DNSFilter

SPOTLIGHT

This is a short summary of our event Oct 29, 2026 at the Nasdaq for our first Investor day and the launch of our platform LUMINATE by DNSFilter™.

© 2026 DNSFilter Inc. All Rights Reserved.



OPENING BELL TO CLOSING BELL

Between Nasdaq's opening and closing bell,

DNSFilter answers around 50 billion DNS queries.

For every blink of an eye we block another 800 threats before your eyes reopen.

Counting just one month's worth of DNSFilter queries would take the same time **as light would take to cross the Milky Way. Twice.**

If the data stored in DNSFilter's Intelligence Engine were songs, you could listen non-stop for over **11,000 years.**

© 2

Security starts at the source

40 million

New domains are identified & scanned by **DNSFilter** each month

235 million

threats blocked per day

5 billion

unwanted content pages filtered per day

6 trillion +

Monthly Queries

3 million

queries per second

10 days faster

in blocking emerging threats



© 2026 DNSFilter Inc. All Rights Reserved.

From filter to platform - key moments in our journey

What started as a single, sharply focused product has grown into something broader, because the problem it was solving grew too.

2015

DNSFilter

The company was founded in 2015

2018

webshrinker

We acquire Webshrinker, the engine that still powers our threat categorization and efficacy today.

2021

We raise a $33.5 million Series A from Insight Partners and Arthur Ventures, one of the largest cybersecurity Series A rounds of the year.

2022

We acquire Guardian, a privacy-protecting firewall for iOS and Android, extending our DNS-first approach to mobile and personal devices.

2023

A Series A extension brings in another $15 million to keep building toward a broader platform vision.

2025

ZORUS

We acquire Zorus, bringing advanced behavior analytics and shadow IT visibility into the fold.

2026

LUMINATE by DNSFilter

© 2026 DNSFilter Inc. All Rights Reserved.

Proven Success





© 2026 DNSFilter Inc. All Rights Reserved.

Deep Sector Experience, Large Scale Contracts



Running the world's largest mesh wifi platform and securing 4 of the Fortune 10



Securing guest and corporate Wi-Fi across global properties worldwide at one of the largest global hotel groups



Protecting clinicians and staff where downtime is not an option. Proud to support hundreds of hospitals and medical technology providers secure their services



When compliance, regulation and safety are paramount - 238 Financial Services look to DNS Advanced Filtering Technology



In store Wifi and back office support in the world’s largest retailer, plus another 206 CPG and Food orgs



Keeping millions of travelers safe and secure as they travel for work and pleasure



Securing students and staff across 343 U.S Education Institutions



Securing stores, from checkout to back office

© 2026 DNSFilter Inc. All Rights Reserved.

Keeping businesses connected and moving...



Securing Public Wi-Fi



Block Inappropriate Content



Reduce Bandwidth Strain



Improve Productivity



Achieve Compliance



Shadow AI



Mitigate Shadow IT



Accelerate Incident Response



Stop Threats



Protect Hybrid Workforces



Secure IoT/OT Devices

© 2026 DNSFilter Inc. All Rights Reserved.

THE PROBLEM

Modern attacks start at the edge

The greatest vulnerability is **the space between your tools.**



Siloed tools don’t share signal.

The attack view is **fragmented**.

FRAGMENTATION



Adversaries move at machine-speed.

Domains weaponized in **minutes**.

VELOCITY



Detection arrives too late.

The payload comes **before** the alert.

LATENCY

© 2026 DNSFilter Inc. All Rights Reserved.

THE PROBLEM

DNS is the most attacked, least defended layer.

79%
of all breaches involve the DNS layer

33%
of breaches are initiated at DNS

85%
of malware actors use DNS in attacks

90%
of orgs have experienced a DNS attack

The AI era widened the gap.

01
AI-Speed Attacks
Adversaries weaponize domains in minutes. Detection arrives only after the payload lands.

02
Fragmented Toolstacks
Siloed tools don't share signal — the attack view is incomplete by design.

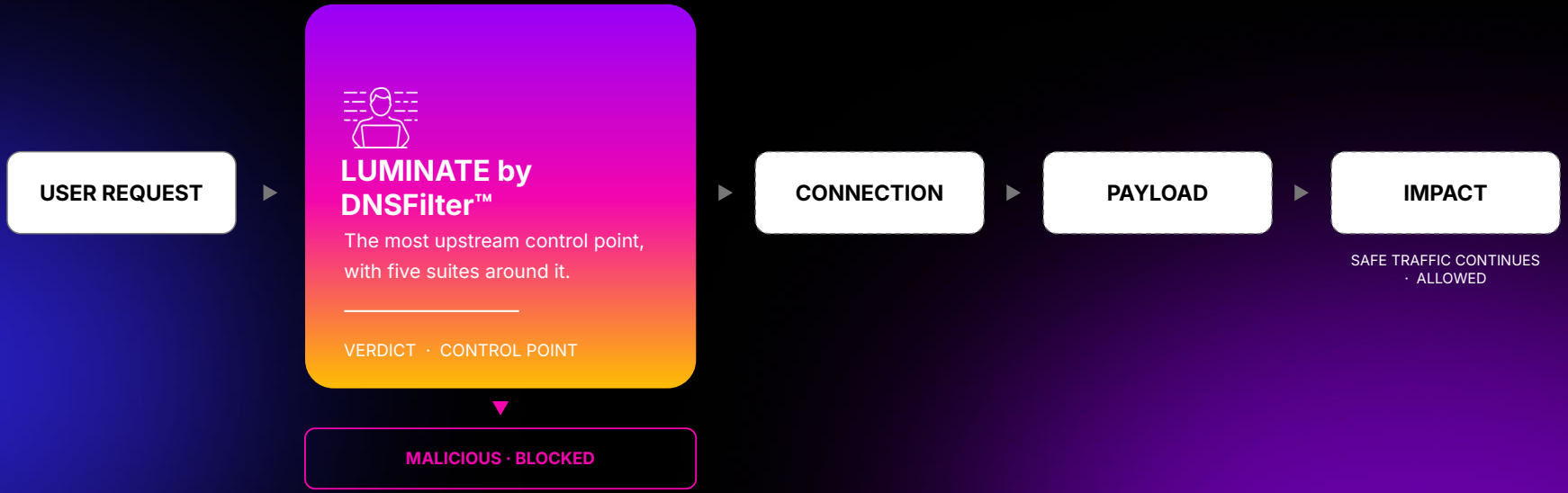
03
Agentic AI Blind Spots
AI agents make autonomous DNS connections legacy tools can't see.

© 2026 DNSFilter Inc. All Rights Reserved.

THE DNS FIRST THESIS

Stop attacks before they happen

Stop the threat at the name lookup and it never becomes a threat.



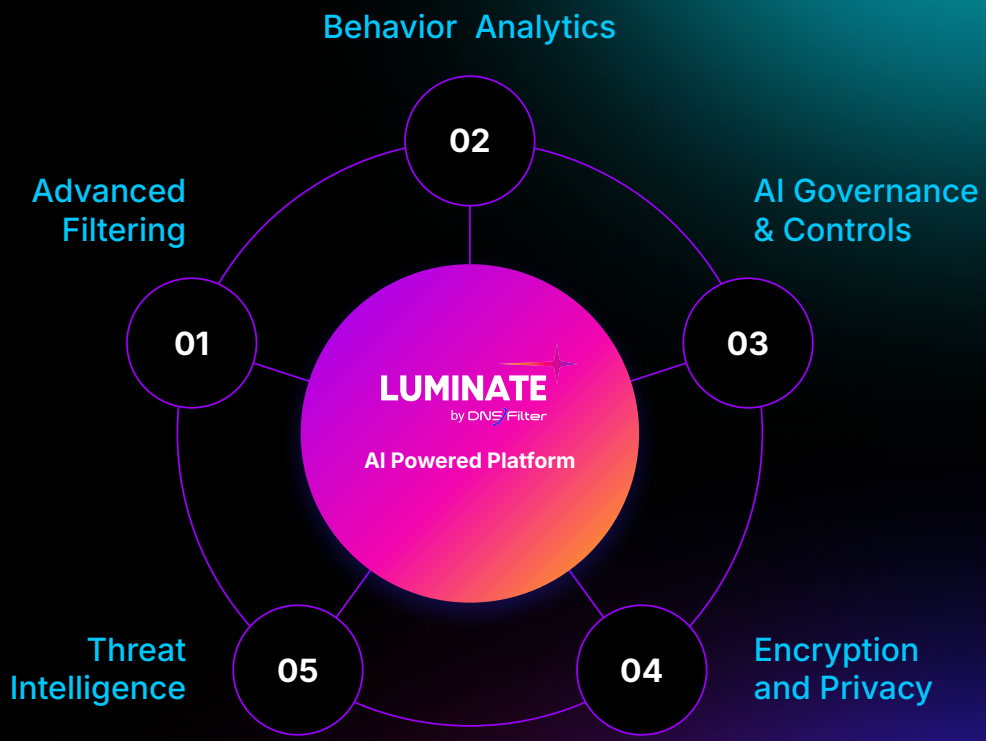
DNS First is a strategy, not a feature.

© 2026 DNSFilter Inc. All Rights Reserved.

THE PLATFORM AT A GLANCE

Five suites. One engine.

Every decision starts at DNS, then propagates to every suite. Powered by AI, infrastructure agnostic by design.



ONE AGENT · ONE CONSOLE · ONE INTELLIGENCE MODEL

© 2026 DNSFilter Inc. All Rights Reserved.

FIVE PRODUCT SUITES

DNS First. Grow at your pace

Each suite is a distinct outcome of shared platform intelligence.

LUMINATE FOR

Advanced Filtering

Every click is a control point, anchored by DNS

LUMINATE FOR

Behavior Analytics

Earlier visibility into intent, anomalies, risk.

LUMINATE FOR

AI Governance & Controls

Govern AI to reduce risk.

LUMINATE FOR

Encryption & Privacy

Privacy enforced as policy.

LUMINATE FOR

Threat Intelligence

DNS-native intel. DGA tracking. Connected to the tools you need.

Deployed in minutes. No replatforming between suites.

© 2026 DNSFilter Inc. All Rights Reserved.

Advanced Filtering

State-of-the-art DNS filtering

- Stop threats before the payload executes
- Protect unmanaged devices and IoT/OT without agents
- Reduce bandwidth consumption by blocking resource-heavy content at DNS
- Help achieve regulatory content compliance
- Flexibility in deployment and controls



WHY IT WINS

We have the **largest** DNS dataset on the market.

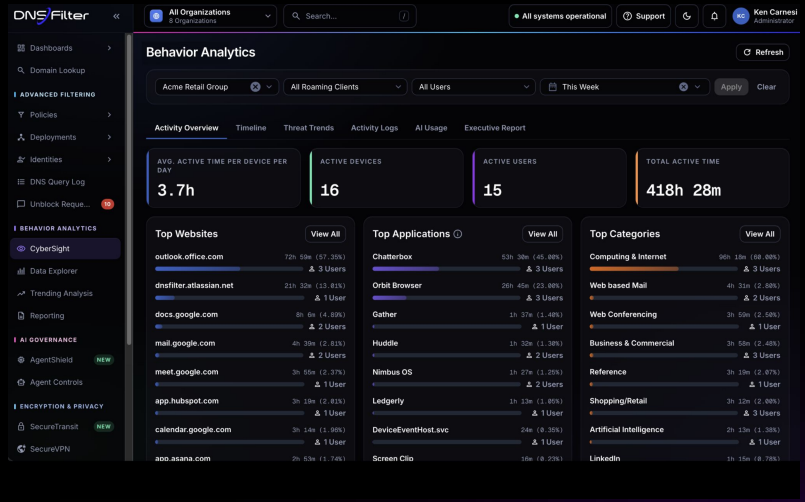
DNS-first content and category controls with AI-driven classification, URL and IP enforcement, and device-aware policy. Best-in-class precision filtering with continuous updates from the global intelligence engine. The **original** DNS-First product.

© 2026 DNSFilter Inc. All Rights Reserved.

Behavior Analytics

Visibility into intent, anomalies, and emerging risk.

- Accelerate incident response with user-to-activity forensics
- Discover and quantify shadow IT across the organization
- Detect behavioral anomalies that signal compromise early
- SaaS application management: Identify unused SaaS licenses and reduce software spend
- Gain minute-level visibility into workplace productivity and tool utilization



WHY IT WINS

Our Behavior Analytics extends the intelligence layer **beyond** DNS filtering into user and device activity.

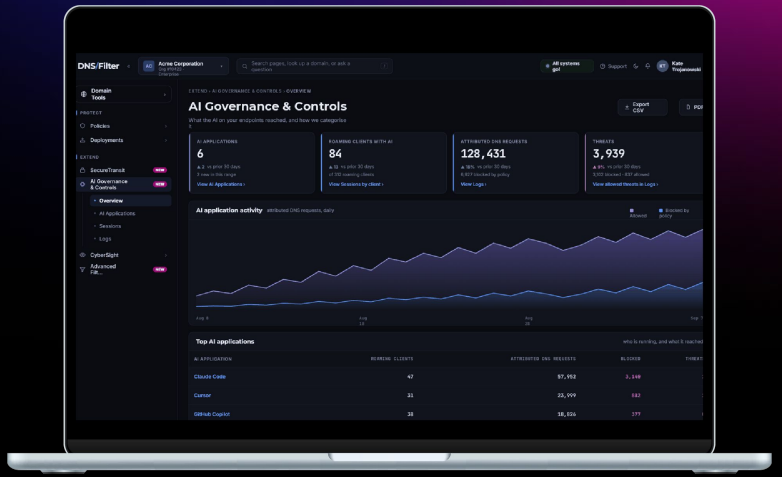
Anomalies and indicators of compromise surface earlier and with higher fidelity.

© 2026 DNSFilter Inc. All Rights Reserved.

AI Governance & Controls

Next-generation AI governance and controls.

- Complete shadow AI oversight across the environment
- Control which cloud applications and AI tools users can access
- Apply policies to AI agents as distinct entities (treat them as you would an employee)
- See agent behavior and human behavior side by side
- Detect and govern agent-to-agent or agent-to-external connections



WHY IT WINS

AI Governance and controls gives you control over both human and agent behavior.

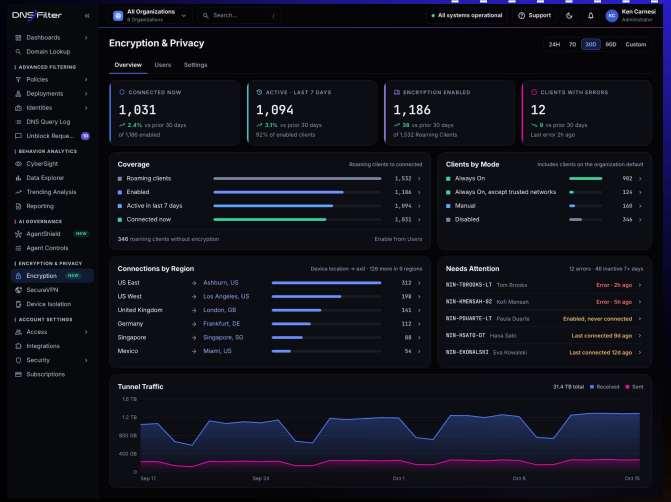
AI risk is classified and enforced, with usage reporting, exposure mapping, and agentic workflow access guardrails. Ideal for both SOC and MSP operations.

© 2026 DNSFilter Inc. All Rights Reserved.

Encryption & Privacy

Encrypted access enforced and managed as policy.

- Zero-trust enforcement governed by DNS First policy
- Encrypt all traffic for off-network users on untrusted networks
- Quarantine compromised or non-compliant devices
- Replace VPN complexity and consolidate security and privacy tools
- Selective tunneling by application, FQDN, and IP



WHY IT WINS

Policy-driven encrypted access with dedicated egress IPs and quarantine controls.

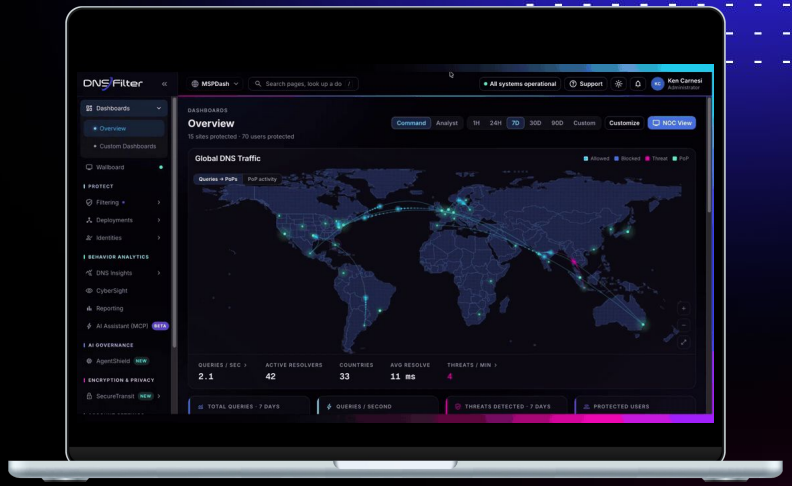
Best-in-class VPN services with no SASE replatforming.

© 2026 DNSFilter Inc. All Rights Reserved.

Threat Intelligence

Stop threats before they reach the endpoint.

- Threat intelligence delivered how you and your agents need it
- State-of-the-art servers and controls
- Detect algorithmically generated domains before they're weaponized
- Triage suspicious indicators in real time during active incidents
- Assess exposure at scale after a breach or threat advisory
- Discover compromised endpoints your existing stack hasn't flagged



WHY IT WINS

Proprietary, DNS-First threat intelligence with patent-pending lookalike domain detection.

10 DAYS

FASTER TO DISRUPT MALICIOUS INFRASTRUCTURE THAN THE COMPETITIVE SET

© 2026 DNSFilter Inc. All Rights Reserved.

Security starts at the source

LUMINATE brings five capabilities into one DNS-first platform, protecting organizations at the layer where most attacks first appear.

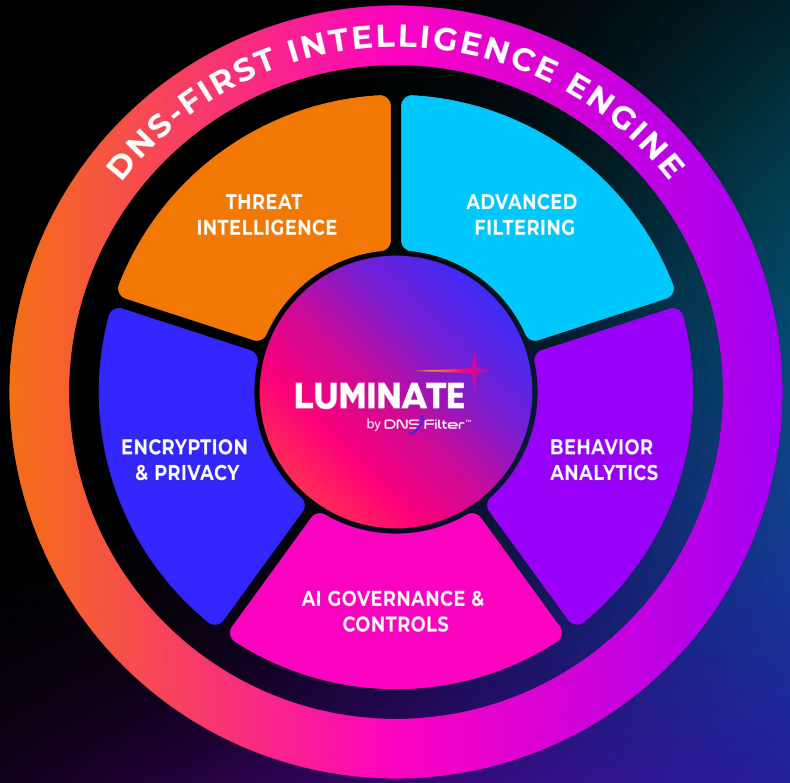
THE ENGINE BEHIND THE SUITES

3M / SEC

DOMAINS SCANNED

235M+

THREATS BLOCKED DAILY



One engine powers all five.

© 2026 DNSFilter Inc. All Rights Reserved.

Five forces are converging. DNSFilter sits where they meet.

01
Attacks move at Machine- speed

Domains get weaponized in minutes.

Our edge is speed: the domain is blocked before it's used.

02
Regulators back protective DNS

CISA, NCSC and NIS2 are driving adoption.

As policy turns to protective DNS, we're already deployed at scale.

03
MSPs run more of SMB IT

SMBs are outsourcing IT at pace.

Every LUMINATE suite adds recurring revenue to an MSP's business.

04
Buyers want fewer vendors

Teams are collapsing vendor counts.

LUMINATE gives them one place to consolidate the DNS security layer.

05
The window is open now

The market is choosing its platforms.

We have the product, the scale and the channel. Now is when it counts.

The category is ours to define.

Five forces meet at the DNS-first control point. No competitor is built there.

LUMINATE by DNSFilter is.

© 2026 DNSFilter Inc. All Rights Reserved.

DNSFilter

SPOTLIGHT

We look forward to continuing the conversation. Thank you for attending.

Contact Rebecca Cradick, Vice President Global Communications and Investor Relations for 1-1 requests.

ir@dnsfilter.com

© 2026 DNSFilter Inc. All Rights Reserved.