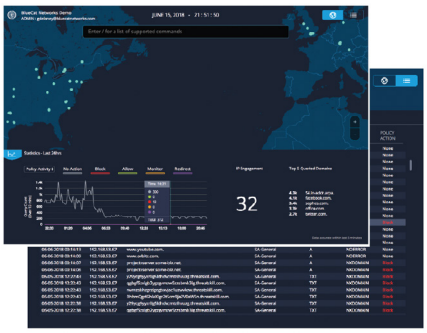
Use DNS data to boost your security posture

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 Edge's flexible policy system.

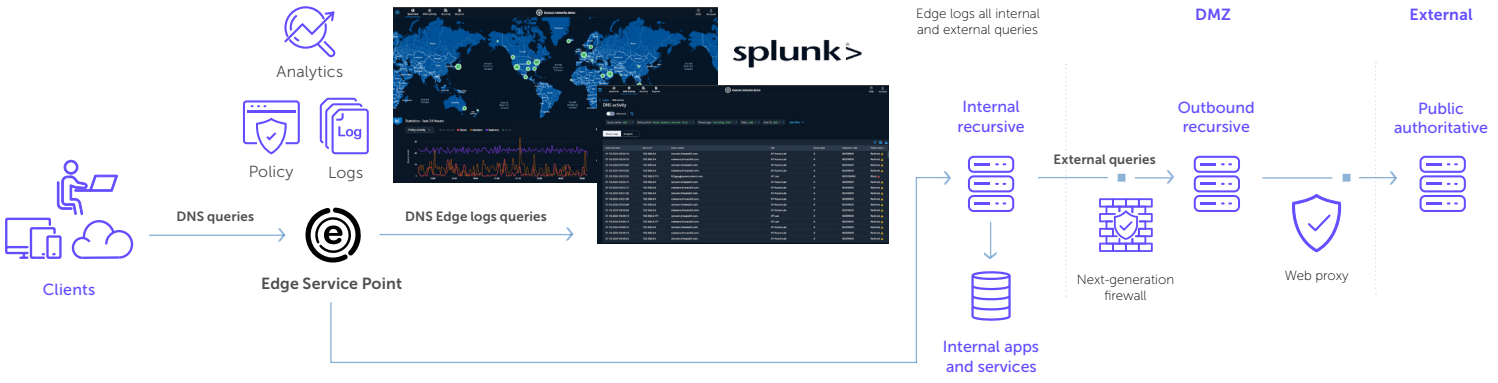
The Solution: BlueCat Edge

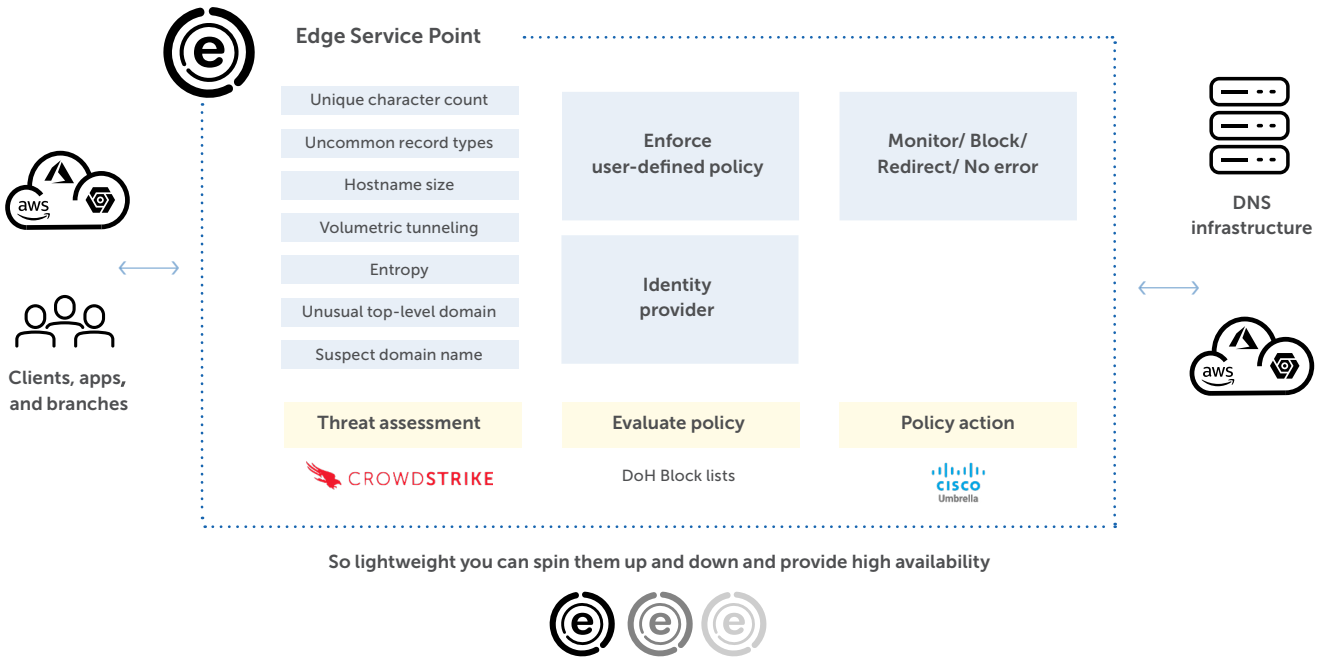
Edge adds a much-needed layer of visibility, control, and detection for DNS. Edge gives network and IT teams unprecedented access to DNS query data with which they can establish smarter network policies, optimize traffic, and meet stringent compliance and logging requirements. Edge also plays a critical role in the overall security of enterprise networks, enabling security teams to leverage the DNS data that Edge captures as yet another layer of intelligence and protection.



Benefits

- **Enhance your existing security stack with DNS data**
  Use the data found in DNS queries to provide extensive information on the sources and targets of traffic on the network.
- **Protect your business from DNS attacks**
  Actively monitor and protect your organization from DNS specific attacks such as tunneling, hijacking, and distributed denial-of-service (DDoS).
- **Unprecedented visibility & control**
  As the first hop of any DNS query, Edge works to intelligently direct DNS traffic, tame conditional forwarding rules, block malicious DNS queries, and help monitor and collect all DNS query and response information for diagnoses and investigations.





- **Export DNS data**
  Integrates with your existing security incident and event management (SIEM) solution, sending only relevant and prioritized DNS security data for threat hunting.
- **Accelerate investigations**
  Easy-to-use interface for deep security investigative work when a SIEM isn't present.
- **Improve collaboration**
  Send relevant threat data to your security team and become a combined, more efficient force.
- **Advanced DNS analytics**
  Tame big data problems and prioritizes alerts of DNS queries.
- **Segmented DNS**
  Segement access to DNS data endpoints, such as IoT devices that actually need it.
- **Stop threats**
  Create policies to alert, block, or allow traffic to proper DNS servers, limiting the chance of DNS attacks such as tunneling, hijacking, and DDoS.
- **Block queries**
  Block queries to or from domains as well as identities that are actively engaged in a DNS attack, giving your team room to investigate and remediate.

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

bluecat.com

Next steps

Get in touch with a BlueCat representative to better secure your network.

Contact us