Your journey, secured.

DATASHEET

Barracuda XDR Server Security

Protect your systems from sophisticated attacks

Cyberattacks cause more than 45% of sensitive data leaks. Businesses need security services that can help them protect, detect, and respond to attacks when they occur. With Barracuda XDR Server Security, you benefit from comprehensive protection that is backed by an around-the-clock Security Operations Center (SOC).

System log visibility

Protect your Windows and Linux systems with proactive monitoring that collects, aggregates, and normalizes critical log data from systems within your environment. By leveraging the XDR analytics platform and threat intelligence, the SOC can identify potential threats, such as password sprays, brute force attacks, privilege escalation, and more.

Gain security expertise

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

- Includes specific detections capable of identifying a compromise within an Active Directory (AD) domain
- Understands attack tactics and predicts the attacker's next steps via detection rule mapping with **MITRE ATT&CK® framework**
- **Correlates telemetry** from multiple sources with your existing security tools to provide greater visibility
- Provides visibility of threat activity in **XDR 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:

- Microsoft Windows
- Linux

For the complete list of integrations, please visit

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

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.