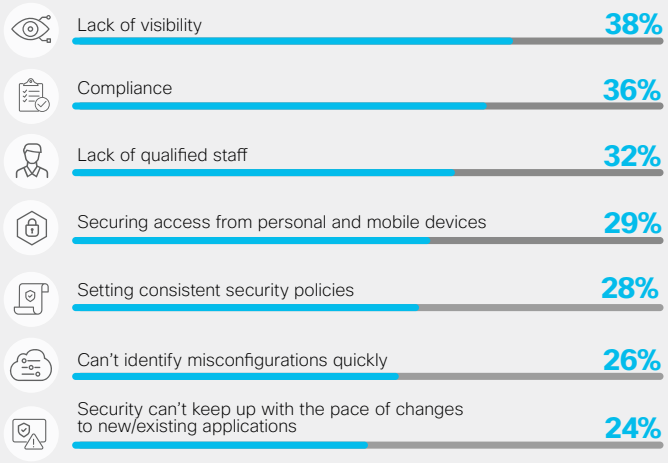
Cybersecurity INSIDERS RECOMMENDED

# PRODUCT REVIEW: BLUECAT EDGE FOR COMPREHENSIVE PROTECTIVE DNS

BLUECAT™

The increasing complexity of hybrid and multi-cloud environments, along with the rising frequency of sophisticated DNS-based attacks, has created significant challenges in managing and securing DNS infrastructure. As a result, organizations face increasingly sophisticated security threats such as DNS tunneling and hijacking, which exploit vulnerabilities in DNS infrastructure.




**What are your biggest operational, day-to-day headaches trying to protect cloud workloads?**

Cybersecurity professionals are faced with numerous day-to-day operational challenges when it comes to protecting cloud workloads. Lack of security visibility tops the list (38%), followed by compliance requirements (36%) and the perennial lack of qualified security staff (32%).

Source: 2022 Security Visibility Report produced by Cybersecurity Insiders

## OVERVIEW

To address these security challenges, BlueCat Edge offers a robust Protective DNS solution that provides advanced visibility, control, and detection capabilities for DNS queries. By capturing detailed DNS query data, it enables network and IT teams to establish smarter policies, optimize traffic, and meet stringent compliance requirements while enhancing the overall security posture through intelligent threat detection and response capabilities, leveraging detailed DNS data for comprehensive protection and analysis.




Bluecat Edge adds a much-needed layer of visibility, control, and detection for corporate DNS

To accomplish this, Edge captures all DNS queries and their associated responses, providing deep, actionable insights into network traffic and resource usage. This detailed DNS data supports threat hunting and investigations, enhancing existing security measures. Serving as the initial hop for all DNS queries, Edge acts as a robust security layer by identifying and blocking malicious queries using threat feeds, security-defined block lists, and its flexible policy system. This capability not only bolsters security but also optimizes network performance and compliance.


Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

## KEY FEATURES

Edge offers a comprehensive suite of features designed to enhance DNS security and performance:

- **DNS Threat Protection:** Utilizes advanced threat feeds, DGA and Tunneling algorithms to rapidly identify and stop DNS threats before they reach critical applications or data.
- **Identity Security Service:** Enriches DNS data with user identities to enable faster investigation and remediation of security threats.
- **Edge Security Dashboard:** Provides a detailed view of the network's security health, highlighting the most compromised or vulnerable endpoints.
- **Cisco Umbrella Integration:** Delivers enhanced context and actionable data for threat identification and mitigation.
- **Comprehensive Logging and Reporting:** Collects and analyzes DNS query data for diagnostic and investigative purposes, integrating with SIEM solutions for enhanced threat hunting.
- **Zero-Touch Deployment:** Allows the deployment of unlimited virtual service points without changes to existing DNS infrastructure.
- **Policy Configuration:** Enables the creation and application of policies to block, redirect, or monitor DNS requests based on security requirements.

## KEY BENEFITS

Edge provides several key benefits that significantly enhance DNS security and performance:

**1 | Enhance Your Security Stack:**
Utilize detailed DNS data on the sources and targets of network traffic to bolster your security stack.

**2 | Protect Against DNS Attacks:**
Actively monitor and protect your organization against DNS-specific threats such as tunneling and hijacking. Implement granular security policies based on comprehensive query insights.

**3 | Gain Unprecedented Visibility & Control:**
Receive complete visibility into DNS traffic from the first hop of any DNS query, down to the individual endpoint IP address, allowing for granular, intelligent traffic management and security policies, threat detection in internal and external queries, blocking of malicious DNS queries, and effective diagnostics and investigation.

**4 | Optimize Network Performance:**
Improve DNS resolution paths and reduce latency, ensuring high network availability and resilience with seamless cloud and on-premises integration.

**5 | Streamline Threat Hunting:**
Integrate with SIEM solutions for advanced threat analysis and hunting, enhancing security team collaboration and efficiency.

## INTEGRATION WITH CISCO UMBRELLA

Network operations and security teams face significant challenges in correlating endpoint threats that move laterally within the network. To address these challenges, Edge integrates seamlessly with Cisco Umbrella, capturing rich DNS data and contextualizing it to provide critical insights into suspicious endpoint activity. This integration allows teams to connect North-South and East-West traffic effectively, answering the essential questions in network security: Who, What, When, and Why. This powerful combination enhances threat detection and response, ensuring robust and comprehensive network security.


Copyright © 2024 Cybersecurity Insiders. All Rights Reserved

## DEPLOYMENT AND PRICING

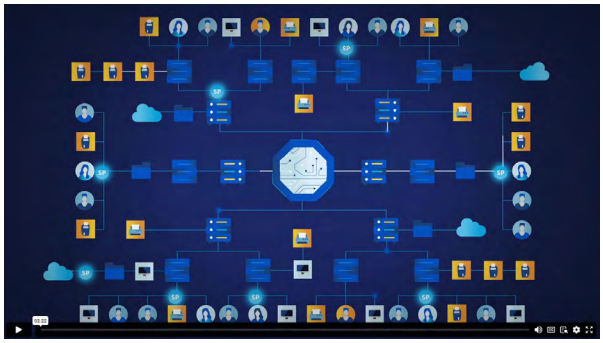
Edge is delivered as a cloud service under the Software as a Service (SaaS) model. Deployment is quick and efficient; using automation tools such as Terraform, the infrastructure can be set up in minutes for hybrid and multicloud environments. The creation of policies, configuration of threat feeds, and integration with Cisco Umbrella can be completed swiftly through the user-friendly GUI.

Commercially, Edge starts with the Smart Cache package, offering basic functions and weekly reporting. Advanced capabilities for security, networking, and cloud can be unlocked through add-ons. Pricing is subscription-based and varies according to the number of active IP addresses, with data retention options available for up to one year.

## CONCLUSION

Edge stands out as a robust solution for addressing the multifaceted challenges of DNS security. With its comprehensive suite of features, including advanced threat protection, identity security services, and seamless integration with Cisco Umbrella, Edge offers unparalleled visibility and control over DNS traffic. It excels in optimizing network performance, streamlining threat hunting, and ensuring high availability through zero-touch deployment.

These capabilities collectively enhance an organization's overall security posture, making Edge an exceptional choice for securing and managing network infrastructure efficiently and effectively.



BlueCat Edge provides advanced threat protection that also blocks malicious queries—so threats never get close to your critical systems. Watch the video.

## ABOUT BLUECAT

BlueCat provides core services and solutions that help our customers, and their teams, deliver change-ready networks. With BlueCat, organizations can build reliable, secure, and agile mission-critical networks that can support network modernization initiatives such as cloud adoption, SD-WAN, SASE and automation of key network provisioning and administration tasks.

**www.bluecat.com | info@bluecatnetworks.com | 1-866-895-6931**


Copyright © 2024 Cybersecurity Insiders. All Rights Reserved