

■ MARKETPLACE PACKAGE · ENDPOINT DNS FILTERING

DNS filtering, *without the middlebox.*

The DNS Sensor brings web filtering and content blocking to the endpoint itself, enforced by the Cylerian agent you already deployed. Every DNS query is intercepted locally and evaluated against your category blocklists and custom domain lists before it ever reaches an upstream resolver. No appliance, no traffic detour, no separate console.

+ ON-ENDPOINT ENFORCEMENT

+ 32 CURATED CATEGORIES

+ CUSTOM LISTS & REGEX

+ HTTPS BLOCK PAGES

+ UNBLOCK WORKFLOW

+ EVENT VISIBILITY

01 WHAT THE SENSOR PROVIDES

01	FILTERING	02	CATEGORIES	03	CUSTOM
DNS-Level Web Filtering The sensor runs as a local DNS proxy. An NRPT rule routes every query through a compact bloom filter before anything goes upstream. + Filter built & pushed by the platform + Dual-path upstream, UDP + DoH race		Category-Based Blocking Choose from 32 curated domain categories, from security threats and adult content to advertising, file sharing, and social media. + Live domain counts per category + Seven groups, Security to Lifestyle		Custom Domain Lists Supplement categories with per-policy whitelists and blacklists, as plain domains or regex patterns with a built-in test field. + Always-allow & always-block entries + Regex mode with live pattern testing	
04	BLOCK PAGE	05	UNBLOCK	06	VISIBILITY
Local Block Page Blocked domains resolve to a local block server. For HTTPS sites, a certificate is minted on demand via SNI so the page renders cleanly. + HTTP & HTTPS block pages + Unblock request button built in		Guided Unblock Workflow Unblock requests raise platform alerts. Approving one whitelists the domain and reconfigures affected endpoints automatically. + Auto-unblock, 15 min to 24 hr + Admin approval always required		Blocked Domain Visibility Blocked activity is deduplicated and logged to the Events index, queryable across the whole fleet. + Query: type=dns subtype=blocked + Independent policies via CyQL filters	

02 HOW A QUERY IS EVALUATED

STEP 1	STEP 2	STEP 3	STEP 4
NCSI Bypass Windows connectivity checks are forwarded directly to avoid adapter resets.	AAAA Suppression IPv6 queries get an instant empty response to prevent browser timeouts.	Network Gate If the network is mid-transition, the query fails fast instead of hanging.	Bloom Filter Lookup The domain is tested against your categories and custom blacklists.
BLOCKED · Resolves to 127.0.0.1, the local block server serves the block page		ALLOWED · Forwarded upstream with per-resolver circuit breaking & backoff	

03 LOOK-ALIKE DOMAIN INTELLIGENCE

07	LOOK-ALIKE	08	EMAIL LINK
Typosquat & Homoglyph Detection Continuously scores domains against your brand and your vendors for typo, homoglyph, and combosquat variants, the exact pattern behind the itallgood897 network. + Brand & vendor look-alike monitoring + Homoglyph & TLD-swap detection		Domain Intel Wired to the Inbox Shares domain verdicts with Cylerian's AI-native email layer, so a flagged look-alike is stopped as BEC and vendor-invoice fraud, not just at the resolver. + Unified domain + email verdicts + Auto-quarantine of matched senders	

Installed from the Marketplace, enforced by the agent.

Install in two clicks, then create block policies scoped to any set of endpoints via CyQL. The platform compiles the bloom filter, ships the binary from its CDN, and configures every in-scope endpoint automatically.

PLATFORM · WINDOWS X64
REQUIRES · CYLERIAN AGENT
VERSION · 0.0.3