

# Barracuda XDR Email Protection

E-Mail-Schutz für die Postfächer Ihrer Kunden - 24/7, 365 Tage im Jahr

E-Mail Angriffe sind komplexer und gefährlicher denn je und jeder Einzelne kann zum Ziel werden. Da 91 Prozent aller Cyberangriffe aus E-Mail-Bedrohungen heraus entstehen, benötigen Unternehmen E-Mail-Schutz, welcher basierend auf Technologie und menschlicher Expertise, für umfassende Sicherheit sorgt. Ab sofort können Sie Ihren Kunden ganzheitlichen Schutz bieten, der sich auf ein rund um die Uhr verfügbares Security Operations Center (SOC) stützt, in dem sich ein Team von Sicherheitsanalysten um Cybersecurity-Fragen kümmert und gleichzeitig einen proaktiven Ansatz verfolgt.

## Umfassender E-Mail-Schutz

Schützen Sie die E-Mail-Umgebungen Ihrer Kunden durch mehrere Schutzebenen. Dazu zählen Gateway Security-Lösungen, Posteingangsschutz kombiniert mit künstlicher Intelligenz und maschinellem Lernen sowie ein Team von Sicherheitsexperten, das die komplexen E-Mail-Bedrohungen von heute erkennt, prüft und darauf reagiert und so die Auswirkungen, die Angriffe auf Ihre Kunden haben, minimiert.

## Globales Netzwerk zur Erkennung von Bedrohungen

Unter Nutzung einer globalen Datenbank zur Bedrohungsanalyse und leistungsstarker KI verknüpft Barracuda seine E-Mail-Bedrohungserkennung mit dem MITRE ATT&CK® Framework, um Bedrohungen frühzeitig zu erkennen. Sogar das weitere Vorgehen der Bedrohung lässt sich prognostizieren, was die Festlegung effektiver Reaktionsstrategien vereinfacht.

## Bedrohungen rund um die Uhr erkennen und darauf reagieren

Ob Zero-Day-Phishing-Angriffe oder raffinierter Business Email Compromise - die Sicherheitsexperten in unserem SOC verhindern mittels Computer Vision, KI und maschinellem Lernen, dass E-Mail-Bedrohungen in die Umgebungen Ihrer Kunden gelangen. Unter Quarantäne gestellte verdächtige oder bösartige E-Mails werden dokumentiert und ermöglichen so einen umfassenden Einblick in die Umgebungen Ihrer Kunden.

### Weitere Informationen finden Sie unter:

[barracudamsp.com/barracuda-xdr](https://barracudamsp.com/barracuda-xdr)

## Das mehrschichtige Barracuda XDR-Sicherheitskonzept im Überblick:

**XDR** - Eine Plattform, die für erhöhte Transparenz sowie erweiterte Erkennung und Reaktion sorgt. In einem Security Operations Center (SOC) kümmert sich eine Gruppe erfahrener Sicherheitsexperten rund um die Uhr um den Support und bietet gleichzeitig ein proaktives Cybersecurity-as-a-Service-Modell für MSPs.

**XDR Endpoint Security** - Weitet die Erkennungs- und Reaktionsfunktionen auf Endpoints aus und vereinheitlicht diese, um Geräte vor häufigen Bedrohungen, einschließlich Malware und Ransomware, zu schützen.

**XDR Email Security** - Bietet umfassende E-Mail-Sicherheit, die Gateway-Security, Schutz vor kompromittierten Konten und vieles mehr umfasst und die Auswirkungen, die ein Angriff auf die E.

**XDR Cloud Security** - Schützt die Cloud-Umgebungen Ihrer Kunden vor unbefugten Zugriffen auf Postfächer in der Cloud, Umgebungsänderungen auf Administratoren Ebene, fehlgeschlagenen Logins oder Brute-Force-Angriffen.

**XDR Network Security** - Erkennt potenzielle Bedrohungsaktivitäten in Ihrem Netzwerk wie Command-and-Control-Verbindungen, Denial-of-Service-Angriffe, Datenexfiltration und Erkundungsversuche.

**XDR Server Security** - Schützt die unternehmenskritischen Server Ihrer Kunden vor Password Spraying, Brute-Force-Angriffen und Privilegien Erweiterung.

## Hauptmerkmale

- **Schützt** vor Spam, Malware, Viren, Spear Phishing und anderen E-Mail-Bedrohungen
- Kann Angriffstaktiken nachvollziehen und das weitere Vorgehen prognostizieren durch die Zuordnung von Erkennungsregeln von **MITRE ATT&CK® Framework Erkennungslücken identifizieren**
- Führt Daten aus vorhandenen Sicherheits-Tools mit verschiedenen Quellen zusammen und erhöht so die Transparenz
- Macht Bedrohungsaktivitäten über das **XDR Multi-Tenancy Dashboard** sichtbar
- Nutzt die Analysefunktionen von **SIEM-Systemen**
- Unterstützt **individuelle Warnmeldungen** und **Self-Service-Berichte**
- Bietet **Rund-um-die-Uhr-SOC-Support** und Problembehebung
- Unterstützt die Einhaltung zentraler brancheninterner und gesetzlicher Auflagen wie **kontinuierliches Monitoring und Protokollierung**

### Die wichtigsten Integrationen:

- Barracuda Cloud Email Gateway Defense
- Barracuda Impersonation Protection
- Barracuda Incident Response und viele mehr

Die vollständige Liste der integrierten Cloud-Infrastruktur finden Sie unter [www.barracudamsp.com/Barracuda-XDR-Integrations](http://www.barracudamsp.com/Barracuda-XDR-Integrations)



#### Über Barracuda MSP

Mit Barracuda MSP, der für MSPs zuständigen Geschäftseinheit von Barracuda Networks, können IT-Managed-Service-Provider ihren Kunden mit preisgekrönten Produkten und einer speziell entwickelten MSP-Plattform mehrschichtige Sicherheits- und Datensicherungsdienste anbieten. Der Partners-First-Ansatz von Barracuda MSP konzentriert sich auf die Bereitstellung von Aktivierungsressourcen, Channel-Know-how und robusten, skalierbaren MSP-Lösungen, die für die Arbeitsabläufe konzipiert sind, nach denen Managed Service Provider Lösungen erstellen und Geschäfte abwickeln. Weitere Informationen finden Sie unter [barracudamsp.com](http://barracudamsp.com).  
[@BarracudaMSP](#) | [LinkedIn: BarracudaMSP](#) | [smartermsp.com](http://smartermsp.com) | 617.948.5300 | 800.569.0155 | [sales@barracudamsp.com](mailto:sales@barracudamsp.com)