ORIENTIERUNG

# EDR, XDR und Netzwerkanalyse: wozu dient das für Ihre Infrastruktur?

*Was EDR und XDR bringen, in welchen Situationen sie zu prüfen sind und wo die Grenzen von Ersatzlösungen liegen. Konkrete Fragen für die Wahl Ihres Schutzes.*

Publié le 17 octobre 2026 — Imprimé le 27 novembre 2026



«Sie brauchen einen EDR.» Dieser Vorschlag ist schwer zu beurteilen, wenn Sie nicht wissen, was das Werkzeug beobachten wird, wer seine Warnmeldungen erhält und was bei einem Vorfall geschieht. Der richtige Vergleich betrifft Funktionen, einen Umfang und eine Organisation der Reaktion.

Die folgenden Orientierungspunkte stellen die technischen Unterschiede dar. Die Situationen und die Auswahlfragen entsprechen der Art, wie Karbonic vorschlägt, eine Installation zu prüfen; sie ersetzen die Analyse Ihrer Infrastruktur nicht.

## Virenschutz, EDR, XDR: worin besteht der Unterschied?

| Mittel | Was es hauptsächlich bringt | Was zu prüfen ist | | --- | --- | --- | | Virenschutz und Schutz der Arbeitsplätze | Bösartige Aktivitäten auf den Geräten verhindern und blockieren. | Aktualisierung, Konfiguration, Abdeckung und Bearbeitung der Warnmeldungen. | | EDR | Die Aktivitäten der Geräte beobachten, Ereignisse untersuchen und Reaktionen ermöglichen. | Verfügbare Informationen, Aufbewahrungsdauer, Aktionen und die für die Betreuung zuständigen Personen. | | XDR | Ereignisse aus mehreren Sicherheitsquellen zusammenführen. | Sensoren, Verbindungen, Lizenzen und Qualität der Zusammenführung. | | Firewall und Netzwerkanalyse | Den im Netzwerk sichtbaren Datenaustausch filtern oder untersuchen. | Ort der Beobachtungen, aufbewahrte Protokolle und Grenzen der Sichtbarkeit. |

Die Funktionen können in einer einzigen Suite zusammengefasst sein. Ein Handelsname oder ein «geschützter» Bildschirm genügt daher nicht, um festzustellen, was tatsächlich eingesetzt wird. Microsoft

unterscheidet zum Beispiel zwischen dem Virenschutz und den EDR-Fähigkeiten von Defender for Endpoint.

## In welchen Zusammenhängen verdient ein EDR eine Prüfung?

Die Frage betrifft das, was ein Vorfall verhindern würde, und die Informationen, die für eine Reaktion nötig sind. Hier sind Ausgangspunkte für das Gespräch, kein Raster, das jedem Unternehmen automatisch ein Produkt zuweist.

| Ihre Situation | Zu prüfende Fragen | | --- | --- | | Eine kleine Struktur mit vertraulichen Dossiers | Wer greift auf die Dossiers zu? Was müsste man bei der Kompromittierung eines Arbeitsplatzes wissen? | | Mitarbeitende unterwegs und gehostete Dienste | Welche Geräte und Konten werden ausserhalb der Räumlichkeiten überwacht? Welche Quellen lassen sich zusammenführen? | | Für die Tätigkeit wesentliche Server | Welche Reaktionsmassnahmen sind möglich, ohne einen kritischen Dienst zu unterbrechen? Wer kann sie genehmigen? | | Ein älteres Gerät, das keinen Agenten unterstützt | Welche Zugriffe lassen sich begrenzen? Welche Überwachung ist anderswo möglich? Was bleibt unsichtbar? |

Eine kleine Installation ist nicht zwingend wenig exponiert. Der Wert der Daten, die Zugriffe und die Folgen eines Unterbruchs zählen ebenso viel wie die Zahl der Maschinen.

## Ist es sinnvoll, sofort XDR hinzuzufügen?

XDR ist interessant, wenn eine Untersuchung mehrere Quellen verknüpfen muss. Dafür müssen aber die nützlichen Sensoren vorhanden und konfiguriert sein. In GravityZone variieren die Möglichkeiten namentlich je nach Lizenzen und eingesetzten Integrationen.

Das von Karbonic vorgeschlagene Vorgehen geht von einigen Vorfallfragen aus: Welche Beobachtungen müssen zusammengeführt werden, wer wird sie prüfen und welchen Entscheid könnten sie ermöglichen? Diese Arbeit hilft, die nützlichen Verbindungen zu wählen und eine Erweiterung auszuschliessen, die keine zusätzliche Antwort auf Ihren Bedarf liefern würde.

## Kann man den vorhandenen EDR ersetzen?

Ja, aber der Ersatz muss Funktion für Funktion verglichen werden: abgedeckte Systeme, Erkennung, Untersuchungsinformationen, Reaktionsmassnahmen, Aufbewahrung der Ereignisse, Zugriffe und täglicher Betrieb. Fähigkeiten, die allenfalls in bestehenden Lizenzen enthalten sind, werden vor einem zusätzlichen Kauf überprüft.

Der Wechsel kann mit einem Pilotbereich beginnen. Kompatibilität, Rückmeldung der Informationen und vorgesehene Aktionen werden vor der Ausserbetriebnahme der alten Lösung überprüft. Die Übernahme muss den Schutz und die für laufende Untersuchungen nötigen Elemente erhalten.

Es ist auch möglich, dass die Schwierigkeit vor allem von der Konfiguration oder der Betreuung herrührt. Das Produkt zu ersetzen, ohne diese Organisation zu korrigieren, würde dann nur einen Teil des Problems lösen.

## Können eine Firewall, Logs oder NetWatch genügen?

Diese Mittel haben ihren Nutzen, aber ihre Funktionen sind nicht austauschbar. Netzwerkprotokolle bieten nicht zwingend dieselbe Beobachtung der Aktivität eines Arbeitsplatzes wie ein darauf installierter Sensor. Eine Zentralisierung von Logs wird nicht automatisch zu einem EDR-System.

NetWatch dient dazu, Informationen zu sammeln und Einsätze zu koordinieren. In der von Karbonic beschriebenen Organisation nutzt es namentlich Informationen von Bitdefender und arbeitet mit der Infrastrukturverwaltung zusammen. Es wird nicht als eigenständiger Ersatz für den Schutz der Geräte dargestellt.

Wenn ein bestimmter Schutz nicht installiert werden kann, werden kompensierende Massnahmen geprüft. Ihre Reichweite und ihre Grenzen müssen genannt werden, ohne vorzugeben, standardmässig dieselben Fähigkeiten zu erreichen.

## Was sollte man behalten, selbst mit einer guten Erkennungslösung?

Aktualisierungen, begrenzte Zugriffe, verstärkte Authentifizierung, Datensicherungen und die Vorbereitung des Wiederanlaufs decken ergänzende Bedürfnisse ab. Die Ressourcen der CISA und das Referenzwerk der ANSSI behandeln sie über die blosse Wahl eines Virenschutzes oder eines EDR hinaus.

Die Verfolgung der Warnmeldungen ist ebenso konkret: Wer erhält sie, wann, mit welchen Rechten und nach welchem Vorgehen? Einsatzzeiten und Eskalationsbedingungen müssen bekannt sein. Der Kauf einer Lizenz schafft keine betriebliche Bereitschaft.

## Welche Fragen sollte man stellen, bevor man eine Offerte annimmt?

- Welche Geräte, Konten und Dienste werden abgedeckt?
- Welche Informationen stehen zur Verfügung, um einen Vorfall zu verstehen?
- Wo werden diese Informationen aufbewahrt, wie lange und mit welchen Zugriffen?
- Wer prüft die Warnmeldungen, und zu welchen Zeiten?
- Welche Aktionen können automatisch oder nach Freigabe ausgelöst werden?
- Was bleibt ausserhalb des Umfangs, und wie wird es überwacht?
- Wie hoch sind die Kosten für Einführung, Lizenz und Betrieb?

Karbonic kann diese Einschätzung auf der Grundlage Ihrer Installation erstellen, die Möglichkeiten vergleichen und die gewählte Betreuung organisieren. Die Offerte unterscheidet die Werkzeuge, die Konfigurationsarbeit und die Verpflichtungen der Begleitung.

Die Sicherheit Ihrer Installation prüfen

## Am 17. Oktober 2026 eingesehene Quellen und Dokumentation

- Microsoft: Fähigkeiten von Defender for Endpoint unter Windows
- Bitdefender: EDR und XDR
- ANSSI: Referenzwerk der Sicherheitsmassnahmen
- CISA: Ressourcen für KMU