DARKTRACE

Von EDR-Abhängigkeit zu Resilienz

Die Lücke zwischen Netzwerken und Endpunkten schließen

Auf einen Blick

EDR und XDR sind unverzichtbar, wurden allerdings nicht entwickelt, um den gesamten Umfang moderner, bereichsübergreifender Bedrohungen abzuwehren. Angreifer nutzen Schwachstellen zwischen Endpunkten, Netzwerken, Cloud-Diensten und OT-Umgebungen aus – genau dort, wo die Transparenz nachlässt und Punktlösungen Schwierigkeiten haben, die Zusammenhänge herzustellen.

Dieses E-Book zeigt, wie Unternehmen ihre Resilienz aufbauen können. Es untersucht, warum Endpunkt-zentrierte Abwehrmaßnahmen allein nicht ausreichen und wie die Vereinheitlichung von Endpunkt-Prozessdaten mit Netzwerktelemetrie eine stärkere Grundlage für die Erkennung, Untersuchung und Reaktion auf Bedrohungen schafft. Dabei werden wir Beispiele für Angriffe hervorheben, die Endpoint-Tools umgangen haben, die Belastung, die diese Lücken für SOC-Teams darstellen, und den Weg in die Zukunft mit gemischter Telemetrie.

EDR/XDR ist notwendig, aber unvollständig
Diese Tools schützen Endpunkte gut, bieten jedoch keine Transparenz über nicht verwaltete Geräte, Umgebungen ohne Agents und netzwerkbasierte Angriffe hinweg.

Gemischte Telemetrie schließt Untersuchungslücken
Die Kombination von Netzwerkaktivitäten mit Endpunkt-Prozessdaten liefert Analysten eine einheitliche Übersicht, die Fehlalarme reduziert, die Selektierung beschleunigt und Bedrohungen früher eindämmt.

Resilienz erfordert eine neue SOC-Grundlage
Selbstlernende, adaptive Plattformen, die auf Netzwerktransparenz basieren, bieten den erforderlichen Kontext und die Effizienz, um die Überlastung von Analysten zu reduzieren, die MTTR zu verkürzen und Blindstellen in verschiedenen Bereichen abzudecken.

Warum EDR notwendig, aber nicht ausreichend ist

Heutzutage investieren die meisten Unternehmen in Endpoint Detection and Response (EDR) oder dessen neuere Weiterentwicklung, Extended Detection and Response (XDR).

EDR wurde **speziell** für Endgeräte entwickelt. Es überwacht Prozesse, den Arbeitsspeicher und Protokolle auf Host-Ebene und ermöglicht die Eindämmung und Behebung von Problemen auf Geräteebene.

XDR wurde von EDR-Anbietern entwickelt, **um das Problem der Ausbreitung zu lösen,** indem Warnmeldungen von mehreren Sicherheitstools auf einer einzigen Plattform zusammengeführt werden. Doch in der Praxis sind die meisten XDR-Angebote nach wie vor EDR-zentriert. Sie erweitern die Sichtweite nach außen, sind aber weiterhin an einen Endpunkt-Agent gebunden.

57 % der Unternehmen planen, ihre XDR-Tools um Network Detection and Response (NDR) zu erweitern.

Gartner, 2023

Erfassungslücken
Wenn die Erkennung auf die Endpunkt-Telemetrie verankert ist, verbleiben Blindstellen in Netzwerken, nicht verwalteten Geräten, Cloud-Workloads und Identitätssystemen. EDR-zentriertes XDR kann laterale Bewegungen oder Aktivitäten in Umgebungen ohne Agents wie OT nicht erkennen, wodurch kritische Infrastruktur ungeschützt bleiben.

Fragmentierte Reaktion
Bei den meisten NDR-Tools fehlt der Endpunktkontext, sodass Analysten zwischen Konsolen hin- und herwechseln müssen, um einen Angriff zu analysieren. Dieser manuelle Aufwand verlangsamt die Ermittlungen, erhöht die MTTR und führt dazu, dass Bedrohungen, die sich zwischen Endpunkten und Netzwerken bewegen, unentdeckt bleiben.

EDR konzentriert sich auf ...

„bekannte bösartige" Bedrohungen: Dies bedeutet, dass es nur dann eine Warnmeldung auslöst, wenn die Aktivität auf dem Endpunkt den „bekannten" Kriterien oder vordefinierten Regeln/Signaturen entspricht.

EDR weiß nicht ...

was für einen Host normal oder anomal ist. Es richtet sich nach den Regeln, die auf dem bekannten Verhalten von Angreifern basieren. Das ist für bereits bekannte Bedrohungen ausreichend, lässt jedoch Lücken bei der Abdeckung von bisher unbekannten Bedrohungen oder Angriffen, die legitime Tools ausnutzen, um sich zu verstecken.

Das Ergebnis ...

Ransomware, Datenexfiltration und mehrstufige Kampagnen sind trotz starker Endpunktabdeckung erfolgreich. EDR ist nach wie vor äußerst effektiv bei der Überwachung der Host-Aktivitäten, aber moderne Angreifer beschränken sich nicht mehr nur auf Endpunkte. Sie nutzen die Lücken zwischen Bereichen aus, wo die Sichtbarkeit nachlässt und Analysten Schwierigkeiten haben, die Zusammenhänge zu erkennen.

Nachweise
Wo die Reichweite von EDR endet

EDR-Umgehung mit Agent-Killern

Angreifer verwenden Tools wie EDRKillShifter und EDRSilencer, um Endpunkt-Agents zu deaktivieren und so Endpunkt-basierte Abwehrmaßnahmen sofort außer Kraft zu setzen. Diese Taktiken zeigen, wie leicht Gegner Agent-basierte Sicherheitsmaßnahmen neutralisieren können, unabhängig davon, wie ausgefeilt diese sind.

Die Lektionen des Red Teams der CISA

Eine CISA-Bewertung der kritischen US-Infrastruktur ergab, dass eine übermäßige Abhängigkeit von EDR zu gefährlichen Lücken in der Netzwerkschicht führte. Die Angreifer blieben monatelang unentdeckt, ohne dass hostbasierte Warnmeldungen ausgelöst wurden – ein Beweis dafür, dass isolierte Transparenz nicht ausreicht.

Zero-Day-Exploit in der Netzwerkebene

Während der 2024 Ivanti Connect Secure Exploitation wurden durch Netzwerktelemetrie 11 Tage vor der öffentlichen Bekanntgabe Anomalien entdeckt, die einen Missbrauch von Anmeldedaten und C2-Aktivitäten aufdeckten, die für Endpunkt-Tools unsichtbar waren. NDR sorgte für die nötige Transparenz, um die Bedrohung frühzeitig einzudämmen.

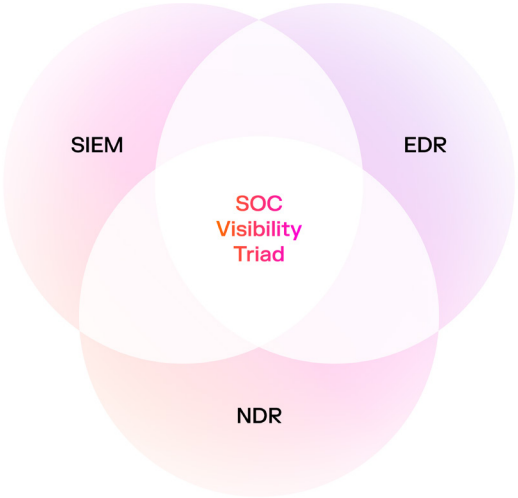
Aufbau einer widerstandsfähigen Abwehr

EDR ist grundlegend, aber nur in Verbindung mit vollständiger Netzwerktransparenz wird es Teil einer umfassenden, widerstandsfähigen Sicherheitsarchitektur. XDR-Lösungen sind zwar umfassender, stützen sich jedoch nach wie vor stark auf hostbasierte Überwachung und bieten oft keine native Netzwerktransparenz.

Einheitliche Transparenz über Endpunkte, Netzwerke, Cloud, OT und Identitäten hinweg.

Integrierte Telemetrie von verwalteten und nicht verwalteten Assets.

Adaptive Systeme, die normales Verhalten verstehen und Unbekanntes erkennen.



Umgehung von EDR

Aktivitäten nach dem Exploit von Ivanti CS/PS-Geräten

Angriffsbeispiel

Diese Ivanti-Kampagne beweist, dass Angreifer genau wissen, wo die Sichtbarkeit von Endgeräten endet. Sie nutzen nicht verwaltete Netzwerkressourcen aus, bewegen sich lateral und verstecken sich im verschlüsselten Datenverkehr. Für die Entwickler von Sicherheitslösungen besteht die eigentliche Herausforderung jedoch nicht nur in der Erkennung, sondern auch in der Weiterleitung an die Mitarbeiter im SOC, die alle Informationen auswerten müssen.

Initiales Beaconing auf seltene externe IP festgestellt. Endpunkt-Agents kamen hier nicht zum Einsatz, da es sich bei der kompromittierten Ivanti-Appliance um eine Netzwerkressource und nicht um einen herkömmlichen Endpunkt handelt. Nur die Netzwerktransparenz hat die Anomalie früh aufgedeckt.

Sekundäre Signalisierung an einen anderen ungewöhnlichen Host erkannt. Die Angreifer erweiterten ihre Zugriffsmöglichkeiten über die Netzwerkebene. Ohne Agent-Abdeckung wären die EDR-Tools nicht in der Lage gewesen, Korrelationen herzustellen.

Ausgenutzte Validierungsaktivität mithilfe von OAST-Diensten identifiziert. Angreifer bestätigten die Ausnutzung über Out-of-Band-Kanäle. Diese Überprüfungen betrafen nie den Endpunkt-Stack, was verdeutlicht, warum Netzwerktelemetrie so wichtig ist.

Große POST-Übertragungen von .dat/.sys-Dateien auf einen externen Server ließen Exfiltration von Hostdaten erkennen. Sensible Systemdateien wurden über das Netzwerk abgezogen. Die Hostprozesse von Endpunkttools konnten diesen ausgehenden Datenverkehr nicht erkennen.

Schädliche Rust-ELF-Payloads, die von AWS S3-Endpunkten bereitgestellt werden. Die Payload-Lieferung nutzte einen Cloud-Dienst. Selbst wenn EDR an anderer Stelle vorhanden war, umgingen diese Eindringlinge die hostbasierten Abwehrmechanismen, indem sie über den Netzwerkrand eindrangen.

Web-Shells und JavaScript-Stealer werden eingesetzt, um Anmeldedaten zu sammeln. Der Diebstahl von Anmeldedaten fand im Rahmen einer Netzwerk-Appliance statt, nicht an einem Benutzerendpunkt. Das bedeutet, dass die Identitätskompromittierung außerhalb der Reichweite von EDR stattfand.

Netzwerkscans und laterale Bewegungen innerhalb der Umgebung beobachtet. Klassisches Beispiel für nicht verwaltete Assets, die von einem Angreifer durchlaufen werden. EDR kann diese Geräte nicht instrumentieren, sodass Analysten ohne NDR „blind“ sind.

Verschlüsselter Command-and-Control-Datenverkehr, der über DNS getunnelt wird, gefolgt von der Bereitstellung von Cryptominern. Verdeckte Netzwerkkanäle ermöglichten Persistenz. Endpunktbasierte Überwachung kann verschlüsselten DNS-Missbrauch nicht zuverlässig erkennen – hierfür ist eine Anomalieerkennung auf Netzwerkebene erforderlich.

Die Netzwerktelemetrie hat diese Anomalien bereits Tage vor der öffentlichen Bekanntgabe der Sicherheitslücken aufgedeckt. Die Erkennung erfolgte nicht anhand von Signaturen oder Endpunktprotokollen, sondern anhand von Verhaltensanomalien im Netzwerkverkehr, was zeigt, warum eine bereichsübergreifende Abdeckung erforderlich ist.

Der Knackpunkt für das SOC
Blindstellen, Burnout und Geschäftsrisiken

Außerhalb der Sichtbarkeit

Angreiferorientierte Erkennungsmethoden können neuartige Bedrohungen nur schwer erkennen, da sie auf statischen Regeln sowie historischen Angriffsdaten basieren und sich auf die Identifizierung „bekannter Bedrohungen" konzentrieren. Diese Tools übersehen häufig schädliche Aktivitäten, die oberflächlich betrachtet legitim erscheinen, wie beispielsweise:

- Living off the Land (LotL)
- Missbrauch gültiger Anmeldedaten
- Insider-Bedrohungen
- Autorisierte Anwendungen von Drittanbietern

Mehr Komplexität = mehr Probleme

In OT-Umgebungen konzentrieren sich die meisten Anbieter auf die Sichtbarkeit von Assets oder regelbasierte Erkennung, ohne zu modellieren, wie Angreifer von der IT zur OT gelangen, exponierte CVEs ausnutzen oder durch falsch konfigurierte Segmentierung kritische Vorgänge stören können.
Ohne echte Konvergenzmodellierung bleiben Abwehrsysteme auf isolierte Ansichten und eine unvollständige Bedrohungsabdeckung beschränkt.

Die Lösung:
Aufbau von Resilienz mit gemischter Telemetrie

Die Lösung für diese Herausforderungen besteht darin, die Endpunkt-Prozessdaten der untersten Ebene und die Netzwerktelemetrie in einem einzigen Datenstrom zusammenzuführen. Die Zusammenführung dieser Datenquellen am Erfassungsort bewirkt:

Schnellere Untersuchungen
Vereinheitlichung von Endpunkt-Prozessdaten und Netzwerkaktivitäten zur Beschleunigung der Analyse.

Einzelansicht von Vorfällen
Verfolgung von Prozessaktivitäten und lateralen Bewegungen, ohne Fragmente aus mehreren Tools zusammenzufügen.

Verbesserte Ergebnisse
Reduzierung von Fehlalarmen, Verkürzung der Selektierungszyklen und Stärkung der Eindämmung.

Diese Fähigkeit **ersetzt jedoch nicht** die bestehenden EDR- oder XDR-Investitionen, sondern ergänzt sie. Endpunkt-Schutzmaßnahmen sind nach wie vor wichtig, aber wenn sie mit Einblicken auf Netzwerkebene kombiniert werden, decken sie auch nicht verwaltete Geräte, Cloud-Workloads und verschlüsselten Datenverkehr ab.

Das Ergebnis ist ein Sicherheitsstack, der die Realität moderner Bedrohungen widerspiegelt und nicht die Grenzen der Endpunkt-zentrierten Sichtbarkeit.

Die SOC-Grundlage überdenken

Um mehr als nur punktuelle Abwehrmaßnahmen zu erreichen, benötigen Sicherheitsteams eine Grundlage, auf der das gesamte SOC aufbauen kann. Diese Grundlage bildet das Netzwerk. Jeder Endpunkt, jede Cloud-Workload, jedes OT-Gerät und jede Identität hinterlässt letztendlich Spuren im Netzwerkverkehr. Indem sie das Netzwerk als „Heimatbasis“ betrachten, erhalten Organisationen eine einheitliche Perspektive, durch die alle anderen Bereiche verstanden werden können.

Diese Grundlage bedeutet nicht, dass es eine Einheitslösung gibt. Jedes Unternehmen verfügt über eine einzigartige digitale Infrastruktur – eine individuelle Kombination aus Cloud-Diensten, Legacy-Infrastruktur, Remote-Endpunkten und OT-Umgebungen. Statische, vordefinierte Erkennungen können nicht jeden neuen Angriffspfad oder jede Konfigurationsabweichung vorhersehen. Deshalb ist Anpassungsfähigkeit gefragt: ein System, das die normalen Muster Ihrer Umgebung erlernen, sich mit ihr weiterentwickeln und auftretende Anomalien hervorheben kann.

Auf der Grundlage der Netzwerktransparenz bietet eine einheitliche Plattform entscheidende Vorteile:

Anpassungsfähigkeit durch kontinuierliches Selbstlernen, auch wenn sich Umgebungen und Bedrohungen ändern.

Effizienz durch Konsolidierung der bereichsübergreifenden Erkennung und Reaktion, wodurch die Anzahl der Anbieter begrenzt wird.

Resilienz durch die Korrelation von Telemetriedaten in Echtzeit, die Reduzierung von Störsignalen und die Hervorhebung wichtiger Vorfälle.

Vorteile von Darktrace

Darktrace ist ein anerkannter Branchenführer im Bereich NDR dank seiner selbstlernenden KI ™, die das normale Verhalten Ihres gesamten Netzwerks versteht, Anomalien intelligent erkennt und komplexe Bedrohungen ohne historische Angriffsdaten abwehrt.

Durch diesen Ansatz, der auf modernem, automatischem maschinellem Lernen basiert, kann Darktrace neue, unbekannte und interne Bedrohungen erkennen, die von herkömmlichen Tools nicht erfasst werden und für andere Anbieter nicht erkennbar sind.

Da Angriffe mittlerweile E-Mails, Cloud, OT, SaaS und Endpunkte umfassen, hat Darktrace einen entscheidenden Sprung nach vorne gemacht: die Vereinheitlichung von Telemetrie und Kontext über diese Bereiche hinweg und die großflächige Anwendung KI-gestützter Untersuchungen. Durch die Kombination von Endpunktdaten auf Prozessebene mit Netzwerktransparenz ermöglicht Darktrace Sicherheitsteams, den gesamten Lebenszyklus eines Angriffs zu erkennen und autonom darauf zu reagieren, wodurch Blindstellen, Untersuchungszeiten und die Belastung der Analysten reduziert werden.

„Darktrace ist nicht nur Technologie. Es ist ein Instrument für **Vertrauensbildung, das gleichzeitig intelligentes Wachstum in unserer System- und** Cybersicherheitslandschaft rechtfertigt und unterstützt.“

- **CIO**

  Behördliche Dienstleistungen

Schauen Sie rein

Darktrace / Endpunkt-Lösungsübersicht

Kurzinformation herunterladen ↗

Demo anfordern

Erfahren Sie, was Darktrace in Ihrer Umgebung entdeckt.

Demo buchen ↗