Barracuda SKOUT Managed Endpoint Protection

AI-based endpoint protection with 24/7 monitoring service

While most cyberattacks begin with an email, the endpoint is where cybercriminals conduct their reconnaissance. Once hackers have access to an endpoint, they can install malware that allows them to harvest credentials, data extortion, and much more. Ensure your customers' endpoints are protected with an AI-based MDR that is backed by a 24x7 Security Operations Center (SOC) to provide peace of mind for you and your customers.

Complete endpoint protection

Available for Windows, Mac, and Linux, Barracuda SKOUT Managed Endpoint Protection monitors every event, across every OS and environment(s), to identify threats and correlate the information to provide automated context and complete attack story.

Contextualized storyline threat detection

The Barracuda SKOUT Managed Endpoint detections automatically correlates telemetry across all OS process relationships and maps it to the MITRE ATT&CK framework, allowing our SOC analysts to detect and get to the root of the cause faster.

24/7 threat detection and response

From zero-day to ransomware, utilizing AI and behavioral-based analysis, our team of security experts will detect, triage, and remediate threats for your customers' environments. All events are responded to and are shown through the Barracuda SKOUT Managed XDR platform, providing full visibility to MSPs.

Key Features

Centralized visibility to all managed endpoints in Barracuda SKOUT Managed XDR Dashboard

Fully managed endpoint protection that includes deployment, monitoring, and management

Built-in static AI and behavioral analysis for advanced threat detection such as malware and ransomware

Autonomous threat response such as quarantining any infected devices from network and rogue device visibility

Single agent for ease of deployment and management

MITRE ATT&CK framework is utilized by SOC team for quick threat detection and gap identification

1-Click Remediation and Rollback for Windows

Application inventory & vulnerability detection for known vulnerabilities

Endpoint controls to help MSPs showcase threat activities and SOC actions completed