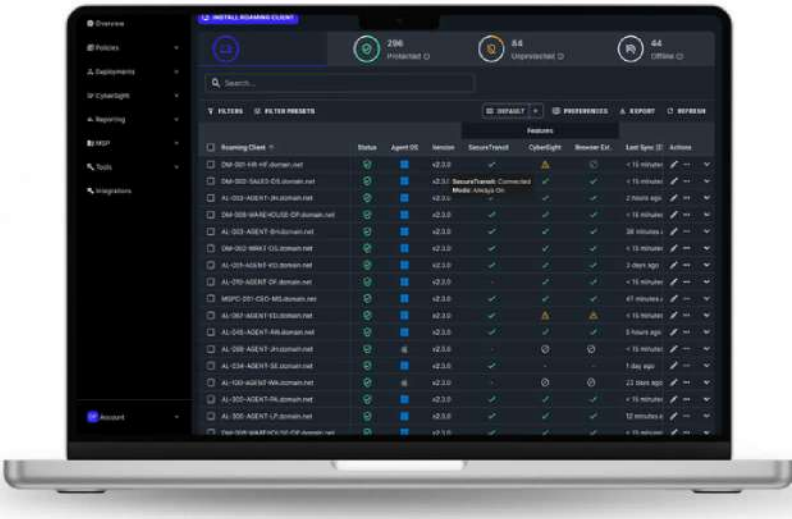
DNSFilter SOLUTION BRIEF

SecureTransit by DNSFilter:

Endpoint privacy, enforced as policy.



The Problem with Most Endpoint Privacy Solutions

Most endpoint privacy solutions in managed environments are poorly enforced. They live as separate tools, in separate consoles, relying on end users to remember to connect. The gap between "user is off-network" and "user remembers to turn it on" is where traffic gets intercepted and trackers profile your team.

SecureTransit closes that gap. SecureTransit is endpoint privacy: the egress layer that encrypts outbound traffic before it crosses an untrusted network, and blocks the trackers and data brokers that observe it once it gets where it's going. One agent. One console. Set by policy, enforced by IT.

Privacy On Top of Protection

DNSFilter protects your users wherever they go. SecureTransit keeps everything else they're doing private.

Every time your team connects from a tradeshow or airport, they're on a network you don't own. Traffic on those networks can be observed and intercepted. And your users have no way to know when that's happening, and no incentive to do anything about it. SecureTransit encrypts that traffic before it leaves the device, so what moves across the wire is unreadable to anyone on the local network.

Beyond the network itself, the sites your users visit are quietly collecting location trackers, mail trackers, data brokers — building profiles in the background on every visit. SecureTransit blocks those connections before they're made, so the data never leaves in the first place.

Your IT admin decides how the tunnel is enforced. Always-On means it's automatic. Users are protected without ever thinking about it. Manual mode hands control to the user on the device. Either way, it's a deliberate policy decision set in the same console your team already uses for DNS filtering.

For MSPs, that means consistent, enforced privacy posture across every client delivered as an add-on to the Roaming Client they already have deployed. One agent. One console. Nothing left to manage separately.

Why SecureTransit?

Policy-Driven Enforcement

Privacy is set by admins and enforced at the org or device level — not left up to users who may not know they're being tracked.

Trackers Blocked At Source

Location trackers, mail trackers, data brokers, and ad networks are cut off before connections are made. With Always-On enforcement, that protection runs regardless of network.

Privacy From Outsiders, Not You

Your admins keep the same DNS query visibility they have today. SecureTransit shields users from local-network observers and third-party trackers — not from your security team.

Per-Device Licensing

License only the devices that need it. Ships inside the Roaming Client — no new agent, no new endpoint footprint. Managed from the same console as your DNS filtering.

DNS blocks the threats. SecureTransit handles the privacy. **Your data should be yours** — on hotel Wi-Fi, on the office network, and inside every site your team visits.

GET IN TOUCH

dnsfilter.com (877) 331-2412 sales@dnsfilter.com

DNSFilter SOLUTION BRIEF

Built For...

IT

Private connections wherever your team works — managed from a single console with the same policy model you use for DNS filtering. Coverage follows the user, not the location.

MSPs

A billable add-on for clients who need consistent privacy posture. License where it matters. Multi-tenant dashboard. Channel margin built in, delivered through the Roaming Client your clients already have.

Security

Continuous enforcement in Always-On mode. Users can't forget, skip, or disable it. Privacy from outsiders, not yourself — your team keeps every DNS query in the same logs they have today.

Use Cases

REMOTE AND HYBRID WORKERS

Connecting from home, hotel Wi-Fi, airport, or conference networks where the local network is hostile or unknown.

EVERYDAY BROWSING PRIVACY

Corporate devices used daily for vendor research, SaaS logins, and ad-laden articles. Tracker profiling cut off regardless of network.

MSP CLIENT ENVIRONMENTS

Where privacy tools have historically been separate, poorly enforced, and split across diverse client deployments. Roll it out as a billable add-on across your client base.

REGULATED INDUSTRIES

Where reducing outbound data exposure to third parties — not just blocking inbound threats — is part of the security posture.

How SecureTransit Works

SecureTransit tunnels traffic to a DNSFilter-managed secure gateway over IKEv2 with AES-256 encryption or WireGuard. It encrypts traffic before it leaves the device and blocks tracker connections at the source — location trackers, mail trackers, data brokers, and ad networks are cut off before data is ever transmitted.

POLICY MODES

Always On
Encrypts traffic so local networks can't intercept it, and blocks the trackers and data brokers that profile your users.

Manual
User toggles the tunnel. When disconnected, the device falls back to DNSFilter's DNS-layer filtering.

Disabled
Tunnel not active. DNS-layer tracker filtering remains in place via the Roaming Client.

HOW THE LAYERS TIE TOGETHER

ZTNA handles *identity:*
Controls who can reach which internal resources, like apps, databases, and admin tools.

DLP controls *content:*
Inspects outbound content to prevent sensitive data — financial, PII, IP — from leaving.

SecureTransit *Monitors:*
Encrypts traffic so local networks can't intercept it, and blocks the trackers and data brokers that profile your users.

GET IN TOUCH

dnsfilter.com (877) 331-2412 sales@dnsfilter.com

DNSFilter

CyberSight™ by DNSFilter:
Actionable User Behavior Analytics

More Context Than Ever Before:

Get the Full Story. Accelerate Incident Response. Optimize Operations.

With CyberSight™, DNSFilter is now the first truly unified protective DNS and user-level intelligence platform built for distributed workforces. We eliminate the security blind spots of 'off-network' devices by combining lightning-fast threat protection with unparalleled user and endpoint visibility.

CyberSight™ gives your security team the full context of user behavior, application usage, and chronological event timelines—all built into your DNSFilter platform. It's the visibility you need to accelerate security forensics, stop Shadow IT, and optimize SaaS spend.

What's Included in CyberSight™?

- Full URL visibility
- Full Application visibility
- Activity Log Report
- Activity Overview
- Threat Trend Report
- Timeline Report
- In the Future: URL and IP Filtering

CyberSight™ is included for Pro and Enterprise customers.

GET IN TOUCH

dnsfilter.com
(877) 331-2412
sales@dnsfilter.com

DNSFilter

Core Benefits & Capabilities

Accelerate Incident Response

When an incident occurs, time is critical. CyberSight™ provides the robust data needed to determine the full scope of a security event.

- See the precise web destination, not just the domain, giving you richer event context through full URL visibility that shows precisely when users took an action.
- Visually reconstruct user actions before, during, and after an alert.
- Pinpoint the who, what, and when of every event. Accelerate incident response to close incidents faster and with greater confidence.

Business Intelligence & IT Operations

Uncovering unauthorized application usage has never been easier thanks to CyberSight™, helping you mitigate Shadow IT and understand exactly what is happening on your network.

- Identify unapproved or unmanaged software to close security gaps.
- Identify risky user patterns and track changes in security posture to proactively implement better policies and reduce organizational threat exposure.
- Gain valuable insights into business operations to optimize productivity.

Cost Optimization

Beyond security, CyberSight™ delivers operational intelligence that directly impacts your budget.

- Use hard data to eliminate underutilized SaaS licenses and deliver measurable cost savings while bolstering your overall security posture.
- Save time by ditching the spreadsheets and regaining control of SaaS application usage.

START YOUR FREE TRIAL TODAY

GET IN TOUCH

dnsfilter.com (877) 331-2412 sales@dnsfilter.com

DNSFilter

DNS PreCheck™

Resilient. Secure. Conflict-Free.

It's time for best-of-both worlds content filtering. DNS PreCheck™ gives you the flexibility to filter locally, before DNS ever gets involved. This revolutionary approach means you gain world-class threat intelligence without changing your core network infrastructure.

DNS PreCheck™ has built-in flexibility and controls, allowing you to customize your Roaming Client deployments more than ever before. Pair this Roaming Client-only deployment with DNSFilter's network protection for robust security in your environment.

No IT Setup Hassles:

No DNS changes required for Windows Roaming Clients, simplifying your deployments.

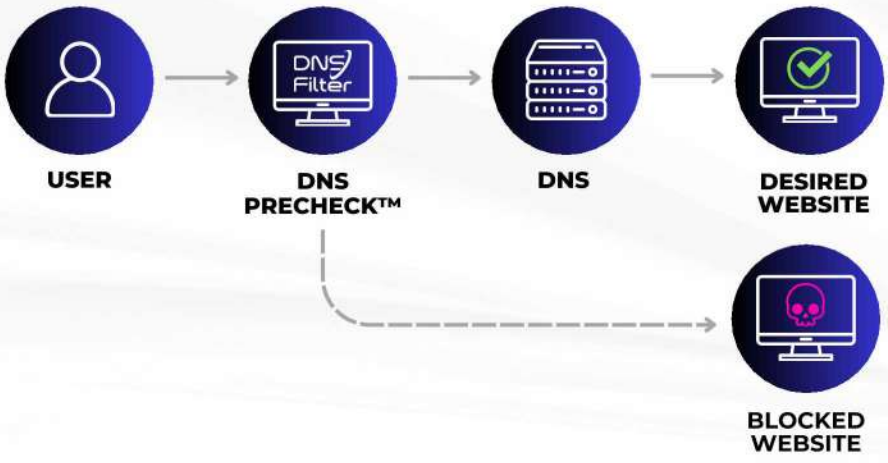
Conflict-Free:

Captive portals and VPNs create conflicts with traditional filtering, DNS PreCheck sidesteps these by filtering locally.

Resilient Protection:

Decrease security gaps by filtering before the query ever leaves your endpoint, all while minimizing latency.

DNS PreCheck™ in Action



Key Configuration Advantages with DNS PreCheck™:

- Uninterrupted connectivity
- Fail open model by default
- Failover behavior controls
- No extra configurations (IPV6, local domains)
- Optional: Filter locally and DNS

START YOUR FREE TRIAL TODAY

dnsfilter.com (877) 331-2412 sales@dnsfilter.com

DNSFilter

Solution Brief
Block & Discover
AI

01 DISCOVER AND CONTROL AI ACROSS YOUR ENTIRE USER BASE

Shadow AI, Seen and Stopped.

See every AI tool your users touch, decide which ones you trust, and block the rest in minutes. **DNSFilter combines DNS-layer blocking with user-level activity visibility** so you can govern AI use across your entire workforce. One platform. No agent fleet. No new console.

- **Curated AI category** classifies hundreds of generative AI services
- **Per-user, per-site, per-group** allow-listing for sanctioned tools
- **Full URL & application visibility** via CyberSight on Windows roaming clients
- **1-year CyberSight retention** of user activity logs, exportable for audit

Hundreds	All users	1 year	< 1 day
OF AI SERVICES CLASSIFIED	NETWORK + ROAMING CLIENTS	CYBERSIGHT RETENTION	FIRST AI REPORT VISIBLE

ONE PLATFORM. BLOCK AT THE RESOLVER. DISCOVER AT THE USER.

Block: DNSFilter Policy

- **Pre-connection prevention.** AI domains, malicious AI clones, and risky GenAI services blocked before TCP.
- **Curated AI category.** Hundreds of generative AI services classified and refreshed as new tools emerge.
- **Identity-aware allow-list.** Block by default. Allow specific tools per user, site, group, or roaming device.

+

Discover: CyberSight

- **Full URL visibility.** Not just the domain. The exact AI prompt page, model, or workspace a user opened.
- **Application visibility.** See which AI desktop apps and unmanaged tools are running on user devices, including activity while idle.
- **Chronological timeline.** Hour-by-hour view of user activity, device state, idle time, and streaming sessions.

DNS-layer policy stops AI before the connection. CyberSight tells you who used what, when, and from which device.

Both capabilities ship inside DNSFilter. No SIEM, no CASB, no endpoint DLP agent fleet required.

FOUR STEPS TO LIVE. FROM ZERO TO AI GOVERNANCE.

1

Turn on DNSFilter

Point network resolvers at DNSFilter, or push roaming clients to laptops. Protection live in under 10 minutes.

2

Watch the AI category

Run in reporting-only mode for a week. Identify which AI tools your users actually rely on and which to sanction.

3

Enable CyberSight visibility

Push the Windows roaming client v3.1+ with the CyberSight browser extension. *Included in Pro and Enterprise.*

4

Block and allow-list

Flip the AI category to block. Add allow-list entries for sanctioned tools. Audit usage in CyberSight timelines.

SHADOW AI DISCOVERY

Inventory every AI tool a user opens, by URL and application, attributed to the person and device.

SANCTIONED AI ENFORCEMENT

Allow your approved LLM for the teams that need it. Block the 50 lookalikes your users would have tried.

DATA-LEAK INVESTIGATION

A blocked AI domain plus a CyberSight timeline of what that user did before and after. One investigation pane.

COMPLIANCE EVIDENCE

1-year CyberSight activity retention. CSV export. Mapped to ISO 27001 A. 8.23 web filtering and NIST AI RMF.

WHY MSPS & IT TEAMS CARE

- **One platform, one bill.** Block, discover, and audit AI in Pro & Enterprise plans. No add-on.
- **No SSL inspection, no agent fleet.** DNS plus a single roaming client + browser extension.
- **Lower MTTR.** Multi-tool, multi-day investigations compressed into one timeline.
- **NFR-friendly.** Run it in your own tenant before recommending to clients.

Block at DNS. Discover at the user. Govern AI once.

Included in DNSFilter Pro & Enterprise · CyberSight requires Windows Roaming Client v3.1+ · partners@dnsfilter.com

Get started:
app.dnsfilter.com

DNSFilter

AI-Powered **Protective DNS for Global Networks**

DNSFilter is a cloud-based protective DNS platform that blocks threats and unwanted content before connections are established. Using advanced AI threat detection and global infrastructure, DNSFilter protects users and networks without adding latency or complexity.

Designed for highly distributed networks, DNSFilter is trusted by connectivity providers, enterprises, and service providers worldwide.

NVIDIA · msc · J.D. POWER · Viasat

200 BILLION+ DNS queries each day

235 MILLION Threats blocked daily

170 SERVERS Power our **Global** Anycast Network

45 THOUSAND organizations trust DNSFilter

Key Markets & Use Cases

MARITIME

Secure connectivity for vessels, fleets, and offshore operations.

- Harden ship networks against phishing and malware
- Enforce acceptable use policies for Wi-Fi and devices
- Slash bandwidth waste by filtering traffic

AVIATION

Secure passenger and operational networks worldwide.

- Protect In-Flight Connectivity
- Enforce acceptable use policies for Wi-Fi and devices
- Zero-hardware deployment

ISP & CONNECTIVITY

High-margin protective DNS for every subscriber.

- Shield users from evolving cyber threats
- Minimize abuse complaints and block malicious traffic
- Unlock new revenue with security add-ons

ENTERPRISE

Protect distributed organizations and remote users.

- Block ransomware, phishing, and malware
- Secure branch offices and remote workforces
- Flexibility at scale across hybrid and global networks

PUBLIC WI-FI

Protect guest networks in hotels, airports, retail, and venues.

- Block unwanted content to mitigate brand and legal risk
- Harden security on open networks
- Deploy effortlessly at scale

WHY DNSFILTER

AI-driven threat detection | Fast global DNS infrastructure | Cloud-delivered security
Easy deployment at scale | Works in *any* network environment

GET IN TOUCH

dnsfilter.com · (877) 331-2412 · sales@dnsfilter.com