MSP Barracuda
Your journey, secured.

DATASHEET

Barracuda XDR Server Security

Protection customers' mission critical servers

Cyberattacks causes more than 45% of sensitive data leaks. Businesses are looking to MSPs to provide security services that can help them prevent, detect, and respond to attacks when they occur. With Barracuda XDR Server 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-services to customers.

eXended server visibliity

Protect customers' servers with proactive monitoring that collects, aggregates, and normalizes log data from the most critical Windows and Linux servers within customer's network. It identifies potential risks, such as password sprays, bruteforce attacks, privilege escalation, and more, using XDR's analytics platform, threat intelligence, and Security Operations Center.

Gain security expertise

Instantly augment internal security resources with a team of tenured security experts and a best-of-breed SOC who works in the background to provide a 24x7, proactive detection and response service for all your managed customers. All identified incidents are triaged, and the MSP is alerted and guided in resolution.

Part of Barracuda XDR multilayered 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 - Comprehensive email protection that includes gateway security, account compromise, and more, minimizing the impact an attack can have on customer's email environment.

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 customers' 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.

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

Key features

- Identifies compromise with Active Directory (AD)
- 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 report**s
- Includes **24x7 365 SOC** support and remediation guidance
- Backs key industry and regulatory compliance standards such as **continuous monitoring and log retention**

Key integrations:

- **Microsoft Windows**
- **Linux**
- **And, many more**

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

MSP Barracuda®
Your journey, secured.

About Barracuda MSP

As the MSP-dedicated business unit of Barracuda Networks, Barracuda MSP enables IT managed service providers to offer multi-layered security and data protection services to their customers through our award-winning products and purpose-built MSP management platforms. Barracuda MSP's partners-first approach focuses on providing enablement resources, channel expertise, and robust, scalable MSP solutions designed around the way managed service providers create solutions and do business. Visit barracudamsp.com for additional information.
@BarracudaMSP | LinkedIn: BarracudaMSP | smartermsp.com

617.948.5300 | 800.569.0155 | sales@barracudamsp.com