BLUECAT™

Leverage DNS To Secure Your Business

The growth in the number and type of new devices connecting to the network has exposed holes in typical enterprise security. DNS is the starting point for connectivity and is used by all devices to connect to applications and sites. BlueCat Threat Protection integrated security intelligence helps cybersecurity teams rapidly identify and stop threats before they can reach business-critical applications or data. That means security teams get an additional layer of defense against malicious Internet content and infected devices.

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 them from accessing malicious content, and further proliferating threats into your network.

Automated real-time threat data update

BlueCat Threat Protection uses the BlueCat Security Feed to gather threat data from leading sources, in real-time. Simply subscribe DNS servers to the security feed, which is automatically delivered through DNS and continuously updated to block threats as they emerge.

Extend defense in depth strategies

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

Protect everything connected to your network

We inject automation workflows to migrate with speed and accuracy. Our BlueCat proprietary tools reduce the risk of human error in network migration by identifying orphaned data and configuration conflicts that can impact timelines. That means network teams can quickly capitalize on new DNS architectures to meet business goals.

Benefits

Comprehensive Threat Coverage - Defend against attacks with the most active repository of threat events, actors, and malware in the industry.
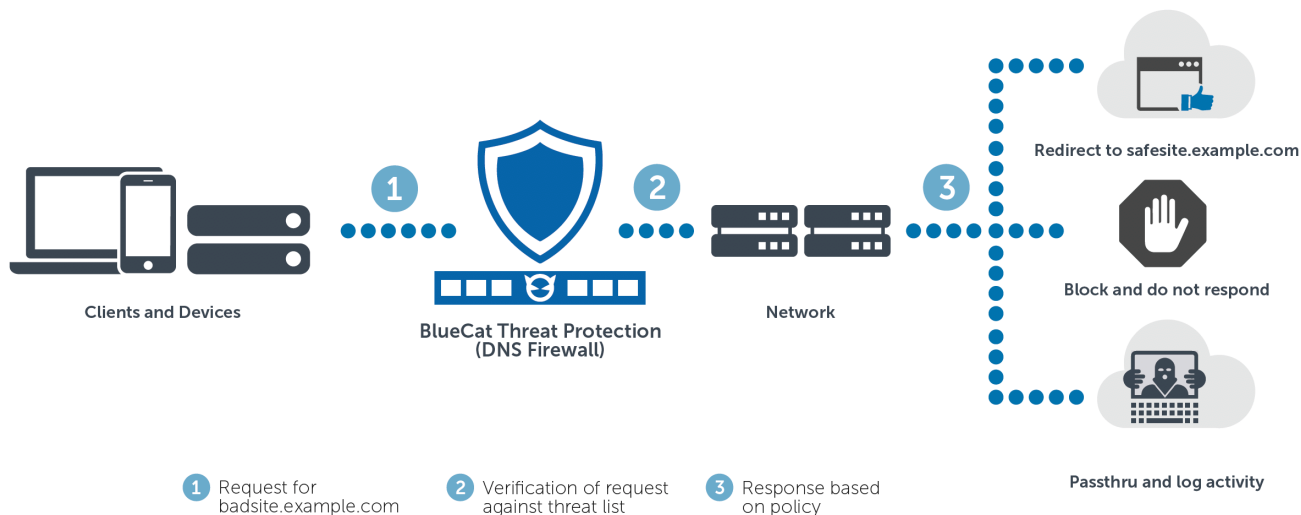
Enhanced Threat Classification - Prioritize threat activities based on severity, frequency and confidence.

Continuous Updates & Expertise - Enrich DNS data with insights from an elite team of threat analysts, and security researchers.

Eliminate SIEM Blind Spots - Correlate detailed information with other data sources by integrating with popular SIEMs.

Redirect to safesite.example.com

Block and do not respond

Passthru and log activity

Clients and Devices

**BlueCat Threat Protection
(DNS Firewall)**

Network

1. Request for badsite.example.com
2. Verification of request against threat list
3. Response based on policy

Features

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

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

Localized Lists - Organizations are able to augment and maintain their own local lists to be used to blacklist additional sites or to whitelist results.

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

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

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.

Flexible Deployment Options

BlueCat DDI solutions can be deployed as virtual or physical servers, or a combination of both. We license and support our software separately from hardware on the physical appliance and offer a perpetual hardware warranty. There is no cost to switch from hardware appliances to virtual appliances.

Next Steps

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

Visit bluecatnetworks. com/contact-us/