Barracuda XDR Email Security

24/7/365 email protection for customers’ 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 an email security service offering that combines technology and human expertise for total protection. With Barracuda XDR Email Security, MSPs can offer comprehensive protection that is backed by an around-the-clock Security Operations Center (SOC), simplifying the delivery of cybersecurity-as-a-service to customers.

Comprehensive email protection

Protect 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 businesses.

Global threat detection network

Using a global threat intelligence database and powerful A.I., Barracuda’s email threat detection is combined with MITRE ATT&CK® framework mapping to ensure threats are detected early. It can even predict their next move, which helps inform the most effective response tactics.

24/7 threat detection and response

From zero-day phishing attacks to malicious business email compromises, utilizing computer vision, A.I., and machine learning, the security experts in Barracuda’s SOC will minimize the damage email threats can cause in customers’ environments. Suspicious or malicious emails that are quarantined are documented, providing full visibility for MSPs into customers’ environments.

Part of the Barracuda XDR multi-layered security family:

- **XDR** - an eXtended visibility, Detection & Response platform that is backed by a group of tenured security experts in a 24x7 Security Operations Center (SOC), providing proactive cybersecurity-as-a-service for MSPs.
- **XDR Endpoint Security** - Unifies and extends detection and response capability to endpoints, protecting them from common endpoint threats, including malware and ransomware.
- **XDR Email Security** - Proactively monitor existing email security solution to enhance protection against spear phishing, business email compromise (BEC), and more.
- **XDR Cloud Security** - Secure customers’ cloud environments from unauthorized access to cloud mailboxes, admin changes in the environment, impossible logins, and brute force attacks.
- **XDR Network Security** - Detect potential threat activity on customer’s network such as command-and-control connections, denial-of-service attacks, data exfiltration, and reconnaissance.
- **XDR Server Security** - Protect customers’ critical servers from attacks such as password sprays, brute force attacks, and privilege escalation.
- **Cyber Warranty** - Financial protection that puts MSP and SMB needs first. Through the use of the Barracuda XDR solution suite, it streamlines application and claim process, speeding the process time from months to days.

For more information visit: barracudamsp.com/barracuda-xdr
Key features

- **Protects** against spam, malware, viruses, spear phishing, and other email-based threats
- Understands attack tactics, predicts their next steps, and identifies gaps in detection coverage via detection rule mapping with MITRE ATT&CK® framework
- Merges data from your existing security tools with multiple sources to provide greater visibility
- Gains visibility of threat activity in XDR’s multi-tenancy dashboard
- Uses SIEM analysis
- Supports for custom alerting and self-service reports
- Includes **24x7 365 SOC** support and remediation guidance
- Backs key industry and regulatory compliance standards such as continuous monitoring and log retention

Key integrations:

- Barracuda Cloud Email Gateway Defense
- Barracuda Impersonation Protection
- Barracuda Incident Response
- Mimecast
- And, many more

For the complete list of integrations, please visit [www.barracudamsp.com/Barracuda-XDR-Integrations](http://www.barracudamsp.com/Barracuda-XDR-Integrations)