Barracuda Email Protection

Umfassende Sicherheit für Microsoft 365

Für Unternehmen, die ihr geschäftliches Umfeld, ihre Marken und ihre Mitarbeiter vor den modernsten E-Mail-Bedrohungen schützen müssen, ist Barracuda Email Protection eine umfassende, benutzerfreundlichen Lösung, die Gateway-Abwehr, API-basierte Abwehr für Posteingänge und Incident Response bietet sowie Datenschutz und Compliance gewährleistet.

Spam, Malware und Zero-Day-Bedrohungen blockieren

Barracuda setzt fortschrittliche Verfahren zur Erkennung von bekanntem Spam und bekannter Malware ein. Es stellt außerdem Email Continuity zusammen mit Outbound Filtering und Verschlüsselung bereit, um Datenverluste zu verhindern. Integrierte Advanced Threat Protection wiederum spürt Zero-Day-Malware anhand von Payload-Analysen und Sandboxing auf. Link Protection sorgt für eine Umleitung von verdächtigen und von Typosquatting betroffenen URLs, und Web-Security blockiert den Zugang zu bösartigen Web-Domains, um zu verhindern, dass Empfänger versehentlich Malware herunterladen.

Echtzeit-Schutz vor Spear Phishing

Dank der einzigartigen API-basierten Architektur von Barracuda kann die KI-Engine Details aus bisherigen E-Mails analysieren und die einzigartigen Kommunikationsmuster individueller Benutzer erfassen. Anschließend können Anomalien in Nachrichten-Metadaten und -Inhalten erkannt werden, um Social-Engineering-Angriffe in Echtzeit zu erkennen und abzuwehren.

Verteidigen Sie Ihr Unternehmen gegen Account Takeover

Barracuda blockt Phishing-Angriffe, mit denen Hacker Zugangsdaten für einen Account Takeover abschöpfen. Es erkennt ungewöhnliches E-Mail-Verhalten und warnt das IT-Team, findet und entfernt dann alle betrügerischen E-Mails, die von kompromittierten Konten gesendet werden.

Auf E-Mail-Bedrohungen nach ihrer Zustellung reagieren

Identifizieren Sie potenzielle Bedrohungen nach ihrer Zustellung und nutzen Sie dafür die Erkenntnisse aus Analysen von zuvor zugestellten E-Mails und Community-basierten Bedrohungsdaten. Schonen Sie IT-Ressourcen durch die automatische Entfernung bösartiger Nachrichten und automatische Reaktionsstrategien. Seien Sie Cyberkriminellen immer einen Schritt voraus und blockieren Sie zukünftige Angriffe mit kontinuierlicher Behebung.

Neueste Bedrohungen erkennen dank Benutzerschulungen

Befähigen Sie Ihre Benutzer dazu, die neuesten Phishing-Taktiken zu erkennen, und verhindern Sie, dass sich Angriffe in Ihrem Unternehmen ausbreiten. Sie erhalten Zugang zu hochinteressanten Schulungsmaterialien und Phishing-Simulationen, die auf realen Bedrohungen beruhen.

Daten sichern, Compliance garantieren

Holen Sie sich Datenschutz und Cloud-Backup für Office-365-Daten ins Haus, einschließlich Exchange-Online-Postfächer, SharePoint Online, OneDrive for Business und Teams. Schnelle punktgenaue Wiederherstellung bei versehentlicher oder bösartiger Löschung. Die Cloud-Archivierung unterstützt Sie bei der Einhaltung von Compliance-Anforderungen mit E-Discovery, detaillierten Aufbewahrungsrichtlinien und unbegrenztem Speicherplatz.

Schützen Sie sich vor lateralen Angriffen

Die digitale Transformation zur Cloud – insbesondere zu Microsoft 365 – hat sich in den letzten Jahren beschleunigt. Dies ging einher mit der Zunahme von Mitarbeitern im Homeoffice, externen Auftragnehmern und BYOD- (Bring Your Own Device-)Richtlinien. Das Ergebnis: eine neue Angriffsfläche, bei der ein kompromittierter Account die gesamte Struktur der Zusammenarbeit für laterale Angriffe anfällig macht. Barracuda verbindet E-Mail-Sicherheit mit Zero Trust Access, sodass Sie die Identität und das Vertrauen Ihrer Mitarbeiter und Geräte kontinuierlich überprüfen können.

Hauptmerkmale

Phishing Protection und Impersonation Protection

- Direkte Verbindung mit Office 365
- Rasche, einfache Einrichtung (weniger als 5 Minuten)
- Abblocken von Spear-Phishing-Angriffen, Business Email Compromise (BEC), Erpressung und weiteren Social-Engineering-Angriffen
- Künstliche Intelligenz zur Erkennung und Abwehr von E-Mail-Angriffen in Echtzeit
- Erkennung von Account-Takeover-Aktivität und entsprechende Warnung
- Benachrichtigung externer Benutzer und Löschen gefährdeter E-Mails
- Verhinderung des Zugangs zu dem gefährdeten Konto durch Angreifer
- Transparenz bzgl. Veränderungen bei Posteingangsregeln und verdächtigen Anmeldungen
- Bedrohungsumgebungsanalyse und -berichterstattung

Incident Response

- Outlook Add-in und Meldung von Bedrohungen mit nur einem Klick
- Warnmeldungen zu Sicherheitsvorfällen
- Geografische Einblicke
- Community-basierte Bedrohungsdaten
- Empfänger- und Verhaltensdaten
- Entfernung von E-Mails aus den Posteingängen von Benutzern
- Festlegung von Richtlinien für eingehende E-Mails
- Blockierter Zugang zu schädlichen Inhalten
- Automatische Problembehebung bei schädlichen Inhalten
- Kontinuierliche Vorfallsbehebung
- Automatisierter Workflow-Generator
- API-Integration für SOAR/SIEM/XDR-Plattformen

Cloud-to-Cloud-Backup

- Backup und Wiederherstellung für Office 365: Exchange Online, SharePoint Online, OneDrive und Teams for Business
- Granulare Terminplanung und Wiederherstellung
- Automatische oder manuelle Backups
- Mehrfachauswahl für Wiederherstellungen
- Granulare Wiederherstellung für SharePoint-Elemente
- Wiederherstellung oder lokales Download von Dateien auf Exchange Online oder OneDrive for Business

Email Gateway Defense

- Cloud-basierter Schutz vor Spam, Malware, Viren, Phishing und anderen Bedrohungen in E-Mails
- Advanced Threat Protection mit Sandboxing und vollständiger Systememulation
- E-Mail-Verschlüsselung und Schutz vor Datenverlust ohne Agenten
- Schutz vor Link- und Typosquatting
- Email Continuity mit Failover auf Cloud-basiertem E-Mail-Dienst
- Emergency Mailbox zum Senden, Empfangen, Lesen und Beantworten von E-Mails

Cloud-Archivierung

- Direkte Archivierung aus Office 365 in einem Cloud-basierten Archiv
- PST-Verwaltung für ältere E-Mails
- Granulare Aufbewahrungsregeln
- Volltextsuche mit mehreren Operatoren

Schulungen zum Sicherheitsbewusstsein

- Bedrohungssimulationen für E-Mail, SMS, Sprachnachrichten und physische Medien
- Vorlagen realer Bedrohungen
- Sicherheitsschulungen und Mikro-Lernvideos
- Quiz und Risikobewertungsumfragen
- Erfassung von mehr als 16.000 Datenpunkten
- Detaillierte Trendanalyse
- Anpassbare Berichte und Dashboards

Domain-Fraud-Vorbeugung

- DMARC-Authentifizierung, -Berichte und -Analyse
- Verhinderung von Domain-Spoofing und Brand-Hijacking

Web-Security

- Schützt vor Bedrohungen aus dem Internet
- Filterung von Webinhalten
- Webfilterprotokolle
- Administrative Berichte
- Automatische Benachrichtigungen

Data Inspector

- Scannt in OneDrive for Business und SharePoint gespeicherte Daten auf sensible Informationen und bösartige Dateien
- Erkennt bösartige Dateien
- Einstellungen zur Datenklassifizierung
- Automatisierte E-Mail-Benachrichtigungen für Administratoren, Compliance-Beauftragte und Benutzer
- Rollenbasierte Zugriffskontrolle
- Erweiterte Verschlüsselungsfunktionen

Zero Trust Access

- Phishing Protection und Blockierung von Bedrohungen auf Geräteebene
- Policy-Engine zur Rollen- und Attribut-basierten Zugriffskontrolle
- Optimierte Bereitstellung
- Globale Umsetzung von Richtlinien
- Compliance

Barracuda Email Protection ist in drei Abonnement-Varianten erhältlich. Finden Sie den für Sie passenden Plan.

KAPAZITÄTEN	ADVANCED	PREMIUM	PREMIUM PLUS
Schutz vor Spam und Malware	✓	✓	✓
Attachment Protection	✓	✓	✓
Link Protection	✓	✓	✓
Email Continuity	✓	✓	✓
E-Mail-Verschlüsselung	✓	✓	✓
Schutz vor Datenverlust	✓	✓	✓
Phishing Protection und Impersonation Protection	✓	✓	✓
Schutz vor Account Takeover	✓	✓	✓
Automatische Vorfallsbehebung	✓	✓	✓
Domain-Fraud-Vorbeugung		✓	✓
Web-Security		✓	✓
Suche nach Bedrohungen und Reaktion darauf		✓	✓
Automatisierte Workflows		✓	✓
SIEM/SOAR/XDR-Integration		✓	✓
Cloud-Archivierung			✓
Cloud-to-Cloud-Backup			✓
Data Inspector			✓
Angriffssimulation			✓
Security Awareness Training			✓
Zero Trust Access			✓

Barracuda®
Your journey, secured.