

DIE GRÖSSTEN VORTEILE VON XDR

XDR-Lösungen spiegeln die kontinuierliche Weiterentwicklung von Cybersecurity-Produkten wider. Tatsächlich stellt XDR den Höhepunkt der Entwicklung von Cybersecurity-Produkten dar und geht weit über den Rahmen von Endpoint Detection and Response (EDR)- und Managed Detection and Response (MDR)-Produkten hinaus.

XDR bietet Einblick in die gesamte Angriffsfläche und umfasst sowohl Cloud- als auch On-Premises-Umgebungen. Mit XDR gewinnen Unternehmen eine verbesserte Bedrohungserkennung und einen besseren Schutz. Sie können präzise Echtzeit-Bestimmungen auf Grundlage von Datenpunkten treffen, die über eine Reihe von Bedrohungseintrittspunkten erfasst und konsolidiert wurden.

Hier sind vier der größten Vorteile von XDR und was sie für Ihr Unternehmen bedeuten.



1. Schnellere Incident Response

XDR hilft Unternehmen, Bedrohungen dank seiner fortschrittlichen Analysefunktionen schneller zu erkennen und darauf zu reagieren.

Was das für Ihr Unternehmen bedeutet:



Es verhindert die Ausbreitung von Bedrohungen und minimiert die Auswirkungen



Es verringert die Wahrscheinlichkeit von Datenverlusten



Reduziert das Risiko von Reputationsschäden

Aber wie viel schneller ist XDR? Werfen Sie einen Blick auf die Tabelle unten, um es herauszufinden.

Wie lange dauert die Behebung in der Regel?

	Ohne XDR	Mit XDR
Typische BEC-Behebung (nur Gateway)	1-2 Monate	1-2 Stunden
Behebung von Identitätsdiebstahl	3-4 Wochen	1-2 Stunden
Behebung von Malware-Infektionen	3-4 Wochen	Ungefähr 1 Stunde
Lösung von Insider-Bedrohungen	3-6 Monate	~ 4 Stunden
Behebung von Erpressungsversuchen ohne XDR	Variabel	< 24 Stunden



2. Verbesserte Sichtbarkeit in Ihrer gesamten Security-Umgebung

XDR vereint die Telemetrie aller Ihrer Systeme von Servern, Netzwerken, Cloud, E-Mail und Endpunkten in einer einzigen Ansicht und bricht so Silos auf.

Was das für Ihr Unternehmen bedeutet:



Es bietet vollständige Übersicht über die Angriffsfläche



Es hilft, Schwachstellen oder Fehlkonfigurationen leichter zu erkennen



Es vereinfacht Compliance und Reporting dank klarerer Prüfpfade



3. Intelligenter Bedrohungserkennung

XDR verwendet KI, fortschrittliche Analytik und Algorithmen für maschinelles Lernen, die ihm helfen, komplexe, mehrstufige Angriffe abzuwehren, die herkömmliche Tools oft übersehen. Es kann sowohl bekannte Angriffe als auch unbekannte Zero-Day-Bedrohungen stoppen. Darüber hinaus bietet es kontextbezogene Einblicke anstelle isolierter Warnungen und liefert Details zu Angriffsarten und -techniken.

Was das für Ihr Unternehmen bedeutet:



Es hält Sie den komplexen Taktiken der Angreifer immer einen Schritt voraus



Es reduziert die Alarmmüdigkeit durch die Automatisierung der Erkennung



Bietet ein besseres Verständnis der Taktiken, Techniken und Verfahren (TTPs) von Angreifern



4. Geringere Sicherheitskosten

Da XDR Ihre Toolsets optimiert und Automatisierung nutzt, werden Ihre Security-Vorgänge effizienter und kostengünstiger.

Was das für Ihr Unternehmen bedeutet:



Verringerung der Doppelzahlungen für Security-Tools



Es werden Mittel für Investitionen in anderen Bereichen freigesetzt



Der ROI bei Security-Investitionen wird maximiert



Dies sind bei weitem nicht die einzigen Vorteile von XDR. Um mehr über die Vorteile und die Funktionsweise von XDR zu erfahren, laden Sie unser E-Book „XDR erklärt: Ein strategischer Ansatz zum Bedrohungsmanagement“ herunter.