SafePi Security & Transparency Report

Interpreted security intelligence for normal people.

Report period	2026-05-25 17:00 - 2026-05-26 16:00
Generated	2026-05-26 16:51
Device	SafePi sample device
Assessment	Protected

Assessment meaning: SafePi actively enforced network policy and denied unauthorized or unwanted traffic, but the observed telemetry did not contain recurring suspicious behavioral patterns, high-confidence security findings, or action-needed events. Observed denied traffic was primarily consistent with normal background internet noise such as analytics, telemetry, advertising, cloud infrastructure, certificate checks, or blocked third-party services.

SafePi reduces unwanted, suspicious, and unauthorized network activity. Depending on configuration, protection may be provided through SafeDNS Guard, SafeWeb Proxy, Pi-hole filtering, or a combination of available SafePi features.

Important: blocked or suspicious-looking network activity does not automatically mean malware. Modern websites, browsers, apps, ads, telemetry systems, and privacy tools often create noisy outbound traffic. SafePi reports should be interpreted calmly and based on repeated patterns.

Executive summary

Observation	Meaning
8 844 unwanted or unauthorized requests denied	SafePi actively prevented traffic outside policy.
0 SafeDNS Guard blocks	Unapproved DNS destinations were prevented.
116 Pi-hole ad/tracker blocks	Advertising, tracking, or community-blocklisted domains were reduced.
8 728 SafeWeb proxy denies	Web requests outside the trusted proxy allowlist were denied.
0 security finding(s)	Higher-signal patterns that may need review or action.
0 operational finding(s)	Retry loops or background behavior, usually not malware by itself.

Protection modes and usage

Mode	Enforcement state	Observed utilization	Meaning
SafeDNS Guard	Not observed	0 Guard blocks	DNS/network-level enforcement and deeper behavioral visibility.
Pi-hole filtering	Observed throughout period	116 Pi-hole blocks	DNS ad, tracker, and community blocklist filtering.
SafeWeb Proxy	Available throughout period	Observed for 22/23 reporting hours	Proxy-based web filtering from clients configured to use SafeWeb Proxy.

This period vs previous period

Metric	This period	Previous	Change	Meaning
Denied requests	8 844	4 148	↑ 113%	Shows whether unwanted or unauthorized traffic increased or decreased.
SafeDNS Guard blocks	0	0	unchanged	Network-level policy enforcement activity.
Pi-hole blocks	116	53	↑ 119%	Ad, tracker, and community blocklist activity.
Security findings	0	0	unchanged	Higher-signal findings requiring review or action.
Operational findings	0	0	unchanged	Retry loops or background behavior, usually not malware by itself.

Key takeaways

Takeaway	Meaning
No urgent findings	SafePi did not identify high-risk or operational findings requiring immediate attention.
Protection active	SafePi denied 8 844 unwanted or unauthorized requests during this period.

Overall environment assessment: **Protected**

SafeDNS Guard and SafeWeb Proxy represent different SafePi enforcement modes. They should be interpreted separately: SafeDNS Guard reflects DNS/network-level enforcement, while SafeWeb Proxy reflects proxy-based web filtering from devices configured to use the proxy.

A protected environment can still show many blocked requests. This usually means SafePi is doing useful work, not that the device is infected.

Protection effectiveness

Layer	Count	Interpretation
DNS queries observed	22 335	DNS activity seen by SafePi.
HTTPS proxy tunnels (CONNECT)	14 913	Encrypted HTTPS sessions observed through SafePi proxy enforcement.
HTTP proxy requests	46	Unencrypted web requests observed through SafePi proxy enforcement.
SafeDNS Guard blocks	0	Unapproved destinations prevented at DNS policy level.
Pi-hole filtering	116	Ad/tracker/community blocklist filtering.
Proxy requests observed	14 959	SafeWeb proxy traffic seen from configured clients.
Proxy requests denied	8 728	Web requests outside trusted allowlist denied.

Meaning: SafeDNS Guard and SafeWeb Proxy measure different SafePi enforcement modes. A device may use one mode or the other depending on configuration. Pi-hole filtering may provide additional DNS-level ad, tracker, or community blocklist filtering when enabled.

Security interpretation

• Most blocked activity observed during this period appears related to advertising, analytics, telemetry, or third-party web infrastructure.

• SafeWeb Proxy denied 8 728 web requests from configured proxy clients during this period.

• No direct evidence of ransomware, spyware, or automated botnet activity was detected from the observed telemetry.

Recommended actions

• No urgent security actions are recommended at this time.

• Large numbers of denied proxy requests are often caused by modern websites loading advertising, analytics, or tracking infrastructure.

• Most blocked DNS activity originated from: Device 1.

• Most denied proxy activity originated from: Device 3.

Activity heatmap

This grid shows when blocked activity occurred. Concentrated activity outside normal use hours can suggest automated background behavior, retry loops, or unattended devices.

Day	00-05	06-11	12-17	18-23
Mon	0	0	■ 535	■■■■ 2 208
Tue	■■■■ 2 222	■■■■ 2 406	■■■ 1 473	0
Wed	0	0	0	0
Thu	0	0	0	0
Fri	0	0	0	0
Sat	0	0	0	0
Sun	0	0	0	0

Device presence by day

LAN devices known to SafePi: 3. Daily counts include only clients seen in blocked DNS or proxy activity.

Day	Unique observed clients	Sparkline
2026-05-25	2	■■■■■■■■■■■■ 2
2026-05-26	3	■■■■■■■■■■■■■■■■■■ 3

Newly observed clients

These clients appeared in blocked DNS or proxy activity during this report period and were not seen in earlier collected report history.

Client	First seen	Blocked hits
Device 2	2026-05-26 09:00	2

Suspicious discoveries

This report was generated without SafeDNS Guard DNS-level telemetry. Some behavioral detections may not be visible in this configuration.

No high-signal suspicious discoveries were recorded during this period.

This does not mean no unwanted traffic existed. It means SafePi did not observe patterns strong enough to highlight as suspicious discoveries.

Top denied destinations

These are the most frequently denied destinations observed by the active SafePi protection mode. DNS denied domains come from DNS-level filtering and SafeDNS Guard observations. Proxy denied domains come from SafeWeb Proxy clients. Many denied domains are advertising, analytics, telemetry, or third-party infrastructure. Their presence does not automatically indicate malware.

DNS denied domains

Domain	Hits	Tag
api2.amplitude.com	101	-
metrics.icloud.com	6	-
default.exp-tas.com	3	-
tag.userreport.com	2	-
ping.chartbeat.net	2	-
cf.iadsdk.apple.com	2	-

Proxy denied domains

Domain	Hits	Method / Result
ws.support-chat.cloudflare.dev	3 811	CONNECT / TCP_DENIED/403
store-eu.gl-inet.com	2 574	CONNECT / TCP_DENIED/403
analytics-xpress.jabra.com	1 291	CONNECT / TCP_DENIED/403
dns.google	477	CONNECT / TCP_DENIED/403
res.public.onecdn.static.microsoft	160	CONNECT / TCP_DENIED/403
oneclient.sfx.ms	152	CONNECT / TCP_DENIED/403
o531h9iheud5j5jc6djll6qh1.litix.io	140	CONNECT / TCP_DENIED/403
officeci-mauservice.azurewebsites.net	20	CONNECT / TCP_DENIED/403
backend-xpress.jabra.com	20	CONNECT / TCP_DENIED/403
ping.chartbeat.net	17	CONNECT / TCP_DENIED/403
one.one.one.one	17	CONNECT / TCP_DENIED/403
x1.c.lencr.org	10	GET / TCP_DENIED/403

Device overview

Device activity helps identify where blocked traffic originated. High counts do not necessarily mean danger; some browsers and apps generate many third-party requests.

Top DNS-blocked devices

Device	Blocked hits
Device 1	102
Device 2	2

Top proxy-denied devices

Device	Proxy denied hits
Device 3	7 884
Device 1	644
Device 4	200

Configuration & Security Changes

This timeline shows important SafePi configuration and security-related actions during the reporting period. Routine background checks are not shown here unless they changed protection state or require attention.

Time	Type	Activity	Change	Details
2026-05-26 16:48	INFO	Post Update Health Check Passed (5×)	healthy	Post-update service health checks passed
2026-05-26 11:27	INFO	Manual sync completed	ok	Manual config sync completed from SafePi dashboard
2026-05-25 17:54	INFO	Manual sync completed	ok	Manual config sync completed from SafePi dashboard
2026-05-25 17:54	IMPORTANT	Allowlist applied	squid_allowlist	Squid allowlist changed and was reloaded successfully

Compliance & governance support

This section maps SafePi report evidence to common governance, risk, and cybersecurity review expectations. It is intended as operational evidence support, not as a certification claim.

Control area	Evidence available in this report
Security monitoring	Aggregated DNS, proxy, and security findings with interpreted trends.
Incident visibility	High-risk findings are separated from operational and informational background activity.
Change accountability	Configuration and protection-related changes are recorded with timestamps.
Network policy enforcement	SafeDNS Guard, Pi-hole, and SafeWeb Proxy enforcement statistics are included.
Trend analysis	Current reporting period is compared with the previous period when enough history exists.
Data minimization	The report excludes page contents, passwords, keystrokes, and packet capture data.

Transparency and privacy

This report is generated locally from SafePi's long-term aggregated statistics database. SafeDNS Guard and SafeWeb Proxy observations are reported separately because they represent different enforcement modes.

This public version of the report was automatically anonymized by SafePi before export. Local IP addresses, device names, and identifying metadata were removed or generalized.

SafePi stores for reporting	**SafePi does not store for this report**
Aggregated hourly security statistics	Full browsing histories
Top denied domains and devices	Page contents
Security findings and recommendations	Passwords or credentials
Protection status snapshots	Keystrokes
Proxy/DNS deny summaries	Packet captures

This design is intended to provide useful security transparency without turning SafePi into an invasive monitoring system.