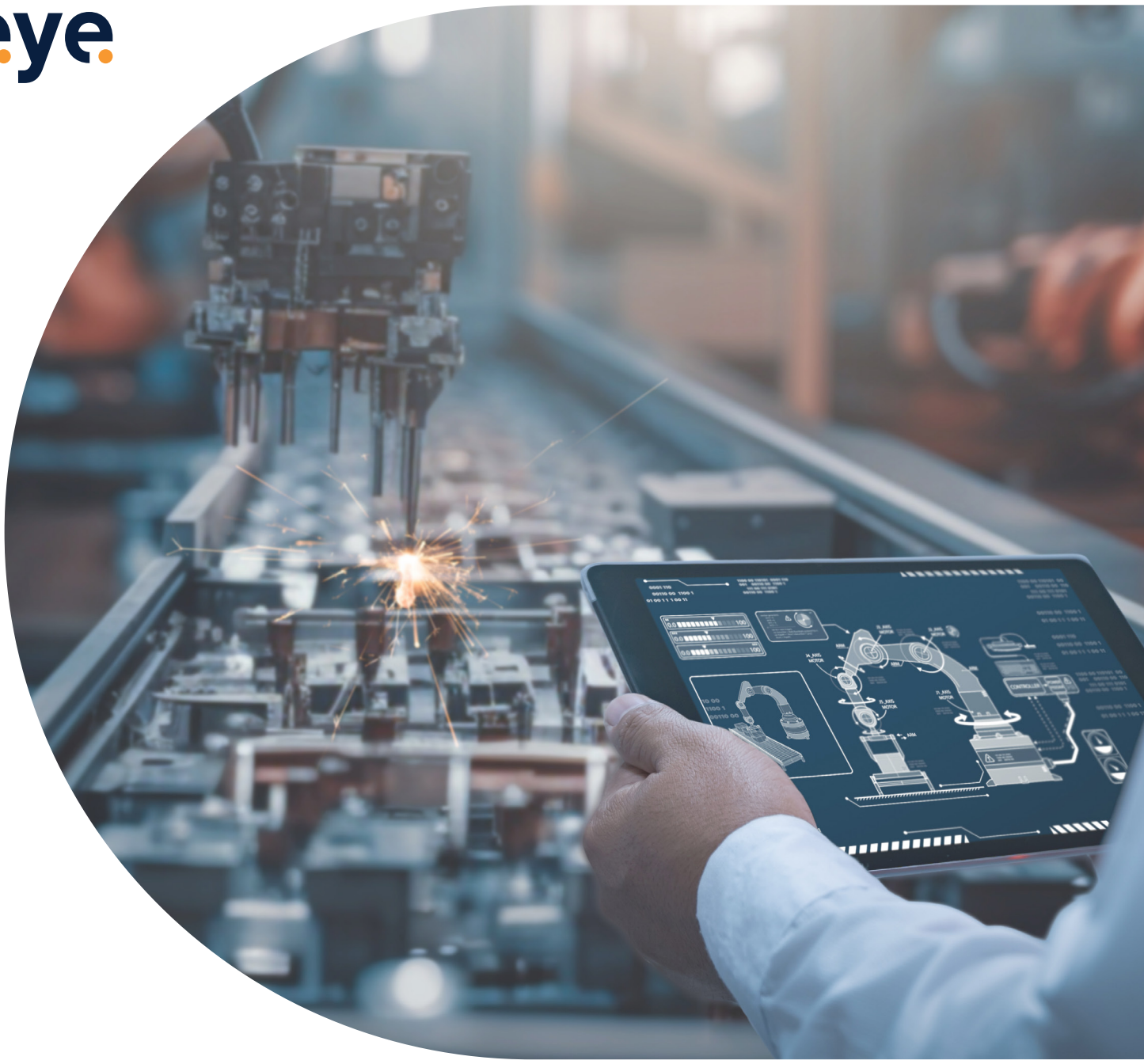

Leitfaden zur Bewertung von MDR-Lösungen

Warum EDR als Grundlage nutzen?

Inhaltsverzeichnis

Dieser Leitfaden richtet sich an Verantwortliche, die MDR-Lösungen evaluieren und nun entscheiden müssen, welche Sicherheitstechnologie als Grundlage für einen Cybersicherheitsservice dienen soll: eine Endpunkt-, eine Netzwerk- oder eine Kombination aus beidem.

MDR-Anbieter lassen sich in eine der folgenden drei Kategorien einteilen:

- **Verwaltete „Endpoint Detection and Response“ (EDR)**
- **Verwaltete „Network Detection and Response“ (NDR)**
- **Verwaltete „Cloud Detection and Response“ (CDR)**

Die meisten Dienstleister bieten eine Form der erweiterten Erkennung und Reaktion („Extended Detection and Response“, XDR) an, und viele nennen ihren Dienst „Managed Extended Detection and Response“ (MXDR). Sie erfassen Signale von einzelnen Sicherheitssystemen und korrelieren sie mit denen von EDR oder NDR. Dabei bildet in der Regel eine dieser Technologien die Grundlage des Dienstes. Es ist Ihre Entscheidung, welche Sie wählen.

Die Hauptunterschiede zwischen EDR und NDR

EDR	NDR
EDR konzentriert sich auf **einzelne Geräte** wie Desktops, Laptops und Server. Ein EDR-Werkzeug überwacht Dateien, Prozesse, Benutzer und Netzwerkaktivitäten auf der Endpunktebene und erkennt Bedrohungen dort, wo sie oft entstehen - auf dem Endgerät.	NDR konzentriert sich auf den **Informationsfluss im gesamten** Netzwerk und erkennt Anomalien oder potenzielle Bedrohungen im Netzwerkverkehr. Ein NDR-Werkzeug überwacht in erster Linie den internen (Ost-West-) oder externen (Nord-Süd-) Datenverkehr.

Warum die Wahl eines Basis-Sicherheitsprodukts wichtig ist

Möglicherweise gehen Sie davon aus, dass die grundlegende Technologie für Sie irrelevant ist, da der Dienstleister für Ihren Schutz verantwortlich ist. Es gibt zwei Gründe, warum Sie darauf achten sollten.

Reduzierung des Risikos eines erfolgreichen Angriffs

Die Reaktionsfähigkeit des MDR-Anbieters kann den Unterschied ausmachen zwischen der erfolgreichen Eindämmung eines Angriffs und dem Verlust und/oder der Verschlüsselung Ihrer sensiblen und unternehmenskritischen Daten. Die Reaktionszeit wird von mehreren Faktoren bestimmt. Dieser Leitfaden soll Ihnen helfen, die folgenden Fragen zu beantworten:

- **Wirksamkeit der Erkennung.** Wie viele Bedrohungen werden in welchem Stadium eines Angriffs erkannt?
- **Geschwindigkeit der Erkennung.** Werden die Signale schnell ausgewertet, um festzustellen, ob ein echter Angriff vorliegt?
- **Genauigkeit der Erkennung.** Werden Warnungen für Aktivitäten mit niedriger Priorität erzeugt, die zu falsch positiven Ergebnissen führen?
- **Sichtbarkeit der Bedrohung.** Bietet die Lösung den Kontext der Bedrohung, um eine schnelle Untersuchung zu ermöglichen?
- **Aktive Reaktion.** Ermöglicht die Lösung Reaktionsmechanismen zur schnellen Eindämmung eines Angriffs mit minimalen Auswirkungen auf den Betrieb?

- **Ermittlungswerkzeuge.** Bietet die Lösung geeignete Tools, die bei der Untersuchung des Vorfalls und der Behebung des Schadens nach einem Angriff helfen?

Ihr Team muss mit den grundlegenden Lösungen vertraut sein

Sie werden Ihre Cybersicherheitsinfrastruktur und -programme nicht vollständig auslagern - nur einige Teile der Erkennung (von Bedrohungen) und der Reaktion (auf Vorfälle). Sie werden weiterhin selbst aktiv mitwirken, abhängig vom Umfang der Leistungen des gewählten Anbieters und der grundlegenden Technologie. Es ist wichtig, dass Sie den Anbieter auswählen, dessen Produkte Sie und Ihr Team am besten beherrschen, und zwar auf der Grundlage Ihrer Erfahrungen und Fähigkeiten. Die folgenden Fragen helfen Ihnen dabei, das zu bewerten:

- Wie komplex ist der Einsatz der Erkennungs- und Reaktionsprodukte?
- Muss ich zusätzliche Agenten und Sensoren einsetzen?
- Muss ich Integrationen mit anderen Sicherheitstools und -anwendungen konfigurieren?
- Ist sichergestellt, dass der Anbieter während eines Angriffs schnell und einfach wichtige Informationen erhält?
- Welche Tools und Informationen stehen zur Untersuchung der Vorfälle sowie zur Schadensbegrenzung zur Verfügung? Wie viel Aufwand muss ich betreiben?

Implementierungsschritte und Sichtbarkeit

Ohne einen umfassenden Überblick über potenzielle Bedrohungen ist es äußerst schwierig, Schutzmaßnahmen zu ergreifen. EDR bietet tiefe Einblicke in das Host-Verhalten von Windows-, Linux- und MacOS-Systemen. Dazu gehören auch (virtuelle) Server und Laptops, unabhängig von ihrem Standort. NDR bietet einen umfassenden Überblick über das Netzwerkverhalten, was jedoch mit einigen Kompromissen verbunden ist.

	EDR	NDR
Installation	Die Verteilung der EDR-Agenten wird über gängigen MDM-Lösungen wie Intune, AD Group Policy oder anderen konfiguriert	Virtuelle oder Hardware-Anwendung, zentral im Netz, passiver SPAN-Port oder in-line (weniger häufig).
Einführung in Phasen	In der Regel werden die Agents im Lern-/Passivmodus eingesetzt, um eine Verhaltensgrundlage zu schaffen, während die Prozesse nicht angehalten/beendet werden (und somit das Unternehmen weniger beeinträchtigt wird).	Die Implementierung eines NDR muss auf der Grundlage der lokalen Netzwerkarchitektur geplant werden. Es müssen Firewalls angepasst und ein Hardware-Wartungsprozess im Team integriert werden.
Time-to-Value (TTV)	Sobald die Verteilung der Agenten konfiguriert ist, werden alle verwalteten Endpunkte innerhalb von Minuten oder Stunden angebunden.	Die Implementierung eines NDR nimmt in der Regel mehrere Wochen oder Monate in Anspruch.

Sichtbarkeit (Telemetrie)	Ein EDR überwacht und sammelt Prozesse, laufende Anwendungen, Dateiänderungen, Benutzeraktivitäten, Cloud-Verbindungen, angrenzende Geräte und sogar **Netzwerkverbindungen zum und vom Endgerät.** Die besten EDR-Lösungen vereinen die Telemetrie aller Agenten in einer zentralen IT-Asset-Übersicht.	Je nach Netzwerkarchitektur überwacht und sammelt ein NDR Metadaten wie Quell-IP- und Ziel-IP-Adressen sowie die entsprechenden Portnummern. Bei sNAT ist die Quell-IP-Adresse nicht verfügbar. **Alle relevanten Datenfelder werden häufig mit TLS verschlüsselt**, wenn kein SSL-Offloading implementiert ist.
Vorbehalte gegen einen wirksamen Einsatz	Die **EDR-Abdeckung** ist der Schlüssel zu einer angemessenen Sichtbarkeit, um nicht überwachte Endpunkte (Schatten-IT) zu minimieren. **Die Telemetrie zur Asset-Erkennung**, die die meisten Best-of-Breed-EDR-Lösungen bieten, muss genutzt werden, um eine EDR-Deckung von nahezu 100 % zu erreichen. Vergessen Sie nicht, **den EDR-Deinstallationsschutz zu aktivieren.**	Sorgen Sie dafür, dass **VPN** in hybriden Umgebungen immer eingeschaltet ist, sonst kann ein NDR den Netzwerk von Remote-Mitarbeiter nicht überwachen. **Erwägen Sie die Entschlüsselung des Datenverkehrs mit SSL-Offloading**, da andernfalls die meisten Meldungen ohne Kontext nicht umsetzbar sind. Vermeiden Sie die Erstellung von (unsicheren) Routen zwischen segmentierten Netzwerken zum NDR, da dies den Mehrwert dieser Segmentierung potenziell neutralisiert
Missbrauchsversuche	Erkennt Missbrauchsversuche mithilfe von Verhaltensanalysen und Threat Intelligence. Liefert Echtzeit-Warnungen und kann den betroffenen Endpunkt isolieren.	Überwacht Netzwerkanomalien, die auf einen Angriff hinweisen, hat aber Probleme mit Angriffen, die ausschließlich auf der Host-Ebene stattfinden.

	EDR	NDR
Daten (Kronjuwelen)	Endgeräte enthalten/ verwalten oft die Kronjuwelen (wie Daten), die Angreifer suchen. Selbst wenn eine frühere Erkennungsmöglichkeit verpasst wird, stellt EDR sicher, dass es mehrere Gelegenheiten entlang des gesamten Angriffsverlaufs gibt, um einen Angreifer zu identifizieren und zu stoppen, bevor erheblicher Schaden entsteht.	Überwacht verdächtige Datenübertragungen und Netzwerkkommunikationen, die möglicherweise sensible Daten betreffen. NDR bietet jedoch keinen Einblick in spezifische Aktionen an den Endpunkten, sodass diese leicht mit harmlosen IT-Verwaltungsaktivitäten wie Backups verwechselt werden könnten. Sobald die Datenexfiltration zu externen IP-Adressen entdeckt wird, ist es oft schon zu spät.

Moderne Cyber-Bedrohungen erkennen

Der jährlich aktualisierte ENISA Threat Landscape (ETL)-Bericht zeigt, dass Ransomware, Phishing und Lieferkettenangriffe zu den größten Herausforderungen für Unternehmen gehören. Die Erkennung dieser Bedrohungen erfordert eine sorgfältige Abwägung zwischen der Maximierung der Erkennungsfähigkeiten und der Minimierung von Fehlmeldungen. EDR und NDR bieten unterschiedliche Vorteile bei der Erkennung dieser modernen Bedrohungen.

	EDR	NDR
Seitwärts Bewegung (Lateral Movement)	Verfolgt ungewöhnliche interne Netzwerkverbindungen, Zugriffsrechteerweiterungen und Prozessanomalien auf Endgeräten. Kann Angreifer erkennen, die versuchen, sich zwischen Systemen zu bewegen oder Zugriffsrechte zu erweitern.	Überwacht je nach Netzwerkarchitektur den Datenverkehr zwischen internen Systemen auf ungewöhnliche Verbindungen oder einen ungewöhnlichen Datentransfer. Auffällige Ereignisse sind aufgrund des fehlenden Endpunktkontextes schwer zuzuordnen.
Ransomware	Erkennt die Verschlüsselung von Massendateien durch Überwachung des Dateisystems und Verhaltensanalyse. Isoliert kompromittierte Endpunkte und beendet die schädlichen Prozesse.	Überwacht ungewöhnlichen ausgehenden Datenverkehr zu C2-Servern, hat aber aufgrund von TLS und des kurzen Lebenszyklus der C2-Infrastruktur (Minuten bis Tage) Schwierigkeiten, Fehlmeldungen zu vermeiden.

Phishing (Versuche)	Überwacht E-Mail-Clients und Browser, um schädliche Anhänge oder URLs abzufangen. Erkennt Versuche, Anmeldedaten zu stehlen, und blockiert die Installation schädlicher Software.	Identifiziert ungewöhnlichen Netzwerkverkehr oder DNS-Anfragen an Phishing-Domänen. Eingeschränkte Möglichkeiten bei der Verhinderung der anfänglichen Kompromittierung und durch die Browser-seitige Erzwingung von HTTPS.
Angriffe in der Lieferkette	Überwacht kompro-mittierte Anwendungen auf ungewöhnliches Verhalten und nutzt IOCs, um vertrauenswürdige Software zu erkennen, die sich schädlich verhält.	Erkennt unvorhergesehene Kommunikationen von kompromittierter Software. Hat Schwierigkeiten, ohne Endpunktkontext legitimen von schädlichem Datenverkehr zu unterscheiden.

Reaktionsmöglichkeiten zur Bekämpfung von aktiven Bedrohungen

Die Erkennung von Bedrohungen ist nur ein Aspekt von EDR und NDR. Erst die Fähigkeit, effektiv zu reagieren, macht eine Lösung leistungsfähig.

- **EDR bietet erweiterte Reaktionsmöglichkeiten,** die über die einfache Meldung an die Sicherheitsteams hinausgehen. Die EDR-Lösung ermöglicht direkte Eingriffe, einschließlich der Isolierung eines Endpunkts, der Beendigung schädlicher Prozesse und der Wiederherstellung von durch Malware vorgenommenen Änderungen. Auf diese Weise können Unternehmen Bedrohungen einschränken und neutralisieren, bevor sie eskalieren und zu Sicherheitsverletzungen führen.
- **Im Gegensatz hierzu sind die Reaktionsmöglichkeiten von NDR begrenzt.** In der Regel kann ein NDR nur TCP-Reset-Pakete senden, um verdächtige Verbindungen zu unterbrechen, wodurch die Bedrohung nicht beseitigt wird. Das Ergebnis ist oft eine Verzögerung bei der Behebung des Problems, da die wahre Ursache der Bedrohung aktiv bleibt. Darüber hinaus kann es ohne den detaillierten Überblick, den ein EDR bietet, schwierig sein, das Gerät zu identifizieren, von dem die schädlichen Netzwerkaktivitäten ausgehen, insbesondere in komplexen oder schlecht dokumentierten Netzwerkumgebungen.

In praktischen Sicherheits-Workflows **wechseln Analysten oft vom NDR zum EDR**, wenn sie die Tiefe und den Kontext einer Warnmeldung verstehen müssen. Dabei kann ein NDR verdächtigen Datenverkehr aufzeigen. Ohne Einblicke auf Endpunktebene ist es jedoch schwierig, den vollständigen Hintergrund zu ermitteln, z. B. welcher Prozess das Verhalten ausgelöst hat oder ob schädliche Änderungen stattgefunden haben. Die EDR-Lösung schließt diese Lücke, indem sie die notwendige Genauigkeit für effektive, fundierte Reaktionen bietet.

Bewertung häufiger Missverständnisse

NDR ist manipulationssicher

Ein weit verbreitetes Missverständnis ist es, dass ein NDR als Out-of-Band-Lösung manipulationssicher ist, wodurch es eine zuverlässigere Option für die Netzwerksicherheit darstellt. Für Angreifer ist es möglicherweise schwieriger, ein NDR zu deaktivieren, da es getrennt von den Endpunkten arbeitet. Aber das macht es auch nicht unangreifbar. Angreifer können ein NDR umgehen, indem sie verschlüsselte Kommunikation oder vertrauenswürdige Plattformen wie GitHub nutzen, um Malware zu verbreiten, so dass ein NDR ihre Aktivitäten nicht mehr überwachen kann.

Der Manipulationsschutz von EDR auf der Kernel-Ebene stellt dagegen sicher, dass es auch dann funktionsfähig bleibt, wenn ein Angreifer Admin-Rechte auf einem kompromittierten Gerät erlangt. Wenn jemand versucht, den Agenten zu manipulieren, wird ein kritischer Alarm ausgelöst. Es gibt zwar Software zum unberechtigten Beenden eines EDR. Um diese als Angreifer zu nutzen, muss man jedoch häufig über administrative Berechtigungen auf einem Endgerät verfügen, so dass sich für ein EDR mehrere Erkennungsmöglichkeiten auf dem Weg des Angreifers zum Erlangen dieser Berechtigungen ergeben.

NDR ist für die Erkennung von Angriffen auf nicht verwaltete Geräte unerlässlich

Ein weiteres Argument für den Einsatz eines NDR ist sein Nutzen bei der Überwachung von Umgebungen, in denen keine Endpunkt-Agenten eingesetzt werden können, wie z. B. bei OT-, IoT- und Legacy-Systemen. Diese Systeme machen jedoch in der Regel nur einen kleinen

Teil der Gesamtinfrastruktur aus und haben oft nur eine begrenzte Netzwerkexposition. Die effektivere Strategie besteht darin, diese Altsysteme zu isolieren und die sie umgebende IT-Infrastruktur mit einem EDR zu schützen, um sicherzustellen, dass Angreifer nicht auf kritischere Systeme ausweichen können.
Darüber hinaus bietet ein NDR zwar Einblicke in netzwerkbasierte Angriffe, doch die meisten Angriffe sind heute auf Endgeräte gerichtet und nutzen häufig Fernzugriffsmethoden, um über das Internet in Systeme einzudringen. Nach unserer Erfahrung sind Angriffe wie Ransomware immer mit einer Remote-Kompromittierung verbunden, bei der ein Endpunkt der Zugangspunkt ist. Ein EDR ist für diese Szenarien ideal geeignet und bietet umfassende Erkennungs- und Reaktionsmöglichkeiten.

Fazit: EDR als Schwerpunkt, NDR als Ergänzung

Nach der Bewertung der Fähigkeiten und Limitierungen von EDR und NDR wird deutlich, warum ein EDR die Grundlage einer effektiven Cybersicherheitsstrategie bildet. Ein EDR bietet Echtzeit-Sichtbarkeit, fortschrittliche Reaktionsmöglichkeiten und den notwendigen Kontext für die Erkennung und Bekämpfung von Bedrohungen.

Ein NDR kann zwar eine ergänzende Rolle spielen, indem es zusätzliche Anomalieerkennung für nicht verwaltete Geräte oder laterale Bewegungen innerhalb bestimmter Netzwerkarchitekturen bietet. Es sollte aber nicht als die primäre Lösung betrachtet werden. Ein NDR ist am effektivsten, wenn es ein EDR unterstützt und dabei hilft, die Lücken zu schließen, die in komplexen Sicherheitsumgebungen entstehen. Im Vergleich zu einem EDR ist ein NDR jedoch in Bezug auf Erkennung, Reaktion und allgemeine betriebliche Effektivität unzureichend.

Um die besten Ergebnisse zu erzielen, sollten sich Unternehmen auf die Implementierung einer erstklassigen, verwalteten EDR-Lösung konzentrieren. Dabei sollte sichergestellt werden, dass die Lösung ordnungsgemäß konfiguriert ist und über einen wirksamen Schutz vor Manipulationen sowie über Playbooks für die Reaktion auf Vorfälle verfügt. Ein NDR sollte als optionale Schicht betrachtet werden, die nur dann eingesetzt wird, wenn spezielle Anforderungen an die Transparenz bestehen, die ein EDR allein nicht erfüllen kann.

Fallstudien

KeyTec Niederlande

Als die Berichte über Ransomware in der Branche immer häufiger wurden, beschloss das Fertigungsunternehmen KeyTec Netherlands, Maßnahmen zu ergreifen. Erfahren Sie, wie Eye Security das Unternehmen dabei unterstützt hat, seine Abwehrkräfte proaktiv zu stärken und eine Sicherheitskultur zu schaffen.

Signature Foods

Da die Internetkriminalität immer raffinierter wird, wenden sich Unternehmen vermehrt an externe Anbieter. Erfahren Sie, wie Eye Security Signature Foods in nur wenigen Wochen zu einem umfassenden Cyberschutz verholfen hat.

Bei Eye Security konzentrieren wir uns auf die Grundlagen, priorisieren die Endpunktsicherheit und empfehlen den ergänzenden Einsatz von Netzwerküberwachung, um Lücken zu schließen. Auf diese Weise ermöglichen wir die Entwicklung einer robusten Sicherheitsstruktur, die Angreifern immer einen Schritt voraus ist und auf neue Bedrohungen reagieren kann.

www.eye.security