BLUECAT

Data sheet

Threat Protection: policy-based workflow for securing DNS queries

Block attacks at the DNS layer, stopping threats before they ever reach your business

Leverage DNS to secure your business

DNS data provides actionable information about how traffic is moving around the network and how DNS clients are using internal and external resources. Security teams can take advantage of this data for threat hunting and investigations, augmenting existing security data with rich DNS query data. Furthermore, you can improve your security posture with an additional defense layer by identifying and blocking malicious DNS queries based on threat feeds, security-defined block lists, or flexible policy system.

The solution: BlueCat Threat Protection

Protect everything connected to your network
Smartphones, point-of-sale (POS) systems, desktops, and security cameras all rely on DNS to connect to the network and external sites. Whether the device is in a fixed location or is mobile and lives beyond the walls of your enterprise, BlueCat Threat Protection can protect it from accessing malicious content and further proliferating threats into your network.

Extend defense in depth strategies
The coordinated use of multiple, complementary security countermeasures is key to enterprise defense in depth strategies. Threat Protection delivers critical contextual network data extending across wired and wireless networks, virtual environments, and mobile endpoints, to augment industry-standard layers of security.

Automated real-time threat data update
Defend against attacks with CrowdStrike threat feeds, the most active repository of threat intelligence in the industry. Subscribe DNS servers to the security feed, which is automatically delivered through DNS and continuously updated to block threats as they emerge.

Protect remote workers with DoH block lists
To protect against malicious activity, networking and cybersecurity teams need to maintain visibility into DNS traffic. Threat Protection provides DoH blocking to retain visibility into DNS queries by preventing lookups to known public DoH resolvers.

Benefits

- **Comprehensive threat coverage**
  Defend against attacks with real-time threat intelligence on millions of domains associated with 100+ unique malware families and 30+ unique threat types.
- **Enhanced threat classification**
  Prioritize threat activities based on severity, frequency, and confidence.
- **Continuous updates and expertise**
  Enrich DNS data with insights from 30B+ daily events, which are reviewed by an elite team of threat analysts and security researchers.
- **Eliminate security blind spots**
  Correlate detailed information with other data sources by integrating with existing security investments and market-leading SIEMs.

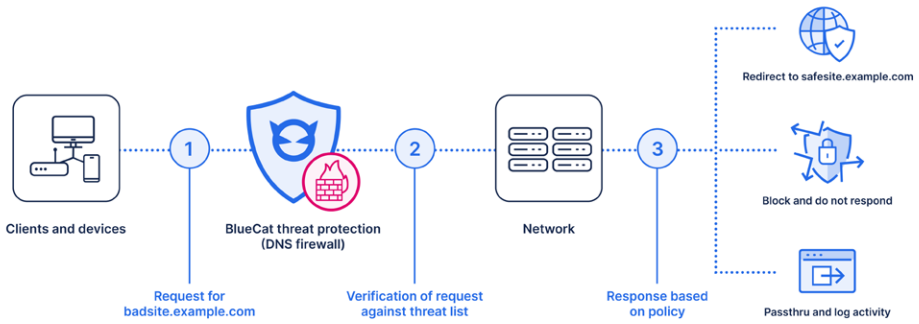

Figure 1. Protect the enterprise by blocking DNS based phishing, DGA, and tunneling attacks

Features

Customizable actions
Each security feed can be configured with its own action, such as redirect, blocklist, do not respond, and log, allowing administrators to tailor the response to their needs.

Reporting
Aggregation of query and response data for a complete view of response policy activity with respect to threat category, source of threat, and targets.

IPAM integration
Integration with BlueCat IPAM, DNS and DHCP solutions enables Threat Protection to be centrally managed and orchestrated through BlueCat Address Manager.

Response policy zones
Provide organizations with the option of maintaining a set of hosts and zones that can be intercepted and handled accordingly.

Logging and visibility
Matches can be logged to determine which devices have attempted to access known malicious content to identify infected systems.

Localized lists
Organizations can augment and maintain their own local lists to blocklist additional sites or allowlist results.

Supported threat feeds
Threat Protection enables seamless integration of security intelligence, including BlueCat DOH blocklists, CrowdStrike, and other third-party threat feeds.

DOH blocking
Retain visibility into DNS queries by blocking lookups to known public DOH resolvers.

BlueCat's Intelligent Network Operations (NetOps) solutions provide the analytics and intelligence needed to enable, optimize, and secure the network to achieve business goals. With an Intelligent NetOps suite, organizations can more easily change and modernize the network as business requirements demand.

Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 I 1-866-895-6931

bluecat.com

Next steps

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

Contact us