Monarx Security

Technical Overview

Prevent Web Shells Before They Cause Damage

Monarx, Inc. HQ
8 E Broadway
Salt Lake City, UT
sales@monarx.com

Table of Contents

Executive Summary

The Application and Cybersecurity community is focused on the symptoms of web server malware, not the source.

Internet-facing websites are a prime target for attackers to monetize and launch attacks. Web Application Firewalls, Patching, and Malware Scanning solutions don't solve the problem. Despite the best efforts of Hosting Providers and Enterprises, websites continue to be compromised by hackers.

38.1[1]% of the internet's websites run a PHP-based open source CMS, and they are a prime target for attackers. In addition to being poorly secured, due to the broad and dynamic set of poorly maintained plugins, themes, and extensions that are available. The very thing that attracts users to open source CMS also creates its largest security problem. The frequency and impact of successful attacks continues to rise to extraordinary levels. Furthermore, 71% of these attacks use a PHP-based backdoor/web shell after successful exploitation. When activated, the shells are used to modify source files, replicate malicious code, deliver malware to website visitors, send spam, mine cryptocurrency, or participate in larger bot activities. Unfortunately, these types of attacks are also the hardest to diagnose and clean up.

Webshell attacks typically have four stages:

1. An initial exploit is used to create an opening to deposit a web shell (payload)
2. Web shell is deposited in a location accessible by the web server
3. The web shell is activated (used) via internet browser
4. Files are modified or embedded across the website, or the shell uploads tools or additional web shells

Monarx has developed a product that provides an unprecedented level of real-time protection against PHP web shell attacks. Monarx detects and prevents all bad outcomes associated with web shell attacks, keeping websites safe before a successful attack can do damage. The software also identifies all web shells and compromised files already on the server.

Web Application Security like Monarx plays a key role in stopping attacks before they become large cleanup projects, use up valuable resources, or erode customer goodwill.

Monarx can add value by delivering a new approach that achieves:

- Automated, accurate prevention of Payload (web shell) attacks without additional overhead to resources
- Visibility into the initial attack vector to prioritize patching and remediation
- A stop to the never-ending cleanup process and customers getting blacklisted
- Enhanced security with marginal impact on system and application performance
- Broad coverage that includes on-prem, cloud, and hybrid environments

This paper provides a technical overview of the components and approach that makes up the Monarx solution.

---

1 https://w3techs.com/

Product Overview

Monarx provides an Application Security solution to protect open source CMS Websites against the top attack method used to compromise these sites. Monarx does this with an easily deployable server-side agent that does not require any configuration or operational changes to an environment. This solution consists of four main components:

Protect

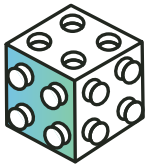
Exploit detection and web shell prevention module That tracks web shell payload deposits and blocks their execution.

Hunter

Malware scanning module that discovers existing compromises, including standalone web shells and compromised source binaries.

Dashboard

A cloud-hosted web-based console for viewing detection information, configuring settings, and generating reports.



Agent

A server-side agent that that is responsible for running Monarx modules and for communicating, configuring, and sending detection information to the Monarx Cloud.

The Monarx Agent is the customer-installed component of the Monarx Solution consisting of the Agent and modules (Protect and Hunter). It was designed for the specific needs of shared and dedicated web Hosting providers and natively supports Hosting provider platforms such as cPanel, Plesk, and Cloud Linux, including cageFS. It also supports LiteSpeed, NGINX, and Apache web servers.

The Agent downloads rules, discovers server configuration information, and executes client-side tasks such as scanning, diagnostics, and updating. The Agent is responsible for all secure communication between the local Monarx modules and Monarx Cloud. This includes detection events and detailed metadata from both Protect and Hunter modules at the server level, giving it visibility across all vHosts. To ensure maximum protection, the Agent should be installed on all supported web servers in a client's environment.

Monarx Hunter

The Monarx Hunter is a PHP malware scanner that is purpose-built to find standalone web shells and compromised source files quickly and efficiently. The Hunter is made up of two components 1) An agent-based scanning engine that leverages an evolving set of curated YARA rules to find any potentially malicious or compromised PHP files. 2) A cloud processing engine where files can be further analyzed using dynamic analysis, analytics, Machine Learning, signatures, and whitelists to keep false positives low and avoids missing anything malicious.

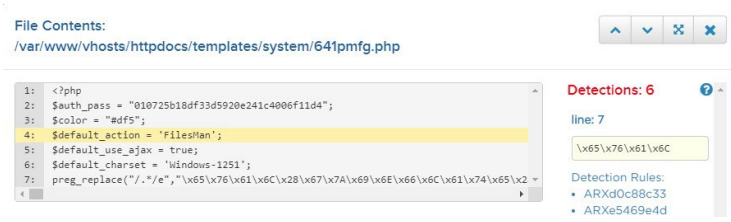
The result:

- Standalone malicious files are categorized as web shells so they can be easily flagged for remediation or blocking with Protect.
- Compromised source files are categorized as injected/compromised and malicious code is highlighted in the application.

At agent install, Hunter automatically determines the web server's doc/app roots for efficient and targeted scanning. It also performs an initial full scan used for a compromise assessment. This establishes the current state of infection on a server before Monarx Protect is in place. Any files identified by Hunter are automatically added to Protect's Watchlist feature to monitor web shell activity even if Protect did not see the initial file deposit. Files added to Protect from Hunter can also be blocked, never allowing future activation, thereby reducing remediation requirements for stand-alone web shells.

Hunter uses two different scanning methods for complete coverage, a weekly scheduled full scan, and a real-time scan. Subsequent full scans help to determine metrics as part of ongoing client remediation efforts. The real-time scanner leverages the operating system and Monarx Protect to analyze files as they get deposited through the file system or PHP. When Hunter detects a malicious file, it provides a rich set of information:

- Device Name
- Virtual host (s)
- Filename
- Path
- Last Modified
- Type (Web shell or compromised)
- 3rd Party Anti-Virus Context
- SHA 256
- Detection Rule (How Monarx found it)
- A highlight of the exact line of malicious code (based on the detection rule) in a detailed view of the file as seen below



As malicious files are introduced across the userbase, Monarx Protect shares them with Hunter creating a more efficient hunting and detection tool. As detection rates rise, insight is gained into the latest methods of web shell creation and obfuscation.

Monarx Protect - Prevention

Monarx Protect provides protection against all PHP based web shells regardless of entry/ deposit method. The software accurately identifies web shells as they are deposited and as they modify PHP scripts. Most commonly, these files appear through exploits of a plugin, theme, or extension or through an existing web shell. Protect prevents these files from being activated in PHP, thus preventing them from doing any damage.

Protect evaluates PHP file deposits based on our industry-leading entry vector determination engine with no initial dependence on definitions, patterns, advanced heuristics, regular expressions, or signatures – meaning Monarx needs no prior knowledge of the exploit or vulnerability. As a result, Protect does not have the 'false positive' problem that is pervasive with traditional signature-based products.

Protect lives in the application stack as a PHP module that observes how files are deposited and then executed by the server-side scripting engine. When Protect determines a file deposit is malicious, it adds the file to the Protect Watchlist. The Watchlist is a component of Protect used to track PHP file introductions/ modifications classified as malicious. When a PHP file is activated via the webserver, Protect compares the request to its watchlist to determine if it should generate an alert or block the action.

Instead of trying to block the initial exploit or trying to determine if a file is malicious after the fact, Protect watches the file as it is introduced and can block the execution before the web shell can be used. We call this approach Post Exploit Prevention because Protect does not attempt to stop the exploit, instead it limits resulting damage to zero by blocking the activation of the payload.

Because the exploit still occurs, the Monarx software also provides deep visibility into each attempted attack including how the malicious script got in, from where, and the origins of any activation attempts. Depending on the action type (Deposit or Activation) Protect captures the following attack information:

- Date
- Device Name
- Virtual Host
- Severity (Malicious/Suspicious)
- Action (Prevent/ Detect)
- Detection Type (Activation/Deposit)
- File Name
- File Directory
- Entry URL
- Line Number
- Exit file name
- Execution Function Name
- IPv4 Address
- IP Address Country
- SHA-256 Checksum
- Classification (Web Shell / Compromised)
- Exploited Plugin or Theme

Application Modes: Protect

Users can configure each server or group to run in any of the available Protect modes:

Disabled: This mode will turn off Monarx's Protect monitoring and protection services. In this mode, Hunter Scanning is still performed, but Protect is no longer watching for new file deposits, file modifications, and activations.

Detect: This mode detects new file deposits, existing file modifications, and file activations that happen via the web server/PHP and flags those deemed malicious by Protect. Detect mode is useful for evaluation purposes, testing the effectiveness of the Monarx solution, and can be instrumental in exposing potential vulnerabilities within the environment.

Block (Prevent): This mode prevents the activation/execution of Protect or Hunter observed malicious PHP files. ***It does not prevent the initial payload from being deposited on the system after the attack.*** The Monarx approach watches the web shell attack happen and then prevents the execution of web shells. All prevention activities are logged along with supporting metadata. Protect Block options are:

- **Malicious** (Web Shells) – blocks the execution of standalone web shells `
- **Malicious** (Compromised) – blocks the execution of source files that have injected code determined to be compromised
- **Suspicious** – blocks the execution of suspicious files such as potentially unwanted applications

Switching between the Protect modes is easy within the Monarx Dashboard and provides organizations an opportunity to test, verify, and deploy the Monarx solution with minimal impact on production servers.

The Monarx Application Security approach is unlike WAF (Web Application Firewall) and traditional malware scanners that rely on preventing the initial attack or having a known signature. It does this by preventing the execution/activation of the malicious file that attackers attempt to use.

Monarx Dashboard

Monarx Dashboard provides a web-based interface for viewing Monarx detection data, key metrics, managing application configuration, defining security policies, identifying device information, downloading reports, and accessing the reporting API key.

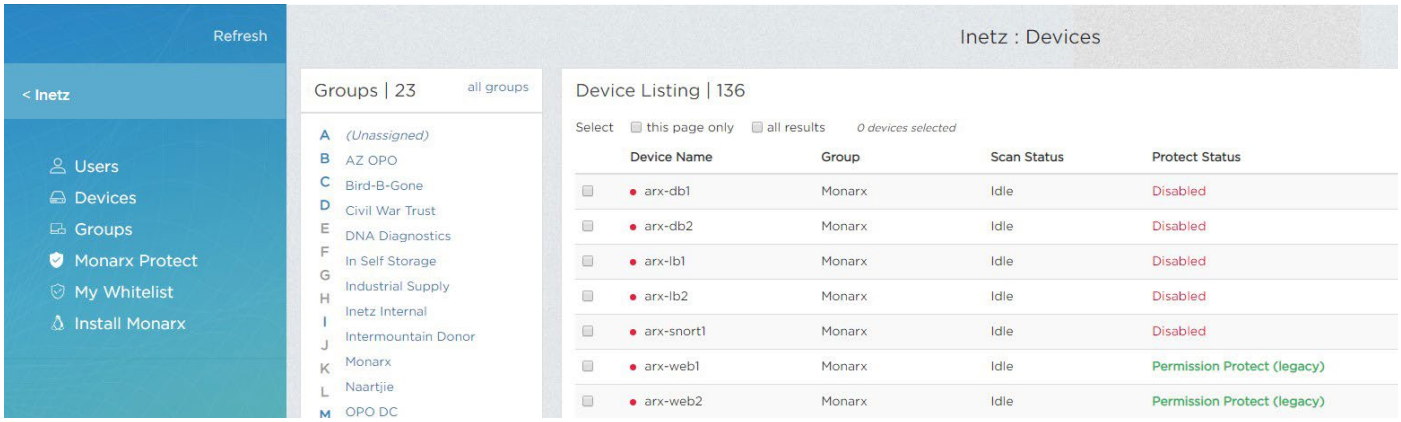
The dashboard has three sections:

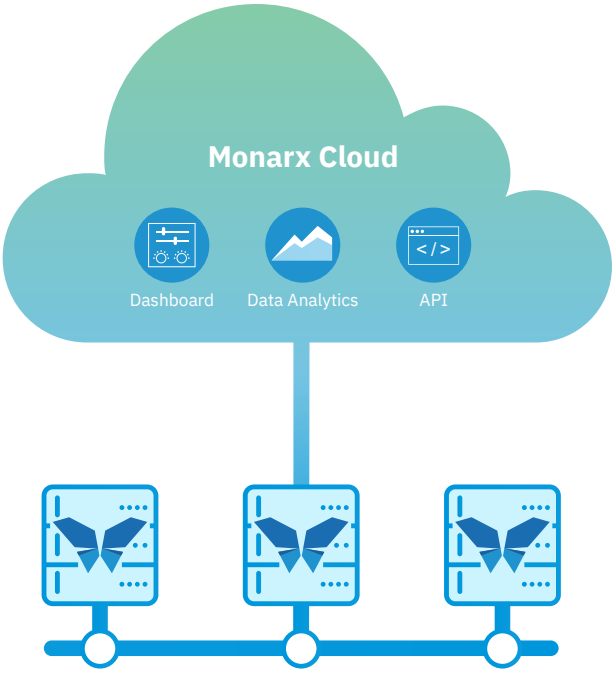
- Protect: Dedicated to viewing Protect detection information
- Hunter: Dedicated to viewing Hunter detection information
- Configuration: Allows a user to create groups, check agent status, initiate scans, and configure Protect

The Protect and Hunter sections have attack specific data visualization widgets to identify key servers and groups. The default detection grid organizes data by time, device, group, vHost, severity, and type. The expanded grid view supports a robust set of filtering, sorting, and report generation. Each detection has a detailed view that adjusts based on the detection type to show supported metadata. All extended metadata in the detailed view for each detection is included in the download report for further analysis.

The detection metrics may be transmitted to custom data stores, made directly available to logging tools, or fed into a Security Information and Event Management (SIEM) system via our RestfulAPI.

Figure 1. Monarx Configuration Manager Home Page





Monarx Protected Web Servers

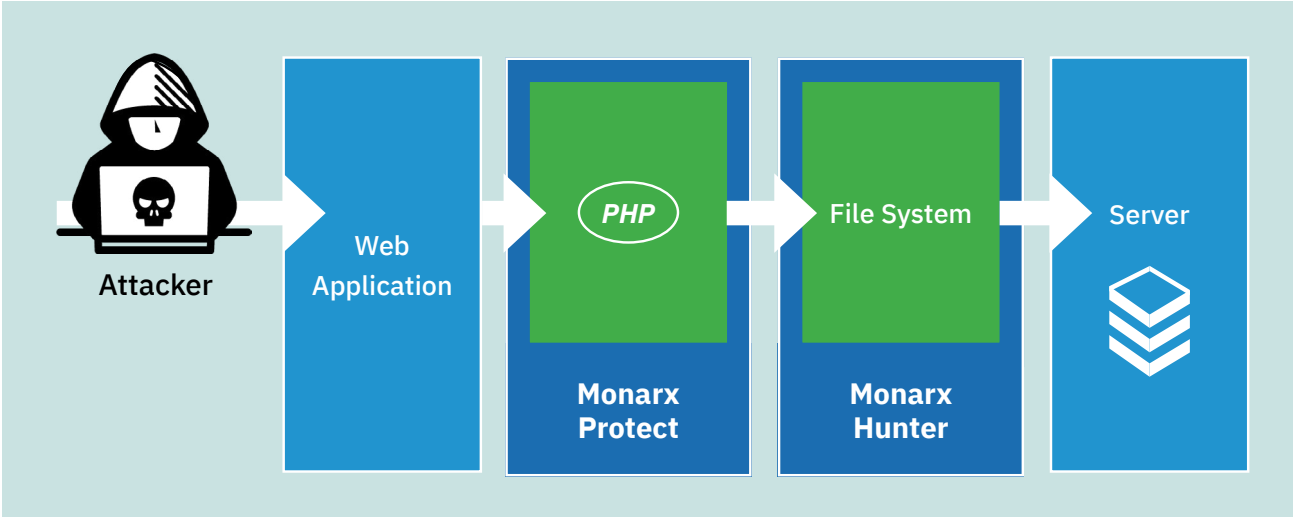
Architecture and Deployment

Monarx is an easy to deploy scalable SaaS solution (no additional hardware required) which can be integrated into different environments based on specific needs and requirements.

Monarx Dashboard - Threat Anylitics

Every deployment includes the Monarx Linux server-side agent that communicates with the Monarx Cloud, access to the Protect Module, Hunter, and the Restful API. Detection data is stored in the Monarx cloud for viewing and further analysis. A single agent will provide complete protection/visibility across all vHosts on the server regardless if it is a dedicated or shared environment. The only requirements are supported Linux Operating System <https://www.monarx.com/quick-start>, and agent connectivity to the Monarx cloud.

A logical representation of Monarx agent and modules:



Overview of Monarx Features

	Hunter	Protect Detect	Protect Block
Exploit detection (ability to identify entry vector for attack)		✓	✓
Web Shell/Payload Deposit detection		✓	✓
Real-time notification of payload (web shell) activations		✓	✓
Real-time blocking/prevention of payload (web shell & compromised file activations)			✓
Real-time notification when a source file is compromised/ injected with malicious code		✓	✓
Identify existing compromised source files	✓		
Identify existing standalone web shells	✓		
New web shell creation outside of PHP	✓		
Integration with SIEMs and log management software via API	✓	✓	✓

The most common customer deployment scenarios include:

- Shared server environment running single or multiple different types of Open source CMS with 100's or 1000's of vHosts and different versions of PHP.
- Dedicated environment running a single instance of a PHP web application

The setup and deployment process are straight forward:

- Go to Monarx.com and click on the Free Scan link
- Create a company account, receive an email with a link to the agent installer and company-specific key
- Install the agent(s) on servers
- Hunter Compromise assessment scan automatically starts (constrained to doc/ app root)
- Protect is enabled to detect mode
- View results of Hunter Malware assessment (detection of standalone and compromised source files that existed before the Monarx agent was installed)
- Review Protect activity (new file deposits and activations)
- Schedule a time to review Monarx Compromise Assessment

Protect Feature Spotlight

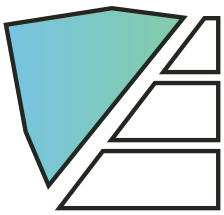
Monarx's Protect stops the leading method used by attackers to exploit/compromise Open source CMS – web shells. Protect identifies how the web shells got in and prevents their execution before they can be used be to do any damage. Two key modules make up Protect's core functionality:

Payload Attack Feature

- **Feature:** Monarx Protect stops all forms of Web shell activations by watching incoming application file execution commands.
- **How It Works:** If the file is on the Monarx Protect Watchlist, and the software is in Block Mode, activation is blocked, rendering the web shell inert. If Detect Mode is enabled, the system will record the activation.
- **Benefit:** The Monarx Protect engine allows hosting providers to create a security buffer between vulnerable plugins and themes and their own critical systems.

Exploit Detection Feature

- **Feature:** The Protect exploit detection module automatically identifies the exact plugin, file, and line of code that was used to perform the exploit and deposit the web shell.
- **How It Works:** By analyzing the runtime flows and calls in the PHP code in conjunction with the Protect entry vector determination engine.
- **Benefit:** This information helps prioritize which plugins/themes should be patched or removed.



Product Benefits

Real-time Post Exploit Payload Prevention

Eliminates the threat of PHP based web shells/ backdoors thereby reducing the risks of getting blacklisted, distributing malware, resource theft via crypto mining, and spamming.

Protection for Vulnerable Plugins & Themes

Unpatched plugins and themes with known vulnerabilities and security issues can be prevented from causing damage, thereby creating a safety buffer.

No More Cleanup

Prevents web shells from being able to inflict damage thus eliminating the time-consuming task of cleaning up a site with compromised source files.

Ease of Implementation

The Monarx solution is delivered as a fully scalable software-as-a-service solution. The only component required is the installation of the Monarx agent which includes Protect and Hunter. No re-configuration or manual whitelisting is required to start taking advantage of Monarx.

Eliminate Zero-day Attacks

Monarx's entry vector determination engine automatically detects and blocks malicious payloads even if the web shell is unknown.

In-depth Threat Intelligence

Monarx captures rich information regarding every attempted attack and makes it available in the dashboard. The detection details enable operation and security teams to understand how web shells are entering and provide visibility into where the attacks originated.

Identify Hacked Plug-Ins and Themes

By tracking how web shells enter the system, Monarx can identify which plugins and themes are being exploited and need attention.

Complimentary Proof of Value

If given an opportunity to perform a compromise assessment, Monarx will identify existing web shells and compromised files on your servers. The software will continue to monitor your servers and vHosts with Protect for 2-3 weeks and identify active shells, new shells, and the utilization of compromised source files. At the end of the Proof of Value, we will provide a compromise assessment report with our findings and recommendations.

No upfront commitment or phone call is required. Just register here, <https://www.monarx.com/quick-start> install the agent on any number of servers and let us do the rest to prove out the value of Monarx.

Conclusion

Monarx was born out of lessons learned from building and operating open source CMS web applications. The frustration of identifying web shells and cleaning up the damage led to the initial product invention. We are laser-focused on preventing the impact of the most common attack vector for hosting providers - web shell/payload attacks. We can give resource constrained teams visibility into the attack source and prevent the attack from causing damage. Web shells can be stopped.

Technical Overview