Barracuda XDR Cloud Security
Proactively monitor your customers’ cloud environments 24/7

By 2025, there will be over 100 zettabytes of data stored in the cloud, according to Cybersecurity Ventures. With more companies adopting cloud services, cybercriminals are evolving their tactics to go after this attack surface. Protect customers’ cloud environments with proactive monitoring to detect unauthorized access to cloud infrastructures, admin changes in the environment, brute force attacks, and more.

Deliver cloud services with ease
Build concentric rings of protection around your customers’ cloud data and user identities. With Barracuda XDR Cloud Security, MSPs can detect attacks such as malicious admin changes, unauthorized delegate access, foreign login, cloud infrastructure attacks, and more.

Access to security expertise
Instantly augment your internal security resources with teams of tenured security experts who work in the background to provide 24/7, proactive detection and response services to your managed customers. All identified incidents are triaged, and you are alerted and guided toward resolution.

Part of the Barracuda XDR suite:

XDR - Proactive cybersecurity-as-a-service platform backed by teams of tenured security experts in a 24/7 Security Operations Center (SOC) built for MSPs.

XDR Endpoint Security - Efficiently and effectively detect and respond to advanced threats such as zero-day attacks, ransomware, and more.

XDR Email Security - Proactively monitors existing email security solutions to enhance protection against spear phishing, business email compromise (BEC), and more.

XDR Cloud Security - Secures your customers’ cloud environments from unauthorized access to cloud mailboxes, admin changes, impossible logins, and brute force attacks.

XDR Network Security - Detects potential threat activity on your customers’ networks, such as command-and-control connections, denial-of-service attacks, data exfiltration, and reconnaissance.

XDR Server Security - Protects your customers’ systems from sophisticated attacks such as password sprays, brute force attacks, and privilege escalation.

Cyber Warranty - Provides financial protection that puts you and your clients’ needs first. The Barracuda XDR suite streamlines the warranty application and claim process, speeding the process from months to days.

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

- Detects potential threats or suspicious activities in the cloud
- Understands attack tactics and predicts the attacker’s next steps via detection rule mapping with MITRE ATT&CK® framework
- Uses Machine Learning (ML) to identify anomalous activity
- Correlates telemetry from multiple sources with your existing security tools to provide greater visibility
- Provides visibility of threat activity in XDR’s multi-tenant dashboard
- Leverages SIEM and SOAR technologies
- Supports custom alerting and self-service reports
- Includes 24/7/365 SOC support and remediation guidance
- Backs critical security controls within industry standards and compliance frameworks such as continuous monitoring and log retention

Key integrations:

- AWS
- Azure
- Duo
- Google Workspace
- Microsoft 365
- OKTA
- And, many more

For the complete list of integrations, please visit www.barracudamsp.com/Barracuda-XDR-Integrations