15-24 September 2026 · Issue No. 1

SHIELD THREAT SNAPSHOT

1. THE WEEK IN NUMBERS

Metric	Observed
Monitoring window	15-24 Sep 2026 (8 days)
Total blocks at the edge	7,042
Typical full-day volume	~1,300 blocks
Peak day	17 Sep - 1,446 blocks
Quietest full day	21 Sep - 489 blocks
Block rule triggered	access_denied (100%)

2. WHAT WAS HITTING

No single campaign spike. The week shows steady, automated scanning: probes testing for open doors around the clock, every day, at roughly constant volume. This is the background radiation of the internet - and exactly what an always-on filter exists to absorb.

Alongside generic scanning we logged targeted vulnerability probes, including requests for exposed version-control data (/.git/config) - the classic first step before an intrusion attempt. All blocked before reaching any origin.

3. TOP SOURCES

The heaviest sources resolve to public cloud ranges - compromised or rented machines doing the scanning, not the attackers' own computers. This is normal: modern probing overwhelmingly comes from cloud IP space.

Source IP	Blocks
34.90.200.218	1,115
3.82.141.143	868
45.138.12.16	722
34.88.92.115	561
34.88.41.74	559
136.64.170.46	549
94.154.46.244	505

4. WHAT SHIELD DID

Every one of the 7,042 requests was stopped at the edge by licence validation and filtering layers. No customer origin was touched by this traffic. Per-request licence checks, WAF auto-banning and tiered rate limiting ran throughout with no intervention and no downtime.

5. METHODOLOGY

Counts come from Shield firewall block logs and security event logs for the stated window, de-duplicated per source, rule and minute. This is a weekly snapshot series, not a projection. Next issue covers the following week. Contact: sales@9genmedia.co.site - 9genmedia.co.uk/shield.