GUIDANCE

EDR, XDR and network analysis: what are they for in your estate?

What EDR and XDR bring, the situations in which to consider them and the limits of replacement solutions. Practical questions to help you choose your protection.

Publié le 17 octobre 2026 — Imprimé le 27 novembre 2026



"You need an EDR." The proposal is hard to assess if you do not know what the tool will observe, who will receive its alerts and what will happen during an incident. The right comparison is about functions, a scope and an organisation for response.

The reference points below set out the technical differences. The situations and the choice questions reflect how Karbonic proposes to examine an installation; they do not replace the analysis of your estate.

Antivirus, EDR, XDR: what is the difference?

| Means | What it mainly provides | What to check | | --- | --- | --- | | Antivirus and workstation protection | Preventing and blocking malicious activity on equipment. | Updates, configuration, coverage and handling of alerts. | | EDR | Observing the activity of equipment, investigating events and allowing responses. | Information available, retention period, actions and the people in charge of follow-up. | | XDR | Bringing together events from several security sources. | Sensors, connections, licences and quality of the correlation. | | Firewall and network analysis | Filtering or examining the exchanges visible on the network. | Where observations are made, logs kept and limits of visibility. |

The functions can be combined in a single suite. A commercial name or a "protected" screen is therefore not enough to determine what is actually deployed. Microsoft, for example, distinguishes between the antivirus protection and the EDR capabilities of Defender for Endpoint.

In which contexts is an EDR worth considering?

The question concerns what an incident would prevent you from doing and the information needed to react. These are starting points for discussion, not a grid that would automatically assign a product to every company.

| Your situation | Questions to examine | | --- | --- | | A small organisation with confidential files | Who accesses the files? What would you need to know if a workstation were compromised? | | Travelling staff and hosted services | Which devices and accounts are monitored outside the premises? Which sources can be correlated? | | Servers essential to the business | What response actions are possible without interrupting a critical service? Who can authorise them? | | Older equipment that cannot support an agent | What access can be limited? What monitoring is possible elsewhere? What will remain invisible? |

A small installation is not necessarily little exposed. The value of the data, access and the consequences of an interruption count as much as the number of machines.

Is it useful to add XDR straight away?

XDR is of interest when an investigation needs to link several sources. You still need to have the useful sensors and configure them. In GravityZone, the possibilities vary notably according to the licences and the integrations deployed.

The approach Karbonic proposes is to start from a few incident questions: which observations need to be correlated, who will examine them and what decision could they make possible? This work helps to choose the useful connections and to set aside an extension that would give no additional answer to your need.

Can the EDR you already have be replaced?

Yes, but the replacement must be compared function by function: systems covered, detection, investigation information, response actions, retention of events, access and day-to-day operation. Capabilities that may be included in existing licences are checked before any additional purchase.

The change can start with a pilot scope. Compatibility, the reporting of information and the actions provided for are checked before the old system is withdrawn. The switchover must preserve protection and the elements needed for investigations in progress.

It is also possible that the difficulty lies mainly in the configuration or the monitoring. Replacing the product without correcting this organisation would then solve only part of the problem.

Can a firewall, logs or NetWatch be enough?

These means have their uses, but their functions are not interchangeable. Network logs do not necessarily offer the same observation of a workstation’s activity as a sensor installed on it. Centralising logs does not automatically turn into an EDR system.

NetWatch is used to gather information and coordinate interventions. In the organisation described by Karbonic, it notably uses information from Bitdefender and works with estate management. It is not presented as a standalone substitute for protecting equipment.

When a particular protection cannot be installed, compensating measures are studied. Their scope and limits must be stated, without claiming to achieve the same capabilities by default.

What should you keep, even with a good detection solution?

Updates, limited access, stronger authentication, backups and preparation for recovery meet complementary needs. CISA resources and the ANSSI framework deal with them beyond the mere choice of an antivirus or an EDR.

Following up alerts is just as practical: who receives them, when, with what rights and what procedure? Hours of intervention and escalation conditions must be known. Buying a licence does not create operational cover.

What questions should you ask before accepting a proposal?

- Which equipment, accounts and services will be covered?
- What information will be available to understand an incident?

- Where will this information be kept, for how long and with what access?
- Who will examine the alerts, and during what hours?
- What actions can be triggered automatically or after validation?
- What will remain outside the scope, and how will it be monitored?
- What are the costs of deployment, licensing and operation?

Karbonic can draw up this reading from your installation, compare the options and organise the monitoring chosen. The proposal distinguishes the tools, the configuration work and the support commitments.

Examine the security of your installation

Sources and documentation consulted on 17 October 2026

- Microsoft: Defender for Endpoint capabilities on Windows
- Bitdefender: EDR and XDR
- ANSSI: reference framework of security measures
- CISA: resources for SMBs