BlueCat Edge and the UK National Cyber Security Strategy

To protect against cyber security threats and business disruption, organisations want to evaluate the alignment of their DNS technology investments with the UK National Cyber Security Strategy. With BlueCat Edge, cybersecurity and network teams gain shared visibility and control over internal and external DNS traffic, through a single platform, to improve network performance and build core competencies in network security.

BlueCat Edge alignment to the UK National Cyber Security Strategy:

Defend - Respond effectively to incidents

Edge allows network security teams to granularly monitor specific IP addresses to provide an additional layer of visibility and control over critical infrastructure. Because most firewalls today cannot identify the source IP address for DNS queries that egress to the internet, trying to monitor all DNS activity becomes overwhelming for network security teams. Edge makes this manageable because it captures the origin of queries, allowing threat hunters to focus on the most critical data quickly, and set specific policies based on the device or network to proactively protect against tunnelling and data exfiltration. Watch this short video

Deter - Detect, understand, investigate and disrupt hostile actions

Edge makes it easy to pinpoint the origin and review the internal and external DNS activity surrounding an incident. It integrates with tools like Splunk, ArcSight, Qradar, and other security information and event management platforms (SIEMs), passing on only the most relevant/ suspicious query data for further analysis and correlation with other security data. This allows security teams to pinpoint relevant insights from DNS data, correlate with other intel, lower costs, and shorten time to remediation, while at the same time preserving a complete record of all traffic for more comprehensive analysis. Watch this video.

Develop - Meet and overcome future threats and challenges

BlueCat Threat Protection integrated with BlueCat Edge enables seamless integration of the most up-to-date security intelligence, including BlueCat DoH blocklists, CrowdStrike, and other third party threat feeds. Organisations can also extend investments in Cisco Umbrella's external threat intelligence by adding lateral threat investigation, with BlueCat Edge, to stop infected devices. Watch this video

Beyond 2021

As outlined in the National Cyber Security Strategy Progress Report of Autumn 2020, there is "an ever greater reliance on digital networks and systems." Coupled with a "wider range of adversaries" and accelerated by COVID-19, expect much of the UK's strategy and guidelines for organisations to be enhanced in the coming months. BlueCat's DNS Security is a vital part of any multi-layered approach to cybersecurity and continues to serve as a best practice.

United States Headquarters
1000 Texan Trail, Suite #105, Grapevine, Texas 76051
+1.817.796.8370 | 1.833.BLUECAT

Canada Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
+1.416.646.8400 | 1-866-895-6931

bluecatnetworks.com

Next Steps

Get in touch with a BlueCat representative to future proof your network.

Visit bluecatnetworks.com/contact-us/