. В прозореца на Windows за разрешение (UAC) проверете издателя: трябва да пише „Проверен издател: CyberGuardian Security EOOD“
4. Ако Windows покаже SmartScreen предупреждение: кликнете „Повече информация“ → проверете, че издателят е CyberGuardian Security EOOD → „Изпълни въпреки това“
5. Следвайте инструкциите на инсталатора и изчакайте да завърши (около 1–2 минути)
6. Инсталаторът сам инсталира и стартира защитната Windows услуга — не е нужно да правите нищо допълнително
7. Отворете CyberGuardian XDR (автоматично след инсталацията или от иконата на работния плот)

СИГУРНОСТ

Всички файлове на CyberGuardian XDR са цифрово подписани от CyberGuardian Security EOOD. Ако издателят е друг или е „Неизвестен издател“ — НЕ инсталирайте файла и се свържете с нас.

Стъпка 3 — Получаване и активиране на лиценза

При първо стартиране се отваря прозорецът за активация:

3А Ако нямате лицензен ключ — закупете план

1. В прозореца за активация кликнете „Don't have a license key? Buy Now“
2. Отваря се страницата с планове — изберете подходящия: Home — €199/год. (до 3 устройства), Business — €299/год. (до 5 устройства), Professional — €499/год. (до 10 устройства, препоръчан)
3. Кликнете на избрания план, попълнете платежните данни и завършете покупката
4. На имейла получавате лицензен ключ във формат CG-XXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
5. Запазете ключа на сигурно място

3В Активирайте лицензния ключ

1. Въведете лицензния ключ в полето „License Key“
2. Кликнете „Activate License“
3. При успешна активация се зарежда главният Dashboard

Не намирате лицензния ключ?

Проверете папка „Спам“ / „Junk“ в имейла. Ако ключът не е пристигнал до 10 минути след покупката, свържете се с нас на support@cyberguardian.bg

Стъпка 4 — Настройки (Settings)

4 Попълнете данните в Settings

1. От лявото меню отворете „Settings“
2. Попълнете данните на вашата организация (Company Name, Contact)
3. В раздел „Email Accounts“ добавете имейл за сканиране: изберете типа (Gmail, Outlook, Yahoo или Custom IMAP), въведете имейл адрес и App Password (НЕ основната парола), активирайте двуфакторна верификация при поискване
4. Запазете настройките

NIS2 — задължително или по желание?

ЗАДЪЛЖИТЕЛНО: за организации, задължени по NIS2 / Закона за киберсигурност (ЗКС). Без попълнени данни системата не може да генерира валидни регулаторни доклади съгласно Директива NIS2 и ЗКС (ДВ бр. 17 / 13.02.2026).

ПО ЖЕЛАНИЕ: за организации без задължение за регистрация по NIS2. Можете да пропуснете и да се върнете по-късно.

Какво е App Password?

App Password е специална парола, генерирана от Gmail/Outlook за приложения. НЕ е вашата основна парола. Генерирайте я от настройките на имейла:

Gmail: Акаунт → Сигурност → Двустепенно потвърждение → App Passwords

Outlook: Акаунт → Сигурност → Разширена сигурност → App Passwords

Стъпка 5 — Проверка на Windows Service

Защитната услуга работи 24/7 — дори когато приложението е затворено.

5 Проверете, че услугата работи

1. От лявото меню отворете „Process Protection“
2. Трябва да видите: „Service Installed“ и „Service Running“ — от версия 2.0.5 инсталаторът ги включва автоматично
3. Само ако някое от тях липсва: кликнете „Install Service“ (разрешете в UAC прозореца), изчакайте 5 секунди и кликнете „Start Service“
4. По желание: „Maximum Protection“ — активира всички защитни механизми

ВАЖНО

Без инсталиран и стартиран Service машината НЕ се появява в Managed Devices и НЕ е защитена напълно.

УСПЕХ

При „Service Installed“ и „Service Running“ CyberGuardian XDR защитава машината дори когато приложението е затворено.

Стъпка 6 — Активиране на блокиране (Detection Overview)

6 Включете активното блокиране на заплахи

1. От лявото меню отворете „Detection Overview“
2. Намерете и кликнете бутона „Enable Blocking“
3. Статусът трябва да стане: „Blocking: Active“

Защо е важно?

Без Enable Blocking системата само ЗАСИЧА заплахи, но не ги блокира. С Enable Blocking системата автоматично БЛОКИРА заплахите в реално време. Препоръчваме винаги да е активирано.

Стъпка 7 — Real-Time Protection

7 Стартирайте защитата на файловата система

1. От лявото меню отворете „Protection“
2. Проверете „Protection Status“ — трябва да е ACTIVE
3. В „Additional Paths“ добавете допълнителни папки за наблюдение (разделени с точка и запетая). Downloads и Desktop се пазят винаги.
4. В „Settings“ задайте „Threat Threshold“ (по подразбиране 75) — файлове с оценка на или над този праг се поставят автоматично под карантина. Активирайте „Auto-Quarantine“.
5. Секцията „What I Am Protecting Right Now“ показва в реално време: Folders Watched (наблюдавани папки), Fingerprints On This PC (познати хешове) и Engine (статус на скениращия двигател).

Как работи защитата?

Защитата се чете директно от машината чрез CyberGuardianXDR service (SYSTEM, 24/7) — това са реалните папки, които двигателят наблюдава, не запазена настройка. Файл с познат непроменен хеш (fingerprint) не се сканира повторно — това пести ресурси.

Стъпка 8 — Първоначално сканиране

8 Изпълнете трите вида сканиране

1. От лявото меню отворете „Scan“
2. Кликнете „Quick Scan“ → изчакайте (около 2 минути)
3. Кликнете „Standard Scan“ → изчакайте (около 10 минути)
4. Кликнете „Deep Scan“ → изчакайте (30+ минути)
5. Прегледайте резултатите в Scan History

Съвет

Стартирайте Deep Scan при инсталация на всяка нова машина — той сканира пълната файлова система и открива скрити заплахи. Изпълнявайте го в извънработно време.

Стъпка 9 — File Integrity Monitoring

9 Проверете целостта на критичните файлове

1. От лявото меню отворете „Integrity“
2. Кликнете „Verify This Device“ — системата сравнява SHA-256 отпечатъците на критичните системни файлове спрямо базовата линия (baseline)
3. Прегледайте резултата: Monitored, Intact, Modified, Missing, Locked, Critical
4. В „Fleet — All Machines“ виждате всички машини централно: Health (HEALTHY), Files OK, Issues и Last Check
5. По желание: „Add File“ за допълнителен файл към мониторинга или „Export Report (PDF)“ за отчет

Какво е File Integrity Monitoring?

FIM създава SHA-256 отпечатък (baseline) на критичните файлове и проверява дали са променени, липсват или са компрометирани. Статус HEALTHY означава, че всички наблюдавани файлове са непокътнати.

Стъпка 10 — Tamper Protection

10 Проверете защитата срещу манипулации

1. От лявото меню отворете „Tamper Protection“
2. Прегледайте „Fleet Lead Protection Score“ (0–100) — обобщена оценка на самозащитата на флота
3. Виждате брояча за: Machines, Protected, Critical и Canary Traps (примамки за ransomware)
4. Всяко устройство докладва състоянието си след стартиране и след това на всеки 6 часа. До първия доклад статусът е „UNKNOWN“.
5. По желание: „Export Report“ за отчет на защитата

Как работи Tamper Protection?

Tamper Protection е самозащита срещу спиране на процеси, подправяне на конфигурация и ransomware. Canary Traps са скрити файлове-примамки: при опит за криптиране (T1486) системата засича и спира атакуващия процес.

Стъпка 11 — Honeypots

11 Проверете honeypot капаните

1. От лявото меню отворете „Honeypots“
2. Ще видите 9 активни honeypot капана със статус „Live“
3. Капаните работят автоматично — не се изисква настройка
4. По желание: „Verify traps“, за да проверите, че всички са активни

Какво са Honeypots?

Honeypots са фалшиви „примамки“ — симулирани мрежови услуги. Когато атакуващ ги достъпи, системата го засича и регистрира методите му. Работят автоматично.

Финална проверка — всичко ли е наред?

След като завършите всички стъпки, проверете Dashboard и потвърдете:

- ☐ Detection Rate показва 100%
- ☐ Protection статус е „Active“
- ☐ Service Installed и Service Running са активни (Process Protection)
- ☐ Enable Blocking е активен (Detection Overview)
- ☐ Integrity статус е „HEALTHY“
- ☐ Tamper Protection е докладвал статус на устройството
- ☐ Всички 9 Honeypots са активни
- ☐ Имейл акаунт е добавен в Settings
- ☐ Quick Scan, Standard Scan и Deep Scan са изпълнени

УСПЕХ

Поздравления! Машината е напълно защитена от CyberGuardian XDR.

РАЗДЕЛ 2 — ЕЖЕДНЕВНА РАБОТА

При засечена заплаха

Когато системата засече заплаха, ще видите оранжев триъгълник с число. Следвайте тези стъпки:

1. Кликнете върху триъгълника, за да видите детайлите на заплахата
2. Проверете нивото на риска — вижте таблицата по-долу
3. Проверете показателя „FP Risk“ (над 50% = вероятен false positive)
4. Отворете „Incidents“ на засегнатата машина за пълна история

Ниво	Препоръчително действие
CRITICAL	Незабавно действие! Изолирайте машината от мрежата. Не я изключвайте от ток.
HIGH	Проверете машината в рамките на 1 час. Свържете се с IT.
MEDIUM	Проверете до края на деня. Прегледайте страницата Incidents.
LOW	Наблюдавайте. Проверете FP Risk — вероятно false positive.

CRITICAL — отговор на системата

При CRITICAL заплаха CyberGuardian XDR автоматично блокира заплахата. От вас се изисква само: отворете Incidents → прегледайте детайлите → следвайте AI Response Playbook. При съмнение се свържете с нас: support@cyberguardian.bg

Статус на машините — Managed Devices

За организации с 2 или повече машини — всички се виждат централно в Managed Devices. Повторете Стъпки 1–11 на всяка машина.

Статус	Значение
Online	Машината е активна и напълно защитена
Offline	Машината е изключена или агентът не работи
0 Threats	Няма засечени заплахи
3 Threats	Има 3 засечени заплахи — кликнете за детайли

False Positives — легитимни програми, засечени като заплаха

! Добавяне на доверен процес

1. От лявото меню отворете „FP Control“
2. Идентифицирайте false positive в списъка с инциденти
3. Кликнете „Add Trusted Process“
4. Въведете точното име на процеса (например „myapp.exe“)
5. Запазете — процесът вече няма да генерира false positive

ВАЖНО

Добавяйте само програми, за които сте 100% сигурни. Не добавяйте „svchost.exe“, „explorer.exe“ или други системни процеси — атакуващите използват тези имена за прикритие.

Обновяване на програмата

CyberGuardian XDR се обновява автоматично по интернет — новите версии са цифрово подписани и проверени, преди да бъдат инсталирани.

1. Отворете „Software Updates“
2. Кликнете „Check for Updates“
3. Ако има нова версия, ще видите „New Update Available“ с описание на промените
4. Кликнете „Download & Install“ → потвърдете
5. Програмата се обновява и рестартира сама. Защитната услуга продължава да работи.

Фирмени инсталации (MSI)

Ако програмата е инсталирана от IT администратор чрез MSI пакет, ще видите съобщение, че обновяванията се управляват от вашия IT администратор. Това е нормално — IT отделът контролира версиите.

Премахване на програмата

1. Отворете Настройки на Windows → Приложения → Инсталирани приложения
2. Намерете CyberGuardian XDR → Деинсталиране
3. Оставете „Delete the application data“ НЕмаркирано, ако ще инсталирате отново — лицензът и настройките се запазват
4. Деинсталаторът сам спира защитата и премахва Windows услугата
5. За да освободите лицензния слот: Managed Devices → намерете машината → „Remove“

Версия 2.0.4 и по-стари

При по-старите версии деинсталацията не тръгва, докато защитата работи. Обновете първо до последната версия (Software Updates) и след това деинсталирайте.

Редовна поддръжка

Ежедневна проверка (5 минути)

- ☐ Dashboard → Detection Rate = 100%
- ☐ Dashboard → Protection = Active
- ☐ Managed Devices → всички машини са Online
- ☐ Managed Devices → Threats = 0 за всяка машина
- ☐ Incidents → без нови High Confidence инциденти

Седмична проверка

- ☐ Integrity → Verify This Device → статус „HEALTHY“
- ☐ Tamper Protection → устройството е докладвало статус
- ☐ Honeypots → всички активни
- ☐ Email Scanner → прегледайте засечените фишинг имейли
- ☐ NIS2 Compliance → проверете compliance score
- ☐ Software Updates → проверете за нова версия

Абонамент и подновяване

План	Устройства	Цена	На месец	Подновяване
Home	3	€199 / год.	≈ €16.58	Автоматично
Business	5	€299 / год.	≈ €24.92	Автоматично
Professional	10	€499 / год.	≈ €41.58	Автоматично
Enterprise	10+	По запитване	—	Ръчно

- Автоматично подновяване: получавате имейл напомняне 30 дни преди изтичане.
- Премахване на машина: Managed Devices → намерете машината → „Remove“.

Често задавани въпроси (FAQ)

В: Машината показва Offline, но е включена. Какво да направя?

О: Process Protection → проверете „Service Running“. Ако не е активно → „Start Service“. Изчакайте 2 минути и проверете в Managed Devices.

В: Виждам заплаха, но не знам дали е реална.

О: Кликнете на триъгълника и проверете „FP Risk“. Над 50% = вероятен false positive. Под 20% = реална заплаха. При съмнение се свържете с нас.

В: Как да добавя нова машина?

О: Инсталирайте CyberGuardian XDR на новата машина с вашия лицензен ключ и изпълнете стъпките от Раздел 1. При достигнат лимит — свържете се с нас за upgrade.

В: Как да премахна машина от лиценза?

О: Managed Devices → намерете машината → „Remove“. Освобождава се един лицензен слот.

В: Получавам много false positives. Какво да направя?

О: FP Control → добавете легитимните програми в Trusted Processes. Може да намалите Threat Threshold в страницата Protection.

В: Как да разбера, че имам последната версия?

О: Software Updates → „Check for Updates“. Ако пише „You're Up to Date!“, версията е последната.

За организации с IT администратор

За организации с 10 и повече машини, които искат централизирана инсталация чрез Group Policy (GPO), има отделен Enterprise пакет: MSI инсталатор + скрипт за автоматично разгръщане.

- Изтегляне: cyberguardian.bg → бутон „Enterprise MSI + GPO скрипт“
- Подробните инструкции са в Enterprise ръководството за инсталация и управление
- Enterprise лицензен ключ: support@cyberguardian.bg

Контакт и поддръжка

- Имейл: support@cyberguardian.bg
- Уебсайт: cyberguardian.bg
- Работно време: понеделник – петък, 09:00 – 18:00 ч. (EET)
- При критичен инцидент пишете на support@cyberguardian.bg — очаквайте отговор до 2 часа.

CyberGuardian XDR е продукт на CyberGuardian Security EOOD, България. Всички права запазени © 2026 CyberGuardian Security EOOD.