MSP Barracuda
Your journey, secured.

DATENBLATT

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.

Cyberhygiene betreiben

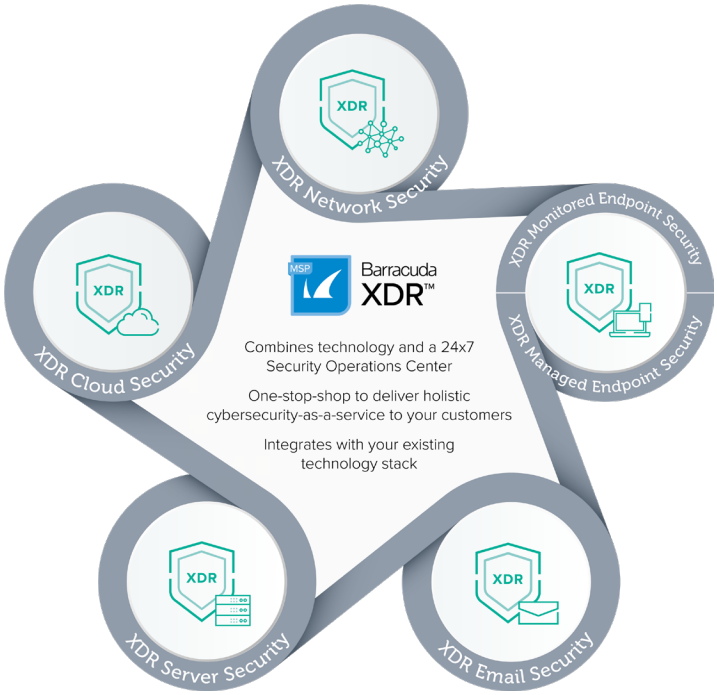
Schützen Sie Ihre Kunden vor den eskalierenden Cyberbedrohungen von heute, indem Sie auf die bewährten Cyberhygiene-Methoden von Barracuda XDR setzen. Durch das proaktive Monitoring von Barracuda XDR verfügen MSPs über eine erhöhte Transparenz und können mit der Unterstützung eines rund um die Uhr verfügbaren Security Operations Centers (SOC) Bedrohungen schneller erkennen und besser darauf reagieren.

Auf Sicherheitsexpertise setzen

Stocken Sie interne Sicherheitsressourcen im Handumdrehen mit einem Team aus erfahrenen Sicherheitsexperten sowie einem erstklassigen SOC, das im Hintergrund arbeitet, auf, damit Sie Ihren Managed-Kunden rund um die Uhr proaktive Detection & Response-Services bieten können. Alle identifizierten Vorfälle werden untersucht und der MSP wird benachrichtigt und bei der Problemlösung unterstützt.

Mehrschichtige Sicherheitslösungen mühelos bereitstellen

Bauen Sie konzentrische Schutzringe um die Daten, Geräte und Benutzer Ihrer Kunden. Diese Defense-in-Depth-Strategie ist notwendig, um Unternehmen den Schutz zu bieten, den sie benötigen. Barracuda XDR schützt wichtige Angriffsvektoren wie Endpunkte, E-Mail, Cloud, Netzwerk und Server.



Weitere Informationen finden Sie unter:
barracudamsp.com/barracuda-xdr

Hauptmerkmale

Erhöhte Transparenz - Mit dieser Cloud-nativen MSP-Plattform können alle Kundenumgebungen über eine zentrale Konsole eingesehen werden. Zusätzlich analysiert die Barracuda XDR-Plattform auch Daten aus bestehenden Technologie-Stacks, um Unternehmen mehr Transparenz zu verschaffen.

Mehrschichtiger Schutz - Bauen Sie Schutzschichten rund um die Daten, Geräte und Benutzer Ihrer Kunden auf. Eine Defense-in-Depth-Strategie ist notwendig, um Unternehmen den Schutz zu bieten, den sie benötigen.

Umfassende Erkennung - Die stetig wachsende Liste der Technologie-Integrationen erlaubt es dem SOC-Team von Barracuda oft nachgefragte Datenquellen zu überwachen. Die proprietären Regeln basieren auf maschinellem Lernen (ML) und werden dem MITRE ATT&CK® Framework zugeordnet, sodass Barracuda XDR Bedrohungen schneller identifizieren, ihr weiteres Vorgehen prognostizieren und mögliche Erkennungslücken sofort schließen kann.

Threat Intelligence - Für bestmögliche Sicherheit nutzt Barracuda ein großes, globales Repository mit Bedrohungsindikatoren, das aus einem breiten Security-Intelligence-Feed aus verschiedenen vertrauenswürdigen Quellen gespeist wird, darunter auch das umfangreiche geistige Eigentum von Barracuda.

Rund-um-die-Uhr-SOC - Echtzeit-Überwachung von Bedrohungen und Anleitung durch Sicherheitsexperten, die in Teams rund um die Uhr Support bieten. Zu den SOC-Bereichen zählen Security, Orchestration, Automation & Response (SOAR) und maschinelles Lernen, um sicherzustellen, dass nur legitime Warnungen zeitnah untersucht und eskaliert werden.

Dokumentierter Mehrwert - Es lassen sich markenfähige und benutzerdefinierte Berichte erstellen, die den Kunden den Wert der geleisteten Arbeit vor Augen führen.

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.

MSP Barracuda®
Your journey, secured.

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 Information finden Sie unter barracudamsp.com.

@BarracudaMSP | LinkedIn: BarracudaMSP | smartermsp.com | 617.948.5300 | 800.569.0155 | sales@barracudamsp.com