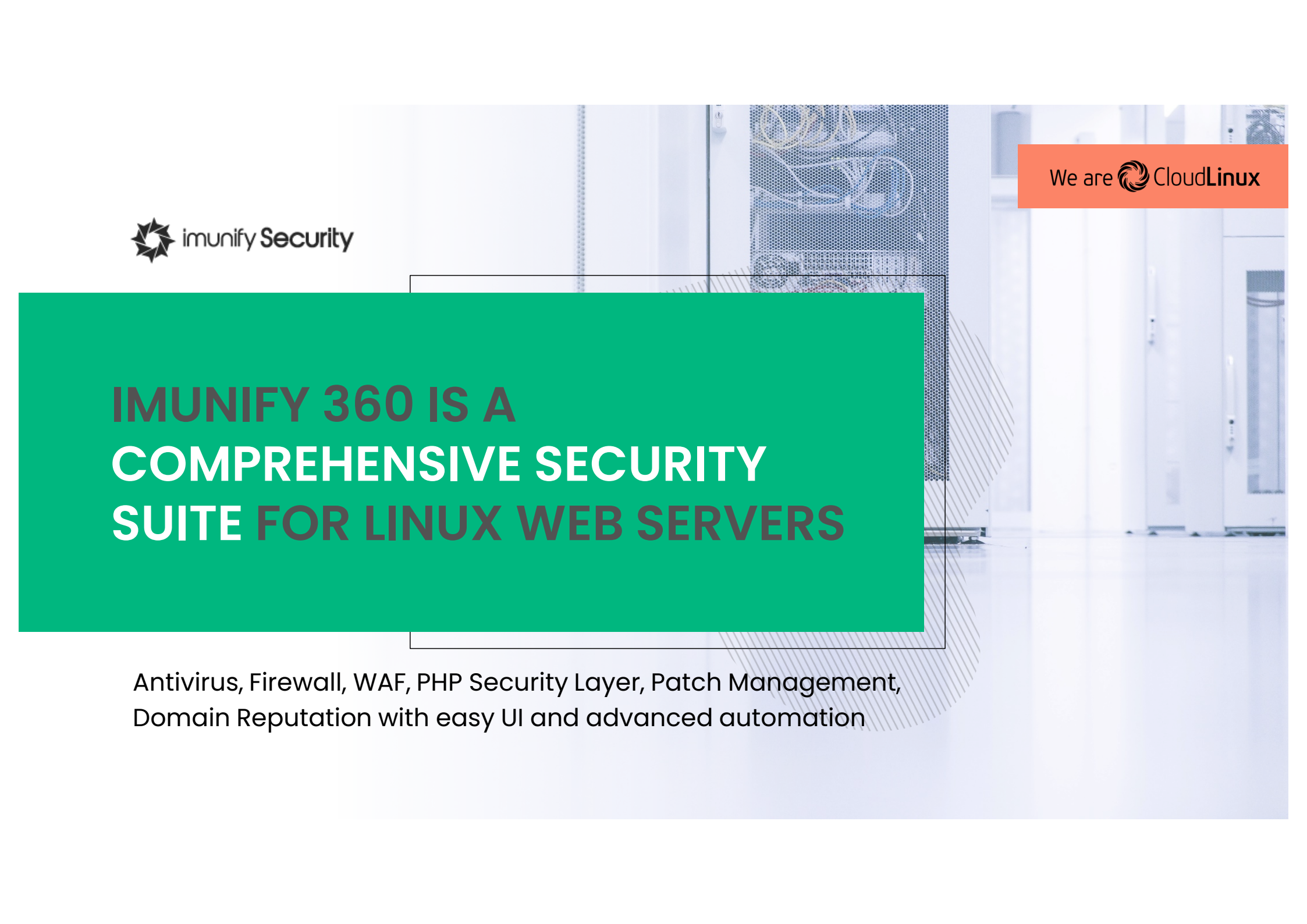


imunify Security

We are CloudLinux

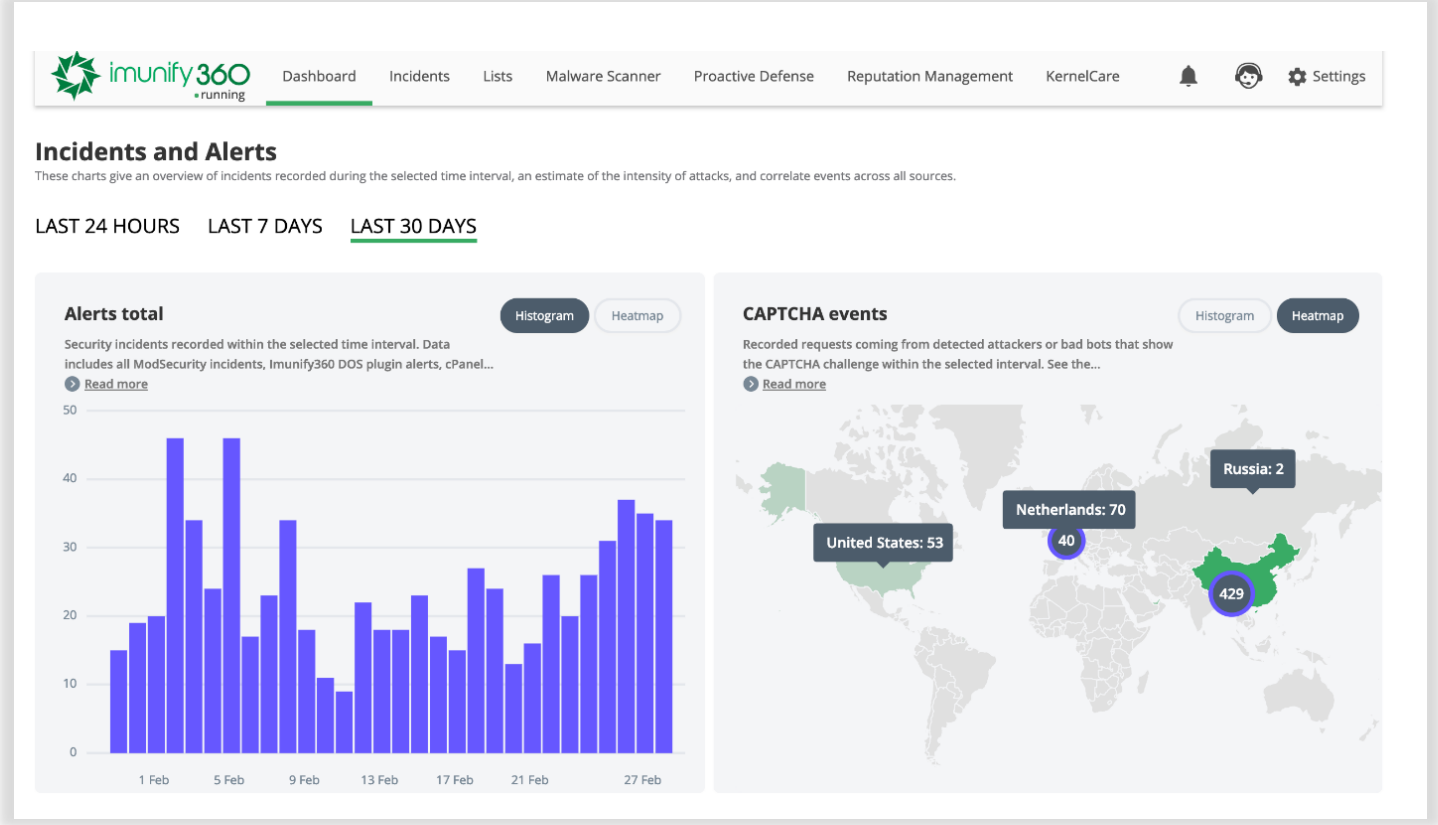
# IMUNIFY 360 IS A COMPREHENSIVE SECURITY SUITE FOR LINUX WEB SERVERS

Antivirus, Firewall, WAF, PHP Security Layer, Patch Management, Domain Reputation with easy UI and advanced automation

imunify Security

# IMUNIFY360 PROTECTS YOUR SERVER AND ALL HOSTED WEBSITES

Imunify 360 protects Linux based web servers and all hosted websites against malware infections, web attacks, vulnerability exploitation and all other threats.



imunify Security

# IMUNIFY360 WILL STOP

Vulnerability exploitations

Malware uploads

Sensitive data access

Website scraping and scanning


Web SPAM

Many other web threats

After extensively testing proactive defense, we're confident that it will stop almost all malware in real-time. Combined with the other features of Imunify360, there is nothing else on the market that offers such a high level of security.

RACK911 Labs

PATRICK WILLIAM
Rack911 Labs

imunify Security

# SEE HOW IMUNIFY TACKLES AND REMEDIES EACH KIND OF WEB-HOSTING ISSUE

## MALWARE ON THE SERVER

Imunify360's tight integration between the Real-time Malware Scanner, File Antivirus, WAF, Automated Cleanup Tool and the Proactive Defense leaves malware no chance to be dropped and run on the server.

Our Malware Scanner will detect and clean up any malicious injections and web-shells from both files and databases keeping websites operational.

## LACK OF PROTECTION BY FREE SOFTWARE

Replace the zoo of free security tools (generic WAF, free antivirus, open-source IDS & IPS) with a highly integrated security solution from Imunify.

It is tailored to identify and block any threat before it can do any harm, get the synergy of the component using shared knowledge about incidents in the system to block them effectively.

imunify Security

# SEE HOW IMUNIFY TACKLES AND REMEDIES EACH KIND OF WEB-HOSTING ISSUE

## TOO MUCH CARE REGARDING SECURITY

Imunify360 is a completely automated security solution working efficiently out of the box. It provides a comprehensive command-line interface and API for advanced control, incident management and configuration of the security suite.

## EXCESSIVE RESOURCE USAGE

Imunify's Advanced Firewall with Cloud-based Heuristics protects against all types of brute-force attacks targeting FTP/SSH/SMTP/Hosting Panel logins/etc. Imunify360 reduces server load caused by DoS / brute-force attacks and malware running on infected websites. Let your customers use server resources, not malware.

imunify Security

# SEE HOW IMUNIFY TACKLES AND REMEDIES EACH KIND OF WEB-HOSTING ISSUE


## BLACKLISTED SERVER IP

Imunify360 keeps IP reputation clean, preventing outgoing SPAM sent by bad actors or malware running on the server.

## OUTDATED SERVER SOFTWARE AND WEB APPS

Imunify360 provides complete real-time virtual and physical patching of vulnerable software by KernelCare, HardenedPHP, WAF and the Proactive Defense modules.

imunify Security

# SIX LAYERS OF SECURITY IN IMUNIFY360

## ANTIVIRUS

It's estimated that ⅛ of new files stored on a server are malicious. Antivirus is a basic component in cybersecurity but often overlooked in web application hosting. Most webmasters know that desktop antivirus is necessary for local device security, but they are unaware that antivirus is also necessary for web application security. Imunify360 identifies and cleans malicious content so that site owners do not need to manually find hacked files.

## FIREWALL

In simple applications, blocking all incoming traffic protects the internal network. This configuration is common for home firewalls, but it's not feasible in a hosting environment that needs advanced analysis for incoming and outgoing traffic. Imunify360 includes an advanced firewall that uses cloud heuristics and artificial intelligence (AI) to detect threats and block brute-force attacks often used to guess a user's credentials.

## WEB APPLICATION FIREWALL (WAF)

A standard firewall analyzes and filters all traffic, but a WAF targets HTTP traffic. By targeting
HTTP traffic, a WAF can block specific attacks against web applications such as XSS, SQL injection, file inclusion and several others. These attacks are commonly misunderstood and often hidden to webmasters who do not know how to monitor them. Traffic passes through the Imunify360 WAF that then analyzes its content to determine if it's malicious. If the request passes validation, it's forwarded to the web application.

imunify Security

# SIX LAYERS OF SECURITY IN IMUNIFY360


## DOMAIN REPUTATION

Imunify360 monitors various blacklists to find out if the domain is de-listed from search engines or blocked for malicious activity. Monitoring domain reputation allows webmasters to quickly remediate any issues should the site be compromised and identified as an attack site that distributes malware, sends spam messages, or hosts phishing content.

## PATCH MANAGEMENT

Cybersecurity of any application is never a “set it and forget it” event. Software vendors including plugin developers frequently deploy patches to remediate newly found vulnerabilities. To continue protecting a CMS, all plugins and the CMS software must be patched every time a new update is published. Imunify360 provides proactive cyber-defenses by patching software after developers deploy an update. By quickly patching the CMS, the webmaster reduces the window of opportunity for an attacker.


## PHP SECURITY LAYER

Web security is more than blocking incoming traffic. It also means identifying content on the site that could be silently performing malicious actions. For example, a PHP script injected into the site could be used to send spam emails to targeted recipients. Imunify360 is a proactive defense that adds an extra PHP Security Layer of protection, prevents malware execution in real-time, and ensures multi-level access blocking to malicious PHP files.