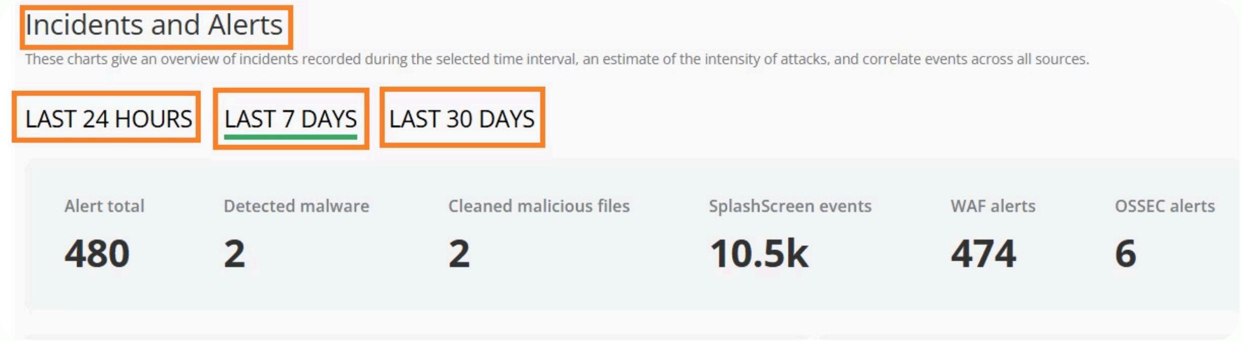
Imunify360: Comprehensive Server Security

Protect your servers with Imunify360's advanced security. This all-in-one solution offers proactive defense, automates threat detection, and enhances server stability.

ActiveServers
WEB HOSTING COMPANY

Why Imunify360 is Essential for Server Management



Incidents and Alerts

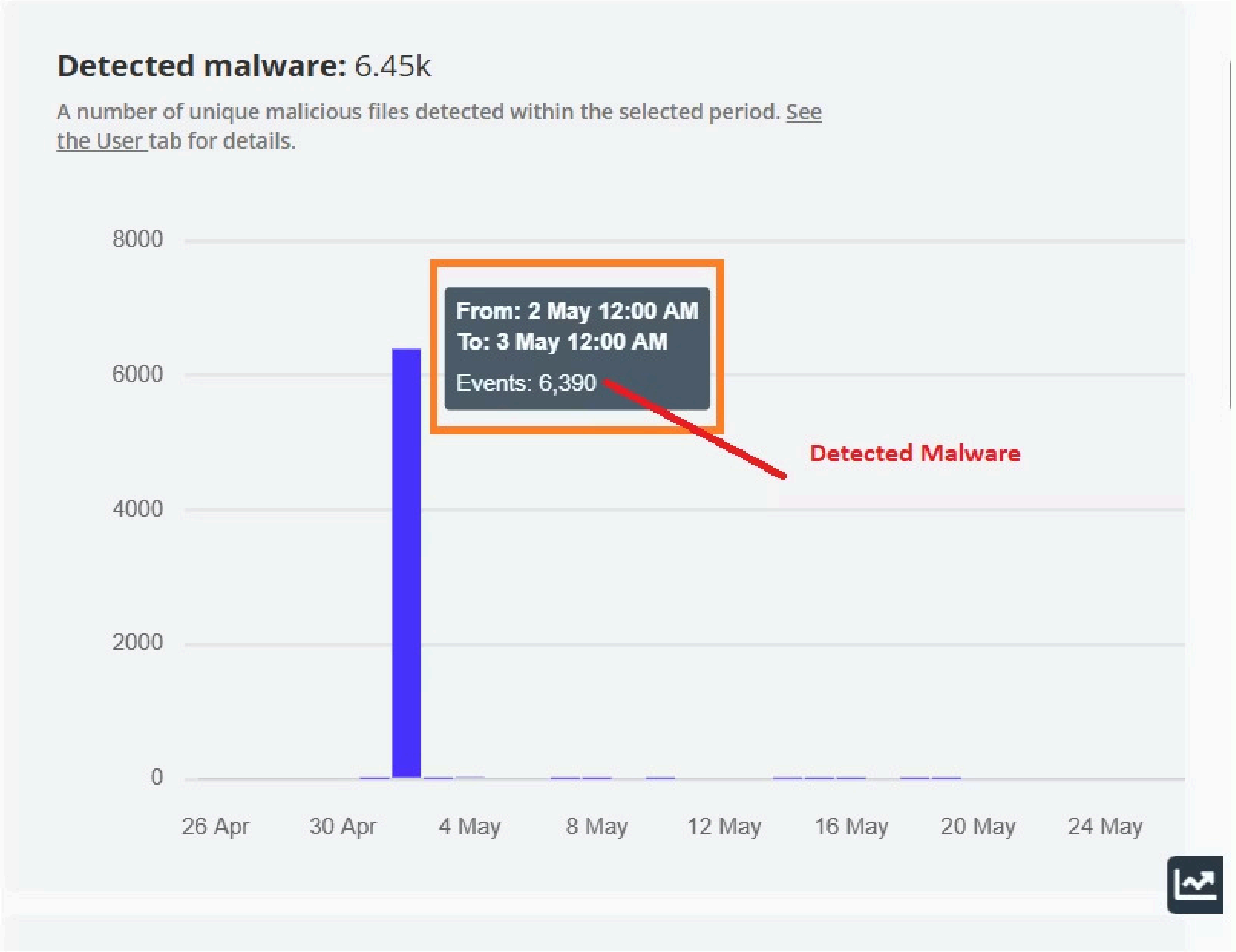
These charts give an overview of incidents recorded during the selected time interval, an estimate of the intensity of attacks, and correlate events across all sources.

LAST 24 HOURS | LAST 7 DAYS | LAST 30 DAYS

Alert total	Detected malware	Cleaned malicious files	SplashScreen events	WAF alerts	OSSEC alerts
480	2	2	10.5k	474	6

1. Real-Time Malware Processing:

Combines malware detection, firewall, patch management, and reputation management.

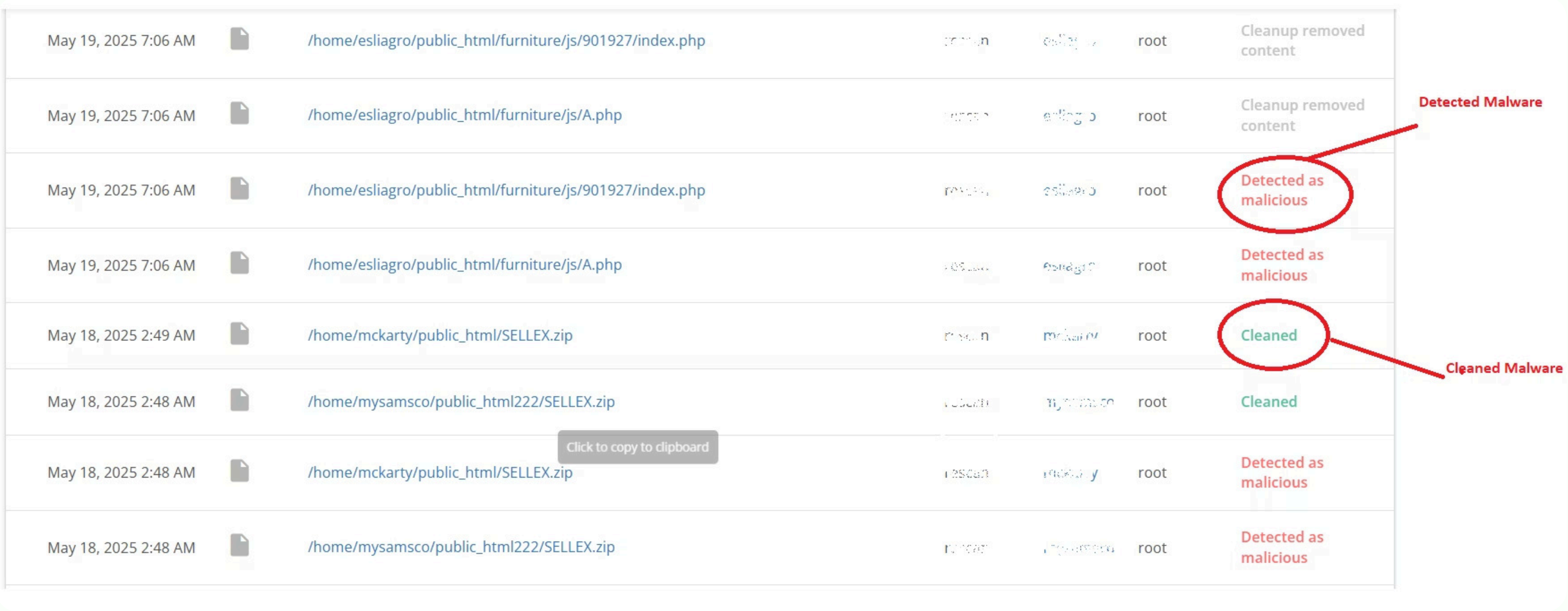


Detected malware: 6.45k

A number of unique malicious files detected within the selected period. See the User tab for details.

2. Malware Database Scanner:

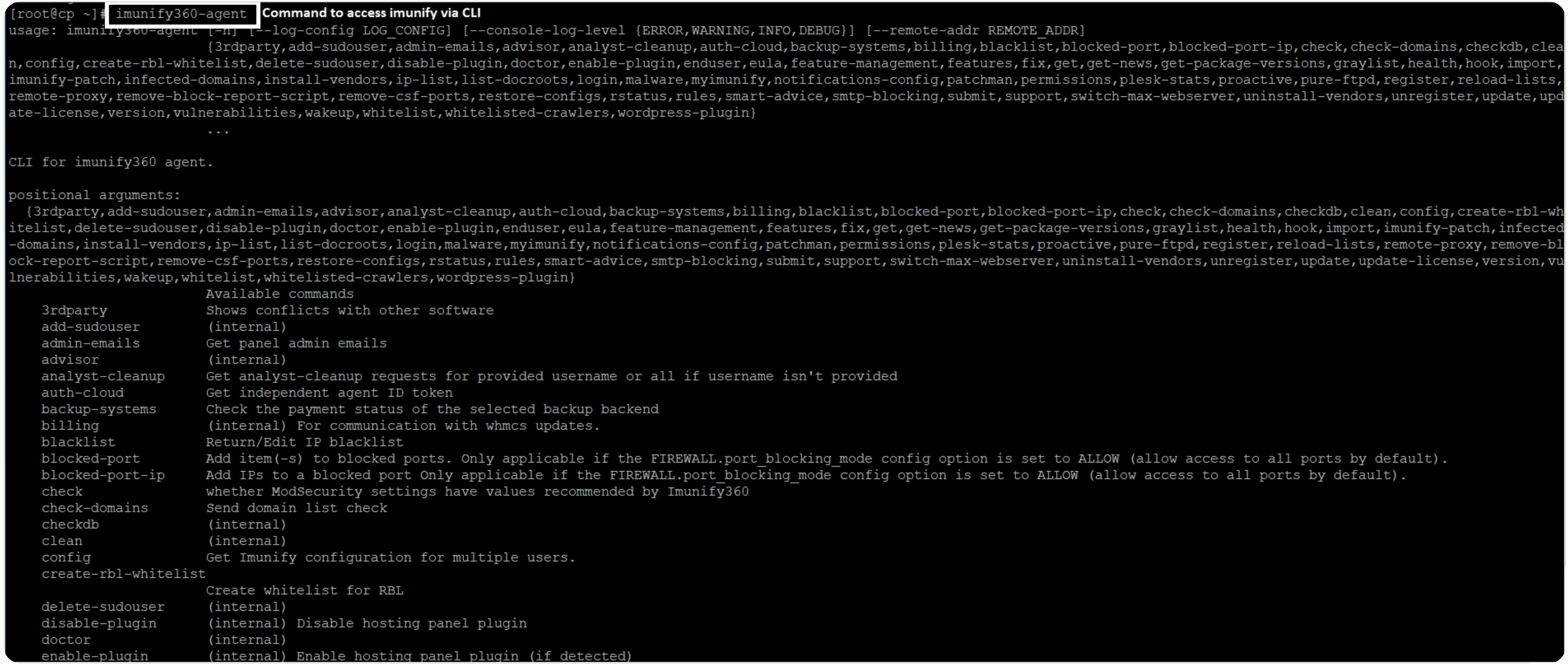
Automatically detects and blocks sophisticated cyber threats and attacks.



May 19, 2025 7:06 AM	📄	/home/esliagro/public_html/furniture/js/901927/index.php	[redacted]	[redacted]	root	Cleanup removed content
May 19, 2025 7:06 AM	📄	/home/esliagro/public_html/furniture/js/A.php	[redacted]	[redacted]	root	Cleanup removed content
May 19, 2025 7:06 AM	📄	/home/esliagro/public_html/furniture/js/901927/index.php	[redacted]	[redacted]	root	Detected as malicious
May 19, 2025 7:06 AM	📄	/home/esliagro/public_html/furniture/js/A.php	[redacted]	[redacted]	root	Detected as malicious
May 18, 2025 2:49 AM	📄	/home/mckarty/public_html/SELLEX.zip	[redacted]	[redacted]	root	Cleaned
May 18, 2025 2:48 AM	📄	/home/mysamsco/public_html222/SELLEX.zip	[redacted]	[redacted]	root	Cleaned
May 18, 2025 2:48 AM	📄	/home/mckarty/public_html/SELLEX.zip	[redacted]	[redacted]	root	Detected as malicious
May 18, 2025 2:48 AM	📄	/home/mysamsco/public_html222/SELLEX.zip	[redacted]	[redacted]	root	Detected as malicious

3. Automation via Command-Line & API:

For access to Imunify360 agent features from command-line interface (CLI), use the following command:



Command to access imunify via CLI

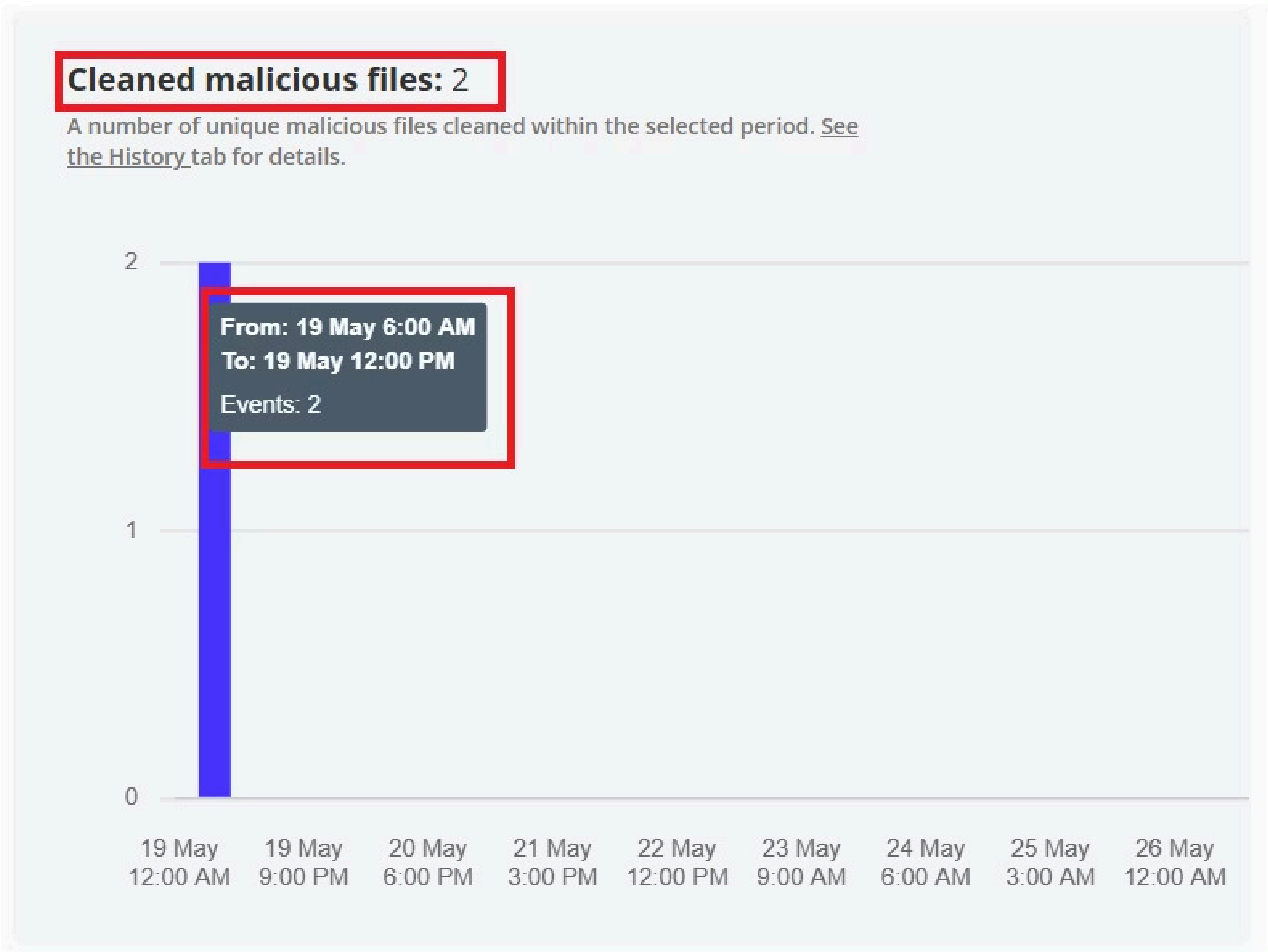
```
[root@cp ~]# imunify360-agent
usage: imunify360-agent [-h] [--log-config LOG_CONFIG] [--console-log-level {ERROR,WARNING,INFO,DEBUG}] [--remote-addr REMOTE_ADDR]
                        {3rdparty,add-sudouser,admin-emails,advisor,analyst-cleanup,auth-cloud,backup-systems,billing,blacklist,blocked-port,blocked-port-ip,check,check-domains,checkdb,clea
n,config,create-rbl-whitelist,delete-sudouser,disable-plugin,doctor,enable-plugin,enduser,eula,feature-management,features,fix,get,get-news,get-package-versions,graylist,health,hook,import,
imunify-patch,infected-domains,install-vendors,ip-list,list-docroots,login,malware,myimunify,notifications-config,patchman,permissions,plesk-stats,proactive,pure-ftpd,register,reload-lists,
remote-proxy,remove-block-report-script,remove-csf-ports,restore-configs,rstatus,rules,smart-advice,smtp-blocking,submit,support,switch-max-webserver,uninstall-vendors,unregister,update,upd
ate-license,version,vulnerabilities,wakeup,whitelist,whitelisted-crawlers,wordpress-plugin}
                        ...

CLI for imunify360 agent.

positional arguments:
  {3rdparty,add-sudouser,admin-emails,advisor,analyst-cleanup,auth-cloud,backup-systems,billing,blacklist,blocked-port,blocked-port-ip,check,check-domains,checkdb,clean,config,create-rbl-wh
itelist,delete-sudouser,disable-plugin,doctor,enable-plugin,enduser,eula,feature-management,features,fix,get,get-news,get-package-versions,graylist,health,hook,import,imunify-patch,infected
-domains,install-vendors,ip-list,list-docroots,login,malware,myimunify,notifications-config,patchman,permissions,plesk-stats,proactive,pure-ftpd,register,reload-lists,remote-proxy,remove-bl
ock-report-script,remove-csf-ports,restore-configs,rstatus,rules,smart-advice,smtp-blocking,submit,support,switch-max-webserver,uninstall-vendors,unregister,update,update-license,version,vu
lnerabilities,wakeup,whitelist,whitelisted-crawlers,wordpress-plugin}
                        Available commands
    3rdparty            Shows conflicts with other software
    add-sudouser        (internal)
    admin-emails        Get panel admin emails
    advisor             (internal)
    analyst-cleanup     Get analyst-cleanup requests for provided username or all if username isn't provided
    auth-cloud          Get independent agent ID token
    backup-systems      Check the payment status of the selected backup backend
    billing             (internal) For communication with whmcs updates.
    blacklist           Return/Edit IP blacklist
    blocked-port        Add item(-s) to blocked ports. Only applicable if the FIREWALL.port_blocking_mode config option is set to ALLOW (allow access to all ports by default).
    blocked-port-ip     Add IPs to a blocked port Only applicable if the FIREWALL.port_blocking_mode config option is set to ALLOW (allow access to all ports by default).
    check               whether ModSecurity settings have values recommended by Imunify360
    check-domains       Send domain list check
    checkdb             (internal)
    clean               (internal)
    config              Get Imunify configuration for multiple users.
    create-rbl-whitelist
                        Create whitelist for RBL
    delete-sudouser     (internal)
    disable-plugin      (internal) Disable hosting panel plugin
    doctor              (internal)
    enable-plugin       (internal) Enable hosting panel plugin (if detected)
```

4. Brute-Force Prevention:

Centralized dashboard that integrates with popular control panels like cPanel.



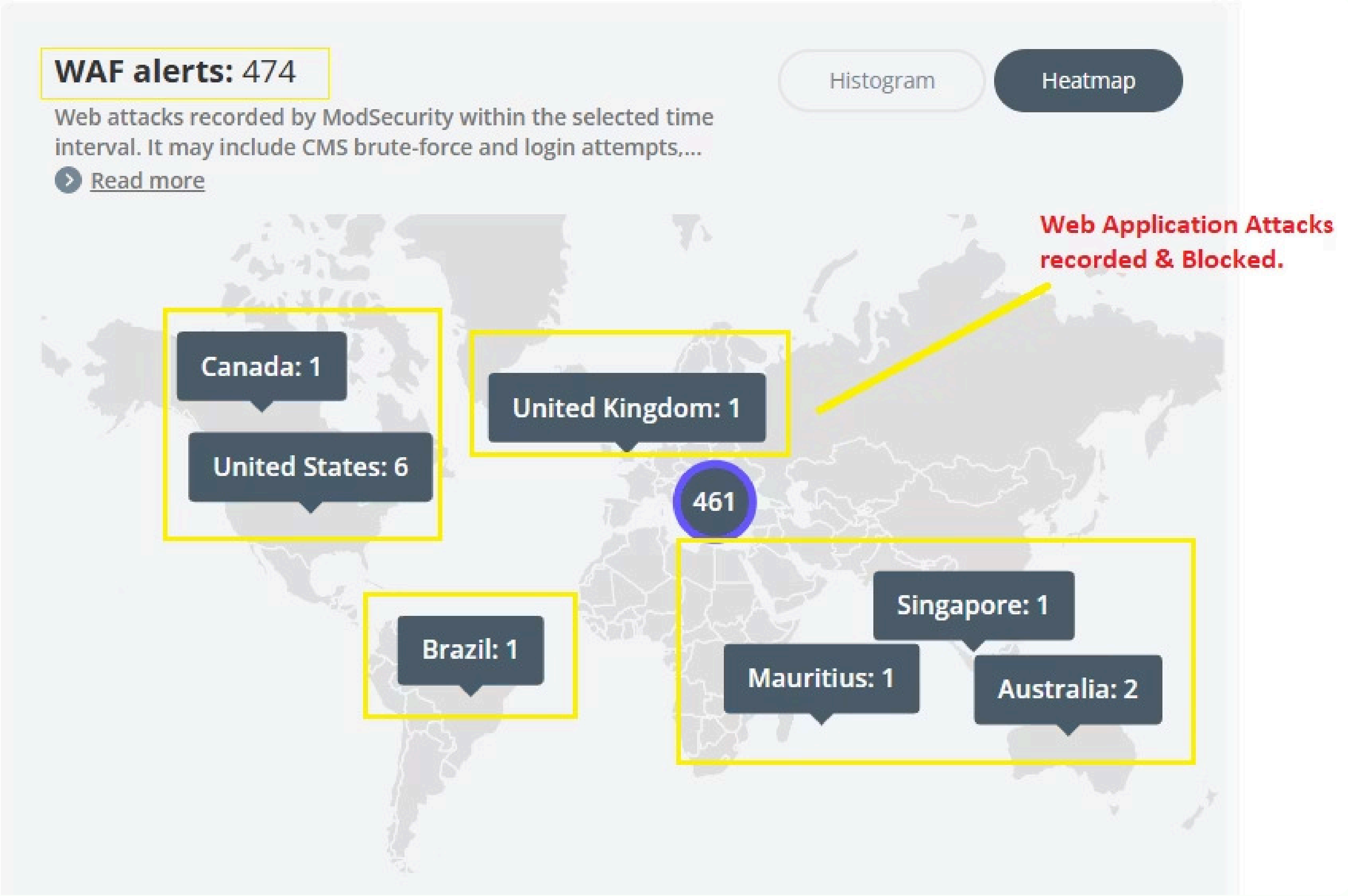
Cleaned malicious files: 2

A number of unique malicious files cleaned within the selected period. See the History tab for details.

From: 19 May 6:00 AM
To: 19 May 12:00 PM
Events: 2

5. Web-Attack Protection:

Blocks web attacks in real-time using WAF and threat intelligence



WAF alerts: 474

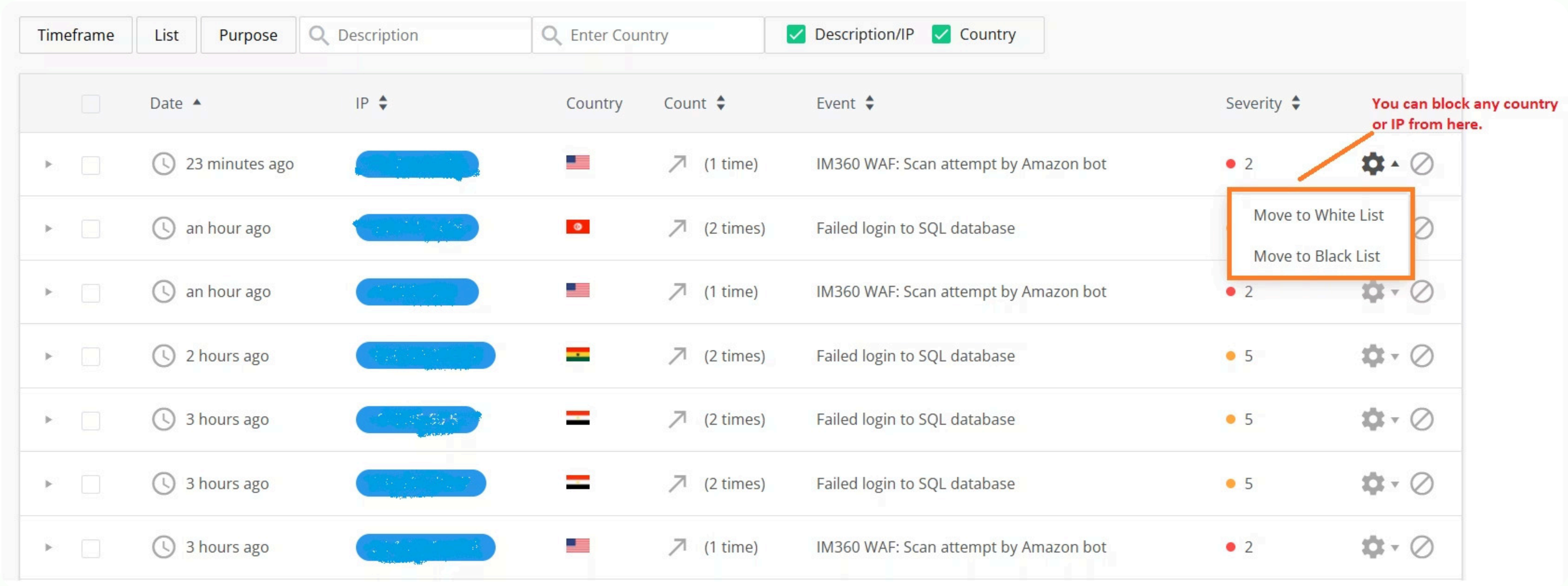
Web attacks recorded by ModSecurity within the selected time interval. It may include CMS brute-force and login attempts,...

Read more

Web Application Attacks recorded & Blocked.

5. Incident Reporting via UI:

Via incidents reporting, you can block and country and IP address.



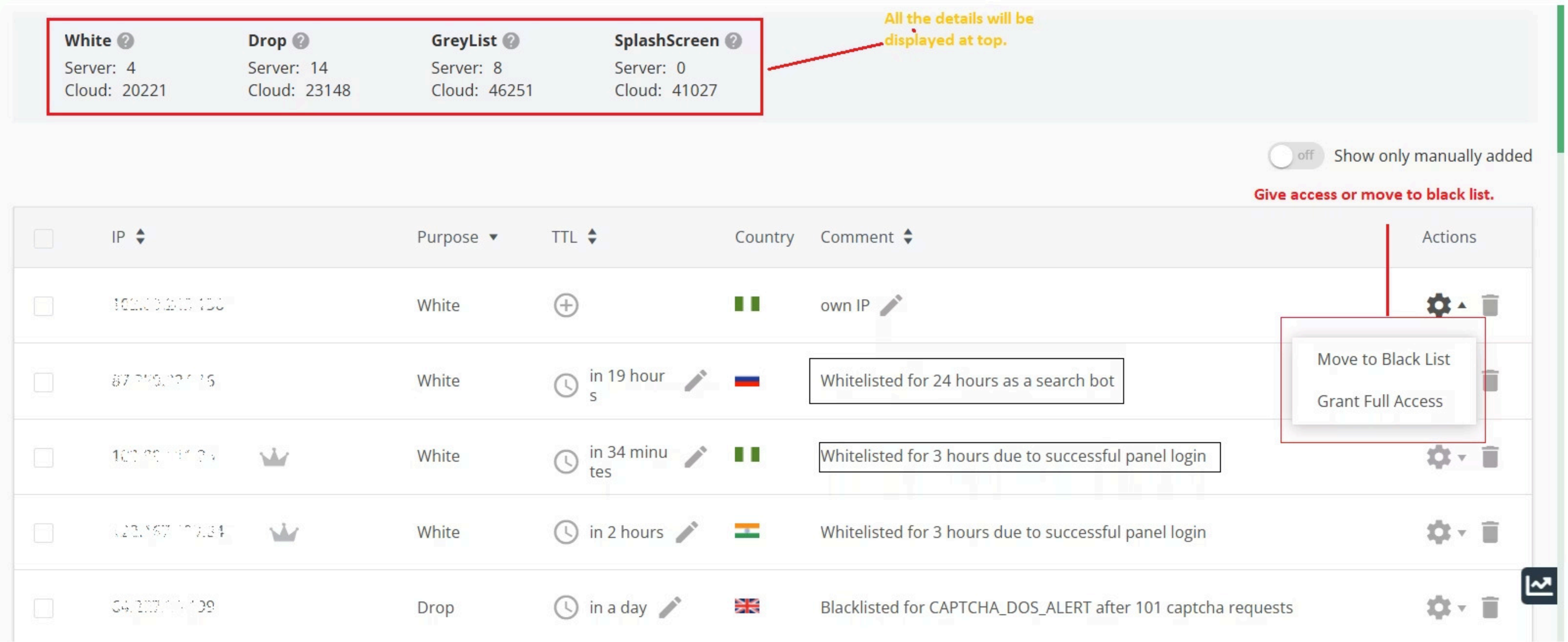
Timeframe | List | Purpose | Description | Enter Country | ☑ Description/IP ☑ Country

	□	Date ▲	IP ⬍	Country	Count ⬍	Event ⬍	Severity ⬍	
▸	□	23 minutes ago	[redacted]	🇺🇸	↗ (1 time)	IM360 WAF: Scan attempt by Amazon bot	● 2	⚙ ▴ ⊘
▸	□	an hour ago	[redacted]	🇹🇳	↗ (2 times)	Failed login to SQL database		⊘
▸	□	an hour ago	[redacted]	🇺🇸	↗ (1 time)	IM360 WAF: Scan attempt by Amazon bot	● 2	⚙ ▾ ⊘
▸	□	2 hours ago	[redacted]	🇬🇭	↗ (2 times)	Failed login to SQL database	● 5	⚙ ▾ ⊘
▸	□	3 hours ago	[redacted]	🇪🇬	↗ (2 times)	Failed login to SQL database	● 5	⚙ ▾ ⊘
▸	□	3 hours ago	[redacted]	🇪🇬	↗ (2 times)	Failed login to SQL database	● 5	⚙ ▾ ⊘
▸	□	3 hours ago	[redacted]	🇺🇸	↗ (1 time)	IM360 WAF: Scan attempt by Amazon bot	● 2	⚙ ▾ ⊘

You can block any country or IP from here.

5. Firewall Support:

Via firewall support, you can give and block access to an IP address.



White	Drop	GreyList	SplashScreen
Server: 4	Server: 14	Server: 8	Server: 0
Cloud: 20221	Cloud: 23148	Cloud: 46251	Cloud: 41027

All the details will be displayed at top.

○ off Show only manually added

Give access or move to black list.

□	IP	Purpose	TTL	Country	Comment	Actions
□	[redacted]	White	⊕	🇳🇬	own IP	⚙ 🗑
□	[redacted]	White	in 19 hours	🇷🇺	Whitelisted for 24 hours as a search bot	🗑
□	[redacted] 👑	White	in 34 minutes	🇳🇬	Whitelisted for 3 hours due to successful panel login	⚙ 🗑
□	[redacted] 👑	White	in 2 hours	🇮🇳	Whitelisted for 3 hours due to successful panel login	⚙ 🗑
□	[redacted]	Drop	in a day	🇬🇧	Blacklisted for CAPTCHA_DOS_ALERT after 101 captcha requests	⚙ 🗑

Key Benefits of Using Imunify360

Advanced Malware Detection

Continuous file scanning and cleanup prevents infections.

Web Application Firewall

Blocks common web attacks such as SQL injection and XSS.

Proactive Defense

AI and heuristics stop emerging threats instantly.

Reputation Management

Keeps your server IP off blacklists to avoid email blocks.

Flexible Pricing Plans for Every Server

Plan	Features	Price Per Server
Single User	Malware scans, firewall, patch management	$6/month
Up to 30 Users	Includes Basic + Proactive defense, AI automation	$10/month
Up to 250 Users	All features + priority support & custom rules	$15/month

Special Offer: Save 40% on Imunify360 Plans

Limited Time Discount

Get 40% off on all Imunify360 plans for new customers.

Maximize Your Security ROI

Protect more servers while lowering costs effectively.

Easy Upgrade Path

Seamlessly upgrade plans as your security needs grow.

Server Admins Trust Imunify360 for Protection

Trusted by Thousands

Industry-proven with millions of servers protected worldwide.

Comprehensive Control

Manage firewall, malware, and patches from one interface.

Reduced Incident Response

Automatic detection and cleanup mean less manual work.

How Imunify360 Enhances Your Server Security Workflow

1 **Detect**

Real-time identification of threats and vulnerabilities

2 **Protect**

Firewall and AI stop attacks before damage occurs

3 **Clean**

Automatic malware removal with minimal admin input

4 **Monitor**

Continuous visibility via dashboard and alerts

Robot
Patching
Monitoring

Takeaways & Next Steps

Imunify360 Secures Servers Efficiently

Combines AI-driven defense and ease of use.

Choose a Plan That Fits Your Needs

Start small and scale your protection as you grow.

Benefit from 40% Discount Now

Take advantage of this limited offer for maximum savings.

Protect Your Infrastructure Today

Ensure server uptime, reduce risk, and simplify security management.

Contact Us

imunify360

Email: info@activeservers.in

Mobile No: +91 8160838458

Websites: activeservers.in | serverssolution.com