Barracuda Total Email Protection

Umfassender Schutz für E-Mails vor Advanced Threats

Sichere E-Mail-Gateways alleine reichen für die Abwehr gegen alle Formen von E-Mail-Bedrohungen nicht mehr aus. Barracuda Total Email Protection ist der umfassendste Schutz gegen alle Arten von E-Mail-Bedrohungen – von Spam über Malware bis hin zu Business Email Compromise und Kontoübernahmen. Der mehrschichtige Ansatz kombiniert ein sicheres E-Mail-Gateway, KI-gestützten Schutz gegen Betrug, Sicherheitsschulungen für Mitarbeiter und automatisierte Reaktionen auf Vorfälle.

Alle 13 Arten von E-Mail-Bedrohungen erkennen und abwehren

Barracuda Total Email Protection setzt fortschrittliche Verfahren zur Erkennung von bekanntem Spam und bekannter Malware ein. 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, um zu verhindern, dass Empfänger versehentlich Malware herunterladen.

API-basierter Posteingangsschutz erlernt anhand von künstlicher Intelligenz das individuelle Kommunikationsmuster eines jeden Benutzers, um böswillige Absichten zu erkennen und auf Betrugsversuche mit Social Engineering sowie Angriffe mit Kontoübernahme aufmerksam zu machen.

Verteidigung gegen Spear Phishing stärken

Barracuda Total Email Protection nutzt eine einzigartige API-basierte Architektur, wodurch die KI-Engine Details aus vergangenen E-Mails analysiert und die einzigartigen Kommunikationsmuster individueller Benutzer erfaßt. Anschließend können Anomalien in Nachrichten-Metadaten und -Inhalten erkannt werden, um Social Engineering-Angriffe in Echtzeit zu erkennen und abzuwehren.

Fortschrittliche und motivierende Schulungen zum Sicherheitsbewusstsein sowie Phishing-Simulationen sprechen Ihre Mitarbeiter an. Gleichzeitig wird Ihr Team darin geschult, die neuesten Phishing-Methoden zu verstehen, subtile Hinweise auf Phishing zu erkennen und E-Mail-Betrug, Datenverlust sowie die Schädigung Ihres Markennamens zu verhindern.

Auf E-Mail-Angriffe schneller und gezielter reagieren

Die automatisierte Reaktion auf Vorfälle bietet Korrekturmaßnahmen, um schneller und effizienter auf Angriffe zu reagieren, als dies mit manuellen Reaktionsprozessen möglich ist. Administratoren können rasch den Umfang des Angriffs abschätzen und schädliche Nachrichten direkt aus den Posteingängen aller betroffenen Benutzer entfernen. Durch die automatische Korrektur werden E-Mail-Nachrichten, die schädliche URLs oder Anhänge enthalten, identifiziert und nach der Zustellung direkt aus den Posteingängen der Benutzer entfernt.

Barracuda Total Email Protection

Barracuda Total Email Protection bietet eine umfassende Plattform zum E-Mail Schutz im Rahmen einer einzigen Lösung, die einfach im Kauf, in der Implementierung und in der Nutzung ist. Vermeiden Sie die komplexen Integrationsaufgaben, den unsicheren Support und die Risiken beim Zusammenstellen Ihrer eigenen Lösung aus lauter Einzelprodukten.

Technische Angaben

Email Security (Gateway)

- Cloud-basierter Schutz vor Spam, Malware, Viren, Phishing und anderen Bedrohungen in E-Mails
- Advanced Threat Protection mit Sandboxing und vollständiger Systememulation
- Agentenlose E-Mail-Verschlüsselung
- Schutz von Links und Typoskripten

Webbasierte Verwaltung

- Über Barracuda Cloud Control verwaltet
- Web-basiertes Verwaltungsportal
- LDAP und Multi-Faktor-Authentifizierung
- Zentral verwaltete Sicherheitsrichtlinien
- Von überall aus zugängliche Berichte
- Mobile Anwendungen

Kontinuität

- Failover auf Cloud-basierten E-Mail-Dienst
- Bis zu 96 Stunden Email Continuity
- Emergency Mailbox zum Senden, Empfangen, Lesen und Beantworten von E-Mails

Sichere Cloud-Rechenzentren

- AES 256-bit-Verschlüsselung im Ruhezustand und bei der Übertragung
- Public-Key-Verschlüsselungsverfahren (RSA 1024)
- Isolierte Datenbanken für Kunden-Metadaten
- Landesintern gespeicherte Daten (basierend auf Colocation)
- Nach SSAE 16 oder SOC geprüfte Rechenzentren

Cloud-Archivierung

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

Cloud-to-Cloud Backup

- Backup und Wiederherstellung für Exchange Online, SharePoint Online, OneDrive und Teams for Business
- Zentrales Management
- Benutzerdefinierte Aufbewahrungsrichtlinien
- 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

API-basierte Posteingangsabwehr

- Direkte Verbindung mit Office 365
- Rasche, einfache Einrichtung (weniger als 5 Minuten)

KI für Echtzeitschutz

- 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
- Automatische Quarantäne für Nachrichten
- Warnungen für Administratoren und Benutzer

Schutz vor Account Takeover

- Erkennung von Kontoübernahme-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

Domain-Fraud-Vorbeugung

- DMARC-Authentifizierung, -Berichte und -Analyse
- Intuitiver Assistent zur Einrichtung der DMARC-Authentifizierung
- Verhinderung von Domain-Spoofing und Brand-Hijacking

Reporting

- Bedrohungsumgebungsanalyse
- Im Laufe der Zeit entdeckte Angriffe
- Aufschluss über Identitätsmissbrauch und BEC-Angriffe

Schulungen zum Sicherheitsbewusstsein

Multi-Vektor-Bedrohungssimulation

- E-Mail, SMS, Sprachnachrichten und physische Medien
- Vorlagen realer Bedrohungen
- Erweiterte Interaktionen: Landing-Pages, Anhänge, Zugangsdaten-Formulare und mehr

Schulung

- SCORM-konforme Kursunterlagen
- Mikro-Lernvideos
- Quiz und Risikobewertungsumfragen
- Poster und Infografiken

Berichte und Analysen

- Erfassung von mehr als 16.000 Datenpunkten
- Detaillierte Trendanalyse
- Anpassbare Berichte und Dashboards

Incident Response

- Schaltfläche zum Melden von Phishing für verschiedene E-Mail-Clients
- SIEM-Integration

Administrationsfunktionen

- Multi-Faktor-Authentifizierung
- Active Directory-Integration
- Unterstützung von mehr als 25 Sprachen

Vorfallsbewältigung

Identifizierung

- Outlook Add-in und Meldung von Bedrohungen mit nur einem Klick.
- Suche nach Bedrohungen

Untersuchung

- Erweiterte Suche mit Kontext und Relevanz
- Prüfung von Benutzern, die mit schädlichen E-Mails interagiert haben
- Identifizierung von Benutzern mit hohem Risiko
- Automatisierter Workflow zur Reaktion auf Vorfälle

Reaktion

- Blockieren zukünftiger E-Mails aus bestimmten Regionen
- Löschen von E-Mails direkt aus den Posteingängen von Benutzern
- Automatische Korrektur nach der Zustellung
- Automatischer Versand von Warnungen an alle betroffenen Benutzer

Barracuda
Your journey, secured.