Barracuda
Your journey, secured.

DATASHEET

Barracuda XDR Cloud Security

Proactively monitor your 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 your cloud environments with proactive monitoring to detect unauthorized access to cloud infrastructure, admin changes in the environment, brute force attacks, and more.

Protect cloud services with ease

Build concentric rings of protection around your cloud data and user identities. With Barracuda XDR Cloud Security, you 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. 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).

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 your existing email security solution to enhance protection against spear phishing, business email compromise (BEC), and more.

XDR Cloud Security - Secures your 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 networks, such as command-and-control connections, denial-of-service attacks, data exfiltration, and reconnaissance.

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

For more information visit: barracuda.com/products/managed-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 the **XDR Dashboard**
- Leverages **SIEM** and **SOAR** technologies
- Supports **custom alerting** and **self-service report**s
- 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

https://www.barracuda.com/products/managed-xdr/integrations

Barracuda®
Your journey, secured.

DATASHEET • US 1 • Copyright 2024 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.