MANAGED CYBER SECURITY · IRELAND

CyberProtect

Every device. Every person. One shield.

Managed cyber security for Irish businesses, in two simple products from IT.ie. Choose Endpoint for your devices, User for your people and Microsoft 365, or both for full cover.



IT.ie | Unit 01, Dublin Airport Logistics Park, Elm Road, St Margaret's, Co Dublin, K67 N237 | hello@it.ie

Over half of Irish office workers admit they have caused a data breach.

IT.ie survey of 1,000 Irish office workers.

Only 15% get the level of training they need to prevent one.

Attacks rarely need a genius. They need one rushed click, one unpatched laptop or one reused password. That is why CyberProtect protects both halves of your business: the devices your team works on, and the people, inboxes and Microsoft 365 data they work with.

What is CyberProtect?

IT.ie's managed cyber security bundle for Irish SMEs, in two products. **Endpoint** protects laptops, desktops and servers. **User** protects your people, email and Microsoft 365 data. Take one, or put both together for one complete shield.

No stack of separate vendors. One bundle, monitored and supported from Ireland.

Eleven ways in. Two products that close them.

Threats that hit your devices — ENDPOINT

- **Ransomware**
  Ransomware detection and EDR
- **Viruses and malware**
  Anti-virus with endpoint detection & response
- **Unpatched software**
  Patch and third-party software management
- **Malicious websites**
  DNS filtering blocks them before they load
- **Devices nobody is watching**
  Remote monitoring & management, 24/7 SOC in Pro

Threats that hit people and 365 — USER

- **Phishing and fake invoices**
  Cloud email protection and anti-phishing
- **Hijacked Microsoft 365 accounts**
  Cloud Detect & Respond (CDR)
- **Deleted or encrypted 365 data**
  Microsoft 365 backup: email, OneDrive, SharePoint, Teams
- **Staff caught out by scams**
  Awareness training and phishing simulations (Pro)
- **Passwords for sale online**
  Dark web monitoring (Pro)
- **Risky Microsoft 365 settings**
  365 tenant security management (Pro)

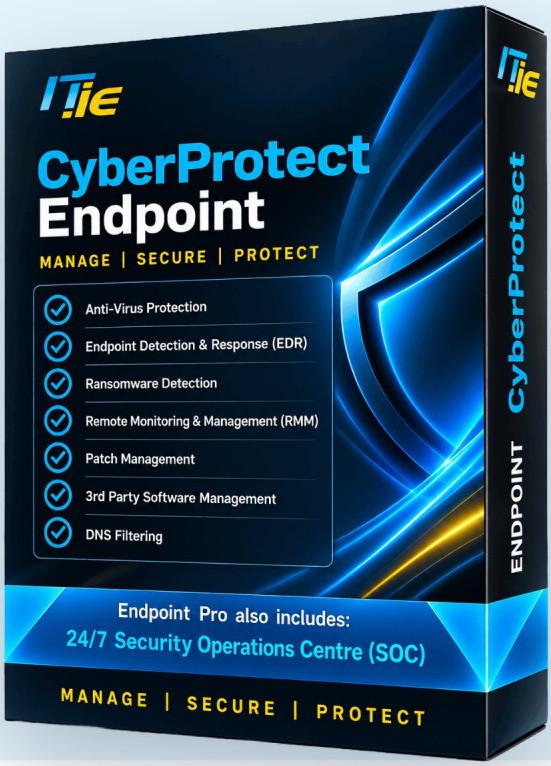
11/11 Take Endpoint and User together and every route on this map is addressed: devices, people and Microsoft 365. Some protections need the Pro edition.

CyberProtect

Endpoint

MANAGE | SECURE | PROTECT

Protection for every laptop, desktop and server in your business, with IT.ie watching device health and fixing problems before they become incidents.



What's on every device

Anti-virus protection
Blocks known malware on every device.

Endpoint detection & response (EDR)
Spots suspicious behaviour and contains attacks that get past anti-virus.

Ransomware detection
Watches for crypto-ransomware and acts to stop it, limiting the damage.

Remote monitoring & management
IT.ie sees device health and can fix issues remotely.

Patch management
Keeps Windows up to date and closes known security holes.

Third-party software management
Keeps everyday apps like browsers and PDF readers patched too.

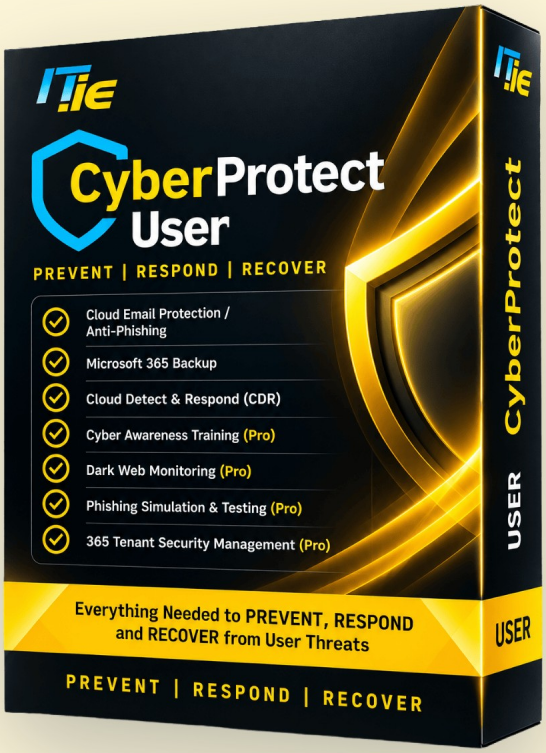
DNS filtering
Stops staff reaching malicious and phishing websites.

24/7 Security Operations Centre
PRO

Security analysts watching for threats around the clock.

Endpoint Essentials
The seven core protections above, deployed, patched and monitored by IT.ie.

Endpoint Pro
Everything in Essentials, plus a 24/7 SOC watching your devices around the clock.



CyberProtect User

PREVENT | RESPOND | RECOVER

Protection for your people, inboxes and Microsoft 365 data, so one bad email or stolen password does not become a business-stopping event.

What protects your people

Cloud email protection / anti-phishing

Filters phishing, malware and impersonation emails before they reach inboxes.

Microsoft 365 backup

Secure backups of email, OneDrive, SharePoint and Teams.

Cloud Detect & Respond (CDR)

Watches Microsoft 365 activity for signs of a compromised account.

Cyber awareness training PRO

Short, regular training that helps staff spot scams.

Phishing simulation & testing PRO

Realistic test emails show who needs more help.

Dark web monitoring PRO

Alerts you when company credentials turn up online.

365 tenant security management PRO

Ongoing checks on your Microsoft 365 settings to close gaps.

User Essentials

Email protection, Microsoft 365 backup and Cloud Detect & Respond.

User Pro

Adds training, phishing simulations, dark web monitoring and tenant security.

Why take both? Many attacks start with a person, such as a phishing email or a stolen password, and end on a device, such as ransomware encrypting a laptop. Endpoint and User together cover both halves.

Compare CyberProtect editions

Essentials covers the core. Pro adds round-the-clock monitoring on devices, and training and deeper Microsoft 365 protection for people. Every edition is managed for you by IT.ie.

CyberProtect Endpoint

MANAGE · SECURE · PROTECT

FEATURE	ESSENTIALS	PRO
Anti-virus protection	✓	✓
Endpoint detection & response	✓	✓
Ransomware detection	✓	✓
Remote monitoring & management	✓	✓
Patch management	✓	✓
Third-party software management	✓	✓
DNS filtering	✓	✓
24/7 Security Operations Centre (SOC)	Not included	✓

CyberProtect User

PREVENT · RESPOND · RECOVER

FEATURE	ESSENTIALS	PRO
Cloud email protection / anti-phishing	✓	✓
Microsoft 365 backup	✓	✓
Cloud Detect & Respond (CDR)	✓	✓
Cyber awareness training	Not included	✓
Phishing simulation & testing	Not included	✓
Dark web monitoring	Not included	✓
365 tenant security management	Not included	✓

Not sure which edition fits? Start with one product and add the other later. Your security assessment recommends the right mix.

CyberProtect and Microsoft 365

Microsoft runs Microsoft 365. Keeping your devices, email, files and accounts safe is your job. Whichever plan you are on, CyberProtect adds what it leaves out.

CyberProtect Endpoint

YOUR DEVICES

ON BUSINESS STANDARD

Standard doesn't include advanced endpoint security. Endpoint fills that gap.

- Adds EDR and ransomware detection to every device
- Addresses endpoint items flagged in your Microsoft Secure Score
- Helps raise your Secure Score

ON BUSINESS PREMIUM

Premium includes strong tools such as Defender and Intune. Endpoint adds the everyday management around them.

- Managed Windows and third-party patching
- DNS filtering and remote monitoring by IT.ie
- 24/7 SOC monitoring with Endpoint Pro

CyberProtect User

YOUR PEOPLE AND MICROSOFT 365

ON BUSINESS STANDARD

Standard includes Microsoft's baseline email filtering. User builds on it with:

- A dedicated anti-phishing and email filtering layer
- Independent backup of email, OneDrive, SharePoint and Teams
- Monitoring for compromised accounts

ON BUSINESS PREMIUM

Premium adds strong tools such as Conditional Access. User adds the backup, monitoring and people side.

- Microsoft 365 backup you can restore from
- Cloud Detect & Respond managed by IT.ie
- Training, phishing simulations and tenant security checks with User Pro

Built to support NIS2 and DORA

NIS2 makes cyber security a management-level duty for in-scope organisations, and pushes the same expectations down to the suppliers they rely on. It expects you to detect incidents, recover data, train staff and show your working. CyberProtect gives you the controls behind each of those, managed for you.

Hour 0
You become aware of a significant incident.

24 hours
Early warning to the national authority.

72 hours
Full incident notification.

You cannot report what you cannot see. CyberProtect's EDR, Cloud Detect & Respond and 24/7 SOC help you spot incidents in time to meet NIS2 Article 23 deadlines.

How CyberProtect maps to NIS2 Article 21(2)

Endpoint · User

21(2)(b)	**Incident handling** Detect, contain and respond to incidents.	EDR · Ransomware detection · 24/7 SOC (Pro) · Cloud Detect & Respond
21(2)(c)	**Business continuity and backup** Backup management and disaster recovery.	Microsoft 365 backup
21(2)(e)	**Vulnerability handling** Security in the maintenance of your systems.	Patch management · Third-party software
21(2)(f)	**Testing that controls work** Assessing the effectiveness of your measures.	Phishing simulations (Pro) · Security reporting
21(2)(g)	**Cyber hygiene and training** Basic hygiene practices and staff training.	Awareness training (Pro) · Email protection · DNS filtering
21(2)(i)	**Access control and asset management** Know your devices and secure your accounts.	Remote monitoring & management · 365 tenant security (Pro) · Dark web monitoring (Pro)

Financial entities face similar expectations under DORA for ICT risk management, incident reporting and resilience. CyberProtect supports compliance; it does not make a business compliant on its own. Governance, policies and risk management matter too, and IT.ie can help with those.

Protected in three steps

From first conversation to fully managed protection, with as little disruption to your team as possible.

Step 1

Assess

We review your IT, Microsoft 365 and current security, then recommend the right CyberProtect editions.

Step 2

Deploy

IT.ie rolls CyberProtect out to your devices and Microsoft 365 with minimal disruption to day-to-day work.

Step 3

Protect and support

Continuous updates, monitoring, local support and expert advice to keep your business running securely.

Book your cyber security assessment

We'll look at where you're exposed today and which CyberProtect editions would close the gaps. No obligation.

CALL US FREE
1800 353 353

EMAIL
hello@it.ie

ONLINE AND LIVE CHAT
it.ie/cyberprotect

We reply within one working day.



Delivered by IT.ie. Powered by Kaseya.