Barracuda Email Security Gateway

Lassen Sie E-Mail-basierten Bedrohungen in Ihrem Netzwerk keine Chance!

Entscheiden Sie sich für eine umfassende Email Gateway Security-Lösung mit modernsten Funktionen, die eine Sicherstellung Ihrer Geschäftskontinuität gewährleistet, egal ob Sie Ihre E-Mails lokal oder in der Cloud hosten.

Barracuda Email Security Gateway bietet Ihnen branchenführenden Schutz vor Spam, Viren und hochentwickelter Malware. Ist die Advanced Threat Protection aktiviert, sind Sie auch vor Zero-Day Ransomware und anderen Bedrohungen geschützt. Outbound-Filter schützen vor Datenverlust und ein 96-Stunden Email Spooling in der Barracuda Cloud sorgt im Falle eines E-Mail-Server-Ausfalls für Kontinuität.

Die Email Security Gateway-Lösung ist als physische und virtuelle Appliance und als cloud-basierte Version auf Amazon Web Services und Microsoft Azure erhältlich.

Umfassender Langzeitschutz

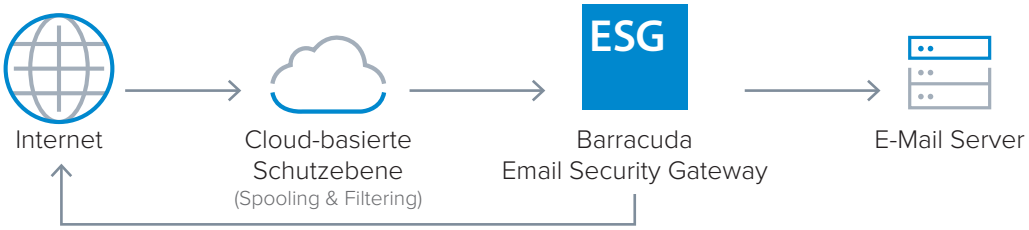
Die Email Security Gateway-Lösung von Barracuda blockiert Spam und Viren, bietet Datenschutz, E-Mail-Kontinuität, DoS-Schutz, Verschlüsselung sowie Richtlinienkontrolle — und das alles in einer umfassenden Lösung. Ergeben sich neue Anforderungen, werden über ein automatisches Update zusätzliche Funktionen integriert, um einen kontinuierlichen Schutz zu gewährleisten.

Umfassender Schutz vor E-Mail-basierten Bedrohungen

Das Barracuda Email Security Gateway bietet mehrstufige Sicherheit, E-Mail-Kontinuität und Data Leak Prevention (DLP). Advanced Threat Protection1 kombiniert Verhaltensanalyse, Heuristik und Sandboxing-Technologien zum Schutz vor Zero-Hour-Attacken, gezielten Angriffen und Ransomware.

Unglaublich benutzerfreundlich

Die schnelle und einfache Einrichtung und das unkomplizierte, intuitive Management sparen Zeit und Ressourcen. Durch die integrierte Barracuda Cloud Protection Layer ist es einfach die Kapazität zu skalieren, wenn Ihr Unternehmen wächst.



Technische Spezifikationen

Umfangreicher Schutz

- Spam- und Virusfilter
- Schutz vor Spoofing, Phishing und Malware
- Schutz vor Denial-of-Service-Angriffen (DoS/ DDoS)
- Schutz vor Verzeichnisangriffen
- Filter für ausgehende Nachrichten

DLP und Reputationsverlust

- Sicherstellung der Compliance
- Schutz vor Reputationsverlust und Blocklisting
- Vordefinierte Filter (z.B. HIPAA, Kreditkarten)

Erweiterte Richtlinienkontrolle

- IP- und inhaltsbasierte Filterung
- Kategorisierung von Bulk E-Mails
- Inhaltsverschlüsselung
- Absender-/Empfängerfilterung
- RBL- und DNSBL-Unterstützung
- Blockierung von Schlüsselwörtern
- Blockierung von Zeichensätzen
- Blockierung von Reverse-DNS
- Blockierung von URL-Mustern und Kategorien
- TLS-Verschlüsselungsrichtlinie
- Zusätzliche Authentifizierung

Absenderauthentifizierung

- SPF und DomainKeys
- Emailreg.org
- Unterdrückung ungültiger Bounce-Meldungen

Spam-Filter

- Rate Control
- IP-Reputationsanalyse
- Fingerprint- und Bildanalyse
- Barracuda Anti-Fraud Intelligence

Virenfilter

- Dreistufige Virenabwehr
- Integrierter Exchange AV Agent
- Entpacken von Archiven
- Blockierung von Dateitypen
- Barracuda Antivirus Supercomputing Grid
- Advanced Threat Protection[1] zum Schutz vor Ransomware, Zero Hour-Attacken und gezielten Angriffen

Administratoren

- Webbasierte Benutzeroberfläche
- Benutzerkontenverwaltung
- Reports, Grafiken und Statistiken
- LDAP-Schnittstelle
- Unterstützung mehrerer Domains
- Sichere Remote-Administration
- Delegierte Domänenverwaltung
- Delegierte Help Desk-Rolle
- Email Spooling
- Backup-to-Cloud Konfiguration

Endbenutzer

- Benutzerbasierte Filterung
- Individuelles Spam-Scoring
- Persönliche Freigabe- & Sperrlisten
- Endbenutzerbezogene Quarantäne und Digest-E-Mails
- Outlook
- Bayes-Analyse

Support-Optionen

Total Protection Plus

- Standardmäßiger technischer Support
- Advanced Threat Protection
- Stündliche Updates der Spamdefinitionen
- Barracuda-Reputations-Datenbanken
- Definitionen für Fingerprint-Prüfung und Absichtsanalyse
- Stündliche Updates der Virusdefinitionen

Instant Replacement Service

- Austauschgeräteversand innerhalb eines Werktags
- Technischer 24-Stunden-Support
- Hardware-Updates alle 4 Jahre

Hardware-Merkmale

Anschlussmöglichkeiten

- Standard VGA
- PS/2 Tastatur/Maus
- Ethernet (siehe nachfolgende Tabelle)

Virtuelle Appliance

- Betriebssystem mit verstärkter Sicherheit
- 7 Modelle zur Auswahl
- Hypervisor Support für VMware ESX und Workstation, Oracle VirtualBox, Citrix Xen sowie Microsoft Hyper-V

Modelle

	300*	400*	600*	800*	900*
KAPAZITÄT					
Aktive E-Mail-Benutzer	1-1,000	1,000-5,000	3,000-10,000	8,000-22,000	15,000-30,000
Domains	250	500	5.000	5.000	5.000
Nachrichtenprotokollspeicherung	12 GB	24 GB	72 GB	120 GB	240 GB
Quarantänespeicherung	20 GB	60 GB	180 GB	360 GB	1 TB
HARDWARE					
Einschubgehäuse	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Abmessungen (cm)	42,7 x 40,6 x 4,6	42,7 x 40,6 x 4,6	42,7 x 57,4 x 4,3	44,2 x 64,8 x 8,9	44,2 x 64,8 x 8,9
Gewicht (kg)	5	5,5	11,8	20,9	23,6
Ethernet	1 x Gigabit	1 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit
AC Eingangsstrom (A)	1,2	1,4	1,8	4,1	5,4
Redundantes Festplattensystem (RAID)		•	Hot Swap	Hot Swap	Hot Swap
ECC-Speicher			•	•	•
Redundante Stromversorgung				Hot Swap	Hot Swap
PRODUKTMERKMALE					
Advanced Threat Protection	•	•	•	•	•
Filter für ausgehende Nachrichten	•	•	•	•	•
E-Mail-Verschlüsselung	•	•	•	•	•
Cloud Protection Layer [2]	•	•	•	•	•
MS Exchange-/LDAP-Beschleuniger	•	•	•	•	•
Benutzerabhängige Einstellungen und Quarantäne	•	•	•	•	•
Delegierte Help Desk-Rolle	•	•	•	•	•
Syslog-Unterstützung	•	•	•	•	•
Clustering und Remote Clustering		•	•	•	•
Domänenabhängige Einstellungen		•	•	•	•
Single Sign-On		•	•	•	•
SNMP/API		•	•	•	•
Kundenspezifisches Branding			•	•	•
Benutzerabhängige Score-Einstellungen			•	•	•
Delegierte Domänenverwaltung			•	•	•

* Auch als Vx (Virtual Edition) verfügbar. Auch als Vx (Virtual Edition) verfügbar.

[1] Spam- und Virenschutz ist auf maximal 50 E-Mail-Adressen limitiert.

[2] Nur gemeinsam mit Advanced Threat Protection erhältlich.

Barracuda
Your journey, secured.