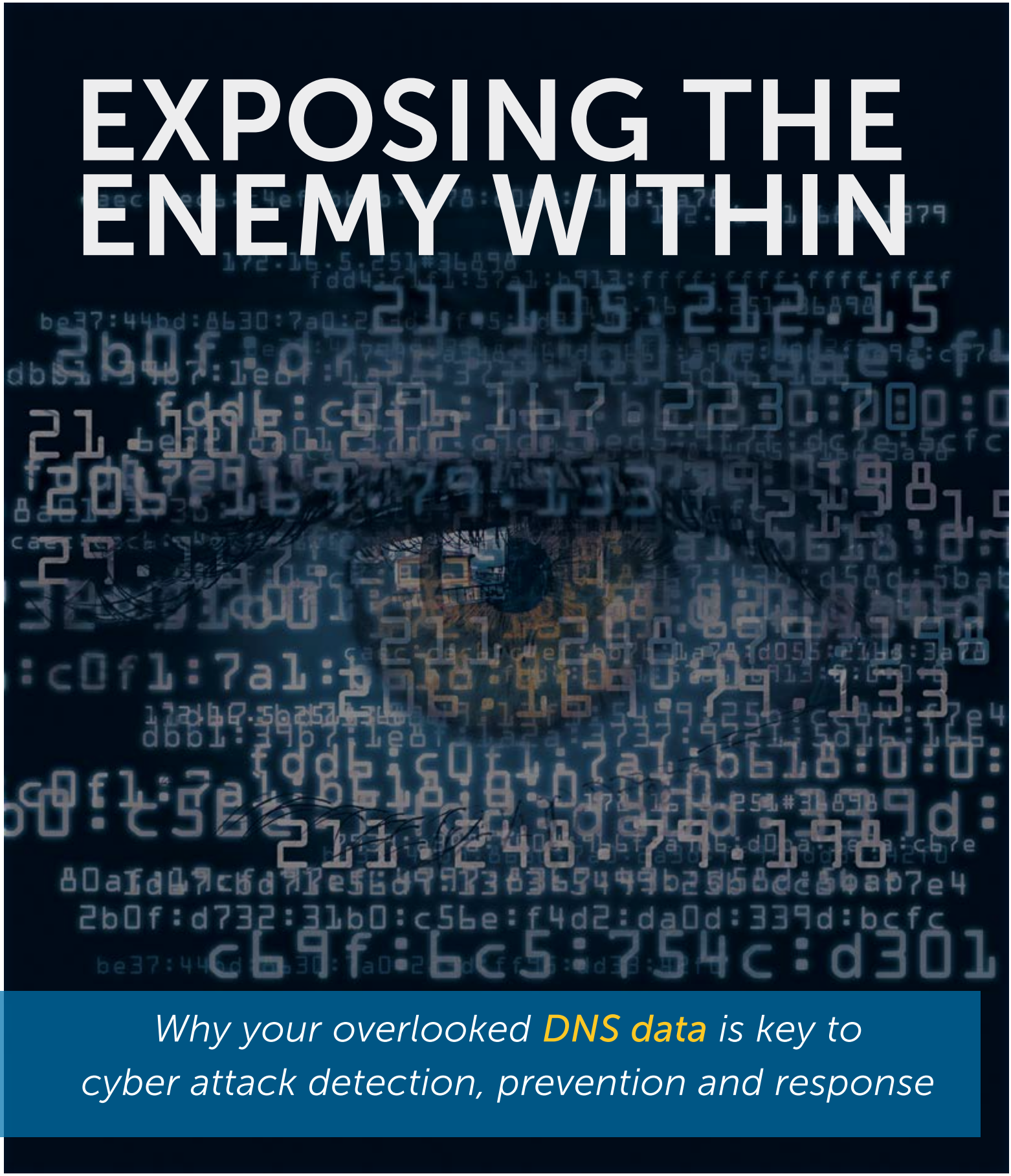
EXPOSING THE ENEMY WITHIN



Why your overlooked DNS data is key to cyber attack detection, prevention and response

BLUECAT™

bluecatnetworks.com

Another week, another dangerous cyber attack unleashed on the world.

Over the last few years, the frequency, sophistication and speed of malware attacks have increased at an astounding rate. According to industry research, 91% of these attacks leverage DNS - a technology that is fundamental to how devices connect to networks. This is how compromised devices receive instructions, exfiltrate data and reverse engineer the network to find other systems to attack.

We live in a digitally connected world. But the promise of innovative consumer and business services that connectivity will unlock comes with an ominous reality: it's only a matter of time before your devices, intellectual property and mission critical applications come under attack.

Long gone are the days when cyber attacks were carried out by lone hackers operating for thrills and reputation alone. Today's attacks are executed by sophisticated nation states and criminal organizations intent on exploiting weaknesses for financial gain or competitive advantage. The business of cyber attacks has been professionalized; exploit kits are easily accessible so that the barrier to entry is very low for highly sophisticated attacks.

Unfortunately, they will succeed; it is not a matter of if, but when. Chances are, one of your business users has unwittingly clicked on the wrong link or opened the wrong attachment. Malware has already penetrated your layered defense strategy, skirted your end point firewalls and is quietly spreading like an unseen plague from device to device. The enemy isn't at

WE'VE TRACED THE ATTACK.
IT'S COMING FROM INSIDE YOUR NETWORK

your gates, it's inside your perimeter. Soon, it will activate a dangerous payload or beacon home to a newly registered domain, transferring invaluable information from your estate to its master like some perverted trojan horse.

The worst part isn't necessarily the economic damage inflicted on your business. It's that you already have the data today to detect, isolate and prevent an attack. It's sitting right there at your fingertips, just waiting to be discovered.

The growing cyber threat

Attackers stole 40 million credit cards from retail giant Target using an HVAC vendor's credentials.

Twitter, Netflix, Reddit and other websites suffered outages when millions of consumer wireless routers, digital cameras and DVR players infected with malware orchestrated a DDoS attack at DNS hosting provider Dyn.

A university was locked out of critical systems after it was attacked by its own malware-laced soda machines and other botnet-controlled IoT devices.

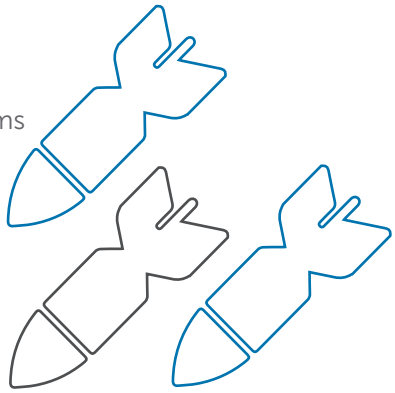
The role of DNS in cyber attacks

The Domain Name System (DNS) is the routing infrastructure which directs all traffic in a network. As the primary connection between servers, users and devices, properly functioning DNS pathways are critical to network health.

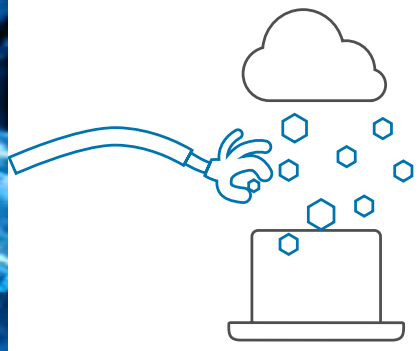
Lenin once said that he "found power lying in the streets and simply picked it up". DNS information is similarly available - to both network administrators and malicious actors. If left unprotected and unmanaged, DNS can be used to steal critical data, and even attack other networks.

It happens in the background. Malware infiltrates entire networks, using DNS to route malicious programs from device to device. Once embedded in the network's core infrastructure, those same DNS channels are used in service of the hacker's goals, such as:

DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS:



In a DDoS attack, computers on the network run malware programs which draw on a trickle of resources, using DNS systems to direct traffic towards the target. When combined, those resources become a tidal wave which can overwhelm even the strongest defense. This kind of attack famously took down Twitter, Netflix, Reddit and other websites last year when millions of consumer wireless routers, digital cameras and DVR players infected with malware orchestrated a DDoS attack at DNS hosting provider Dyn. But this same technique can be used internally to take down your network. In fact, in recent years a university was locked out of critical systems after it was attacked by its own malware-laced soda machines and other botnet-controlled IoT devices.

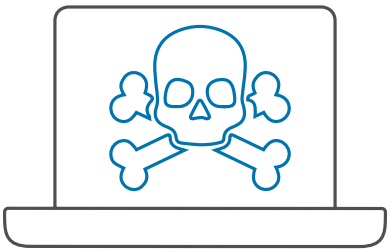


DATA EXFILTRATION ATTACKS:

In an exfiltration attack, malware uses DNS to transmit sensitive files to a remote server. In an effort to hide their tracks, some hackers use random domain name generators to send information in multiple directions at once, or embed the stolen data in DNS requests themselves.

COMMAND AND CONTROL:

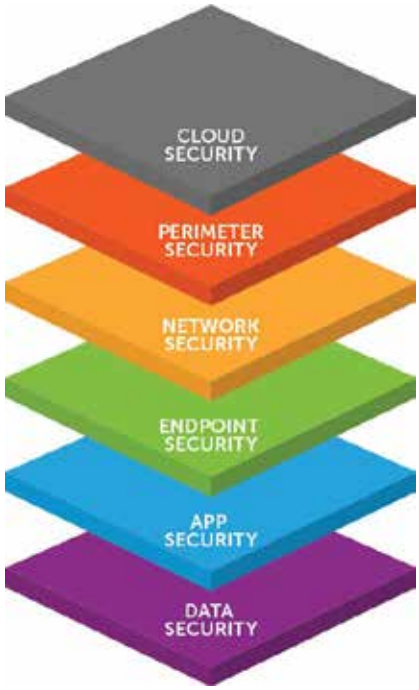
Once an endpoint is infected by malware, DNS can be used to control its actions. Infected endpoints can be instructed to attack other parts of the network, launch external actions, steal data or perform other unwanted activities.



CLOUD SECURITY
CASB, Content Filtering, Traffic Inspection

NETWORK SECURITY
NGFW, IDS/IPS, NAC, DLP, Messaging

APPLICATION SECURITY
WAF, DB Security, Code Scanners.



PERIMETER SECURITY
Firewalls, Content Filters, Honeypot

ENDPOINT SECURITY
AV, DLP, Patch Mgmt, Client Firewalls, IDS/IPS

DATA SECURITY
Encryption, IDAM, DLP, Integrity, DRM

Your layered defense strategy is missing a layer.

But enterprise security teams haven't focused on DNS in their defense strategy. Instead, they've doubled down on risk mitigation measures using a variety of new "layers" for their defense-in-depth strategy. Enterprises have become masters at embracing the latest security trend, whether it is Data Loss Prevention (DLP) or next-generation firewalls in an effort to find the silver bullet to fully protect their infrastructures. Unfortunately, adding layers simply is an acknowledgement that none of those layers are completely effective, and gaps will always exist in each one that malicious parties can exploit to gain access to critical systems or data.

Yet, as recent history has shown, this strategy isn't effective. As hackers automate their attacks and infiltrate networks through increasingly sophisticated means, an exterior defense of the network is simply unsustainable. It only takes one breach to bring down the entire system, and experience has shown that no defense is 100% effective.

Rather than securing every network device through expensive, awkward endpoint solutions, DNS data offers a cheaper and ultimately more effective way to secure a complex, distributed network. By monitoring DNS data flows for anomalies, network administrators can pinpoint the exact source and characteristics of an attack, even as it happens.


THERE'S GOLD IN
YOUR DNS DATA

As the network's traffic control mechanism, DNS data offers critical insights into the health and proper functioning of any IT system. It is the digital paper trail that shows the intent of every device on your network. With proper identity management policies, it can also demonstrate the intent of every user on your network. DNS data shows that an incident is currently in progress, allowing network administrators to respond immediately. Even more, DNS patterns can pinpoint the origin and spread of a cybersecurity incident, providing IT managers with the real-time information they need to get to 'patient-zero' and prevent further damage.

CONSIDER THE FOLLOWING DNS PATTERNS:

- A sudden spike in traffic to a domain which the system has never accessed before
- Multiple, simultaneous queries of a domain in a pattern that no human could produce
- Attempts by single-function network devices to access domains unrelated to their primary use
- Traffic to computer-generated domain names that do not correspond to any human language
- DNS Queries heading out to the internet from networks that were supposed to be segmented from the internet.

This activity is evident in DNS logs and indicates that deterrence has failed. Firewalls and filters are a band aid once DNS has been infiltrated and used in an attack. Security professionals must fix it at the source.

Existing SIEM tools aren't enough

Network administrators know that DNS data is critical to cybersecurity, yet the current efforts to harness to power of DNS data are hamstrung by many factors:

UNINTERPRETED DATA:

There are plenty of tools which can collect and monitor DNS information, including every Security Information and Event Management (SIEM) system on the market. Yet without the intelligence and analytics to interpret the data, IT administrators have no basis on which to act.

INCOMPLETE DATA:

Even when DNS data can be harvested from individual servers, much of it is either truncated or held for relatively short periods of time - both in the name of minimizing storage requirements for their data lake or SIEM.

DISPARATE DATA:

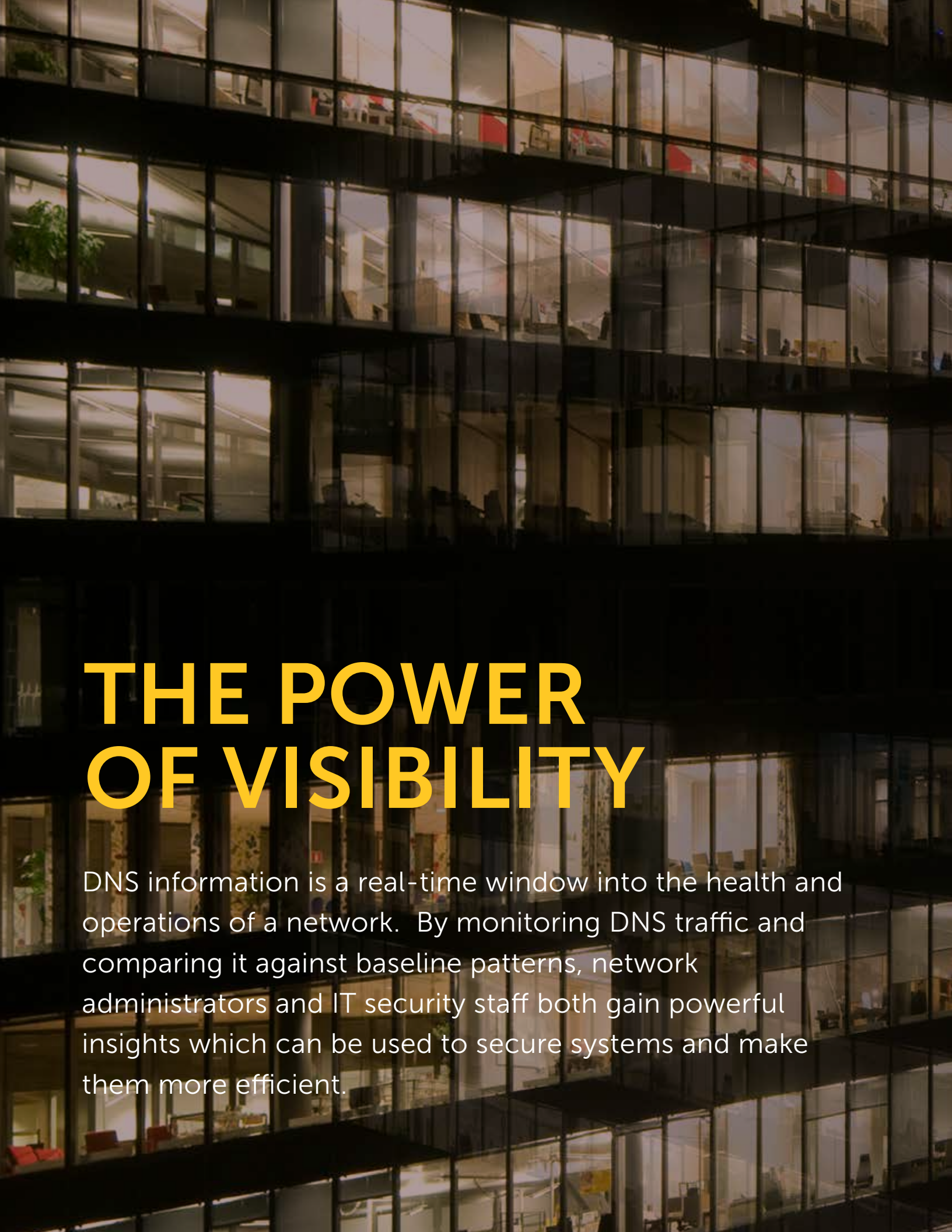
Microsoft Active Directory logs DNS data separately for each server. Given the thousands of servers which can populate a complex network enterprise, this makes data collection an extremely difficult, time-consuming process.

ZERO ABILITY TO ENFORCE POLICY:

Even if your security operations team can detect suspicious activity in DNS logs, what then? DNS data is often collected at the egress point, making client identification almost impossible. What enterprise organizations need is the ability to quickly enforce policies via DNS that isolates devices to prevent the spread of malicious software.

Some network administrators have devised workarounds, monitoring piecemeal DNS data from far-flung servers. Yet this is hardly ideal - compiling the data involves significant resources and is rarely comprehensive. By the time all the relevant data is pulled together and properly analyzed, it's too dated to result in any relevant action.

When cyber attacks are flowing through a DNS infrastructure, most network administrators are hard-pressed to identify anomalies in real time. Without a single source of data which can both pull DNS data together and analyze it against historical patterns, system administrators have little insight into the spread of cyber attacks on their networks.



THE POWER OF VISIBILITY

DNS information is a real-time window into the health and operations of a network. By monitoring DNS traffic and comparing it against baseline patterns, network administrators and IT security staff both gain powerful insights which can be used to secure systems and make them more efficient.

KNOW WHO'S ON YOUR NETWORK

DNS data provides instant visibility into all activity on the network. Tracking system resource patterns by regular users, guests, and the devices they bring provides a real-time picture of network security.

KNOW WHAT'S HAPPENING ON YOUR NETWORK

With DNS information at a network administrator's fingertips, understanding the specifics of how information flows through a system becomes far simpler. By tracking the source and destination of data, activity of specific individuals and devices can be monitored and assessed.

TRACE ACTIVITY TO ITS SOURCE

In the wake of a cybersecurity incident, DNS data is often the most effective way to trace the origin ("patient zero") of an attack. Forensic analysts often spend a great deal of time compiling and poring through DNS records in order to determine how an attack occurred. Network administrators who already have stores of comprehensive DNS information and the historical patterns of its use will spend far less time (and far less money) searching for the cause of cyber attacks and can more quickly move to mitigation and clean-up activities.

IDENTIFY AND CLOSE GAPS

DNS information is a powerful tool for preventative cybersecurity, particularly when it comes to the Internet of Things. Most connected devices only require a single network access point - any attempt to connect with another server is suspect by definition. Through monitoring DNS connection patterns, administrators can identify anomalous activity and shut it down before it becomes a problem.

BLOCK KNOWN THREATS

Many internet locations have known associations with malicious activity. DNS administrators have a clear need to block traffic to these places across the board as a preventive measure. DNS tools can create, maintain, and implement a functional domain blacklist.

MANAGE NETWORKS EFFICIENTLY

Beyond the cybersecurity realm, DNS data also has a great deal of value for network administrators looking to streamline their systems and maximize computing resources. As networks scale and grow more complex, maintaining the same routing rules can quickly overwhelm network capacity. By assessing the routing of information through a system, DNS data can be used to rebalance traffic in a way that eases the strain on network architecture.

Put your DNS data to work

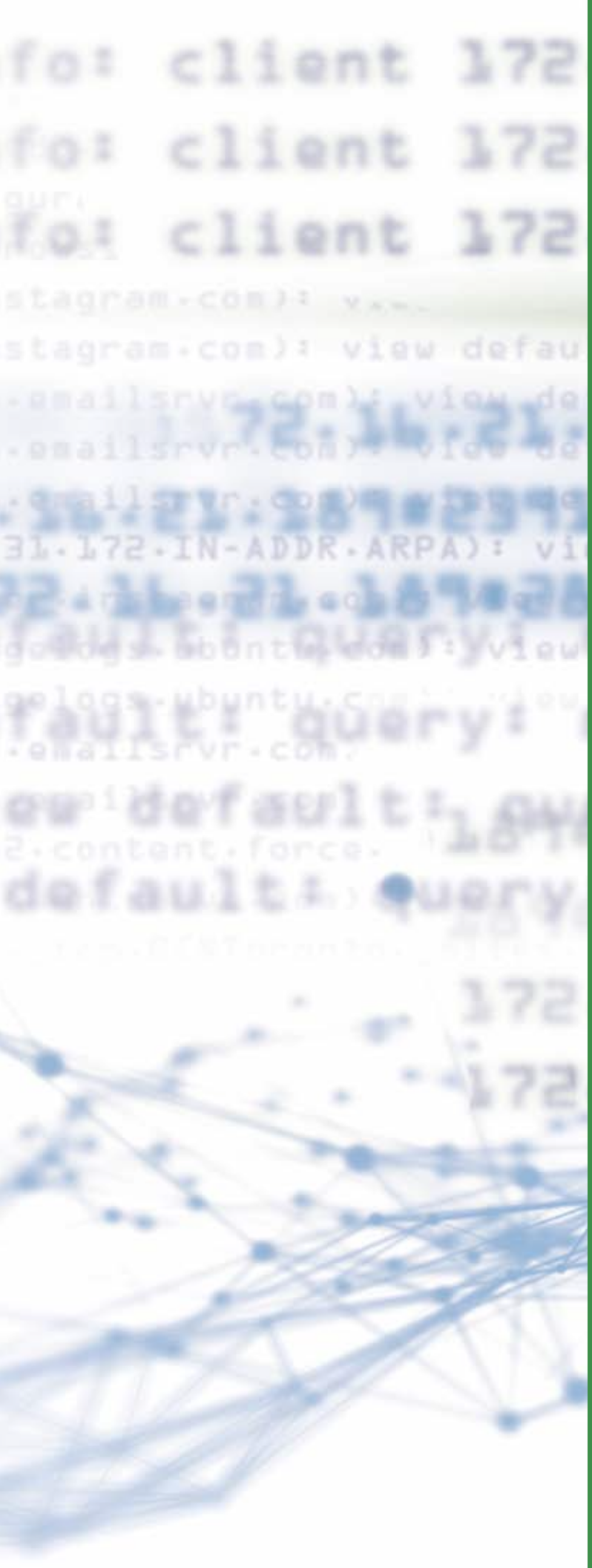
Network experts have long recognized the value of DNS as a critical element of network control, compliance and service delivery. Advances in automation, integration and the cloud are allowing modern IT organizations to rapidly deliver DNS to business users so they can access information and data across the enterprise.

But DNS is more than infrastructure, and its power extends far beyond simply connecting devices together. Every day, your DNS system logs hundreds of thousands of queries from internal and external systems. Inside those logs is a massive store of intelligence about the health of your enterprise and its vulnerability to attack.

The power of DNS data is hiding in plain sight. But without the proper tools to access it, your security operation is missing a significant opportunity to improve your organization's defense posture. It's not enough to merely collect DNS data - even systems that can identify DNS anomalies don't go far enough. What is needed are sophisticated tools that can interpret exactly what the information is saying so you can improve threat detection, prevention and response.

Malicious actors realized long ago that DNS is the lynchpin of any network, and therefore a prime attack vector by which to gain access to valuable assets. But for the good guys, DNS data may just be the key to thwarting their efforts and turning the tide.

It's time to look at DNS data in a new light and take advantage of this huge untapped resource.



WHO REALLY OWNS DNS IN YOUR ORG?

In organizations with large, complex networks, DNS is a core part of the network admin mission - to operate and maintain an efficient architecture. Yet that system generates data of increasing interest to their colleagues in cyber security roles. So who should own DNS?

Both teams. DNS is relevant to both network infrastructure administrators and CISOs alike. Network admins want to monitor DNS data for system optimization reasons. If information is being routed inefficiently, if servers should be rebalanced to minimize strains on a system, these are issues which clearly fall within the purview of the network staff.

CISOs need DNS data to monitor and detect potential anomalies. During normal operating periods, a consistent monitoring regime based on DNS can identify potential weaknesses in a network, allowing security staff to preventively close loopholes. When a cyber attack happens, DNS data allows CISOs to cut off the threat in real time and trace its origins.

“I’m sorry sir, but your card was denied”

You’re trying to make a purchase and your card is denied. How embarrassing. But wait - You’ve paid your balance every month without fail. What gives?

What likely happened is that some sophisticated software at your financial institution detected a spend anomaly and took action to prevent fraud. Today, these tools are incredibly powerful, sifting through terabytes of data to detect even slight deviations in behavioral models like a sequence of small charges at online vendors or sudden spending on new product categories. These are common signs of fraud that can raise red flags.

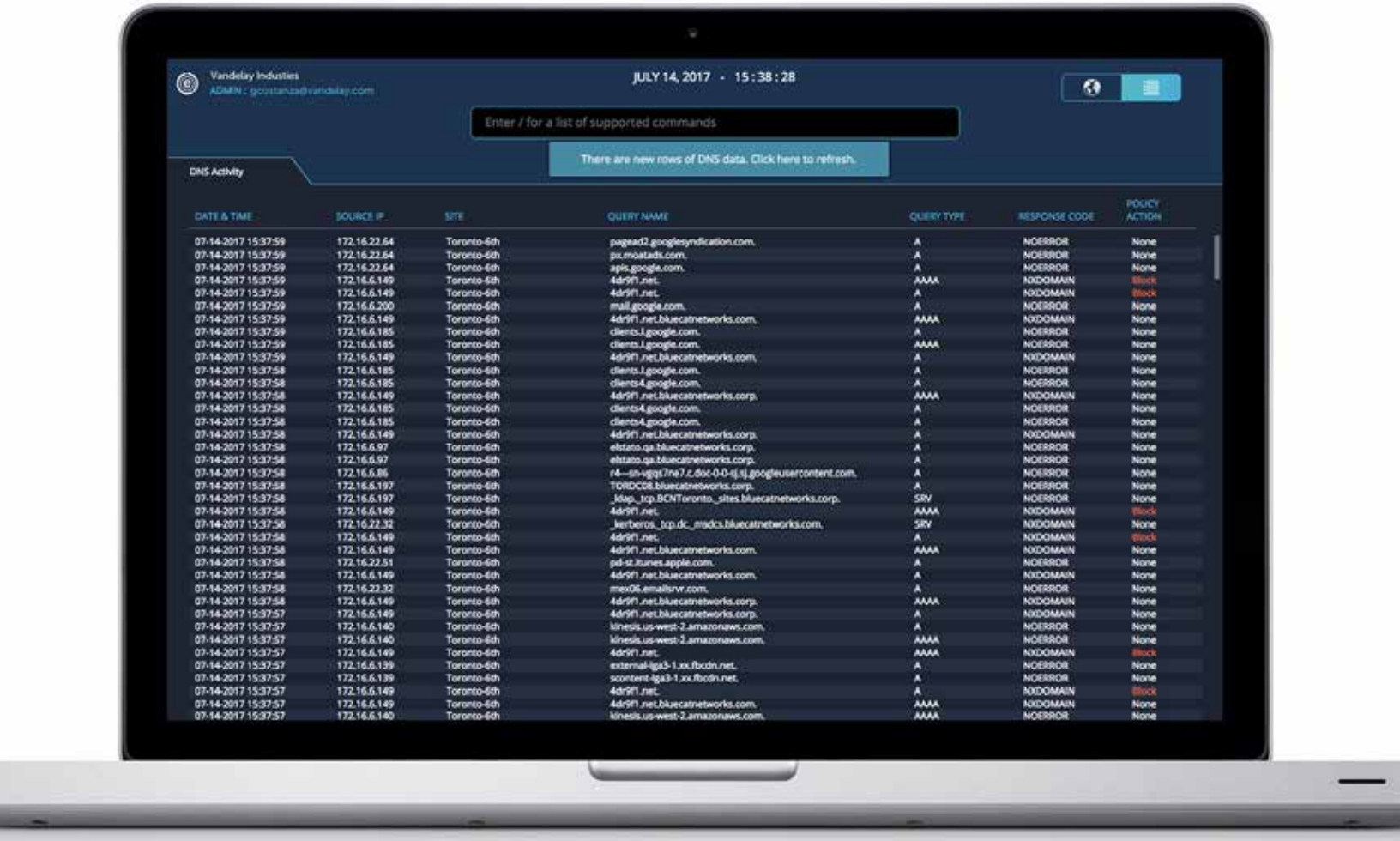
Now consider your DNS data. You have massive amounts of DNS query data being generated daily by every user, device and application on your network as they go about their daily routine. Much of that data falls into patterns that can be modeled and analyzed for anomalies.

Just as you don’t suddenly change your personal spending habits, your networked security cameras shouldn’t suddenly try to connect to recently registered domains in China. That would be a red flag - if you had the software to detect it.

About BlueCat

BlueCat is the Enterprise DNS company. We work with the world's largest and most recognizable brands - like SAP, Facebook, Disney, Toyota, Apple, Dell, 3M, and Nike - to manage and secure their networks so that employees can access the computing resources they need, when they need it.

BlueCat DNS Edge is a new approach to enterprise security that utilizes the pervasive nature of your DNS infrastructure to gain enterprise-wide visibility into the actions of every device on your network. Managed in the cloud, BlueCat DNS Edge uniquely leverages DNS data to identify and assess threats, and proactively works to block them before they can reach business-critical applications or data. BlueCat DNS Edge is the first DNS security solution with the flexibility to deploy wherever businesses need it – on premise or in cloud.



FOR MORE INFORMATION ON DNS-BASED SECURITY, VISIT BLUECATNETWORKS.COM