Leverage DNS data to reduce risk

Breaches happen. It's not a question of if. It's a question of when and how.

Sure, there are ways to reduce risk upfront. Security controls, security standards, and security training can make it more difficult to penetrate your network. But nothing is foolproof.

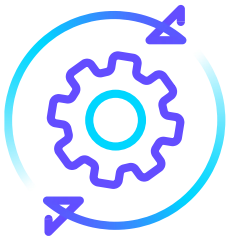
Nobody can control how a breach will happen. What you can control is the response.

Root Cause Analysis

Most enterprises are drowning in security alerts. When a breach happens, you need to be able to pluck the relevant incident(s) out of the alert haystack and trace it back to a specific device and action.

Timeliness

On average, the mean time to remediate a breach (MTTR) is eight hours. That figure should be shocking to any security manager. Every business should be working to bring down its response time.



Mitigation

Once you know the cause of a threat, the cleanup process can begin. That usually means isolating the impacted area (a device, a network), removing malicious software, and testing to ensure that the breach is truly gone.

Reducing your MTTR is achievable, if you have full visibility into what's happening on your network and the ability to apply security policies consistently. **That's a huge "if".**

Here's the reality:

Most security and network teams can't see what's happening on their networks - particularly when hybrid cloud is involved.

They can track data flowing through strategic choke points and analyze it in a SIEM. They can react to alerts. But they don't have a way to trace those alerts back to "patient zero" in a timely manner, let alone test if their mitigation strategies are actually working.

What if there was a consistent source of data that flowed through every application and device on your network?

Surprise! The data does exist. It's sitting on your network right now, just waiting to be used. **It's called DNS.**

Yes, that DNS. The protocol that's been around since the dawn of the internet. The data that flows effortlessly through your network every day, working its magic quietly in the background.

BLUECAT™

Every user, device, and application on your network produces a treasure trove of DNS queries every day. Think about what you could learn about your network if all of that data was at your disposal:

Malicious activity:

91% of malware uses DNS to navigate through networks, establish command and control, and exfiltrate data. Paying attention to malicious DNS queries could stop these exploits in their tracks.

Network performance:

DNS query patterns are often the first indicators of significant errors and misconfigurations. Stopping a pattern of NXDOMAIN responses can save a lot of remediation time (and admin hours, and bandwidth costs) down the road.

BLUECAT™

If DNS data is so amazing, why don't more security teams use it?

It's hard to compile.

If you're managing DNS through a decentralized system like Microsoft DNS or BIND, capturing DNS data means manually compiling it, server by server. That's weeks or months of work for every incident.

It's hard to act on.

Compiling DNS data is difficult enough. Applying security policies to it across the enterprise? For decentralized DNS architectures, that's an even greater lift.

It belongs to the network team.

In most IT organizations, DNS is managed by the network team, not the security team. Compiling all that data and acting on it usually involves complicated interdepartmental negotiations around who has access, what's delivered, and when.

BlueCat Adaptive DNS turns your DNS data into security gold.

BlueCat Adaptive DNS brings the untapped potential of your DNS data to life. By deploying a simple VM at the "first hop" of every network query, BlueCat provides unprecedented visibility into what's happening on your network and the ability to control the entire enterprise.

Collect, filter, and analyze DNS data in real-time:

BlueCat compiles and analyzes all of your DNS data. And we mean "all" - including the internal DNS queries which make up 60% of your network traffic, the source IPs of compromised devices, and much more. With this data at your fingertips, security teams can find the source of a breach in minutes, not weeks.

Configure, deploy, and enforce DNS policies consistently:

BlueCat enforces security policies through DNS right at the network edge, ensuring a consistent approach across hybrid cloud environments, IoT devices, and internal traffic. No need for time-consuming agents.

Integrate with leading security and network tools:

BlueCat adds DNS security to the defense-in-depth strategy you're probably already using. From powerful Crowdstrike threat feeds to integration with Cisco Umbrella, BlueCat integrates seamlessly with your existing security playbook.

We're guessing that your interest is piqued. You've probably got a lot of questions about how it all works.

You're in luck.

We've got all the technical detail you need right here.

Learn more about BlueCat's DNS security solutions

bluecatnetworks.com