inCONTROL

WEB FILTERING

BLOCK ONLINE THREATS & INAPPROPRIATE CONTENT

DNS filtering is defensive software that prevents cyber security threats by following simple logic: if a website has something **potentially dangerous** within it, DNS filtering blocks a user from visiting it in the first place.

It's a zero-trust solution that leaves nothing to chance.

EASY POLICY CREATION

With **inCONTROL**, creating a DNS filtering policy takes just 3 clicks. We allow our users to block 36 content categories, 8 threat categories, and ads and trackers. We also offer easy, one-click CIPA compliance.

BLOCK THREATS AT THE DNS LEVEL

According to a report by public resolver Quad9, 35% of security breaches could have been blocked by a web filter. **inCONTROL** protects users from accessing malicious and suspicious sites that are the cause of nearly ⅓ of security incidents.

FLEXIBLE DEPLOYMENT

We offer DNS filtering via agentless deployment - just point your network to our resolver - we'll take it from there. Or, easily install **inCONTROL** on individual devices for more granular tracking, reporting and policy creation.

5 REASONS WHY YOUR ORGANISATION SHOULD FILTER DNS

1. Stop threats before they hit your network

2. Granular control over how your network and devices are used

3. Insight into what types of threats might impact your network

4. Increase productivity by blocking time-waster sites

5. User-level reporting on sites and apps used by employees

inTEC BUSINESS

0345 565 1767 | info@intecbusiness.co.uk