



ADRIA FORUM 2026 · 29.09.2026.

Battle before the breach

Why DNS security belongs on the investment side of the budget

Andrej Anđelić
Regional Manager, CEE

THE FRONT LINE

66

threats the average internet user was likely to run into every day in 2025.

Up from 29 a year earlier. Threat volume on the DNSFilter network grew 30% in 30% in twelve months.

Losing the battle has never been more expensive

\$4.99M

Global average cost of a data breach, a record high and 12% up on last year

IBM, 2026

16%

Of breaches started with phishing, the most common initial attack vector

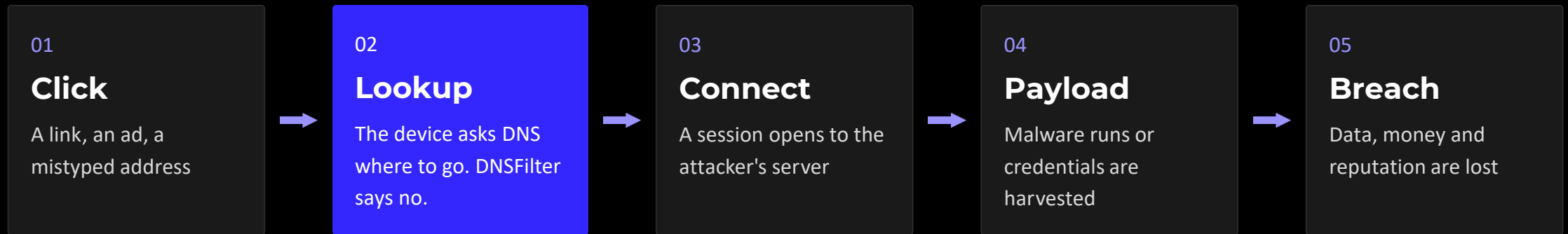
IBM, 2025

\$1.93M

Average saving for organisations using AI and automation extensively in security security

IBM, 2026

Almost every attack asks for directions first



Stop it at step 2 and steps 3 to 5 never happen: no payload to detect, no incident to handle, no breach to report.

Security gets booked as a cost

How the budget sees it

- A licence fee per user, per month
- A line to trim when budgets get tight
- Value nobody can point to on the P&L

How the business should see it

- Losses avoided that you can estimate
- Hours your team gets back every month
- Revenue and contracts it helps you win

The return is real. It shows up as incidents that never happened.

Three ways DNS security pays back

01

Avoid

Losses that never reach the P&L

02

Save

Time and effort your team gets back

03

Earn

Revenue and deals it helps you win

Put a number on the risk you remove

EXPECTED ANNUAL LOSS

Likelihood of a breach
× cost of a breach

Protective DNS lowers the first factor, at the cheapest point in the attack chain.

[€__] cost of the impact × [__]% likelihood = [€__] per year

~1/3

of breaches in a Global Cyber Alliance study could potentially have been stopped by a DNS firewall

3,668 of ~11,000 incidents analysed, 2019

Give your team its time back



Less clean-up

Blocked before the payload: no reimaging, no downtime, no weekend call-outs.



Live in minutes

Most customers are running within a day. MSPs onboard a new client in under ten minutes.



Faster answers

DNS logs show which device went where, turning hours of investigation into minutes.

Security that helps you win business

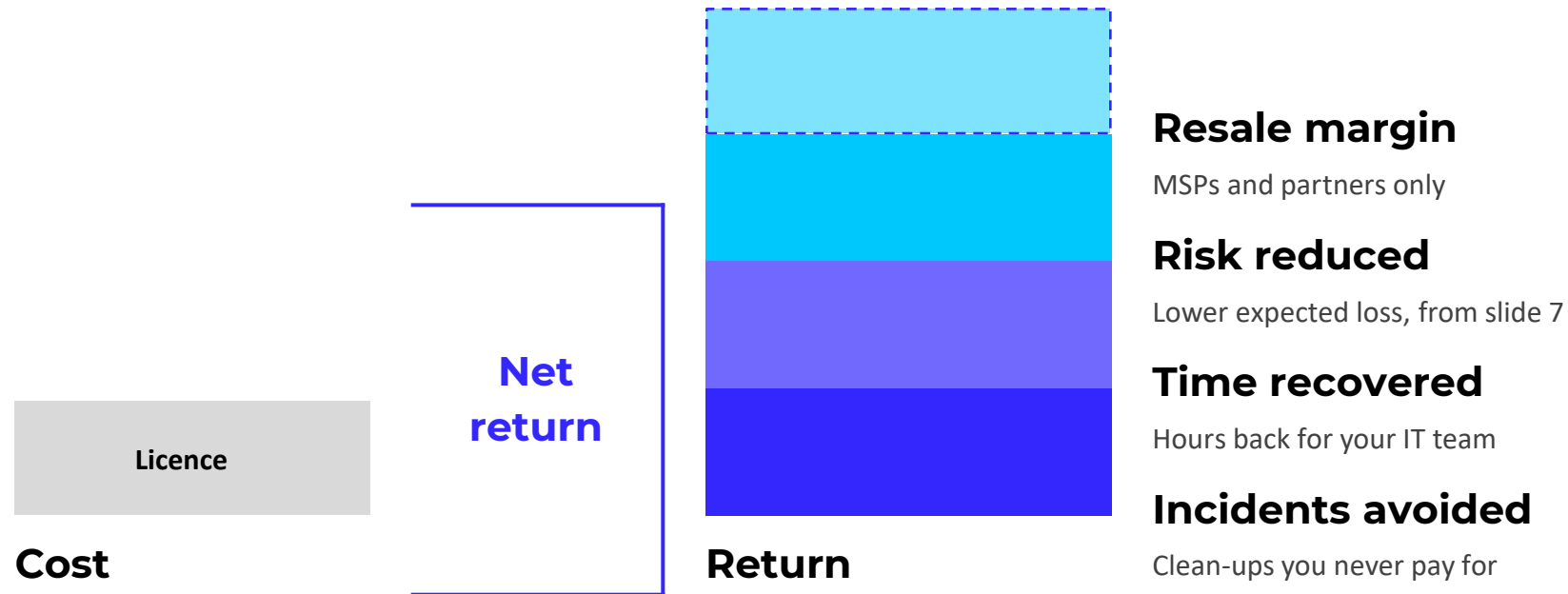
For businesses

- **Win and keep contracts:** pass NIS2 and GDPR supplier checks
- **Answer the insurer:** evidence for cyber-insurance questionnaires
- **Protect revenue:** tills, production lines and web shops stay up
- **Protect your brand:** safe guest and public Wi-Fi

For MSPs and partners

- **Recurring revenue:** a per-user managed service with healthy margin
- **Low cost to deliver:** one multi-tenant console, global policies
- **Grow with us:** Select, Accelerator and Strategic partner tiers

One cost line, four return lines



Want this with your real numbers? **We will build it with you.**

WHO WE ARE

DNSFilter at a glance

240B+

DNS queries processed
processed every day

43,000+

organisations protected
protected worldwide

6,000+

MSP partners

10 days

earlier threat blocking
blocking than traditional
traditional feeds

Founded 2015 · Washington, D.C. · AI-driven protective DNS and content filtering · Market Leader, Global InfoSec Awards at RSAC 2026

HOW IT WORKS

Without vs. with DNSFilter

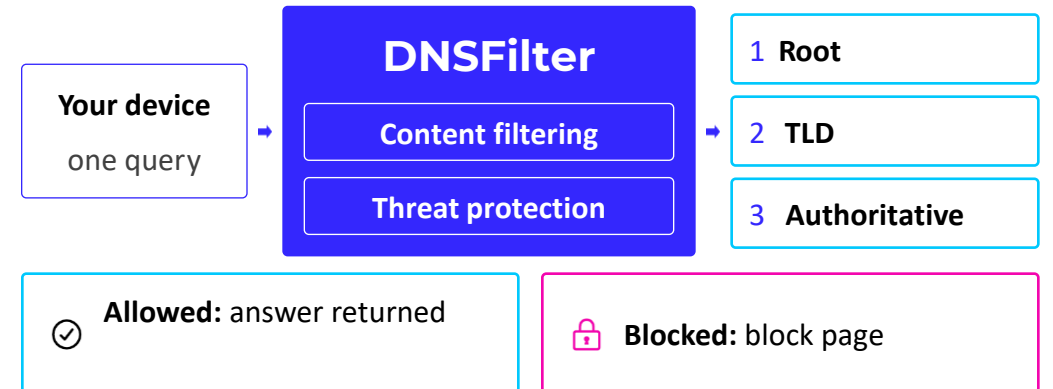
Without DNSFilter



The query walks the DNS hierarchy on the open internet. Each step just points onward to the next.

 **No checks:** phishing and malware domains resolve too

With DNSFilter



Office A • DNS forwarding

Firewall or router points to our Anycast IPs

Visibility: per site

Office B • DNS Relay

On-site Relay, internal domains stay local

Visibility: per device

Anywhere • Roaming Client

Agent on the device, any network, optional DoT

Visibility: per device and per user



AVOID · SAVE · EARN

Win the battle before the breach

Start a free trial, or talk to us about becoming a customer or a partner.

Andrej Anđelić

aandelic@dnsfilter.com

+385 99 365 2697

dnsfilter.com