Comparison with Barracuda Vulnerability Manager

https://campus.barracuda.com/doc/67174826/

Barracuda Networks has two tools associated with web application vulnerabilities. The scanning engine in both tools is identical; the difference is in the additional capabilities provided beyond the scan.

This article helps you to distinguish between them and choose which one is right for you.

Barracuda Vulnerability Manager

The Barracuda Vulnerability Manager is a fast and easy way to assess the security of your web application. It is designed as an **informative** tool, determining and reporting your security status. It is free, easy-to-use, and requires no set-up.

If you **do not have** a Barracuda Web Application Firewall, use the Barracuda Vulnerability Manager to assess your security and help you understand how you can improve your web application security.

Barracuda Vulnerability Remediation Service

The Barracuda Vulnerability Remediation Service is a full-fledged tool that not only finds vulnerabilities, but remediates (fixes) them using the Barracuda Web Application Firewall. It also allows you to implement automated workflows to periodically scan your applications and mitigate newly-found vulnerabilities. It is included with your purchase of a Barracuda Web Application Firewall and requires use of the Barracuda Web Application Firewall.

If you **have already purchased** a Barracuda Web Application Firewall, use the Barracuda Vulnerability Remediation Service to simplify deployment and increase security.

Feature Comparison

Feature	Barracuda Vulnerability Manager	Barracuda Vulnerability Remediation Service

Cost	Free	Currently available free of charge to customers who have purchased a Barracuda Web Application Firewall with an active Energize Update subscription.
Scan Scheduling	Users can schedule a single scan for a specified time.	Users can schedule any number of recurring scans (daily, weekly, monthly).
Vulnerability Reports	Users can view the report for a single scan.	Users can choose between two types of reports per scan: executive summary and technical detail report. Users can also view a consolidated Vulnerability view, which aggregates scan results across all scans of a single web application.
Mitigation Process	Manual: Users export the report from the scanner and import it into their WAF.	Automatic: Users can mitigate vulnerabilities on a Barracuda WAF with a single click from within the tool.
Mitigation Testing	None.	Users can apply a mitigation in "passive mode", also known as "test mode." In this mode, violations are logged, but not blocked. This allows the user to verify there are no false positives before enabling the mitigation in "active mode" or "block mode." For more information, see Understanding Passive Mode and Active Mode .
Mitigation Automation	None.	Users can select one of three automation policies for new vulnerabilities: 1. **Manual**: Mitigations are not applied automatically. 2. **Passive Mode**: Mitigations are applied immediately in "passive mode," so the user can confirm there are no false positives before applying them in "active mode." 3. **Active Mode**: Mitigations are applied immediately in "active mode."
Mitigation Monitoring	None.	Users can select a specific mitigation, and view Web Firewall logs from the Barracuda WAF that are related to that particular mitigation.
Email Notifications	Users can receive an email notification when a scan completes.	Users can receive an email notification either when a scan completes, or only when the scan detects new vulnerabilities. The email also contains a summary of the newly detected vulnerabilities.