Barracuda
Your journey, secured.

Barracuda XDR

A unified approach to cybersecurity

Cybersecurity is a journey. And today's essential cybersecurity best practices require more than standalone security products. Unlike many competitors, Barracuda eXtended Detection & Response (XDR) combines its advanced analytics platform with a 24/7 Security Operations Center (SOC).

Uplevel your cybersecurity approach

Protect your organization against today's pervasive cyberthreats by applying cybersecurity best practices with Barracuda XDR. Leveraging Barracuda XDR, your team gains the ability to proactively protect, detect, and respond to threats with the support of a 24/7 Security Operations Center (SOC).

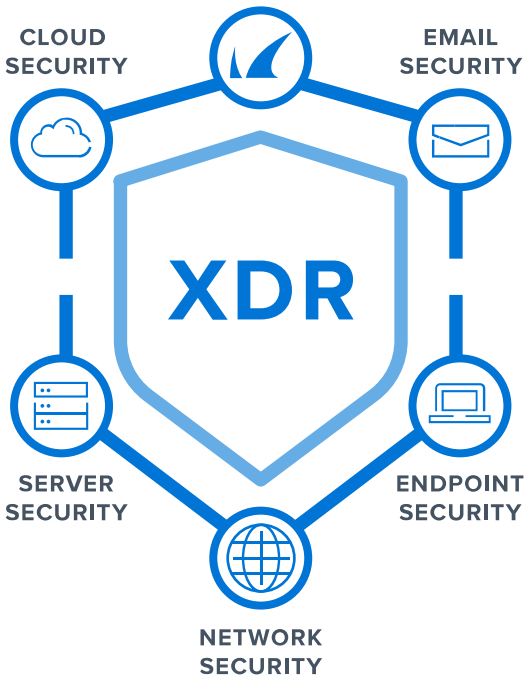
Defense-in-depth

Build concentric rings of protection around your data, devices, and users. Multiple security layers are necessary in order to provide the protection organizations need. Barracuda XDR adds additional layers of protection for major attack surfaces such as email, endpoints, servers, firewalls, and cloud devices.

Gain security expertise and technology

Instantly augment your internal security resources with teams of tenured security experts and an innovative SOC platform. Each SOC team works in the background to provide proactive detection and response services. The SOC teams continually research and develop new security advancements and optimization, ensuring Barracuda XDR stays ahead of the ever-evolving cyberthreat landscape.

The Barracuda XDR platform unifies security information and event management (SIEM), security orchestration, automation, and response (SOAR), and a threat intelligence platform (TIP) with over 11 billion Indicators of Compromise (IOCs). The combined result ensures that the SOC teams can efficiently and effectively detect and triage incidents, and provide you with enriched alerts and prescriptive guidance to resolve incidents promptly.



Key Features:

eXtended visibility - Go beyond the traditional visibility triad of endpoint, network, and logs. This cloud-native cybersecurity platform offers a single pane of glass view of additional telemetry within your environments. The Barracuda XDR platform also analyzes data from existing security solutions to provide centralized visibility.

Defense-in-depth security - Build layers of security around your data, devices, and users. A defense-in-depth strategy is necessary to provide the protection that organizations need.

Vendor-agnostic telemetry - The growing list of technology integrations allows the Barracuda XDR teams to monitor commonly requested data sources. Proprietary detections are powered by machine learning (ML) and are mapped to the MITRE ATT&CK® framework, allowing Barracuda XDR to detect threat actors faster and predict their next move.

Threat intelligence - Barracuda utilizes a large global threat indicator repository informed by a rich security intelligence feeds from diverse sources, including Barracuda's proprietary intelligence to take effective actions to protect your valuable assets.

24/7/365 SOC - Real-time threat monitoring and guidance from security experts are divided into dedicated teams for around-the-clock coverage. The SOC infrastructure includes Security, Orchestration, Automation & Response (SOAR) and machine learning to ensure that only legitimate alerts are investigated and promptly escalated**.**

Demonstrate value - Customizable reports are available to illustrate the work completed.

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

Barracuda®
Your journey, secured.