

URL Filtering & DNS Protection

DNS Protection

Secure Every Connection.
Strengthen Every User.





DNS-level protection that works quietly, instantly and intelligently.

CyberSift DNS Protect empowers organisations to block threats before they reach users. A platform designed to secure networks and prevent threats while browsing the internet. With intelligent filtering, real-time phishing and malware protection, and over 80+ content categories, IT teams gain full control over network activity - creating a safer, cleaner, and more productive browsing environment.

Why CyberSift DNS Protect

Traditional DNS reacts. CyberSift DNS prevents.

CyberSift DNS Protect stops attacks at the DNS level, long before they reach your network. With machine learning-powered detection, real-time threat intelligence, and granular category controls, organisations gain a proactive layer of defence that enhances both security and productivity.

Key characteristics

Phishing Protection:

Detects and blocks deceptive websites using ML and BrightCloud™ intelligence.

Malware Infiltration:

Prevents access to domains known for distributing harmful software.

Domain Filtering:

Manage 80+ categories to control content by department or need.

Ad & Tracker Blocking:

Removes intrusive ads and stops behavioural tracking for cleaner browsing.

Network Visibility:

Monitor user behaviour through DNS activity to identify unusual patterns and emerging threats.

Full Administrative Control:

Whitelist or blacklist domains with flexible, policy-based controls.



Explore DNS Protect

How DNS Protect works

- 1. Account Provisioning**
Your CyberSift DNS Protect account is provisioned quickly, ensuring a fast and seamless start.
- 2. Quick Deployment**
Deployment takes just 30 minutes through a simple setup process, with no disruption to your workflow.
- 3. DNS-Based Protection Activation**
Once active, the solution protects your network from phishing sites, malware distribution, and advertising tracking.
- 4. Policy-Based Content Control**
Users can block or allow access across 80+ content categories, tailored to organisational needs.
- 5. Monitoring & Network Visibility**
DNS activity is monitored to provide visibility into user behaviour and support the identification of unusual patterns and potential threats.



Protection Through Collective Intelligence

At CyberSift, we believe cybersecurity should be intelligent, accessible, and built to empower everyone.

Born from a fusion of research and real-world expertise, we transform advanced AI into clear, strategic protection - enabling every organization to stay secure and resilient.

Guided by our vision to make cybersecurity accessible to everyone and to serve as a protector for the unprepared, we stand as a trusted partner in a world where digital threats evolve faster than awareness.

We don't just protect systems - we protect confidence, continuity, and growth.

Protection, at its core, is not about standing alone - it's about standing together. Like in nature, where every instinct contributes to survival, our technology learns, adapts, and protects as one.