Barracuda Managed XDR

Prevent breaches with fully managed comprehensive protection

If cybersecurity is the destination, Barracuda Managed XDR is the way. This fully managed, next-generation solution, powered by Barracuda's 24/7/365 global security operations center (SOC), leverages advanced AI analytics and threat intelligence to prevent breaches before they impact your organization. As an open XDR platform, it integrates seamlessly with your existing tools, boosts operational efficiency and delivers true defense-in-depth.

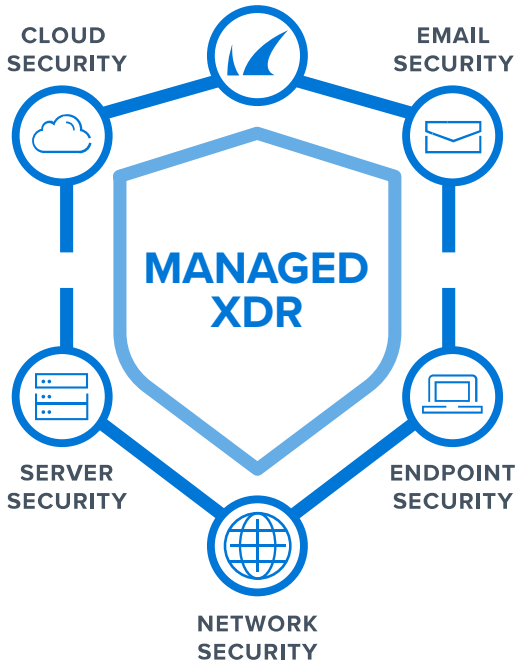
Expertise meets innovation

Barracuda Managed XDR provides peace of mind with 24/7/365 support from a global SOC. Staffed by five specialized teams of seasoned cybersecurity analysts and security engineers, the SOC ensures continuous protection and rapid response. The SOC's Red Team has developed more than 1,000 detection rules — each mapped to the industry-standard MITRE ATT&CK framework, a trusted knowledge base of tactics, techniques and procedures (TTPs) used by today's adversaries.

With Barracuda's SOC, rest assured that your cybersecurity posture is constantly monitored and protected. This proactive approach ensures that potential threats are quickly mitigated before they escalate and cause harm.

Barracuda Managed XDR harnesses advanced AI trained on vast telemetry and Automated Threat Response (ATR) to revolutionize how organizations defend against cyberattacks. Using AI-driven threat detection and mitigation without the need for manual intervention, it significantly reduces response times and minimizes risk.

ATR automatically executes predefined playbooks to swiftly contain and neutralize threats. Compromised endpoints and accounts are automatically isolated, and malicious traffic is blocked at the firewall. This proactive automation reduces alert fatigue by filtering out false positives and maintains a true-positive rate of 90% or higher, enabling security teams to focus on genuine threats.



AI further strengthens this capability by correlating data across multiple sources, providing historical context to detect patterns and prevent recurring attacks. Together, AI and ATR transform your security operations — accelerating response time, improving accuracy and boosting your overall security posture and operational efficiency.

Overcome your key challenges

Barracuda Managed XDR is purpose-built to address the critical challenges organizations and managed service providers (MSPs) face in today's complex threat landscape. For teams with limited resources, it offers a complete, fully-managed solution — eliminating the need to manually manage alerts, logs and telemetry across disparate systems.

As an open XDR platform, Barracuda Managed XDR seamlessly integrates with your existing tech stack — eliminating further tool sprawl. By consolidating data and translating alerts into actionable insights, it significantly reduces alert fatigue, allowing your team to focus on real threats without being overwhelmed by noise.

Key features

SOC-powered protection, around the clock

Barracuda Managed XDR is a fully managed service powered by an elite 24/7/365 global SOC. Staffed by five specialized expert teams, it instantly extends your IT capabilities, eliminating coverage gaps, reducing alert noise and false positives and preventing team burnout.

One XDR to rule them all

Barracuda Managed XDR is an open XDR platform that seamlessly integrates with your existing technologies — across endpoints, servers, cloud, email and firewalls. This frictionless deployment enhances both your security posture and operational efficiency, all from a unified single-pane-of-glass dashboard.

360° defense-in-depth

Barracuda Managed XDR delivers next-generation cybersecurity with full-spectrum, 360-degree protection across the entire attack lifecycle, delivering true defense-in-depth to your organization.

Enterprise-grade threat intel

Barracuda Managed XDR identifies true positives amidst the noise, reducing time to respond (TTR) to seconds. It leverages over 11 billion indicators of compromise (IOCs) and 1,000+ machine learning-enriched detection rules aligned with the MITRE ATT&CK framework.

AI-driven Detection and Automated Threat Response (ATR)

Powered by advanced AI trained on extensive datasets, Barracuda Managed XDR detects sophisticated attack patterns and delivers actionable insights into threats and threat actors. Barracuda ATR enables proactive, real-time threat detection and response without human intervention, available 24/7/365.

Scalable XDR solution

Barracuda Managed XDR is built to scale, ingesting trillions of events and telemetry signals across your environment. It combines the power of Barracuda AI, global threat intelligence, machine learning-enriched detection rules, security information and event management (SIEM), and security orchestration, automation, and response (SOAR) technologies.

Single-pane-of-glass dashboard

Without centralized visibility, organizations struggle with fragmented threat detection, slower response times and higher operational costs from managing disconnected security tools. Barracuda Managed XDR solves this with a unified, single-pane-of-glass dashboard — giving you complete oversight across your entire security ecosystem for more efficient cybersecurity operations.

Simplified regulatory compliance

Evolving regulatory and compliance landscapes demand a stronger security posture. Many sector regulations now require organizations to implement sophisticated solutions, such as SIEM, SOAR and vulnerability management, to meet increasingly stringent standards. Barracuda Managed XDR helps you meet these evolving standards by delivering these technologies as part of a fully managed solution along with detailed reporting to streamline audits and support ongoing compliance efforts.

Part of the Barracuda Managed XDR suite

The more data sources your organization integrates with Barracuda Managed XDR, the greater your visibility and protection become. While Barracuda recommends a unified approach encompassing all the components below, your organization's unique needs may dictate a tailored strategy.

XDR Endpoint Security

Safeguards endpoints — including laptops, desktops, workstations and servers — with SentinelOne's industry-leading endpoint detection and response (EDR) solution. Fully managed by Barracuda's SOC, SentinelOne protects your Windows, Linux and macOS endpoints from advanced threats, such as zero-day attacks, ransomware and more.

XDR Email Security

Proactively monitors email security solutions, enabling early threat detection and rapid response to email-based attacks, strengthening your organization's defenses against phishing, malware, business email compromise (BEC) attempts and more.

XDR Cloud Security

Secures your cloud environments from unauthorized access to cloud mailboxes, unexpected admin changes, improbable and impossible logins, and brute force attacks.

XDR Network Security

Detects potential threat activity on your networks, including command-and-control connections, denial-of-service, data exfiltration and reconnaissance-based attacks.

XDR Server Security

Collects, aggregates and normalizes log data from Windows and Linux servers, providing advanced visibility into sophisticated attacks that EDR solutions often miss, such as privilege escalation, password sprays and brute force attacks.

Managed Vulnerability Security

Offers regular vulnerability scans that provide comprehensive insights into your security landscape. Managed by Barracuda's SOC, this service includes expert reporting to help you understand vulnerabilities in context, prioritize remediation, strengthen defenses and ensure compliance with regulatory requirements.