CyberGuardian XDR

Ръководство за потребителя

Business / Professional план • до 10 машини

Версия 2.0 • 2026

cyberguardian.bg
cgs.xdr@gmail.com

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_2.0.2_x64-setup.exe
4. Запазете файла на лесно достъпно място (напр. Работен плот)

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

Стъпка 2 — Инсталация

> ⚠ **ВАЖНО**
> Задължително стартирайте инсталатора като администратор. Без администраторски права инсталацията ще се провали.

2 Инсталирайте CyberGuardian XDR

1. Намерете изтегления файл CyberGuardian XDR_2.0.2_x64-setup.exe
2. Кликнете с десен бутон върху файла
3. Изберете "Изпълни като администратор" (Run as administrator)
4. Ако Windows покаже SmartScreen предупреждение:
   → Кликнете "Повече информация"
   → Кликнете "Изпълни въпреки това"
5. Следвайте инструкциите на инсталатора
6. Изчакайте инсталацията да завърши (около 1–2 минути)
7. CyberGuardian XDR се отваря автоматично след инсталацията

Стъпка 3 — Получаване и активиране на лиценза

При първо стартиране се отваря прозорецът за активация:

3A 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 за вас:
   • Home — €89/год. — до 3 устройства
   • Business — €379/год. — до 5 устройства
   • Professional — €669/год. — до 10 устройства ★ Препоръчан
3. Кликнете на избрания план
4. Попълнете платежните данни и завършете покупката
5. На имейла получавате лицензен ключ във формат:
   CG-XXXX-XXXX-XXXX-XXXX-XXXXXXXX
6. Запазете ключа на сигурно място

3B Активирайте лицензния ключ

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

i Не намирате лицензния ключ?
Проверете папка "Спам" / "Junk" в имейла.
Ако ключът не е пристигнал в рамките на 10 минути след покупката,
свържете се с нас на: cgs.xdr@gmail.com

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

i 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.

i Какво е App Password?
App Password е специална парола генерирана от Gmail/Outlook за приложения. НЕ е вашата основна парола. Генерирате я от настройките на вашия имейл:
Gmail: Акаунт → Сигурност → Двустепенно потвърждение → App Passwords
Outlook: Акаунт → Сигурност → Разширена сигурност → App Passwords

Стъпка 5 — Активиране на Windows Service

Това е най-важната стъпка. Без нея машината НЕ е напълно защитена.

5 Инсталирайте и стартирайте Windows Service

1. От лявото меню отворете "Process Protection"
2. Кликнете "Install Service" → разрешете в UAC прозореца
3. Изчакайте 5 секунди
4. Кликнете "Start Service"
5. Трябва да видите: ☑ Service Installed и ☑ Service Running

— Допълнителна защита (препоръчително) —

6. Кликнете "Enable Self-Healing" — автоматично възстановяване при срив
7. Кликнете "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 успех виждате "☑ Service Installed" и "☑ Service Running". От този момент 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" ☑

i 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. Кликнете "Protection Status" за да активирате мониторинга
3. По желание задайте "Watch Paths" — директории за наблюдение
4. Изберете Sensitivity Profile:
   - Low Sensitivity — минимални false positives
   - Medium Sensitivity — препоръчително за повечето организации
   - High Sensitivity — максимална защита

Стъпка 8 — Първоначално сканиране

8 Изпълнете трите вида сканиране

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

i Съвет
Стартирайте Deep Scan при инсталация на всяка нова машина. Той сканира пълната файлова система и открива скрити заплахи.
Изпълнявайте го в извънработно време — не натоварва значително системата.

Стъпка 9 — File Integrity Monitoring

9 Генерирайте и верифицирайте Integrity Manifest

1. От лявото меню отворете "Integrity"
2. Кликнете "Generate Manifest" — системата създава SHA-256 checksums
3. Изчакайте операцията да завърши
4. Кликнете "Verify All Files"
5. Статусът трябва да показва "HEALTHY" ☑

Стъпка 10 — Tamper Protection

10 Активирайте защитата срещу манипулации

1. От лявото меню отворете "Tamper Protection"
2. Кликнете "Start Watchdog" — стартира процесен watchdog
3. Кликнете "Verify" — верифицира конфигурационните файлове
4. Кликнете "Config" — прегледайте настройките
5. Кликнете "Enable Protection" — активира пълна tamper защита
6. Статусът трябва да показва "System Protected" (зелено) ☑

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 кликнете "Verify traps" за да проверите, че всички са активни

i Какво са Honeypots?
Honeypots са фалшиви "примамки" — симулирани мрежови услуги.
Когато хакер ги атакува, системата го засича и регистрира методите му.
Работят автоматично и са ключова част от активната защита на CyberGuardian.

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 показва "System Protected"
- ☐ Всички 9 Honeypots са активни (Deception + Honeypots)
- ☐ Email акаунт е добавен в Settings
- ☐ Quick Scan, Standard Scan и Deep Scan са изпълнени

✓ УСПЕХ
Поздравления! Машината е напълно защитена от CyberGuardian XDR.

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 "FP Risk" показателя (над 50% = вероятен false positive)
4. Отидете на засегнатата машина → отворете "Incidents" за пълна история

Нива на заплахи и препоръчителни действия

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

При CRITICAL заплаха

● CRITICAL — Отговор на системата

При CRITICAL заплаха CyberGuardian XDR автоматично блокира заплахата. От вас се изисква само:

1. Отворете Incidents → прегледайте детайлите
2. Следвайте AI Response Playbook
3. При съмнение се свържете с нас: cgs.xdr@gmail.com

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.

Статуси на машините

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

Ако системата засече легитимна програма като заплаха, добавете я в FP Control:

! 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 (напр. "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 системни процеси — хакерите използват тези имена за прикритие.

Редовна поддръжка

Препоръчваме редовна проверка на следните показатели.

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 All Files → статус "HEALTHY"
- ☐ Tamper Protection → статус "System Protected"
- ☐ Honeypots → всички активни
- ☐ Email Scanner → прегледайте засечените фишинг имейли
- ☐ NIS2 Compliance → проверете compliance score

Абонамент и подновяване

План	Устройства	Цена	На месец	Подновяване
Home	3	€89 / год.	≈ €7.42	Автоматично
Business	5	€379 / год.	≈ €31.58	Автоматично
Professional ★	10	€669 / год.	≈ €55.75	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 ⚠ 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 всички стъпки от Раздел 1. При достигнат лимит — свържете се с нас за upgrade.

В: Как да премахна машина от лицензa?

О: Managed Devices → намерете машината → натиснете "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 Sensitivity Profile от High на Medium в Protection страницата.

За организации с IT администратор

В редки случаи организацията може да има IT специалист, който управлява централно инсталацията на всички машини — с една admin машина и останалите като endpoints.

В този случай процесът на инсталация е различен и изисква специална конфигурация.

i Свържете се с нас

Ако вашата организация разполага с IT администратор и желаете централизирана инсталация на множество машини, моля свържете се с нас за допълнителни инструкции и конфигурационен ключ:

● cgs.xdr@gmail.com

cyberguardian.bg

Контакт и поддръжка

ℹ Свържете се с нас

● Имейл: cgs.xdr@gmail.com

● Уебсайт: cyberguardian.bg

Работно време: Понеделник – Петък, 09:00 – 18:00 ч. (EET)

При критичен инцидент пишете на cgs.xdr@gmail.com

Очаквайте отговор в рамките на 2 часа при критични случаи.