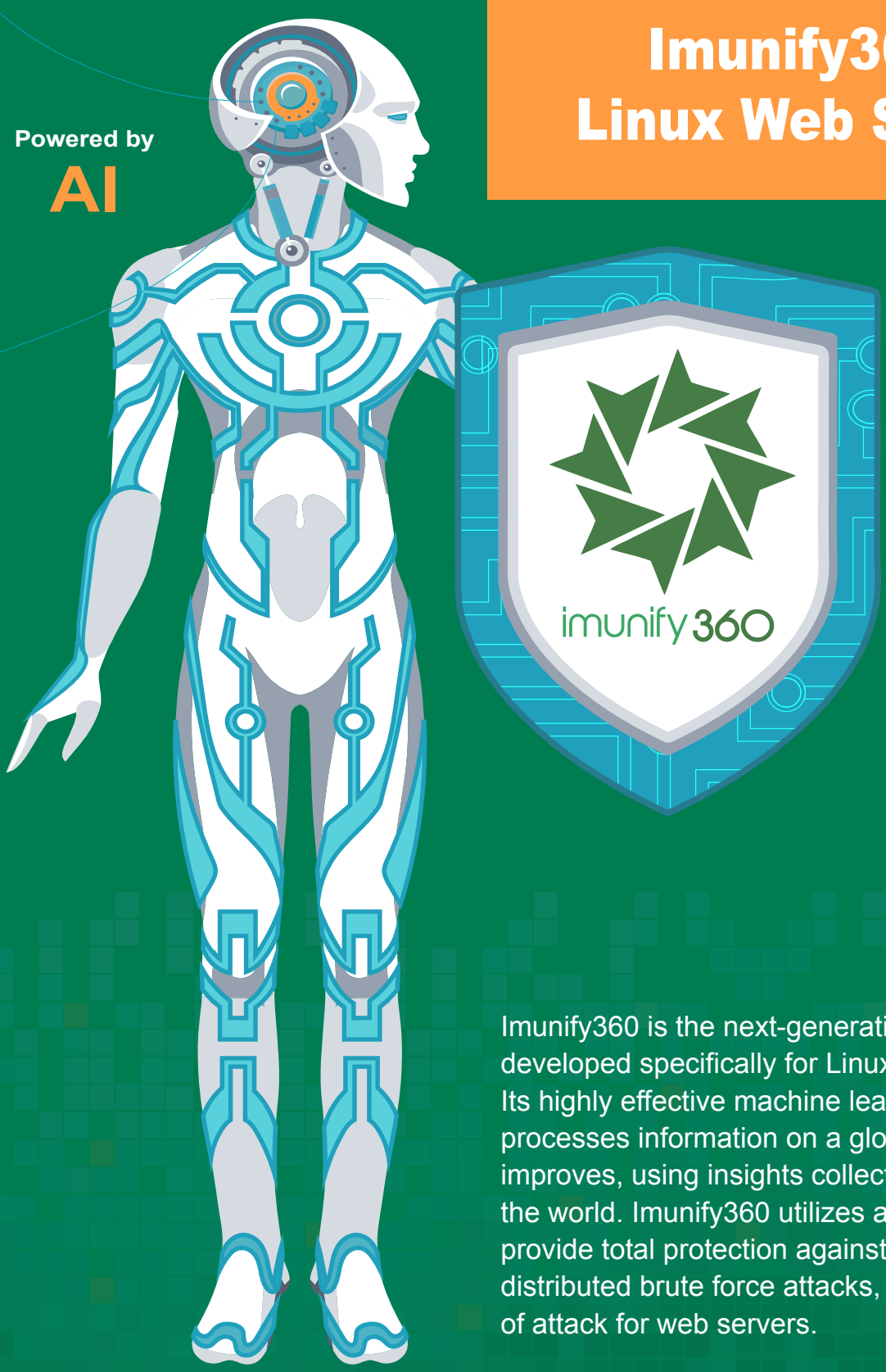
POOJA INFOTECH

Imunify360 Keeps Linux Web Servers Safe

Powered by AI



Imunify360 is the next-generation security solution developed specifically for Linux web servers. Its highly effective machine learning technology processes information on a global scale and constantly improves, using insights collected from servers all over the world. Imunify360 utilizes a six-layer approach to provide total protection against threats, including distributed brute force attacks, the most common type of attack for web servers.

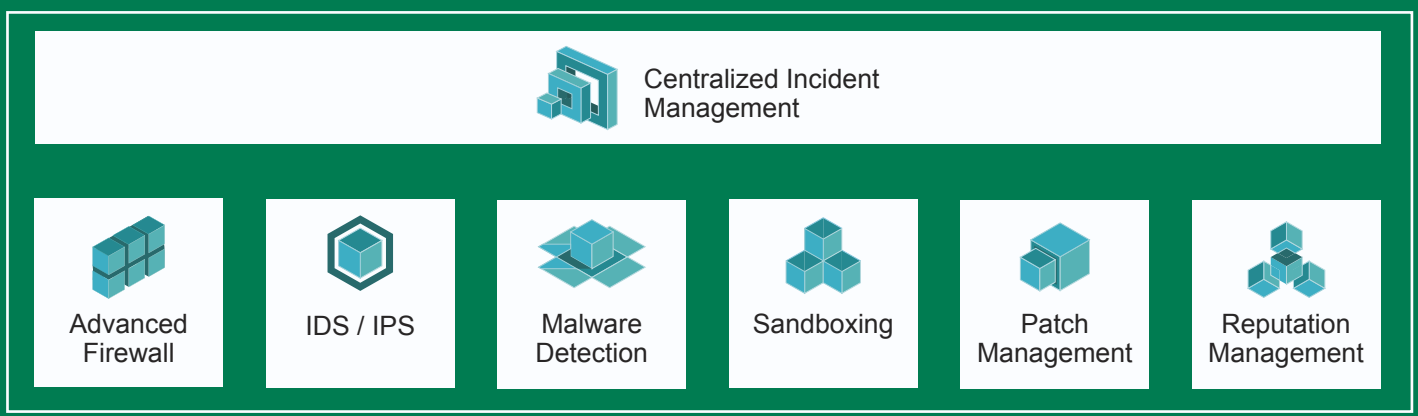
Imunify360, Powered by AI

Imunify360 constantly collects and processes a massive amount of information about new attacks from servers all over the world. It analyzes the web traffic that hits your servers, understands all security threats, and uses powerful AI technology to dynamically update its rules and prevent malicious attacks that could cause harm. It uses machine learning technology and extensive, signature-based algorithms to identify patterns of abnormal behavior in near real-time to quickly prevent new attacks.

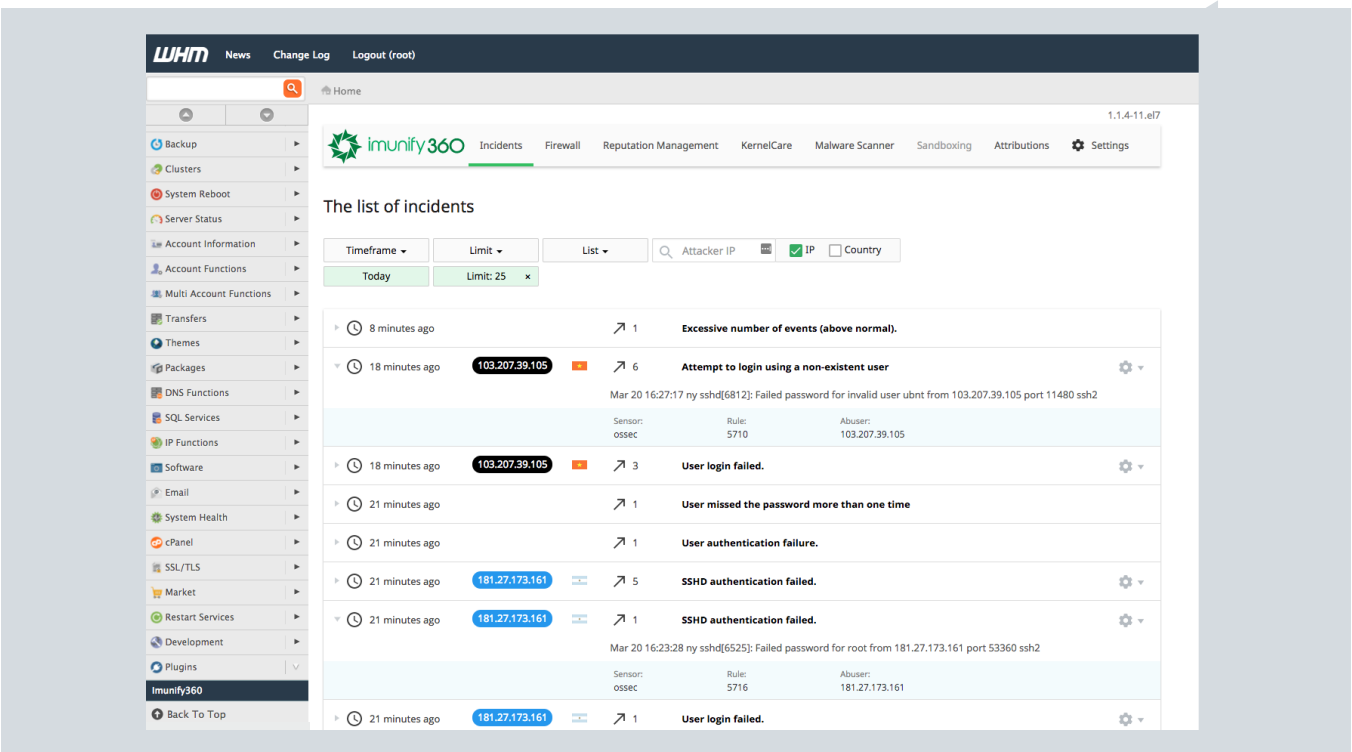
The Imunify360 difference

- Delivers sophisticated detection and display of security threats, powered by the self-learning firewall with herd immunity.
- Protects servers against many threats, including distributed brute force attacks, the most common threat to web servers.
- Analyzes insights from the global network to ban attackers before they even attack you.
- Protects web applications against malware injections and defacement attacks.
- Automatically secures your kernel and older PHP versions.
- Is highly effective in catching more bad guys while stopping fewer good guys, because it is powered by the smart intrusion detection that collaborates with the central intrusion system.
- Includes additional features such Reputation Management and an advanced Captcha system for vetting website visitors.
- Is a responsive system with a high frequency of scanning that does not degrade the performance of your servers.

Imunify360



All-in-one, automated security solution with self-learning capability and a centralized management dashboard for VPS, dedicated, and shared servers



Imunify360 delivers:

Better security: Sophisticated detection of security threats, including distributed brute force attacks, powered by the self-learning firewall with herd immunity.

Cost efficiency: Hands-off automation with fewer actions required to keep web servers secure. All security settings are managed from a single dashboard. No need to handle different solutions from different vendors.

High customer satisfaction: Secure servers deliver increased uptime and performance while live patching of kernels eliminates reboots associated with security updates.

Ease of use: You are able to start with the default setting - the intelligent automated configuration is sufficient in most cases - and have the option to manually configure if/when desired. Incredibly easy to install. Integrated with your control panel.*

Increased profits from VPS/dedicated customers: Offer Imunify360's comprehensive security to your customers as part of your product offering - bundled into your packages or sold individually - to generate additional revenue and offer more secure web servers without support headaches.

**** To learn more, visit http://poojainfotech.com/vps.html***

Key Features

Centralized Incident Management dashboard	Allows you to quickly check in on the overall state of your server and manage all aspects of its security. Displays all security events and the latest incidents updated every 30 seconds.	
Advanced Firewall with herd immunity	Prevents unauthorized users from accessing your servers. Uses herd immunity and artificial intelligence to detect new threats. Capable of defending against brute force attacks, DoS attacks, port scans, as well as many other types of attacks.	
Smart Intrusion Detection System	Collaborates with the central intrusion detection system to decrease the number of false positives and false negatives.	
IDS / IPS	Includes a comprehensive collection of “deny” policy rules to quickly block all known attacks. Monitors server logs and scans log files from all different angles and bans IPs that show malicious signs.	
Malware Scanning	Automatically scans file systems for malware injection and quarantines infected files	
Security Scanning	Detects outdated software components on your server.	*Coming soon*
Patch Management	Automatically updates outdated components or notifies you about them so you can take action manually.	*Coming soon*
Intelligent Web Applications Sandboxing	Learns what is and is not OK for your web applications to do and can create safety sandboxes around your applications - it prevents hackers from injecting malware, defacing your site, or escalating privileges.	*Coming soon*
Rebootless Secure Kernel (powered by KernelCare)	Enables running a secure kernel at all times by automatically patching kernels without having to reboot the server.	
LibCare	Automatically patches Glibc against vulnerabilities without having to restart the server.	*Coming soon*
Hardened PHP	Keeps your server secure by patching all PHP versions against known vulnerabilities. This allows you to run any version of PHP without having to update programs.	
Website Reputation Monitoring	Analyzes if your site or IPs are blocked by any blacklists and notifies you accordingly so that you can take action.	 *(domains only)*

To learn more visit http://poojainfotech.com/vps.html