Barracuda Managed Vulnerability Security

Identify vulnerabilities and prioritize remediation with ease

Protect your business from a potentially devastating breach with Barracuda Managed Vulnerability Security. This enterprise-grade vulnerability scanning service is fully managed by cybersecurity experts in Barracuda's Security Operations Center (SOC). Powered by Rapid7's best-in-class InsightVM, Barracuda Managed Vulnerability Security proactively identifies weaknesses across your networks and cloud infrastructure. It delivers unparalleled asset visibility and real-time risk prioritization. The resulting reports provide actionable insights for remediation, empowering your organization to enhance its cyber resilience while ensuring compliance with industry regulations.

Proactive vulnerability security

Strengthening an organization's security posture is crucial in today's fast-evolving threat landscape, where malicious threat actors are increasingly prevalent and sophisticated. Barracuda Managed Vulnerability Security plays a vital role in this endeavor by providing your organization with regular vulnerability scans conducted and managed by Barracuda's SOC. These proactive assessments help you identify potential weaknesses before they can be exploited. By using Barracuda Managed Vulnerability Security, your organization stays ahead of cybercriminals and significantly reduces the risk and likelihood of a breach.

Fully managed by Barracuda

With Barracuda Managed Vulnerability Security, organizations alleviate the strain on existing resources and avoid the need for significant investments in extensive cybersecurity infrastructure. This is possible because Barracuda's SOC handles the vulnerability scanning for you. In addition to benefiting from the SOC's expert oversight and guidance, you and your team can dedicate more time to focusing on other critical business operations.

Enhance cyber resilience

By leveraging Barracuda Managed Vulnerability Security, organizations effectively mitigate risk and enhance their overall resilience to cyber threats. The service identifies vulnerabilities and provides actionable recommendations for remediation, empowering you to take informed steps that strengthen your security posture. This proactive approach protects valuable assets and sensitive data, as well as fosters a culture of security awareness in the organization. In an era where cyber threats are a constant concern, investing in robust vulnerability management solutions like Barracuda Managed Vulnerability Security is essential for maintaining a strong security posture and ensuring long-term organizational success.

Simplify regulatory compliance

In today's digital landscape, organizations must comply with various regulations and compliance frameworks, such as GDPR, HIPAA and NIS2. These and many other compliance requirements address risk mitigation, vulnerability management and the importance of regular vulnerability scanning to identify and address potential weaknesses.

Barracuda Managed Vulnerability Security is ideally positioned to bolster your compliance initiatives through regular, recurring vulnerability scans that are expertly managed by the Barracuda SOC. This service identifies potential vulnerabilities and provides comprehensive reports that facilitate your compliance efforts, significantly easing the burden on your organization.

Thorough post-scan reports

Following the completion of each vulnerability scan, the SOC provides your team with four detailed reports to facilitate, plan and prioritize the remediation of the security weaknesses. The Audit report identifies vulnerabilities in the IP-addressable assets scanned. It includes per asset risk scores, severity breakdowns, policy evaluation results, and summary charts. With this information, auditors and engineers can see exactly what was found. The Remediation Plan report ranks vulnerabilities and suggests an order to remediate them, with the highest risks prioritized. It provides actionable steps, download links and an estimation of the remediation effort. The Top 25 Remediations by Risk report ranks and documents what the impact would be of remediating the top 25 weaknesses. Finally, the Risk Scorecard report distills the scan results into a letter grade for a specific site, office, application set, operating system, or asset tag by comparing the average asset risk score for that segment with the overall environment.

How it works

Barracuda Managed Vulnerability Security simplifies the vulnerability scanning process, allowing organizations to focus on their core operations. The service begins with a straightforward setup involving the Barracuda SOC, where customers collaborate with a Barracuda Solutions Architect (SA) to define the scope of the scanning. This includes answering a few routine questions about the number of sites and IP addresses to be scanned. After, the customer provides the necessary physical or virtual machines to host the Rapid7 InsightVM security console and scan engine. The Barracuda SOC manages the deployment, ensuring the scanning components are installed correctly and efficiently.

Once the Security Console and Scan Engine are operational, the SOC takes over the management of vulnerability scans, running them according to a schedule tailored to the organization's needs. Customers can expect the scans to be non-intrusive, with minimal impact on their network performance. As the vulnerability database is updated every six hours, you can expect vulnerability scans with the latest threat data. This proactive, up-to-date approach enhances the organization's security posture and allows IT teams to concentrate on other critical business functions, knowing their vulnerability security is in expert hands with Barracuda.

Key features

- Fully managed recurring vulnerability scans performed by Barracuda SOC
- Quarterly, bi-monthly or monthly vulnerability scans
- 1 ad hoc scan per quarter
- Scans any IP-addressable asset
- Scans on-premises and cloud assets
- Scans only customer-selected assets
- Proactive recurring scans performed at customer's convenience
- No network performance degradation
- Delivers 4 reports per scan to prioritize and empower vulnerability remediation
- Reports suitable for regulatory compliance needs
- Vulnerability severity scores compatible with MITRE Common Vulnerabilities and Exposures (CVE) index
- All vulnerabilities indicate severity with industry-standard CVSS scores
- Dedicated Barracuda support team access for inquiries
- Permits credentialed scans when requested by customer (recommended)

Responsibilities

ACTIVITY	BARRACUDA	PARTNER/CUSTOMER
Configure and administer vulnerability scans	✓	-
Schedule and execute vulnerability scans	✓	-
Verify and disseminate reports	✓	-
Maintain and update scan application components	✓	-
Monitor system health and assure service	✓	-
Review vulnerability scan reports	-	✓
Prioritize and remediate vulnerabilities	-	✓
Notify if asset or site changes	-	✓
Provision, install, maintain dedicated scan engine and security console hosts	-	✓

System requirements

SECURITY CONSOLE			
Assets to scan	Processor	Memory	Storage
<= 5,000	X86_64, 4 cores	16 GB	1 TB
20,000	X86_64, 12 cores	X86_64, 12 cores	2 TB
Physical Server, Virtual Server.			
SCAN ENGINE			
Scan volume	Processor	Memory	Storage
5,000 assets/day	X86_64, 2 cores	8 GB	100 GB
20,000 assets/day	X86_64, 4 cores	16 GB	200 GB
Physical Server, Virtual Server, Docker Container.			
OPERATING SYSTEMS			
Ubuntu Linux 24.04 LTS, 22.04 LTS; Oracle Linux 8; SUSE Linux Enterprise Server 12; Alma Linux 9; Rocky Linux 9; Red Hat Enterprise Linux Server 9, 8; CentOS 7; Microsoft Windows Server 2022 (Microsoft Windows Server Desktop (experience only, core not supported)).			
BROWSERS			
Google Chrome (Recommended), Mozilla Firefox, Mozilla Firefox ESR, Microsoft Edge.			