Barracuda
Your business, secured.

# Barracuda Managed Vulnerability Security

Barracuda's Managed Vulnerability Security offers a proactive approach to securing networks and preventing breaches. Managed Vulnerability Security is a vulnerability scanning solution managed by the Barracuda SOC.

WHITE PAPER

## Introduction

Barracuda Networks has expanded its cybersecurity offerings with the introduction of its new managed vulnerability scanning product. This innovative solution is designed to help organizations proactively identify and remediate vulnerabilities across their IT environments, enhancing their overall security posture.

## Key features

1. Comprehensive Scanning: The Managed Vulnerability Security product provides thorough assessments of all network systems. It identifies vulnerabilities that could be exploited by attackers, ensuring that organizations can address potential security gaps before they are compromised.
2. Detailed Reporting: Users receive detailed reports that highlight vulnerabilities, their severity, and recommended remediation steps. This streamlines the vulnerability management process, allowing security teams to focus on critical issues in an efficient manner.
3. Fully Managed by 24/7 Security Operations Center (SOC): Barracuda's award-winning XDR team provides continuous monitoring and support, ensuring that vulnerabilities are managed effectively. This around-the-clock service helps organizations maintain a proactive security stance.

## Benefits

- Proactive Threat Identification: Vulnerability scanning helps organizations identify security weaknesses before they can be exploited by attackers. By regularly scanning systems, businesses can discover vulnerabilities in software, hardware, and network configurations.
- Risk Management: By identifying vulnerabilities, organizations can assess the potential risks associated with them. This allows for prioritization of remediation efforts based on the severity of the vulnerabilities and the potential impact on the organization.
- Regulatory Compliance: Many industries are subject to regulations that require regular vulnerability assessments and reporting. Conducting vulnerability scans helps organizations comply with standards such as PCI DSS, HIPAA, and GDPR.
- Improved Security Posture: Regular vulnerability scanning contributes to an overall stronger security posture. By continuously identifying and addressing vulnerabilities, organizations can reduce their attack surface and enhance their defenses against cyber threats.
- Informed Decision-Making: Vulnerability scanning provides valuable insights into the security landscape of an organization. This information can inform strategic decisions regarding security investments and resource allocation.

## End-to-end process for Managed Vulnerability Security

### Scoping

To get started using Managed Vulnerability Security, a Barracuda Solutions Architect will gather the necessary information and data in order to properly establish the scope. This is a crucial step to ensure all assets and sites will be covered. The key information that needs to be defined at this stage is the expected volume of assets (any device/system with an IP address connected to the network) that exist within the organization's networks, the number of sites the organization has and how they are connected, and lastly the environment in which the scanning applications will be installed; Windows or Linux servers and physical servers, virtual servers, or cloud resources.

### Deployment

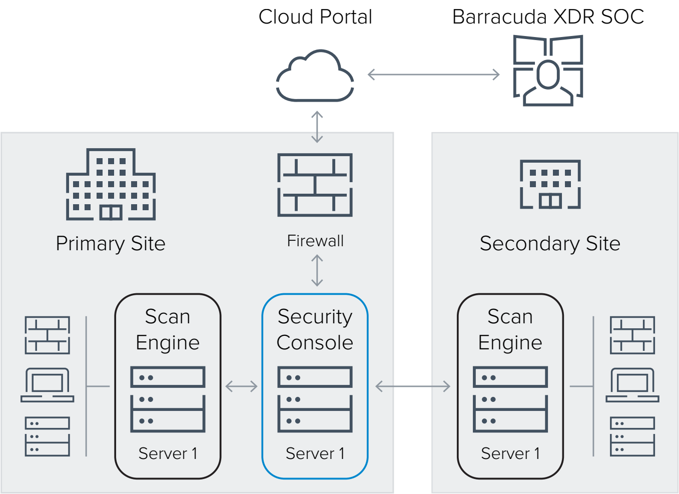
Once the scope is defined, the deployment process begins. A member of the Barracuda XDR Enablement Engineering team will provide the organization with step-by-step instructions to deploy the service, tailored to the established scope. The deployment itself is quite simple and typically can be completed in a day or two. Below is an overview of the process.

1. The organization provisions the required dedicated servers to host the scanning applications. Note that the organization is responsible for providing this infrastructure. The benefit of this approach is that the bulk of the scan data lives on the organization's network, on infrastructure which they own.
2. Once the dedicated servers are provisioned, the scanning applications will need to be downloaded and installed.
   - The first dedicated server will host the "Security Console" application.
   - The second dedicated server will host the "Scan Engine" application.
   - For organizations with multiple sites or larger volumes of assets, additional scan engine(s) may be needed.
3. While installing the scanning applications, the Barracuda Enablement team will provide components needed to complete the install. This includes a product key, credentials for setup, and a certificate for the Security Console.

4. Once the installation of the applications is complete, the organization will pair the Scan Engine(s) with the Security Console.

5. Next the organization will configure a NAT policy within their firewall or perimeter systems to allow connectivity between the Security Console and the SOC secure network. This will allow the SOC to fully manage the scanning.

6. The last step in the deployment process is optional but recommended for best results. This step is for the organization to configure a service account on the domain to be used for credentialed scanning. Credentialled scanning is not required, however it does provide better detail and insights compared to traditional scanning. More detail on the differences can be found in the "Running Scans" section below.



## Initial configuration

Once the deployment is complete, it's time for the SOC to configure the scan. The SOC team will work with the organization to gather some additional technical information in order to design the scan for the best results. This information includes:

1. The target subnet(s) to be scanned.

2. Exclusions if there are any. Some organizations prefer not to scan certain systems connected to the network such as printers or VOIP systems.

3. Preferred days/times for the scans to run. Some organizations may prefer to run the scans outside of business hours to avoid any unforeseen interruptions. Other organizations may prefer to run the scans during business hours to maximize the number of devices connected to the network at the time of the scan. There is no right or wrong answer on scan timing, it's based on the organization's preference.

By default, the scans will be scheduled to run on a quarterly basis. This cadence aligns with typical compliance requirements and allows for ample time between scans for IT teams to remediate the identified vulnerabilities. If the organization prefers, the frequency of the scans can be increased to an every-other-month, or a monthly schedule. The SOC will also offer customers the ability to request 1 ad hoc scan per quarter.

## Running scans

Once the scans have been configured, they will run on an automated basis per the pre-defined scan schedule. The scan is designed to detect and assess vulnerabilities that exist within the networks.

The scan will identify active services, open ports, and running applications on each asset in an effort to find vulnerabilities that may exist based on the attributes of the known services and applications. The vulnerability data is automatically updated and refreshed every six hours to ensure scans are being run using the latest data available so that even the newest vulnerabilities can be effectively identified.

The scans are designed to be non-obtrusive, meaning it shouldn't even be noticeable while running. The organization and its users shouldn't expect to experience any sort of interruptions, latency, or resource consumption. This can vary based on certain factors such as if outdated systems are in use or available bandwidth and resources are already constrained. But typically, no interruption or impact should occur when running the scan.

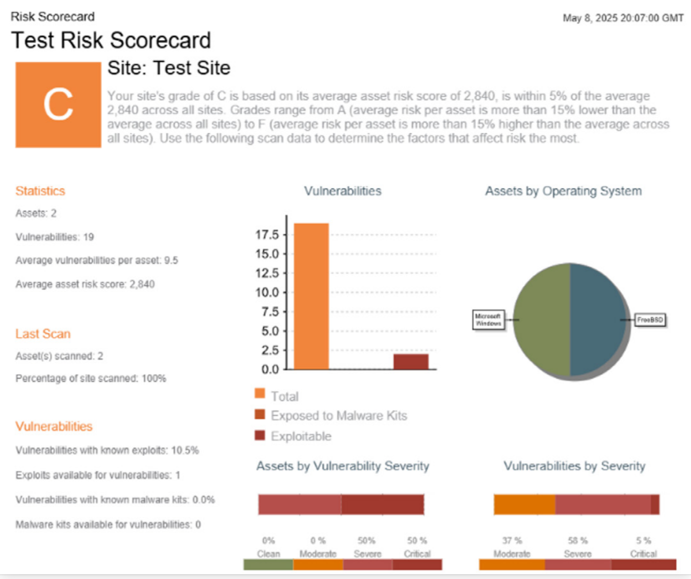
As previously mentioned, credentialed scanning is recommended for the best results. By allowing the scan engine to authenticate to each system on the network, it will have greater visibility and gather the most data. This provides for a more in-depth vulnerability analysis and finds exposures that would be hidden without authentication. Non-credentialed scans offer more of a surface level assessment of vulnerabilities that can be seen from the network.

The scan time varies based on several factors affecting network conditions, including the volume of assets, network bandwidth, and resource capacity on the systems. Most organizations can expect their scan to complete within 2-6 hours. Some organizations may take longer, the 12-24 hours time range is not entirely uncommon.

## Reporting

Shortly after the scan is completed, the SOC team will provide the organization with reports containing the findings of the scan. Four reports will be provided:

1. The audit report: contains the full results of the scan, from an executive summary with easy to digest visualizations, to each individual vulnerability found and the necessary remediation actions to address it.
2. The top remediations report: a more focused report outlining the top 25 remediations by risk score — which is a calculation that factors in the number of vulnerabilities addressed by a single remediation, the number of assets impacted, and severity factors. This report outlines the remediations which if addressed will have the largest impact on securing the organization's environment.
3. The remediation plan report: a detailed guide for IT teams to use in order to mitigate the vulnerabilities found. The report is organized by risk level, providing organizations with a simple to follow strategy on how to prioritize remediation efforts.
4. The risk scorecard report: a high-level overview of the organization's overall risk as calculated based on the scan results and vulnerabilities present. The report provides a letter grade along with other visualizations and metrics to score risk.



Risk Scorecard

May 8, 2025 20:07:00 GMT

Test Risk Scorecard

C

Site: Test Site

Your site's grade of C is based on its average asset risk score of 2,840, is within 5% of the average 2,840 across all sites. Grades range from A (average risk per asset is more than 15% lower than the average across all sites) to F (average risk per asset is more than 15% higher than the average across all sites). Use the following scan data to determine the factors that affect risk the most.

Statistics

Assets: 2

Vulnerabilities: 19

Average vulnerabilities per asset: 9.5

Average asset risk score: 2,840

Last Scan

Asset(s) scanned: 2

Percentage of site scanned: 100%

Vulnerabilities

Vulnerabilities with known exploits: 10.5%

Exploits available for vulnerabilities: 1

Vulnerabilities with known malware kits: 0.0%

Malware kits available for vulnerabilities: 0

## Remediation

Having received the aforementioned vulnerability reports from the SOC, the organization is responsible for remediating the identified exposures. Fortunately, this process is made easy by specific remediation guidance being provided for each vulnerability directly in the reports delivered. IT teams will easily be able to review the report and know, without having to research, what actions need to be taken in order to reduce the organization's risk. If any clarification or assistance is required, the organization may contact the SOC (soc@barracuda.com) and an expert from the SOC team will provide the needed support.

| CATEGORIES | BARRACUDA MANAGED XDR | PARTNER/ CUSTOMER |
|---|---|---|
| Scan configuration and administration | ✓ | |
| Scheduling and execution | ✓ | |
| Report verification and notifications | ✓ | |
| Maintenance and updates of scan aps/ components | ✓ | |
| Health monitoring and service assurance | ✓ | |
| Reviewing scan reports | | ✓ |
| Patching | | ✓ |
| Notifications for network changes | | ✓ |
| Maintenance of host VMs | | ✓ |

## Conclusion

Barracuda's Managed Vulnerability Scanning product is a vital addition to the overall XDR suite, providing organizations with the tools they need to enhance their cybersecurity defenses. By combining comprehensive scanning capabilities with expert support, Barracuda empowers businesses to stay ahead of potential threats and maintain a robust security posture.

For more information, you can visit the Barracuda Managed XDR product page.

Your business, secured.