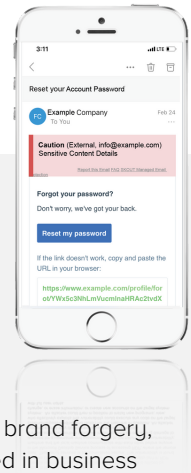
RIZQ Consulting
Powered by MSP Barracuda

Email Protection

Supports Office 365

SKOUT Email Protection is a cloud-based email security product that detects business email compromise, spam, and phishing-type emails and attacks. The product catches malicious emails by utilizing computer vision, AI, and machine learning. SKOUT Email Protection is fully managed and provides you with the option to either inform your users of suspicious or malicious emails through an HTML banner or block them with quarantine features. Driven, curious, mobile, and growing smarter by the subject line, SKOUT Email Protection adds an important layer of protection to your inbox.





Key Features

Detects VIP spoofing, brand forgery, and other attacks used in business email compromise and phishing

Provides user-friendly warnings in way of banners on malicious and suspicious email

Sanitizes embedded links to help protect users from potentially malicious websites

AI and Computer Vision models to catch evasion techniques

Easy “Report to SOC Button” for human analysis

Fast Deployment built into dashboard

Phishing, Zero-Day Phishing, 3rd Party Brand Impersonation

AI, machine learning, and computer vision identify patterns in text, image, and html to identify potential threats. The unique banner system allows for borderline threats to be flagged without compromising business functionality

VIP Impersonations

Identifies attempts to impersonate VIPs via email spoofing, typo squatting, or other malicious tactics

Malicious Files

Scans for malicious links, infected PDFs, and embedded code including scripts. Analyzes text within each email and attachment(s) to determine if sensitive words or phrases are used such as: password, invoice, payment, etc.

Malicious Links

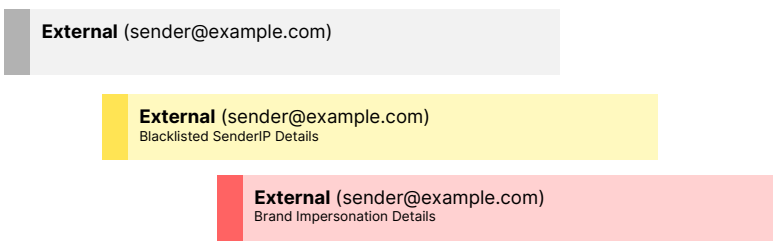
All links in emails are sanitized using a sandboxed server. The user cannot access the link directly. They are brought to a landing page showing a screenshot.

Personal Device & Home Attacks

Attacks on personal devices are mitigated by conducting analysis on the server side and injecting the results into the email, completely removing the need for remote software such as dedicated email clients

Malicious Insider

Machine learning develops behavior profiles and social graphs that identify suspicious emails that don’t match a known profile, triggering an impersonation warning



RIZQ Consulting
Powered by MSP Barracuda

O365 Security Monitoring

AI Powered Network Protection

SKOUT Office 365 Security Monitoring is a managed security product that monitors Office 365 activity using SKOUT's analytics platform, SIEM, threat intelligence, and 24/7 365 Security Operations Center to identify threat-like behavior such as unauthorized access to cloud mailboxes, admin changes in the environment, impossible logins, and brute force attacks.



Key Features

Multi-Tenancy Dashboard

SIEM Correlation & SOC Analysis

Support for custom alerting and reports

Visibility to login activity in the dashboard

Detects potential threats of suspicious activity in Office 365

Supports Industry & Regulatory Compliance requirements



Malicious Admin Changes

Tracks admin activity and changes to the O365 tenant



Unauthorized Delegate Access

Tracks when emails delegates are added



Failed or Unauthorized Access

Detects failed or suspicious login attempt



MFA Removed

Detects changes to MFA



Foreign Login

Monitors geolocation access with IP location sourcing and login from suspicious or unusual countries



Impossible Login

Detects logins from different geolocations within a short period of time



Suspicious Email Forward

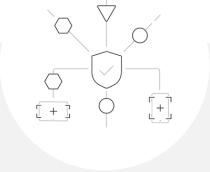
Alerts when email forwarding rules have been created outside of the domain

Endpoint Protection

AI Powered Log Collection & Correlation

RIZQ Consulting
Powered by MSP Barracuda

SKOUT Endpoint Protection is an endpoint-based malware detection and response (MDR) solution that detects and stops malicious files and processes (known as malware or ransomware) on Windows, Mac or Linux devices. Unlike traditional signature-based Anti-Virus, this product uses machine learning models to detect zero-day malware as well as known variants, fileless, script-based memory, and external device-based attacks. It is backed by the SKOUT Security Operations Center to continuously monitor for major infections and to identify infection sources.



Key Features

- AI and behavioral-based
- Automated blocking
- Protection while offline
- Zero-Day Prevention
- Memory Exploitation Detection and Prevention
- Script and Fileless Malware Detection
- Easy deployment via dashboard
- Visibility to all managed endpoints in dashboard
- Low memory and CPU footprint
- Supports a variety of operating systems including Windows XP



Malware & Ransomware

Identifies and blocks malicious executables



APT & Zero-Day Prevention

Threat intelligence and constant machine learning modeling keep new variants of threats from being successful



Fileless Attacks

Eliminates the ability for attackers to use fileless malware attack techniques on protected endpoints



Remote Worker Attacks

Protect users not connected to the company network with protection that doesn't rely on signature updates



Malicious Scripts

Controls the way scripts execute to prevent attacks, including PowerShell



Email Payloads

Prevents malicious email attachments from detonating their payloads