Barracuda XDR

Ein einheitlicher Cybersecurity-Ansatz

Cybersecurity ist ein Prozess. Heutzutage erfordern die wichtigsten Best Practices im Bereich Cybersecurity mehr als nur eigenständige Sicherheitsprodukte. Im Gegensatz zu vielen Mitbewerbern kombiniert Barracuda eXtended Detection & Response (XDR) seine fortschrittliche Analyseplattform mit einem 24/7 Security Operations Center (SOC).

Cybersecurity-Ansatz optimieren

Schützen Sie Ihr Unternehmen vor den allgegenwärtigen Cyberbedrohungen von heute, indem Sie mit Barracuda XDR bewährte Cybersecurity-Praktiken einsetzen. Barracuda XDR ermöglicht Ihrem Team, dank eines rund um die Uhr verfügbaren Security Operations Centers (SOC) Bedrohungen proaktiv zu erkennen, zu schützen und darauf zu reagieren.

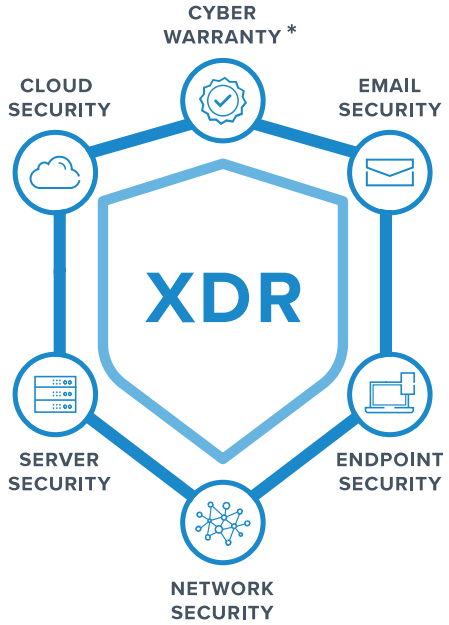
Auf Sicherheitsexpertise und Technologie setzen

Ergänzen Sie Ihre internen Sicherheitsressourcen sofort mit Teams von etablierten Sicherheitsexperten und einer innovativen SOC-Plattform. Jedes SOC-Team arbeitet im Hintergrund, um proaktive Erkennungs- und Reaktionsdienste bereitzustellen. Die SOC-Teams erforschen und entwickeln kontinuierlich neue Sicherheitsmaßnahmen zur Optimierung und sorgen so dafür, dass Barracuda XDR der sich ständig weiterentwickelnden Cyber-Bedrohungslandschaft immer einen Schritt voraus ist.

Die Barracuda XDR-Plattform vereint SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response) und TIP (eine Threat Intelligence Platform) mit über 11 Milliarden IOCs (Indikatoren für Kompromittierungen). Mit dieser Kombination wird gewährleistet, dass die SOC-Teams Vorfälle effizient und effektiv erkennen und einordnen können und Ihnen datengestützte Warnmeldungen und präskriptive Anleitungen bereitstellen, um Vorfälle umgehend zu beheben.

Tiefgreifende Verteidigungsmechanismen

Bauen Sie konzentrische Schutzringe um Ihre Daten, Geräte und Benutzer. Es sind mehrere Sicherheitsschichten erforderlich, um den Schutz zu gewährleisten, den Unternehmen benötigen. Barracuda XDR fügt zusätzliche Schutzebenen für wichtige Angriffsflächen wie E-Mail, Endpunkte, Server, Firewalls und Cloud-Geräte hinzu.



Hauptmerkmale:

Erweiterte Transparenz – Gehen Sie über das traditionelle Dreigespann aus Endpunkt, Netzwerk und Protokollen hinaus. Diese cloudnative Cybersecurity-Plattform bietet eine einheitliche Sicht auf zusätzliche Telemetrie in Ihrer gesamten Umgebung. Die Barracuda XDR-Plattform analysiert auch Daten aus bestehenden Sicherheitslösungen und bietet einen zentralen Überblick.

Security, die in die Tiefe geht – Bauen Sie Schutzschichten um Ihre Daten, Geräte und Benutzer auf. Eine Defense-in-Depth-Strategie ist notwendig, um den Schutz zu gewährleisten, den Unternehmen benötigen.

Herstellerunabhängige Telemetrie – Die wachsende Liste der Technologieintegrationen ermöglicht es den Barracuda XDR-Teams, häufig angeforderte Datenquellen zu überwachen. Proprietäre Erkennungsalgorithmen basieren auf maschinellem Lernen (ML) und sind dem MITRE ATT&CK® Framework zugeordnet, sodass Barracuda XDR Bedrohungsakteure schneller erkennen und ihren nächsten Schritt vorhersagen 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, um wirksame Maßnahmen zum Schutz Ihrer wertvollsten Assets zu ergreifen.

24/7/365-SOC – Echtzeit-Überwachung von Bedrohungen und Anleitung durch Security-Experten, 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 benutzerdefinierte Berichte erstellen, die den Wert der geleisteten Arbeit vor Augen führen.

Teil der Barracuda XDR-Suite:

XDR – Proaktive Cybersecurity-as-a-Service-Plattform, unterstützt von Teams erfahrener Sicherheitsexperten in einem 24/7 Security Operations Center (SOC).

XDR Endpoint Security – Erkennt und reagiert effizient und effektiv auf fortschrittliche Bedrohungen wie Zero-Day-Angriffe, Ransomware und mehr.

XDR Email Security – Überwacht proaktiv Ihre bestehende E-Mail-Sicherheitslösung, um den Schutz vor Spear Phishing, Business Email Compromise (BEC) und weiteren Bedrohungen zu verbessern.

XDR Cloud Security – Schützt Ihre Cloud-Umgebungen vor unbefugtem Zugriff auf Postfächer in der Cloud, vor Administratoränderungen, fehlgeschlagenen Logins und Brute-Force-Angriffen.

XDR Network Security – Erkennt potenzielle Bedrohungsaktivitäten in Ihren Netzwerken, wie Command-and-Control-Verbindungen, Denial-of-Service-Angriffe, Datenexfiltration und Erkundungsversuche.

XDR Server Security – Schützt Ihre Systeme vor ausgeklügelten Angriffen wie Password Spraying, Brute-Force-Angriffen und Privilegienerweiterung.

Weitere Informationen finden Sie unter:

de.barracuda.com/products/managed-xdr

Barracuda®
Your journey, secured.