imunify Security

CASE STUDY

STREAMLINE YOUR OPERATIONS WITH IMUNIFY360, KERNELCARE AND CLOUDLINUX OS

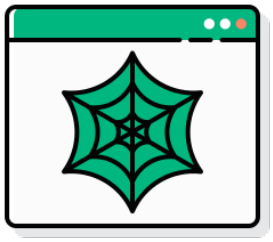
Server security is critical in any environment, but keeping up with the numerous sites hosted on a single server can exhaust administrator resources. Many of the security maintenance and monitoring necessary for good server security can be automated.

Without security automation, administrators can be overwhelmed with hacked sites, ongoing aggressive attacks such as distributed denial-of-service (DDoS), and malware abusing server resources. The result can be a drop in server performance and overall poor reputation for the shared provider. With automation tools, many of these issues can be mitigated and eradicated before they affect server performance and security.

SHARED HOSTING AND HACKED WEBSITES

Even the most secure host server could be vulnerable to malware. Research shows that the most well-known biggest host providers can be vulnerable to common cyber-attacks. In a shared hosting environment, WordPress is the dominant content management system (CMS) installed on customer websites. It also accounts for 90% of sites hacked every year. Most hacked content comes from vulnerable themes and plugins, but site owners are unaware of risks associated with third-party code and the importance of updating and patching software.

The trouble of chasing hacked sites in a shared environment is that some responsibility is left to the customer to keep their software updated and take the necessary steps to stop malware. Site owners don't have the experience and knowledge to block attacks, which leaves them vulnerable. For example, many site owners leave their WordPress software outdated including plugins.



Outdated software is one of the OWASP Top 10 for threat agents and has a high impact on the chance for a site to get hacked eventually. If site owners do not log into their sites occasionally to update software, the WordPress plugins and core software are left vulnerable to the latest exploits.

Another common issue is web shell scripts and other malware uploaded to misconfigured sites. No one should be able to upload files to the file system, but poorly configured sites allow uploads. It's also common for attackers to exploit plugins and features of WordPress that allow uploads of any file type. An attacker will upload these scripts or malware executables to distribute them to other victims or obtain higher privileged access on the hosting server. The attacker stores these files on the hacked site storage, which means it sits on the hosting server waiting for an attacker to trigger it or other victims to download the malicious content.

A hacked site can host a myriad of malicious content including backdoors, executables, trojans, phishing pages, and spam mailers. Since a shared host provider has potentially thousands of sites on one server, numerous hacked sites could affect performance from overutilization of compromised site requests. Poor performance on a shared host server results in customer loss, a poor reputation, and revenue loss. It's essential for administrators to find automated means to monitor and remove malware from hacked sites.

ABOUT INTERSERVER.NET

InterServer.net is a US-based hosting service with a good reputation for quality service at an affordable price. They have two datacenters on the east and west coast of the US to service their thousands of customers including small individual site owners to Fortune 500s. InterServer.net prides itself on fast servers and customer response.

Because InterServer.net prides itself on fast technician response times, it's critical that they stay proactive about security issues. When technicians are overloaded with support tickets, they cannot respond to all customers within a reasonable time delaying a response and frustrating site owners. InterServer.net looked to Imunify360 to mitigate growing issues with hacked sites on their servers so that they could respond faster to issues and automate security.

InterServer.net looked to Imunify360 to monitor for malware and CloudLinux OS to harden security. Both products quickly became a fan favorite among support technicians and their CTO as a way to provide fast customer service while still hardening security across physical servers. In addition, InterServer.net used KernelCare to update the operating system without requiring a reboot. Because they no longer needed to reboot servers after updates, InterServer.net could avoid complications associated with rebooting servers.

HOW A COMBINATION OF IMUNIFY360, CLOUDLINUX OS AND KERNELCARE MADE INTERSERVER.NET MORE EFFICIENT

Before working with Imunify360, InterServer.net experienced a high increase in hacked sites. They struggled to keep up with the service demands of customer support tickets. InterServer.net implemented Imunify360 to alleviate much of the support technician overhead on hacked sites and cleaning these sites from malware. They leveraged Imunify360's ability to detect hacked content and clean it automatically. This saved much of the support technician's time to respond to other important customer issues.

When searching for cybersecurity solutions, InterServer.net looked for a malware solution in Imunify360 and a security hardening system in CloudLinux OS. Combined, these two services lowered incidents of hacked sites. In addition to CloudLinux OS and Imunify360, KernelCare became a favorite within the business for updating and patching the Linux kernel without requiring a server reboot. With these three services, InterServer.net could automate cybersecurity and kernel patching, saving technicians and administrators overhead and time.

The CloudLinux, Imunify360, and KernelCare team became a partnership with InterServer.net. It's this partnership that kept InterServer.net growing internally and expanding CloudLinux products across their environment. They also found that the Imunify360 team was always available for support, and they could work together to resolve issues. It's this support and service that continues to be one of the major factors in InterServer.net's continual loyalty to all three CloudLinux products.

SHARED HOSTING SUPPORT TECHNICIANS FACE INCREASED FRUSTRATIONS WITHOUT SECURITY AUTOMATION

Without automation, hosting providers are stuck finding manual ways to mitigate and remove malware. In a shared environment, this isn't an efficient solution or manageable for server technicians. Just like InterServer.net needed a more efficient way to monitor and block malware, shared hosting providers that use manual methods are not leveraging the tools necessary to free up technician time and protect server resources from malware.

Lack of automation can cause several issues and creates unnecessary overhead for support technicians. A shared hosting provider that does not introduce security monitoring can face.

Manual management of security solutions. Manually managing cybersecurity requires extensive time, consumes resources unnecessarily, and introduces a higher chance of human error. Human errors can lead to catastrophic mistakes leading to critical downtime and data breaches. It's estimated that human errors account for 60% of data breaches. As an example, Capital One Financial Corporation misconfigured security features on their web application firewall allowing an attacker to exfiltrate 100 million customer records. The data breach is still one of the biggest to date.

SHARED HOSTING SUPPORT TECHNICIANS FACE INCREASED FRUSTRATIONS WITHOUT SECURITY AUTOMATION

Imunify360 has several automation features including a web application firewall that stops malicious requests. It contains a command-line interface to configure it's features, but it also works effectively out-of-the-box with little implementation effort. Administrators can work with advanced controls using the command-line interface, API, incident management and overall configurations of the security suite.

> The combination of Imunify360, CloudLinux OS, and KernelCare are an easy solution to manage all aspects of your business.
>
> **INTERSERVER.NET**

Another issue facing shared host providers working with manual security is lack of support options for customers 24/7. Most providers need comprehensive customer support, but they will work with fewer staff during off-peak hours. Imunify360 provides a way for shared host providers to give site owners 24/7/365 cybersecurity support. The Imunify360 team also provides their own highly experienced professionals to assist the shared host provider's technicians and administrators should they have any questions. Their 24/7/365 support team is what InterServer.net considers one of the most valuable factors in continually using Imunify360 as a cybersecurity automation solution.

In addition to convenience and better support, Imunify360 takes care of much of the security associated with shared hosting servers and the hacked sites that use critical resources. It helps support technicians who might not be familiar with the latest cyber-attacks to better mitigate and eradicate threats from the server allowing them to focus on other critical maintenance.

CONCLUSION

With CloudLinux OS, KernelCare and Imunify360, shared hosting providers have full-scale security mitigation, prevention and eradication. CloudLinux OS hardens security against attackers, Imunify360 removes malware, and KernelCare patches the kernel to remediate vulnerabilities. These three solutions together automate many of the security processes leaving your support team free to focus on other business essentials and still keep servers safe from malware.

Try Imunify360 Security suite for free for 14-days and forget about malware on the server and endless customer complaints.

Automate your web-server security now!