swpanel

SEGURIDAD 360 · SOC · NGFW

Seguridad 360 report
swpanel.com

What the NGFW firewall has detected and blocked on swpanel.com (203.0.113.10) from 13 September to 12 October 2026.

• 47 of 58 threats blocked · 24 critical

CUSTOMER	SERVICE	PERIOD
SWPanel Demo, S.L.	swpanel.com · 203.0.113.10	13-09-2026 to 12-10-2026 · 30 days
DOCUMENT	**ISSUE DATE**	**SENSITIVITY**
SW-S36-EJEMPLO-2026	16-10-2026	Blocks from medium severity

Contents of the report

Dashboard 2

01 The consultant's introduction 3

02 Threats 6
- By severity, type and application 7
- Most frequent, origin and destination 8
- What changed: the last 6 months 9

03 Access and files 10
- Authentication and suspicious files 11

04 What to do 12
- Most serious first 13

05 Per-host detail 15
- Host 203.0.113.10 16
- What each threat is 18

06 Seguridad 360 21
- Seguridad 360 diagnosis 22
- SOC: open findings 24
- Access and sensitive changes 25
- Country blocking 26
- Bot blocking 27
- Code analysis 28
- Adaptive WAF 29
- What was done in the period 30
- What we did for you 31
- Resources and availability crossed with security 32
- Pending risks and what to decide 33
- Plan for next month 35

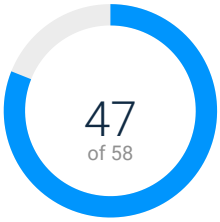
07 Conclusions of the analysis 36

Glossary 39

Annex: AI compute 41

NGFW report of swpanel.com generated by SWPanel

Dashboard



81 % BLOCKED

Of the detected events with a block action, from 13-09-2026 to 12-10-2026

swpanel.com · 203.0.113.10 · blocks from medium severity

11 of low severity were only logged, as the sensitivity requires.

• 24 critical, all blocked

58	47	11	1	0
THREATS DETECTED	BLOCKED	LOGGED	ILLEGITIMATE ACCESS ATTEMPT	SUSPICIOUS FILES

By severity



• Critical **24** • High **11** • Medium **12** • Low **11**

Compared with the customer average

58	1	0	1
threats per host Average: 944,7	intrusion attempt Average: 659,9	suspicious files Average: 70,3	application on the network Average: 1,2
93,9 % less	**99,8 % less**	**None**	**18,9 % less**

What you should do

CRITICAL

24 critical threats, all blocked. Most of them are «Code execution». Keep the server and its software up to date.

REVIEW

11 threats were only logged. They are low severity and the sensitivity blocks from medium severity. If you want to block them too, lower the sensitivity in the panel.

1 brute-force attempt(s) (WordPress Login Brute Force Attempt). If you use WordPress, limit login attempts.

NGFW report of swpanel.com generated by SWPanel

01

The consultant's introduction

Your situation in one minute, what we analysed and what deserves your attention.

NGFW report of swpanel.com generated by SWPanel

Introduction by the consultant

IA **Written by the SWPanel AI security assistant**

In the last 30 days, the NGFW blocked 47 threat events while logging 11 others due to our medium sensitivity policy.

ATTENTION

Your situation in one minute

The NGFW blocked 47 threat events, mostly code-execution and info-leak attempts. Some of these may be relevant to your service and need closer inspection.

1. Check if PHP 8.3 is affected by the phpunit vulnerability and update if needed.

2. Review the logs for the WordPress login attempt to see if it targeted a known user.

3. Verify if any of the blocked code-execution attempts could apply to your site's software.

What I analysed

I reviewed the NGFW report for your service, swpanel.com, over the past month. The firewall detected 58 threat events, with 47 blocked and 11 logged without action, as per the medium sensitivity policy. This means only events rated medium or higher severity were blocked, while lower ones were recorded for review.

Compared to the previous period, the number of threats is lower than the average of other customers, but it's still important to understand what happened and why. The main focus is on the types of attacks and whether they could affect your service.

One brute-force attempt was observed, and several code-execution and info-leak threats were blocked. Some of these may or may not apply to your setup, so we need to check a few things to be sure.

Your SWPanel AI security assistant

Should I worry?

You should stay alert but not alarmed. The NGFW is doing its job, but we need to confirm if any of the blocked threats could have affected your site. A few checks will help us be sure.

What this report covers and what it does not

This report shows what the NGFW observed and acted on. It does not include normal traffic, encrypted content, or what happens inside the server. Only the protected IP 203.0.113.10 is covered.

NGFW report of swpanel.com generated by SWPanel

What I found and why it matters

Each finding with what we saw, what it is based on, what it means for your service, what is still to be checked, what we recommend and how we will know it is solved.

HIGH IMPACT

phpunit Remote Code Execution Vulnerability

What we observed: Blocked 4 times. This vulnerability is applicable because your service runs PHP 8.3.
What it is based on: Threat event log
What it means: If your site uses phpunit and it's vulnerable, an attacker could run code on your server.
Still to be checked: We don't know if your site uses phpunit or which version is installed.
What we recommend: Check if phpunit is installed and update it if needed.
How we will verify it: After checking, we'll know if the version is up to date and not vulnerable.

MEDIUM IMPACT

WordPress Login Brute Force Attempt

What we observed: One attempt from a Cloudflare IP. The real source is behind it.
What it is based on: Threat event log
What it means: Someone tried to guess a WordPress login, but we can't see the real IP because it's behind Cloudflare.
Still to be checked: We don't know if the login was for a real user or if it was blocked by WordPress itself.
What we recommend: Check your WordPress logs for any failed login attempts around that time.
How we will verify it: If the logs show no failed logins, the attempt was likely harmless.

LOW IMPACT

FTP Protocol Evasion Attempt

What we observed: Logged 5 times. This event is logged but not blocked under the current policy.
What it is based on: Threat event log
What it means: Someone tried to bypass FTP detection rules, but the firewall didn't block it.
Still to be checked: We don't know if your server runs an FTP service or if this was a false positive.
What we recommend: Check if FTP is running and if it's needed. If not, disable it.
How we will verify it: After checking, we'll know if FTP is active and whether it's a risk.

NGFW report of swpanel.com generated by SWPanel

02

Threats

What has arrived, how severe and of what type, through which application and from where.

NGFW report of swpanel.com generated by SWPanel

Threats in the period

IA **The consultant's view**

The NGFW blocked several code-execution and info-leak attempts, some of which may be relevant to your service. We need to verify if your software is affected.

The NGFW has detected 58 threats in the period. It has blocked the 47 of medium, high or critical severity and logged without blocking the 11 of low severity.

• 47 blocked • 11 logged

By severity



• Critical **24** • High **11** • Medium **12** • Low **11**

By type

Type	Severities	Blocked	Logged	Total
Code execution	• Critical • Low	**23**	**5**	28
Information leak	• High • Medium • Low	**19**	**1**	20
Protocol anomaly	• Low	**0**	**5**	5
Denial of service	• High	**4**	**0**	4
Brute force	• Critical	**1**	**0**	1
Total		47	11	58

By application

Application	Blocked	Logged	Total	Share
web-browsing	**37**	**5**	42	**72 %**
ftp	**0**	**6**	6	**10 %**
soap	**5**	**0**	5	**8,6 %**
ssl	**4**	**0**	4	**6,9 %**
portmapper	**1**	**0**	1	**1,7 %**

NGFW report of swpanel.com generated by SWPanel

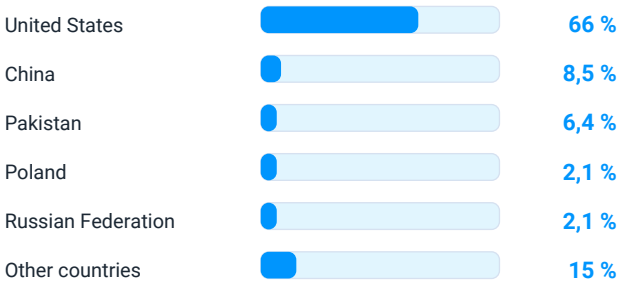
Most frequent, origin and destination

The 10 most frequent

Threat	Type	Severity	Attempts	Action
HTTP /etc/passwd Access Attempt ID 35107 · web-browsing	**Information leak**	• High	7	• Blocked
Apache Shiro Improper Authentication Vulnerability ID 58590 · web-browsing	**Code execution**	• Critical	6	• Blocked
HTTP Directory Traversal Request Attempt ID 30844 · web-browsing	**Information leak**	• Medium	6	• Blocked
D-Link DSL Soap Authorization Remote Command Execution Vulnerability ID 58483 · soap	**Code execution**	• Critical	5	• Blocked
FTP Protocol Evasion Application Detection ID 39826 · ftp	**Protocol anomaly**	• Low	5	• Logged
phpunit Remote Code Execution Vulnerability ID 55852 · web-browsing	**Code execution**	• Critical	4	• Blocked
Netgear DGN Device Remote Command Execution Vulnerability ID 40741 · web-browsing	**Code execution**	• Critical	4	• Blocked
OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability ID 58033 · ssl	**Denial of service**	• High	4	• Blocked
ZGrab Application Layer Scanner Detection ID 57955 · web-browsing	**Information leak**	• Medium	4	• Blocked
GPON Home Routers Remote Code Execution Vulnerability ID 37264 · web-browsing	**Code execution**	• Critical	3	• Blocked

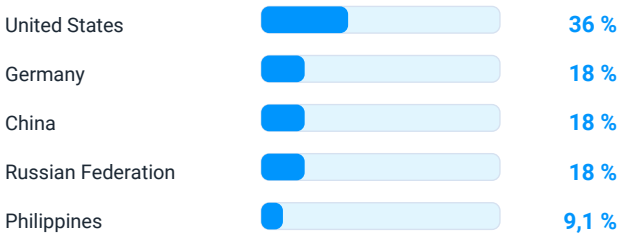
Origin of the blocked

47 threats, by country



Origin of the logged

11 threats, by country



NGFW report of swpanel.com generated by SWPanel

Most frequent, origin and destination (continued)

Destination

All 58 threats went to swpanel.com (203.0.113.10), the only service in this report.

What changed: the last 6 months

Month	Events	Blocked	Logged	Critical	High	Brute force
May 2026	**0**	0	0	0	0	0
June 2026	**0**	0	0	0	0	0
July 2026	**22**	11	11	11	0	0
August 2026	**51**	35	16	24	1	0
September 2026	**92**	77	15	38	16	1
October 2026	**0**	0	0	0	0	0

Calendar months; the last one, up to the end of this report's period. Comparing with your own history says more than any average.

NGFW report of swpanel.com generated by SWPanel

03

Access and files

Attempts to force your way in and suspicious files.

NGFW report of swpanel.com generated by SWPanel

Access and suspicious files

IA The consultant's view

One brute-force attempt was observed, but it's unclear if it targeted a real user. WordPress logs can help clarify this.

Brute-force access attempts

The NGFW has blocked 1 attempt(s) to force entry, compared with 660 on average per host for other customers. Many of these attacks are automated and launched against any machine on the internet: with an up-to-date system, well-configured applications and strong passwords they pose no real risk.

Threat	Service	Source IP	Attempt	Action
WordPress Login Brute Force Attempt ID 40044	**swpanel.com**	**198.51.100.21** Cloudflare (proxy)	1	• Blocked

SSH sessions

Nobody reached the SSH login prompt in the period.

Suspicious files

No suspicious files were detected, blocked or logged. The customer average is 70 per host.

NGFW report of swpanel.com generated by SWPanel

04

What to do

What each type of threat detected is and how to protect yourself, in order of what is at stake.

NGFW report of swpanel.com generated by SWPanel

WHAT TO DO

How to protect yourself

Only the types detected in this period, from most to least serious.

Code execution · 28 attempts

• Critical • Low

Attempts to make the server run the attacker's commands. Exploits and ransomware fall into this category and can compromise the whole system. They reached swpanel.com through soap, web-browsing; 8 different threat(s).

WHAT TO DO

Filter threats at layer 7, install an antivirus and keep the server and its software up to date.

Brute force · 1 attempts

• Critical

Trying many usernames and passwords in a row until one works. They reached swpanel.com through web-browsing; 1 different threat(s).

WHAT TO DO

Strong passwords and automatic blocking of IPs that fail several times in a row, both in the firewall and in the application login.

Information leak · 20 attempts

• High • Medium • Low

Attempts to extract internal information from the server: configuration files, passwords or personal data. They reached swpanel.com through ftp, portmapper, web-browsing; 6 different threat(s).

WHAT TO DO

Make sure sensitive information cannot be read from outside: encrypt the files that hold it and grant access only to the user groups that need it.

Denial of service · 4 attempts

• High

Attempts to make a service stop responding by flooding it or making it fail. They reached swpanel.com through ssl; 1 different threat(s).

WHAT TO DO

Use layer 3 and layer 7 firewalls to detect and cut repeated connections, and keep exposed software up to date.

NGFW report of swpanel.com generated by SWPanel

How to protect yourself (continued)

Protocol anomaly · 5 attempts • Low

Traffic that does not behave like the protocol it claims to be, usually to go unnoticed. They reached swpanel.com through ftp; 1 different threat(s).

WHAT TO DO

Close the ports you do not use and let the NGFW identify the application before letting it through: whatever is not recognised is better blocked.

NGFW report of swpanel.com generated by SWPanel

05

Per-host detail

Every threat received by each service, with its reference.

NGFW report of swpanel.com generated by SWPanel

Host 203.0.113.10

IA **The consultant's view**

No suspicious files or SSH sessions were observed. The NGFW did not detect any signs of unauthorized access.

swpanel.com has received 58 threats of 17 different kinds, from most to least serious.

ID	Threat	Severity	Attempts	Action
58590	**Apache Shiro Improper Authentication Vulnerability** Code execution · web-browsing	• Critical	6	• Blocked
58483	**D-Link DSL Soap Authorization Remote Command Execution Vulnerability** Code execution · soap	• Critical	5	• Blocked
55852	**phpunit Remote Code Execution Vulnerability** Code execution · web-browsing	• Critical	4	• Blocked
40741	**Netgear DGN Device Remote Command Execution Vulnerability** Code execution · web-browsing	• Critical	4	• Blocked
37264	**GPON Home Routers Remote Code Execution Vulnerability** Code execution · web-browsing	• Critical	3	• Blocked
54617	**Mirai and Reaper Exploitation Traffic** Code execution · web-browsing	• Critical	1	• Blocked
40044	**WordPress Login Brute Force Attempt** Brute force · web-browsing	• Critical	1	• Blocked
35107	**HTTP /etc/passwd Access Attempt** Information leak · web-browsing	• High	7	• Blocked
58033	**OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability** Denial of service · ssl	• High	4	• Blocked
30844	**HTTP Directory Traversal Request Attempt** Information leak · web-browsing	• Medium	6	• Blocked
57955	**ZGrab Application Layer Scanner Detection** Information leak · web-browsing	• Medium	4	• Blocked
32796	**RPC Portmapper DUMP Request Detected** Information leak · portmapper	• Medium	1	• Blocked
34804	**PHP CGI Query String Parameter Handling Information Disclosure Vulnerability** Information leak · web-browsing	• Medium	1	• Blocked
39826	**FTP Protocol Evasion Application Detection** Protocol anomaly · ftp	• Low	5	• Logged
58098	**Possible HTTP Malicious Payload Detection** Code execution · web-browsing	• Low	3	• Logged

NGFW report of swpanel.com generated by SWPanel

Host 203.0.113.10 (continued)

ID	Threat	Severity	Attempts	Action
54469	**Suspicious File Downloading Detection** Code execution · web-browsing	• Low	2	• Logged
40391	**Application Identification Evasion Attempt Through Malformed FTP Traffic** Information leak · ftp	• Low	1	• Logged

NGFW report of swpanel.com generated by SWPanel

What each threat is

ID 58590 · Code execution • Critical

Apache Shiro Improper Authentication Vulnerability

Apache Shiro is prone to an improper authentication vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable improper authentication vulnerability.

Attempts **6** Blocked CVE-2020-11989 Ref. **lists.apache.org**

ID 58483 · Code execution • Critical

D-Link DSL Soap Authorization Remote Command Execution Vulnerability

Dlink DSL is prone to a command injection vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable command injection.

Attempts **5** Blocked CVE-2018-19986 Ref. **github.com**

ID 55852 · Code execution • Critical

phpunit Remote Code Execution Vulnerability

phpunit is prone to a remote code execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable remote code execution.

Attempts **4** Blocked CVE-2017-9841 Ref. **phpunit.vulnbusters.com**

ID 40741 · Code execution • Critical

Netgear DGN Device Remote Command Execution Vulnerability

Netgear DGN devices is prone to a remote code execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of privilege checks on the request, leading to an exploitable remote code execution.

Attempts **4** Blocked Ref. **seclists.org**

ID 37264 · Code execution • Critical

GPON Home Routers Remote Code Execution Vulnerability

GPON Home Routers are prone to a Remote Code Execution vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable Remote Code Execution vulnerability.

Attempts **3** Blocked CVE-2018-10561 Ref. **blog.netlab.360.com**

ID 54617 · Code execution • Critical

Mirai and Reaper Exploitation Traffic

This signature detects exploitation attempts from Mirai and Reaper malware families. Detection of this traffic indicates an attempt to exploit various IoT device vulnerabilities including: the D-Link DSL-2750B - OS command injection vulnerability, the MVPower DVR unauthenticated command execution...

Attempts **1** Blocked

ID 40044 · Brute force • Critical

WordPress Login Brute Force Attempt

This event indicates that someone is using a brute force attack to gain access to WordPress wp-login.php.

Attempts **1** Blocked

ID 35107 · Information leak • High

HTTP /etc/passwd Access Attempt

There is a /etc/passwd access attempt has been detected while parsing certain crafted HTTP request. A successful attack could allow an attacker to access sensitive information that could launch further attacks.

Attempts **7** Blocked

NGFW report of swpanel.com generated by SWPanel

What each threat is (continued)

ID 58033 · Denial of service • High

OpenSSL SSL_check_chain NULL Pointer Dereference Vulnerability

OpenSSL is prone to a NULL pointer dereference vulnerability while parsing certain crafted SSL requests. The vulnerability is due to the lack of proper checks on SSL requests, leading to an exploitable NULL pointer dereference vulnerability.

Attempts **4** Blocked CVE-2020-1967 Ref. **openssl.org**

ID 30844 · Information leak • Medium

HTTP Directory Traversal Request Attempt

A directory traversal vulnerability has been discovered in parsing malformed HTTP requests. This vulnerability is due to a lack of proper checks in HTTP URI requests.

Attempts **6** Blocked Ref. **imperva.com**

ID 57955 · Information leak • Medium

ZGrab Application Layer Scanner Detection

This signature indicates that an attacker is trying to collect information about the network by using the ZGrab Scanner.

Attempts **4** Blocked

ID 32796 · Information leak • Medium

RPC Portmapper DUMP Request Detected

Most Unix server can be retrieved information through a normal portmapper request.

Attempts **1** Blocked

ID 34804 · Information leak • Medium

PHP CGI Query String Parameter Handling Information Disclosure Vulnerability

PHP-CGI based setups such as Apache's mod_cgid, contain a vulnerability when parsing query string parameters from php files. In such a setup php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the p...

Attempts **1** Blocked CVE-2012-1823 Ref. **kb.cert.org**

ID 39826 · Protocol anomaly • Low

FTP Protocol Evasion Application Detection

This signature detects applications or tools that tunnel SSH traffic over FTP protocol traffic.

Attempts **5** Logged Ref. **room362.com**

ID 58098 · Code execution • Low

Possible HTTP Malicious Payload Detection

This signature detects malicious payload in HTTP traffic.

Attempts **3** Logged Ref. **unit42.paloaltonetworks.com**

ID 54469 · Code execution • Low

Suspicious File Downloading Detection

This signature detects WGET and CURL command execution in HTTP request URL parameters, which is pervasively exploited by attackers to get subsequent malicious payload.

Attempts **2** Logged

NGFW report of swpanel.com generated by SWPanel

What each threat is (continued)

ID 40391 · Information leak • Low

Application Identification Evasion Attempt Through Malformed FTP Traffic

The signature detects an application identification evasion attempt which sends malformed traffic through tcp port 21.

Attempts **1** Logged Ref. **jira-hq.paloaltonetworks.local**

NGFW report of swpanel.com generated by SWPanel

06

Seguridad 360

All the protections of your service: their state, what they saw and what is left to solve.

NGFW report of swpanel.com generated by SWPanel

Seguridad 360 diagnosis

IA **Written by the SWPanel AI security assistant**

MEDIUM ATTENTION

The service has some active protections but lacks full coverage in bot and country blocking, and some critical email security records are missing.

Your service had 58 detected threat events in the last 30 days, with 47 blocked by the NGFW. The most common threats were attempts to access sensitive files and exploit known vulnerabilities, but many of these are not yet confirmed to affect your specific setup.

The NGFW is working as configured, but some protections like the WAF and bot blocking are not fully active.

The biggest immediate concern is the lack of SPF and DMARC records for your domain, which makes it easy for attackers to spoof your emails. Also, a WordPress brute-force attempt was blocked, but the source IP is behind a Cloudflare proxy, so we can't block it directly.

You should review the logs of that proxy to check for repeated failed login attempts.

The traffic to your site is mostly from the US, Germany, and the Netherlands, with a high share of scanning activity. While the NGFW is blocking most of these, the lack of active bot and country blocking means many scans reach your server. This could increase the load on your system over time, even if it hasn't yet.

The NGFW and SOC data are complete, but bot and country blocking, WAF, and fail2ban are not verified or not active. The code analysis and SSH logs are reliable.

State of each protection

The system decides it with what it can check: configured is not the same as working.

WORKING AND VERIFIED

NGFW firewall

WORKING AND VERIFIED

SOC: monitoring and findings

NGFW report of swpanel.com generated by SWPanel

Seguridad 360 diagnosis

NO COVERAGE
Bot blocking

NO COVERAGE
Country blocking

NO COVERAGE
AntiDDoS

CONFIGURED, NOT VERIFIED
Fail2Ban: blocking failed logins

CONFIGURED, NOT VERIFIED
Adaptive WAF
modo observa: detecta y propone, no bloquea

WORKING AND VERIFIED
SSH access

WORKING AND VERIFIED
Code analysis

NGFW report of swpanel.com generated by SWPanel

SOC: open findings

IA **The consultant's view**

The SOC found 71 open issues, including missing SPF and DMARC records, and several IPs with suspicious activity. The most urgent is the lack of SPF, which allows anyone to send emails pretending to be from your domain.

0	4	13	38
CRITICAL	HIGH	MEDIUM	OPEN FINDINGS

2	5	0	23
NEW IN 7 DAYS	SOLVED IN 7 DAYS	PEAKS IN 30 DAYS	BLOCKED IPS

The most serious findings

3
active_check · SWP01
Falta DMARC | Sin registro _dmarc: el dominio es facilmente suplantable en correos de phishing

3
ip_reputation · SWP01
198.51.100.77 | red de bots (spamhaus, riesgo critical) | 41 peticiones

3
ip_reputation · SWP01
198.51.100.82 | escaner conocido (abuseipdb, riesgo alto) | 18 peticiones

NGFW report of swpanel.com generated by SWPanel

SOC: open findings

Access and sensitive changes

IA The consultant's view

There was one successful SSH login, no logins from non-admin IPs, and 248 failed attempts from 11 IPs. No root logins with password were detected.

1	0	0	248
SSH LOGINS	FROM NON-ADMIN IPS	ROOT WITH PASSWORD	FAILED ATTEMPTS

11	0	0
IPS WITH FAILURES	NEW USERS	SUDO BY NON-ROOT USERS

NGFW report of swpanel.com generated by SWPanel

Country blocking

IA The consultant's view

Traffic is mostly from the US, Spain, and France. No country blocking is active, so all this traffic reaches your server. Blocking high-risk countries could reduce the number of scans and attacks.

8.564	8.061	10.481	0
REQUESTS FROM PEOPLE	FROM ROBOTS	FROM SCANNERS	BLOCKED COUNTRIES

Activity by country

Country	People	Robots	Scanners	Block
United States of America	2.517	2.887	4.855	—
Spain	710	1.934	1	—
France	961	23	1.301	—
Singapore	1.273	5	718	—
Japan	363	8	961	—
Korea, Republic of	14	960	22	—
Belgium	366	3	507	—
Hong Kong	131	361	225	—
Lithuania	214	4	477	—
Canada	180	96	365	—
India	69	331	214	—
Brazil	177	216	162	—
Netherlands	187	45	145	—
Germany	234	65	65	—

Requests to your websites in the period, by IP location. A blocked country that still receives requests after the block means the block is not applied.

NGFW report of swpanel.com generated by SWPanel

Bot blocking

IA The consultant's view

6 bots were blocked in the last 10 days, mostly AI scrapers. The current bot-blocking profile (B) blocks some but not all suspicious bots. A stricter profile (C) would block more, but might also affect some AI tools that are allowed.

3.361	2.830	2.643	2.532
REQUESTS FROM PEOPLE	FROM KNOWN BOTS	FROM UNCATALOGUED ROBOTS	FROM SCANNERS

38	6	8	B
BOTS DETECTED	BLOCKED BOTS	NEW AGENTS DISCOVERED	CURRENT PROFILE

The bots detected

Bot	Family	Requests	State
GPTBot (OpenAI)	IAG	57	• Blocked
Meta-WebIndexer (Meta AI)	IAG	55	• Blocked
Googlebot	BUS	51	Allowed
PerplexityBot	IAG	45	• Blocked
Bytespider (ByteDance)	IAG	34	• Blocked
AhrefsBot	SEO	32	Allowed
ChatGPT-User	IAG	32	• Blocked
OnCrawl	SEO	31	Allowed
ClaudeBot (Anthropic)	IAG	30	• Blocked
Kimi-SearchBot (Moonshot AI)	IAG	30	Allowed
Qwenbot (Alibaba)	IAG	29	Allowed
DuckAssistBot (DuckDuckGo)	IAG	29	Allowed
Applebot	BUS	28	Allowed
KimiBot (Moonshot AI)	IAG	27	Allowed
YouBot (You.com)	IAG	26	Allowed

NGFW report of swpanel.com generated by SWPanel

Bot blocking

The blocking profiles and what each would cut

Profile	Bots cut	New	Requests	Main ones
A	2	2	184	
B · advisable	6	4	642	
C	11	5	1.415	

Code analysis

IA **The consultant's view**

The code of your site has a score of 86 (out of 100), with no malware or critical issues found. No WordPress checks failed, and no suspicious files were detected.

86	1	0	0
CODE SCORE	SECURITY FINDINGS	CRITICAL	SUSPICIOUS FILES

3	0	0	PHP 8.3
CODE ERRORS	SQL ERRORS	5XX RESPONSES	PHP VERSION

Last complete analysis: 16/10/2026 · 4 analyses in the period.

NGFW report of swpanel.com generated by SWPanel

Bot blocking

Adaptive WAF

IA The consultant's view

The WAF is in 'protect' mode and has triggered 20 shadow rules. It has 72 active findings, but only 8 have been reviewed and corrected. The WAF is active but needs more attention to ensure it’s blocking the right threats.

Observes only	aplica	7	20
MODE	AI AUTONOMY	RULES	SHADOW TRIGGERS

OBSERVES

The adaptive WAF is in observation mode: it detects and proposes rules, but does not block by itself. Switch it to automatic if you want it to act.

What the WAF did in the period

Action	Who	Result	Times
hallazgo:alta	panel	abierto	72
hallazgo:no_visto	panel	corregido	8
hallazgo:visto	panel	abierto	7

NGFW report of swpanel.com generated by SWPanel

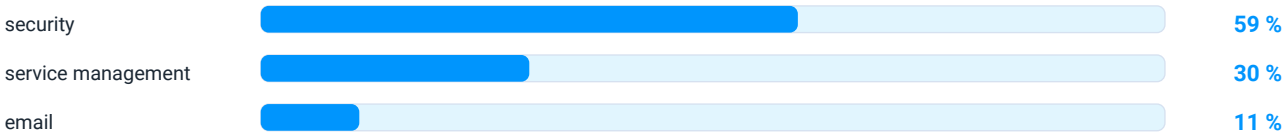
What was done in the period

IA **The consultant's view**

SWPanel and its AI took 64 actions in the period, including blocking 9 IPs and managing 38 security-related tasks. The SOC solved 5 findings in the last 7 days.

64	11	4	0
ACTIONS RECORDED	DONE BY SWPANEL AI	BY API	IPS BLOCKED IN THE FIREWALL

By area



The latest actions

Date	Who	Service	What
2026-10-14 09:12	**Account holder**	SWP01	IP 203.0.113.50 (office) added to the FireWall allow list.
2026-10-12 03:40	**SWPanel (AI)**	SWP01	The AI consultant prepared a report on the bots visiting the website. Recommended profile: B.
2026-10-11 18:05	**Account holder**	SWP01	Bot blocking profile B applied (6 bots blocked).
2026-10-09 02:15	**SWPanel**	SWP01	The adaptive WAF enabled a rule against attack paths to /wp-login.php and /.env.
2026-10-07 11:30	**Account holder**	SWP01	PHP version changed from 8.1 to 8.3.
2026-10-03 04:02	**SWPanel (AI)**	SWP01	The AI consultant prepared a report on traffic by country. Recommended scenario: A.
2026-10-02 16:48	**API**	SWP01	IP 198.51.100.77 blocked for 24 hours after repeated access attempts.
2026-09-28 10:20	**Account holder**	SWP01	SSL certificate for swpanel.com renewed.
2026-09-22 08:15	**SWPanel**	SWP01	Full backup verified successfully.

NGFW report of swpanel.com generated by SWPanel

What we did for you

What SWPanel, its SOC and its AI did for your service in the period, taken from the records: these are actions done, not intentions.

9	87	5	4
IPS BLOCKED BY SWPANEL	WAF ACTIONS	FINDINGS SOLVED (7 DAYS)	RECENT AUTOMATIC ACTIONS

SWPanel's latest actions

Date	Who	What
2026-10-12 03:40	**SWPanel (AI)**	The AI consultant prepared a report on the bots visiting the website. Recommended profile: B.
2026-10-09 02:15	**SWPanel**	The adaptive WAF enabled a rule against attack paths to /wp-login.php and /.env.
2026-10-03 04:02	**SWPanel (AI)**	The AI consultant prepared a report on traffic by country. Recommended scenario: A.
2026-09-22 08:15	**SWPanel**	Full backup verified successfully.

NGFW report of swpanel.com generated by SWPanel

Resources and availability crossed with security

IA The consultant's view

CPU and RAM usage are low, with no outages or performance issues. The server is stable and not under stress from traffic or attacks.

1,1 % AVERAGE CPU	**29 %** MAX CPU (DAILY AVERAGE)	**1,7 / 4** MAX LOAD / VCORES	**49 %** MAX RAM
0 OUTAGES	**0 min** DOWNTIME	**0** DEGRADATION EPISODES	**0** SECURITY STOPS
0 HOURS AT THE LIMIT	**0** HIGH SEVERITY	**0** 5XX RESPONSES	**0** TIMEOUTS

The crossing: security and performance

IA Written by the SWPanel AI security assistant

There were no performance issues or 5xx errors in the last 30 days, and no traffic peaks that could be linked to attacks or bots. This suggests that the NGFW is effectively blocking most threats before they reach your application.

However, the high number of scan attempts (10,481) reaching your server could increase the load over time, especially if the number of scanners grows. While the server isn't stressed now, this could become a concern if the traffic increases or if the NGFW rules change.

NGFW report of swpanel.com generated by SWPanel

Pending risks and what to decide

IA **Written by the SWPanel AI security assistant**

MEDIUM IMPACT

Missing SPF and DMARC records

What we observed: No SPF or DMARC records are configured for your domain.

What it is based on: Without these records, attackers can easily spoof your domain in phishing emails or spam.

What it means: Your domain is vulnerable to email spoofing, which can damage your reputation and expose users to phishing attacks.

Still to be checked: You need to configure SPF and DMARC records in your DNS settings.

What we recommend: Set up SPF and DMARC records through your DNS provider. SWPanel can help you generate the correct records.

How we will verify it: Check the SOC findings or use a DMARC validation tool to confirm the records are active.

MEDIUM IMPACT

WordPress brute-force attempt

What we observed: A brute-force login attempt was blocked against your WordPress site from a Cloudflare IP.

What it is based on: The attacker used a known IP proxy, which means we can't block the source directly.

What it means: Someone is trying to guess your WordPress login credentials. This is a common tactic used in phishing or data theft.

Still to be checked: You need to check the login logs of your WordPress site for repeated failed attempts.

What we recommend: Enable two-factor authentication for your WordPress admin account and review the login logs regularly.

How we will verify it: Check the WordPress login logs or enable a plugin like Wordfence to monitor login attempts.

NGFW report of swpanel.com generated by SWPanel

Pending risks and what to decide

LOW IMPACT

Missing bot blocking

What we observed: No bot-blocking rules are currently active on your server.

What it is based on: Many of the requests to your site are from bots and scanners, which can increase server load and expose vulnerabilities.

What it means: Your site is receiving a lot of bot traffic, which could lead to performance issues or security risks if not managed.

Still to be checked: You need to enable a bot-blocking profile to reduce the number of unwanted bots and scanners.

What we recommend: Enable the recommended bot-blocking profile (B) to block the most suspicious bots without affecting legitimate traffic.

How we will verify it: Check the bot-blocking settings in SWPanel and review the traffic logs to see if bot traffic decreases.

What you should decide

Enable the recommended bot-blocking profile (B) to reduce the number of suspicious bots and scanners reaching your site. This will help reduce server load and improve security. If you're unsure, start with a stricter profile (C) and monitor the impact on your traffic.

NGFW report of swpanel.com generated by SWPanel

Plan for next month

THIS MONTH

Enable bot-blocking profile B

Why: To reduce the number of suspicious bots and scanners that reach your site.

Who: You

How we will check it: Check the bot-blocking logs in SWPanel to see if the number of blocked bots increases.

THIS MONTH

Set up SPF and DMARC records

Why: To prevent email spoofing and protect your domain from being used in phishing attacks.

Who: You

How we will check it: Use a DMARC validation tool to confirm the records are active and working.

THIS WEEK

Review WordPress login logs

Why: To ensure no unauthorized access is attempted or successful.

Who: You

How we will check it: Check the WordPress login logs or enable a plugin like Wordfence to monitor login attempts.

NGFW report of swpanel.com generated by SWPanel

Seguridad 360 conclusions

Your service is currently protected by the NGFW, which is blocking most of the detected threats. However, some protections like bot blocking and email security are missing or not active. Enabling these will help reduce the risk of attacks and improve your overall security posture.

The most urgent actions are setting up SPF and DMARC records and enabling a bot-blocking profile. These steps will help protect your domain from email spoofing and reduce the number of unwanted bots and scanners reaching your site.

Your server is stable and not under stress, but the high number of scan attempts could increase over time. Taking action now will help prevent potential issues in the future.

07

Conclusions of the analysis

What your consultant concludes after seeing all the figures, and your action plan.

NGFW report of swpanel.com generated by SWPanel

Conclusions of the analysis

IA **Written by the SWPanel AI security assistant**

The NGFW blocked 47 threats, showing active attempts to exploit weaknesses or guess access. The most repeated was an HTTP /etc/passwd access attempt, which could mean someone is testing for misconfigurations.

Compared to the previous month, the total threats dropped, and the number of low-severity alerts decreased. This suggests a slight improvement in the overall threat landscape.

Some alerts, like the Apache Shiro and OpenSSL vulnerabilities, need verification since we don't have a complete software inventory. This means we don't know for sure if those services are installed or vulnerable.

The brute-force attempt came through a Cloudflare proxy, so it's hard to trace the real source. Still, it's a reminder to keep WordPress passwords strong and to review login logs regularly.

The FTP protocol evasion attempt was logged but not blocked, as per the medium sensitivity policy. It's worth checking if FTP is needed, as it can be a security risk if not properly configured.

Your action plan

THIS MONTH

Check if phpunit is installed and update it if needed

Why: A critical vulnerability in phpunit was detected and blocked by the NGFW. If installed, it could be exploited to run code remotely.

Who: You

How we will check it: Confirm the version of phpunit in the server or disable it if not in use.

THIS MONTH

Review WordPress login logs for the IP 198.51.100.21

Why: A brute-force attempt was logged against WordPress. Checking the logs can help confirm if there were failed login attempts and if any accounts were at risk.

Who: You

How we will check it: Share the WordPress login logs for the relevant time period with SW Hosting support.

NGFW report of swpanel.com generated by SWPanel

Conclusions of the analysis

MEDIUM TERM

Check if FTP is running and if it's needed

Why: An FTP protocol evasion attempt was logged. If FTP is not required, it’s better to disable it to reduce the attack surface.

Who: You

How we will check it: Confirm whether FTP is active and its purpose in the server configuration.

I’m here to help you understand and act on these findings. We’re in this together.

Your SWPanel AI security assistant

Text written by the SWPanel AI Assistant from the data in this report, with a model running on SW Hosting's own servers: your data never leaves our infrastructure. The figures are computed by the system; the AI only interprets them.

NGFW report of swpanel.com generated by SWPanel

Glossary

The technical terms used in this report, in alphabetical order.

Application
Type of traffic the NGFW recognises by its content (web-browsing, ssl, ftp), not only by its port.

Blocked threat
One the NGFW stopped before it reached the server, according to the chosen sensitivity.

Brute force
Trying many passwords in a row until one works.

Code execution
Attack that tries to make the server run the attacker's commands.

CVE
Public code that identifies a known vulnerability, for example CVE-2020-1967.

Denial of service
Attack that floods or breaks a service until it stops responding.

Exploit
Program or request that takes advantage of a specific vulnerability.

Inbound and outbound traffic
Data arriving at your services and data leaving them.

Information leak
Attempt to extract internal data from the server, such as configuration files or passwords.

Logged threat
One detected and recorded but not blocked, because its severity is below the sensitivity.

NGFW
Next Generation Firewall: a firewall that inspects traffic content to detect and block threats.

Protocol anomaly
Traffic that does not behave like the protocol it claims to be.

Sensitivity
Severity from which the NGFW blocks. Below it, it only logs.

NGFW report of swpanel.com generated by SWPanel

Glossary (continued)

Session
A complete connection between two machines, from the first packet to the last.

Severity
Risk level of a threat: critical, high, medium or low.

SQL injection
Sneaking database commands into the data sent to an application.

Threat ID
Identifier of the threat in the NGFW vendor's catalogue.

Vulnerability
Security flaw in a program that an attacker can exploit.

NGFW report of swpanel.com generated by SWPanel

Annex: AI compute

IA **What it took to write this report with AI**

The assistant and the translations in this report were generated by a language model running on SW Hosting's own servers: your data never leaves our infrastructure.

AI compute

qwen3-32b MODEL	**vLLM** ENGINE	**2** MODEL CALLS
4.312 TOKENS READ	**1.629** TOKENS WRITTEN	**33.7 s** COMPUTE TIME

Infrastructure

NVIDIA A100 GPU	**80 GB** HBM2E	**312 TFLOPS** FP16/BF16

Energy and cost

0.0054 kWh COMPUTE ENERGY	**0.0135 kWh** TOTAL ENERGY (WITH COOLING)	**3.4 g** CO2 EMITTED
0.0194 € COMPUTE COST		

Estimate: GPU at 575 W, cooling of 1.5 kW per kW of compute, 0.185 EUR/kWh, 1.8 EUR per GPU hour and 250 g of CO2 per kWh.

NGFW report of swpanel.com generated by SWPanel

swpanel

https://www.swpanel.com

Document: SW-S36-EJEMPLO-2026

Report automatically generated by SWPanel · https://www.swpanel.com