Hosted.com Adds Monarx and Imunify360 to Counter Zero-Day Website Threats

Hosted.com has integrated Monarx and Imunify360 across its hosting platform, pairing runtime behavioral prevention with signature-based malware scanning.



Hosted.com has integrated Monarx and Imunify360 across its Web Hosting and WordPress Hosting platforms, adding runtime behavioral prevention and automated malware scanning to every account.

CA, UNITED STATES, September 10, 2026 /EINPresswire.com/ -- Hosted.com has integrated two independent security engines, Monarx and Imunify360, across its Web Hosting and WordPress Hosting platforms. The pairing combines runtime behavioral prevention with signature and reputation-based scanning, an approach intended to narrow the window in which newly discovered software flaws and automated attacks can reach customer websites.

The integration places both engines inside the hosting environment itself, rather than treating security as an add-on that customers install and configure after their site is live. Detection, quarantine, and response run continuously at the server level for every account on the platform.

> “Most small businesses will never hire a security engineer. A host's job is to make that unnecessary, so detection and recovery are already running before anyone notices a problem.”
>
> *Wayne Diamond*

Why the Patch Window Is the Problem

A zero-day vulnerability is a software flaw that attackers find and exploit before the vendor has released a fix. The term refers to the number of days the vendor has had to respond: zero. The exposure period runs from the moment an exploit begins circulating until a patch is published and, critically, until the site owner actually applies it.

That second gap is where most small websites are compromised. A patch that exists but has not been installed offers no protection. For a business running WordPress with a dozen plugins, several of which may be updated infrequently by their developers, the practical exposure

window can extend well beyond the vendor timeline.

The scale of the underlying problem is documented. Google Threat Intelligence Group, in its report "Look What You Made Us Patch: 2025 Zero-Days in Review" published in March 2026, tracked 90 zero-day vulnerabilities exploited in the wild during 2025, up from 78 in 2024. Exploitation has remained in a range of roughly 60 to 100 per year over the past five years, an elevated baseline compared with pre-2021 activity.

Two Detection Models, Deliberately Different

Monarx and Imunify360 were selected because they identify threats in fundamentally different ways. Running both means a threat that evades one model can still be caught by the other.

Monarx uses runtime application self-protection, commonly abbreviated as RASP. Rather than comparing files against a list of known malware signatures, a RASP engine observes what a script actually does while it is executing and blocks behavior associated with compromise. Because the method targets behavior rather than known code patterns, it can act on malware that has never been catalogued. Monarx applies this to threats including web shells, phishing kits, adware injections, and file uploaders. The analysis workload is offloaded to the Monarx cloud service, which limits the processing burden placed on hosting servers.

Imunify360 approaches the same problem from the opposite direction, through a layered stack of established controls. Its web application firewall inspects incoming traffic for SQL injection, cross-site scripting, and illegal resource access. Its intrusion detection and prevention system monitors server logs for patterns such as repeated failed logins and blocks the originating addresses. Its malware scanner operates in real time and on demand across server files, the databases of content management systems including WordPress, and scheduled cron jobs, which are a common persistence mechanism for attackers.

A separate Proactive Defense engine analyzes PHP script behavior as it runs and can patch known vulnerabilities at that layer to prevent reinfection through the same route.

Imunify360 also draws on a shared threat intelligence network. When an attacking address is identified on one protected server, it is blocked across every server in the network, which shortens the useful life of an attack pattern once it has been observed anywhere in the system. Signature-based scanning is fast and accurate against threats that have already been documented. Behavioral prevention covers the period before documentation exists. Running the two together is intended to reduce the gap that either would leave on its own.

The Wider Security Stack

The two engines sit within a broader set of controls already in place across Hosted.com hosting plans. FortiGate firewalls filter traffic at the network edge, alongside distributed denial-of-service protection. CageFS, a CloudLinux technology, isolates each hosting account in its own file system, so a compromise contained to one account cannot read the files of another on the same shared server. SpamExperts filters inbound and outbound email.

Recovery is handled separately from prevention. Daily backups run through Acronis and can be restored if a site is damaged or encrypted. WordPress plans include a staging area, allowing plugin and theme updates to be tested on a copy of the site before they reach the live version, which reduces the incentive to delay security updates out of concern that they will break something. Free SSL certificates are included across plans, and the platform carries a 99.9 percent uptime commitment.

Where AI Fits, and Where It Does Not

Hosted.com has framed the role of artificial intelligence in current website attacks in measured terms. According to the company, generative and automated tooling has not created an entirely new category of website threat. What it has changed is throughput. Reconnaissance that once required an attacker to manually probe a target can now be scripted across large numbers of sites, and the work of adapting a technique when a first attempt fails has become considerably cheaper.

The practical consequence for a small website is that the interval between a vulnerability becoming public and that specific site being probed has narrowed. Defenses that depend on a human noticing a problem and responding to it are poorly matched to that timescale, which is the reasoning behind placing automated detection and containment at the hosting layer.

Designed for Businesses Without Security Staff

Most of the businesses running the affected sites do not employ anyone whose job is security. A small firm typically has one person handling updates, monitoring, customer data, and uptime, usually alongside unrelated responsibilities. Security work competes with that list and frequently loses to it.

Moving detection, isolation, and recovery into the hosting platform shifts a category of work off that person entirely. Scans run without being scheduled, suspicious files are quarantined without a ticket being opened, and a clean restore point exists without anyone remembering to create one.

Hosted.com has been explicit that no configuration eliminates risk. The stated aim of the integration is narrower and more defensible: to shorten the interval between compromise and containment, and to ensure a recovery path exists when prevention does not hold.

"Most small businesses will never hire a security engineer. The job of a host is to make that unnecessary, so detection and recovery are already running before anyone notices a problem." Wayne Diamond, Founder and CEO of Hosted.com

Availability

Monarx and Imunify360 protection is active across Hosted.com Web Hosting and WordPress Hosting plans at no additional cost. Details of the security features included with each plan are

published at www.hosted.com.

About Hosted.com
Hosted.com provides Web Hosting, Domain Registration, and WordPress Hosting services for businesses, freelancers, and entrepreneurs. The company focuses on reliability, consistent performance, and accessible support to help customers set up, manage, and maintain their websites and hosting. Desku.io, a division of Hosted.com, is an AI-powered support and helpdesk solution that helps small businesses manage customer communication. It brings live chat, WhatsApp, social messaging, and email into a single shared inbox, with a no-code AI chatbot built for faster responses without requiring coding.

About Wayne Diamond
Wayne Diamond is the founder and CEO of Hosted.com and also serves as CEO of Desku.io, an AI-powered support management solution. With more than 25 years of experience in the web hosting and domain name industry, he has led the development of services that help businesses and individuals manage websites, domains, hosting, and customer support.

Marketing Department
Hosted.com
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/939721129

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.