Barracuda SKOUT Managed Email Protection

24/7/365 email protection for your customers' Microsoft 365 mailboxes

Email attacks are more complex and dangerous than ever, and everyone is a target. With 91 percent of cyberattacks starting from email-based threats, businesses require email security that combines technology and human expertise for total protection. Now, you can offer your customers comprehensive protection that is backed by an around-the-clock Security Operations Center (SOC), who can simplify cybersecurity services for you, while taking a proactive approach.

Comprehensive email protection

Protect your customers' email environments with multiple layers of defense, including gateway security, inbox protection combined with artificial intelligence and machine learning technology, and a team of security experts to detect, triage, and respond to today's sophisticated email threats to minimize the impact the attacks have on your customers.

Global threat detection network

Barracuda combines a global threat intelligence database and artificial intelligence with a team of security analysts to stop email threats. Our intelligence database collects email, network, and application threat data from over 200,000 companies worldwide, allowing us to detect threats faster.

24/7 threat detection and response

From zero-day phishing attacks to malicious business email compromises, utilizing computer vision, AI, and machine learning, our team of security experts will stop email threats from entering your customers' environments. Suspicious or malicious emails which are quarantined are documented, providing full visibility to customers' environments.

Key Features

Cloud-based protection against spam, malware, viruses, phishing and other email-based threats

Advanced threat protection using full-system emulation sandbox

Central security policy management

API-based inbox defense with direct connectivity to Office 365

Artificial intelligence to detect and stop spear-phishing attacks, Business Email Compromise (BEC), and user Account Takeover Protection

Incident response management with built-in automated workflow

Centralized dashboard with visibility into inbox rule changes, suspicious sign-ins, and more

Access control to block attackers' access to compromised account

Threat environment analytics of attacks detected over time with insights into impersonation and BEC attacks