DNS & CYBERSECURITY COMPLIANCE:

A PRACTICAL GUIDE

Compliance shouldn't be complex

BLUECAT™

bluecatnetworks.com

Introduction

Cybersecurity and compliance may be the most over-used and under-explained terms in the world of IT. We all want our networks to be secure. We all want our networks to be compliant. But what does that mean in practice?

Cybersecurity and compliance are often used as crutches – or worse, as excuses for inaction. When someone isn't on board with an IT initiative, they usually raise cybersecurity or compliance as a roadblock, substituting those terms for more meaningful technical requirements which are often more difficult to explain in detail.

At BlueCat, we know that DNS has a strong role to play in advancing both cybersecurity and compliance. But we also know that it's not enough to simply say that. We have to show in a very specific way how centralized management of DNS infrastructure and the power of DNS-based security advance concrete compliance controls. That's what this eBook is all about.

We know it's complicated

Of course, compliance is a complicated issue – no single publication can address all of the nuances of how cyber security controls are implemented on the ground. This eBook is designed to frame the conversation we hope to have with you about your compliance needs and how BlueCat can assist in meeting them. We encourage you to reach out to our knowledgeable staff to learn more and start a more detailed conversation about what compliance means in the context of your network.

How To Use This Guide

In the next few pages, we'll outline the role DNS plays in different cybersecurity compliance regimes, and talk about the concrete ways that BlueCat's enterprise approach to DNS fulfills specific compliance controls. Our goal is to show how BlueCat's DNS tools can take your cybersecurity compliance regime to the next level. In this eBook, we'll cover:

For each standard, there's an overview of the role DNS plays in compliance and the specific ways that BlueCat's enterprise approach to DNS meets the standards.

Overview: NIST Cybersecurity Standards & FISMA

The cybersecurity compliance suite created by the National Institute of Standards and Technology (NIST) is increasingly accepted as a universal standard. Compliance officers, IT administrators, and C-level executives in both government and industry turn to the NIST documents for both strategic and tactical guidance on how to secure their networks in meaningful ways, reducing risk and enhancing control.

The NIST compliance controls are built around a common structure, making them interoperable and in many ways interchangeable.

- At the strategic level, the NIST Risk Management Framework (also known as the Cybersecurity Framework) lays out the broad framework for implementing a cybersecurity program, creating a checklist of functional areas which organizations should address.

- Through an exhaustive series of technical and procedural controls, NIST 800-53 functions as a practical manual, translating the broad principles of the Cybersecurity Framework into concrete actions.

- NIST 800-171 addresses the specific requirement to protect sensitive government information, using the frameworks and controls of the Cybersecurity Framework and NIST 800-53 to prevent unauthorized access to protected data.

- For Federal agencies, NIST standards and controls are mirrored in the data points collected under the Federal Information Security Management Act (FISMA), making NIST 800-53 controls the de facto foundation of any FISMA compliance program.

We'll go through the NIST 800-53 controls which directly touch on DNS management as a cybersecurity issue, and look at how DNS-based security satisfies the controls on monitoring and network visibility. By satisfying these tactical level requirements, organizations will also address the strategic needs of the Risk Management Framework and FISMA.

FOR A MORE IN-DEPTH LOOK AT THE ROLE OF DNS IN FISMA COMPLIANCE:

Check out our FISMA eBook here. If you'd like to learn more about how the DNS controls in NIST 800-53 relate to NIST 800-171 compliance, take a look at our blog post on the subject.

Implementation: NIST 800-53 Controls

SC-20: Secure Name/Address Resolution Service (Authoritative Source)

DNS was built as a naïve system – network queries resolve against internal and external servers automatically, without questioning whether a server is actually authorized to perform a resolution. That works great if you're trying maximize the speed of a network, but it also presents an extreme security vulnerability. If DNS will naïvely resolve any query that comes along, malicious actors can stand anywhere in the chain of trust and divert network traffic from where it is supposed to go.

SC-20 requires network administrators to adjust their DNS settings from "resolve anything" to "trust but verify". Doing this requires an overlay of security information – digital signatures and cryptographic keys – on top of DNS queries to help confirm the identity and authenticity of resolving servers. The common term for this is DNSSEC.

DNSSEC takes a standard DNS query and adds a layer of authentication information about the server of origin. For the query to successfully resolve, that authentication information has to perform a successful "handshake" with the destination server, exchanging cryptographic keys and verifying it as a trusted source.

For DNSSEC to be truly effective, it has to be present in every layer of a DNS query. If the parent zones have DNSSEC but the child zones don't, malicious actors have an opening which can be exploited. That's why SC-20 requires that both parent and child domains operate as part of a "chain of trust" when operating as part of a distributed, hierarchical namespace.

Implementing SC-20

Without a unified enterprise DNS system in place, implementing DNSSEC is a significant logistical challenge.

Implementing DNSSEC in BIND requires a series of onerous command-line changes to configure each server. Generating the DNSSEC keys, attaching them to the relevant machines, and testing the infrastructure takes a lot of time. Then you have to do it for every parent and child server in the network – a significant drain on IT resources.

In Windows, implementing DNSSEC is similarly work-intensive. First, you sign a zone and verify that the signing scheme is operating correctly. Then you use "trust anchors" to distribute that signing scheme to the child zones. Unfortunately, those "trust anchors" won't automatically adjust themselves when the parent zone is re-signed, requiring network administrators to constantly re-distribute "trust anchors" to the child zones when the parent signatures change.

In contrast, BlueCat's enterprise approach to DNS makes implementation of DNSSEC ridiculously simple. In BlueCat's unified DNS Integrity system, you check a box, and the DNSSEC scheme is automatically implemented throughout the entire zone. No command lines, no manual distribution of trust anchors, no wondering whether it's actually working – it just happens for the parent and child zones in one click.

With BlueCat, the DNSSEC scheme is automatically implemented throughout the entire zone with a simple box check in the DNS Integrity user interface.

SC-21: Secure Name/Address Resolution Service (Recursive or Caching Resolver)

The baseline SC-20 control demonstrated the need for DNSSEC to verify the accuracy of network queries, adding a bit of cybersecurity savvy to the normally naïve DNS infrastructure. As noted, DNSSEC has to be applied consistently across every layer of a DNS query to be truly effective, touching both parent and child zones.

SC-21 takes that DNSSEC requirement in a slightly different direction. Locking down the security of parent and child zones is important, but it doesn't cover all types of DNS queries which occur on a network. In order to truly cover the waterfront, the recursive or caching layers must also be secured.

Recursive or caching servers hold information about past DNS queries. These are used as a shorthand in future network activity, speeding up the resolution process by shortening the number of "hops" it takes to find the right information.

Like DNS itself, recursive or caching servers were designed for speed but not necessarily for security. When DNS queries are diverted to malicious domains, sometimes those malicious domains are stored in the recursive or caching servers for future use. Eventually the faulty information will time out, allowing the real domain to take its place. Yet as long as the redirection instructions are sitting on the recursive or caching server, they will continue to pose a security threat.

SC-21 extends the DNSSEC requirement to the recursive or caching layer. By definition, queries resolved by these servers have been seen before, and presumably they have already passed through the DNSSEC measures put in place as part of the SC-20 control. Yet by adding DNSSEC as a redundant form of protection in the recursive or caching layer, network administrators can ensure consistent coverage of their entire infrastructure. Closing off this "back door" into the DNS architecture is just another form of proper cyber hygiene.

Implementing SC-21

Just like implementation of SC-20 required a series of onerous changes to individual server settings, putting SC-21 in place without a unified enterprise DNS system takes a great deal of time.

As previously noted, adding DNSSEC functionality into recursive or caching servers operating on BIND or Windows requires a series of labor-intensive configuration changes. Generating the DNSSEC keys, attaching them to the relevant machines, and testing the infrastructure adds up to a great deal of strain on IT resources. Keeping these configurations up-to-date as network architectures change requires that administrators manually alter the settings continuously.

BlueCat's automated enterprise DNS management makes extending DNSSEC throughout the network quick and easy. The same simple box you check for DNSSEC on an authoritative server works for recursive or caching servers as well. No command lines, no manual distribution of trust anchors, no wondering whether it's actually working – it just happens for the parent and child zones in one click.

SC-22: Architecture and Provisioning for Name/Address Resolution Service

As the "dial tone" of the internet, keeping DNS up and running is of paramount importance for any network administrator. The SC-22 control is designed to build a layer of redundancy to make sure DNS systems can stay online even in the middle of a DDoS attack, data center outage, or other network compromise.

To accomplish this, the SC-22 control recommends designation of a fail-over authoritative DNS server in case the primary is compromised or overwhelmed. Ideally, the two servers would be in separate facilities (and even in different geographic regions) as a hedge against natural disasters, power outages, or other physical security problems.

SC-22 also recommends a separation between internal and external DNS servers – an "air gap" strategy which is commonly used in government agencies. With this type of deployment, responsibility for resolving internal and external DNS queries is separated out, so that no single point of failure or compromise can bring down the entire network.

Some DNS servers are designated to handle just internal traffic, resolving requests for files which are meant to be kept within the network. Others are designated for external resolution, facing the "wild west" of the public internet without a connection to sensitive internal information. At its core, the separation strategy reduces the attack surface, minimizing exposure to external attacks.

It's worth noting that this control is not a cure-all for network security, but merely a way to make the job of malicious actors that much harder. In a world where advanced persistent threats have probably infiltrated most networks already, organizations can't assume that a DNS-based separation will deter malware from identifying and exfiltrating critical data. To truly leverage the power of DNS for data, a larger toolset and more comprehensive approach is required.

Implementing SC-22

As the experts in DNS infrastructure and security, BlueCat works with a wide range of customers in the commercial, government, and nonprofit sectors to implement the SC-22 control in their network architecture.

In our experience, the process of creating fail-overs and separating internal from external DNS merely proves the need for an enterprise approach to DNS management. When network architectures start to get complicated, the functionality and usability of distributed management schemes like BIND and Microsoft tend to suffer. Just because the network is separated and redundant doesn't mean that your management of the network should take more time and effort than necessary.

The benefits of a centralized approach become clear when implementing the SC-22 control. In a centrally managed DNS system, the architecture acts as a cohesive whole. Failover schemes can be changed quickly and easily from a single management platform which dynamically determines network availability. Creating "air gaps" between internal and external DNS servers by designating masters and slaves for different purposes is simple. Perhaps most importantly, in a centralized system none of these decisions has to be permanent – changing architectures on the fly is easy to do.

In decentralized Microsoft architectures, the SC-22 control is attainable but far more difficult to set up and adjust. Failover servers can be designated in advance, but without a centralized method to gauge the status of DNS services, the failover scheme could lead to a rolling outage where failovers default to servers that may be down themselves. Designating internal and external DNS servers is simple enough, but when the exercise is replicated across the enterprise it quickly becomes a significant drain on IT department time and resources.

SC-7: Boundary Protection

In today's cyber security environment, boundary protection is a no-brainer. With all of the threats out there, of course you'd want to control the traffic coming into and out of your network. The question is not "if" but "how". To address that question, it's important to define "boundary" a little more clearly.

Most administrators think "external boundary" when they put network protections in place. It makes sense on a surface level – monitor and deal with any malicious traffic before it gets into the network, leaving interior traffic to move freely.

The assumption doesn't hold water in an operational environment, however. The rise of advanced persistent threats means that no part of the network should be considered immune from attack. Placing all of your security resources on the exterior boundary of the network leaves internal traffic vulnerable to exploitation.

That's why the SC-7 control talks about the need for protections at the external network boundary as well as "key internal boundaries". Those internal boundaries will be different for every network, and can be defined to fit with whatever fits with the local architecture.

Is that enough? If threats can truly attack at any point on the network, doesn't it make sense to place those boundary-level protections in front of every client? SC-7 notes the need to "prohibit traffic…that spoofs addresses". Thinking of this kind of traffic in terms of internal and external no longer makes sense, given the ubiquitous nature of today's cyber threats. Spoofing traffic

happens everywhere and anywhere on the network, making the need for protection similarly consistent across the enterprise.

Looking at the control enhancements attached to SC-7, it quickly becomes clear that effective cybersecurity considers every client a "boundary" that must be protected. Implementing those enhancements – restrict threatening outbound communications traffic, prevent exfiltration, host-based protection – requires insight into everything that happens on the network and the ability to act on it before a cybersecurity incident occurs.

This is why BlueCat sees DNS as the basis of effective network security. As a pervasive sensor which undergirds all network activity, DNS provides an ideal way to monitor traffic and enforce security policies. Using DNS for boundary protection extends security throughout the network.

Implementing SC-7

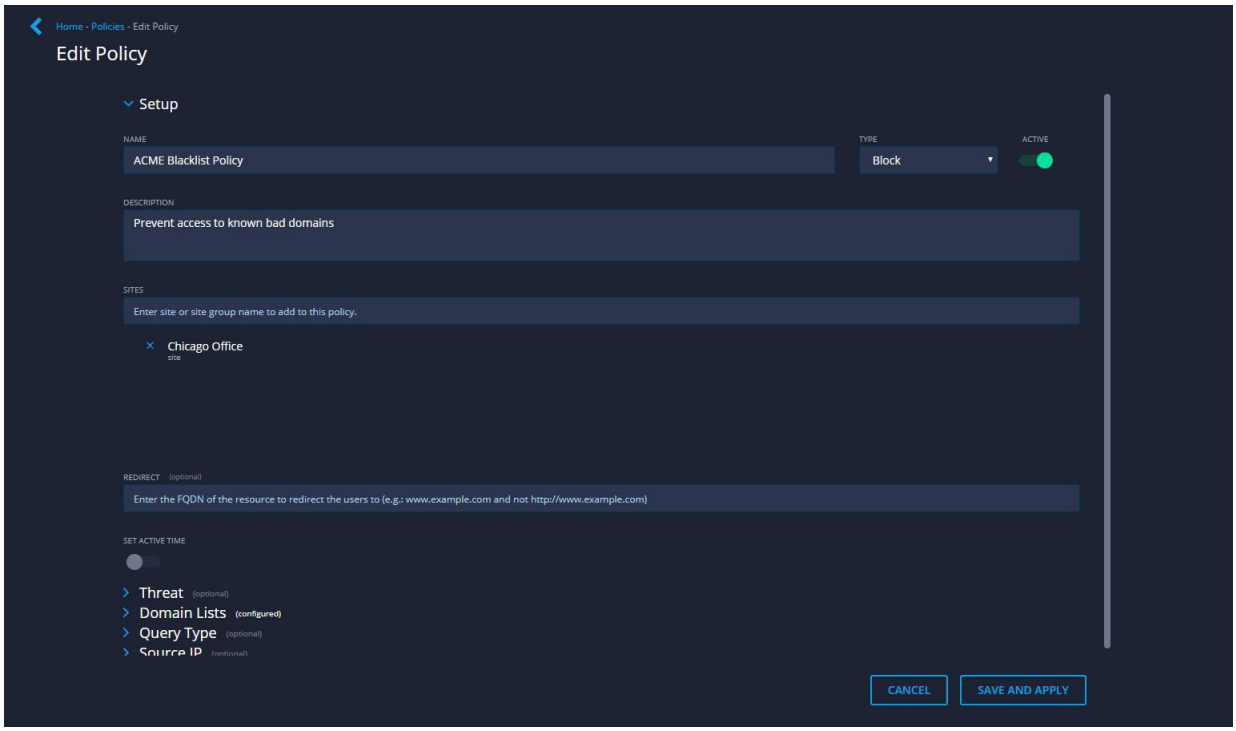
There are plenty of filters and firewalls out there, and some of them even use DNS information in the service of network security. Unfortunately, all of these sit on the external network boundary, missing the opportunity to leverage DNS to maximum effect.

BlueCat's DNS Edge product brings effective boundary protection to the client level by using DNS to monitor traffic and implement security policies. DNS Edge sits on the "first hop" service points, controlling access to both internal and network.

Deploying DNS Edge is fairly straightforward – it sits on existing network infrastructure, with just a few small configuration changes to direct network traffic through the proper channels. The entire system can usually be deployed in less than an hour.

Once deployed, implementing the SC-7 control enhancements is as easy as creating a policy and putting it in place. Administrators can create a policy to route traffic to authenticated proxy servers, for example. Or a policy can prevent exfiltration by blocking "beaconing" traffic to unknown or unusual web addresses. Perhaps most powerfully, DNS Edge allows for effective enforcement of a "deny

by default, allow by exception" rule through blanket policies which are enforced right at the first hop.



Implement DNS-based policy in BlueCat DNS Edge to enable protections for not just the external network boundary but "key internal boundaries" as well.

SI-4: System Monitoring

Visibility is the basis of all network security. If you know what's happening on your network, you'll be in a position to do something about it. Unfortunately, the opposite is also true – without visibility into what's happening on the network, easily remedied issues can morph into serious threats right under your nose.

Unlike some of the NIST 800-53 controls which focus narrowly on a single technical issue, the SI-4 control encompasses a broad range of potential actions, all under the general umbrella of visibility. Given the ever-changing nature of cyber threats, the SI-4 control recommends monitoring data at multiple levels of the security stack, with an eye toward overlapping or even redundant information collection to detect threats.

At BlueCat, we see DNS as the ultimate security sensor and the most compelling way to implement the SI-4 control. As the basis of all network

traffic, DNS offers a stream of data with a breadth and depth that no other network visibility tool can match. When deployed at the client level, DNS sensors provide visibility into both internal and external network traffic with a level of specificity which allows network admins to take immediate action on a wide range of threats.

DNS-based security may be the Swiss Army knife of the SI-4 control. The supplemental guidance notes that a "variety of tools and techniques" may be necessary to gain true visibility, but DNS sensors can check the box on most if not all of the recommended functionality. Looking at the list of examples in the SI-4 supplemental guidance, DNS-based security can act as an intrusion detection system (monitoring internal and external DNS queries), intrusion prevention system (blocking malicious DNS queries at the client level), scanning tool, audit record monitor, and more.

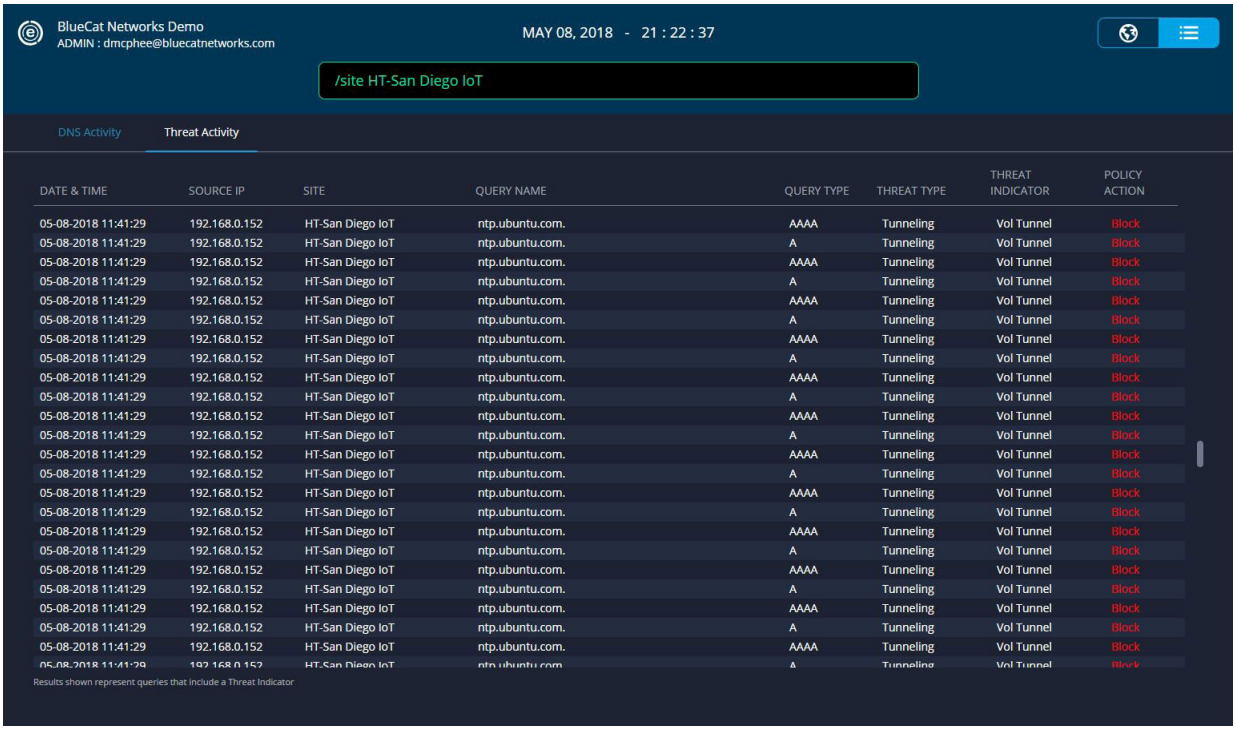
Implementing SI-4

Addressing parts (a) and (c) of the SI-4 control, BlueCat's DNS Edge product places its sensors at the first "hop" of a DNS query. (The sensors are placed on a service point and are completely software-based.) The sensors collect and log data on all of the DNS queries which flow through them, providing a baseline for analysis and action. DNS Edge can then apply policies and controls based on the organization's defined monitoring objectives to meet the requirements of the SI-4 control.

For known attack vectors, bad domains, and domain-generating algorithms, BlueCat provides blacklists based on regularly updated threat information. On top of this, organizations can identify their own internal policies on access to sensitive systems, blocking inappropriate access. Over time, the patterns of normal DNS usage will appear, allowing for further fine-tuning of policies and identification of marginal anomalies for investigation (satisfying part (e) of the control).

For part (b), DNS Edge goes further than merely identifying unauthorized use by allowing administrators to block access to any domain (internal or external) which fails to correspond to the user or client's role. In most cases, that will mean

limiting user access to certain areas of the network. For IoT devices, restricting unauthorized use will often mean limiting access to perhaps one or two IP addresses on the network – one for transmission of data, one for periodic software updates.



Gain visibility into both internal and external network traffic from every client on the network with BlueCat DNS Edge.

Part (d) addresses the data security question – how to adequately protect all of the information harvested from security sensors. BlueCat's solution is to anonymize the data as it flows through the cloud-based analytics engine, ensuring that only authorized personnel at the customer site have access to the raw information.

Overview: PCI-DSS

The Payment Card Industry Security Standards Council is an organization created by the major US credit card companies. Its purpose is to promote greater security within the payments industry, primarily by providing common controls for payment-related networks.

The Council is responsible for the Payment Card Industry Data Security Standard (PCI-DSS), a set of twelve controls designed to secure the networks of any part of the payment data chain, including any entity that stores, processes, or transmits cardholder data and/or sensitive authentication data. The incentive for compliance is significant – vendors must meet the PCI-DSS standards if they want to have any business connection with the major payment providers. In the absence of PCI-DSS compliance, vendors are not allowed to process payments from most credit card companies.

Implementation: PCI-DSS

DNS is specifically called out in the scope section of the PCI-DSS standard as one of the core systems which comprise the "cardholder data environment". As the transmission network for all payment-related data, securing DNS is critical to maintaining data integrity and trust.

There are two controls within the PCI-DSS framework which specifically call for DNS-related security and architecture changes.

Control 2.2.1

In this control, the PCI-DSS standard mandates a consistently high level of security by requiring the separation of network functions onto different servers. In smaller organizations, it is likely that servers are deployed as multi-use devices, hosting several services of differing security levels on the same device. This often leads to a de facto lowering of security standards, as a compromise of the service with the lowest security standards could impact higher security services housed on the same server.

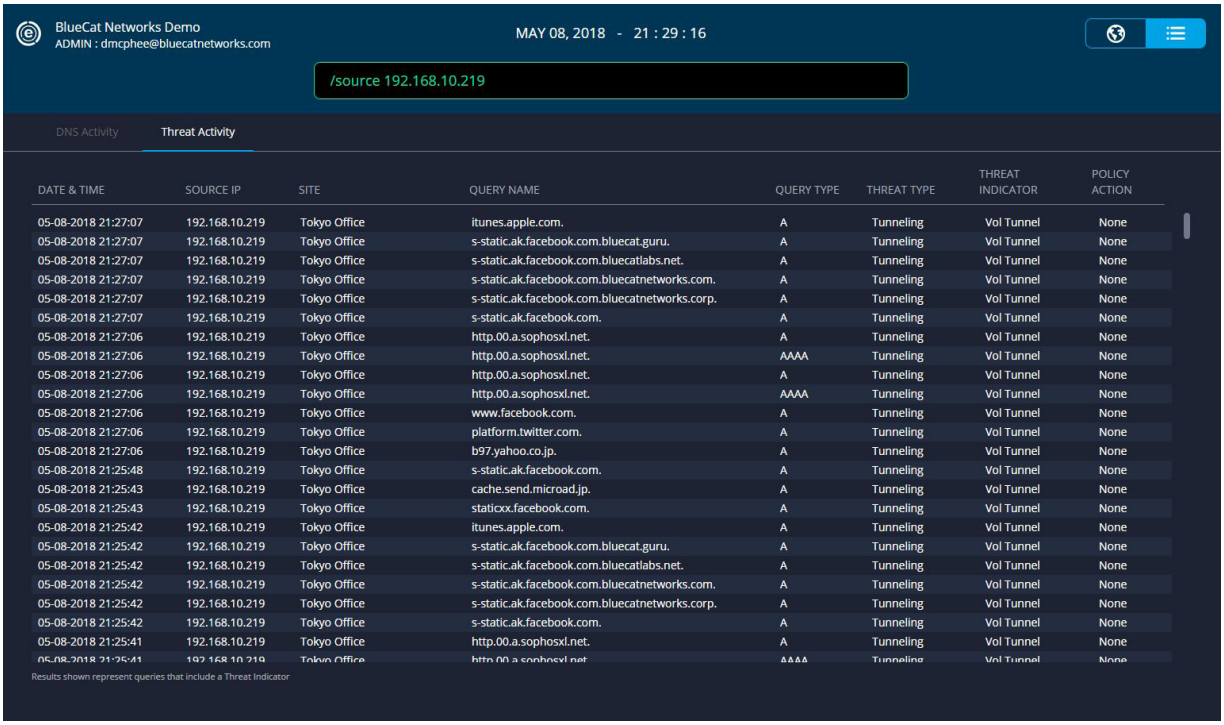
The PCI-DSS standard requires organizations to use different servers to house each IT service. This ensures that varying security controls do not compromise each other when housed in the same place, and eliminates the risk that a compromise of one system would bleed over into additional core systems.

Implementing Control 2.2.1

BlueCat's implementation of a centralized DNS management platform meets control 2.2.1 by definition. When deployed as a stand-alone piece of hardware, BlueCat's enterprise DNS does not allow for mixed services on the same piece of equipment. When deployed as a virtual machine, BlueCat's enterprise DNS only performs one function per virtual component.

Control 6.1

This is a wide-ranging control which asks organizations to monitor their networks for security vulnerabilities using outside resources. The idea is to ensure a degree of vigilance when it comes to network operations, constantly scanning for anomalous activities, assigning levels of priority to potential threats, and putting policies in place to mitigate against those threats.



Isolate DNS query data down to a specific source IP with BlueCat DNS Edge.

Implementing Control 6.1

DNS-based security offers an extremely attractive solution for network monitoring and control. Since DNS is a pervasive sensor which is the foundation of all network activity, it makes sense that applying policies based on that data would provide greater security throughout the network. BlueCat's enterprise DNS products sit at the client level, allowing users to implement policies for all network queries – both internal and external.

In addition to the standard white lists and black lists which identify known malicious domains, BlueCat's DNS-based security system learns about the norms of your network over time. Once this baseline is established, BlueCat users can further train the system to spot historically abnormal activity and act on it in accordance with evolving security trends.

Requirement 10 Controls

Throughout Requirement 10, the PCI-DSS standard mandates the creation of an audit trail to link access to financial information with individual user activity on the network. In the event of data theft, exfiltration, or another compromise, this audit trail will help to establish accountability for a breach and form the basis of a forensic investigation.

Implementing Requirement 10

DNS is an excellent proxy for user intent. When DNS queries leave the client system for other parts of the network, they intrinsically contain data on what information is being requested, the level of access involved, and contextual information such as date/time stamps.

All of this information is incredibly useful in the context of a forensic investigation. Network boundary-level filters and firewalls can only measure user intent for external queries, leaving some data in the recursive layer where it is difficult to obtain and correlate with user sessions. BlueCat's client-level DNS solutions capture the complete picture of user queries, enabling a quick and easy correlation between data sets in the event of unauthorized access.

Even more significant, the ability to implement DNS-based policies at the client level can cut off the possibility of a breach in the first place. By restricting access to irrelevant or sensitive portions of the network, BlueCat's DNS-based security platform keeps every client within its administrator-defined lane.

BlueCat also provides interfaces with common SIEM platforms such as Splunk, ArcSight, and QRadar, allowing users to secure their log information by sending it to these secure enclaves.

Overview: SEC Cybersecurity Guidance and 23 NYCRR 500

The Securities and Exchange Commission (SEC) is increasingly concerned about cyber risk. While there are no direct legal requirements for financial firms to address cybersecurity in any specific way, the SEC has issued several pieces of guidance in which it draws upon long-standing disclosure regulations to draw greater attention to this important issue.

In Regulation S-K Item 503, financial firms are required to disclose any of "the most significant factors that make the offering speculative or risky". Recent SEC communiqués interpret "risk" to include cybersecurity, and urge companies to address the potential impact of a breach as part of their standard disclosure practices. Specifically, the Commission is asking firms to address the material risk to reputation, legal risk, and revenue risk associated with a cybersecurity incident, tying that material risk to reporting requirements in the 1933 Securities Act. Under the Sarbanes-Oxley Act of 2002 (commonly known as SOX), C-level officials must sign off on these disclosures, making them ultimately accountable for the firm's stance on cybersecurity.

The State of New York has implemented similar guidelines which will impact the large number of financial firms which are headquartered in or operate in that state. The state's Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500) require that all covered entities establish a cybersecurity plan, designate responsible security officials, and perform regular testing to ensure readiness.

Implementation: SEC Cybersecurity Guidance and 23 NYCRR 500

Neither the SEC nor the State of New York specify a set of cybersecurity standards or controls which financial firms must meet. Their guidance simply

notes that firms should either document their own cybersecurity requirements for internal use or adopt an accepted set of best practices (most likely NIST 800-53 and the Risk Management Framework).

While financial regulators do not provide tactical controls for financial firms to meet, their emphasis on network visibility and audit capabilities has direct relevance to the DNS-based security systems which BlueCat provides. By collecting and analyzing query data from every client, BlueCat's enterprise DNS systems provide visibility into everything that happens on the network. Beyond mere visibility, the ability to implement policies to monitor or block malicious traffic will greatly minimize the cybersecurity risk highlighted by the SEC and the State of New York.

Collecting DNS data also creates a far more robust audit function in the event of an incident. Since most network security systems sit on the network boundary, they are unable to link network activity to a specific computer or user. BlueCat's position at the client level allows it to log network activity with a level of granularity which allows for association with individual users. In an audit situation, this client-level data saves weeks of poring through log files, allowing for real-time responses which in turn minimize cyber risk.

Overview: HIPAA

The Health Information Portability and Accountability Act (HIPAA), enacted in 1996, outlines a series of information security requirements for health care organizations which were enacted through a series of binding regulations. Most of these are specifically geared towards user authentication and privacy controls, but there are some more general provisions which touch on cybersecurity writ large.

In the HIPAA implementation regulations, 45 CFR §164.306 notes that health care organizations are required to protect networks against "any reasonably anticipated threats or hazards" as well as "disclosures...that are not permitted".

Implementation: HIPAA

The HIPAA regulations do not specify a particular cybersecurity standard or method to protect unauthorized disclosures of health information, assuming that protections will change over time to address evolving threats. (Although it is worth noting that the Department of Health and Human Services references the NIST Risk Management Framework on its HIPAA security guidance page and maps HIPAA requirements to relevant NIST 800-53 controls.)

In practice, most healthcare organizations have used access control as the primary (or sometimes only) way to protect information from unauthorized disclosure. The inherent assumption in this approach is that system users with the need to know will always handle patient information appropriately – an assumption which has not panned out in practice. In fact, insiders are one of the most prominent threats to information security today.

Access control alone is not enough to satisfy the HIPAA guidelines. Only a system which protects both access to the data and use or transmission of that data satisfies the spirit of the regulations.

This is where DNS can play a critical role in meeting the standard. With a client-facing DNS-based security system in place, healthcare organizations can link the authenticated identities associated with access control measures to network

activity. By capturing user intent for both accessing data and transmitting that data to other parts of the network or external sources, DNS creates a robust audit trail.

Applying client-level policies is another way to enhance privacy protection for healthcare data. By restricting access to servers with sensitive information, a DNS-based security system can ensure that neither unauthorized insiders nor the malware which may be hiding on the network can access HIPAA-protected data.

The HIPAA requirement to protect against "reasonably anticipated threats or hazards" to a network is extremely broad. When the law was put in place in 1996, those reasonably anticipated threats were relatively unsophisticated. Today's advanced persistent threats, powered by a significant increase in computing power, are probably already lurking on most healthcare networks already. Anticipating and mitigating these new kinds of threats requires a security system which covers every part of the network. Since it draws on the foundational infrastructure of the network, only DNS-based security can truly cover the full spectrum of network activity that HIPAA mandates require.

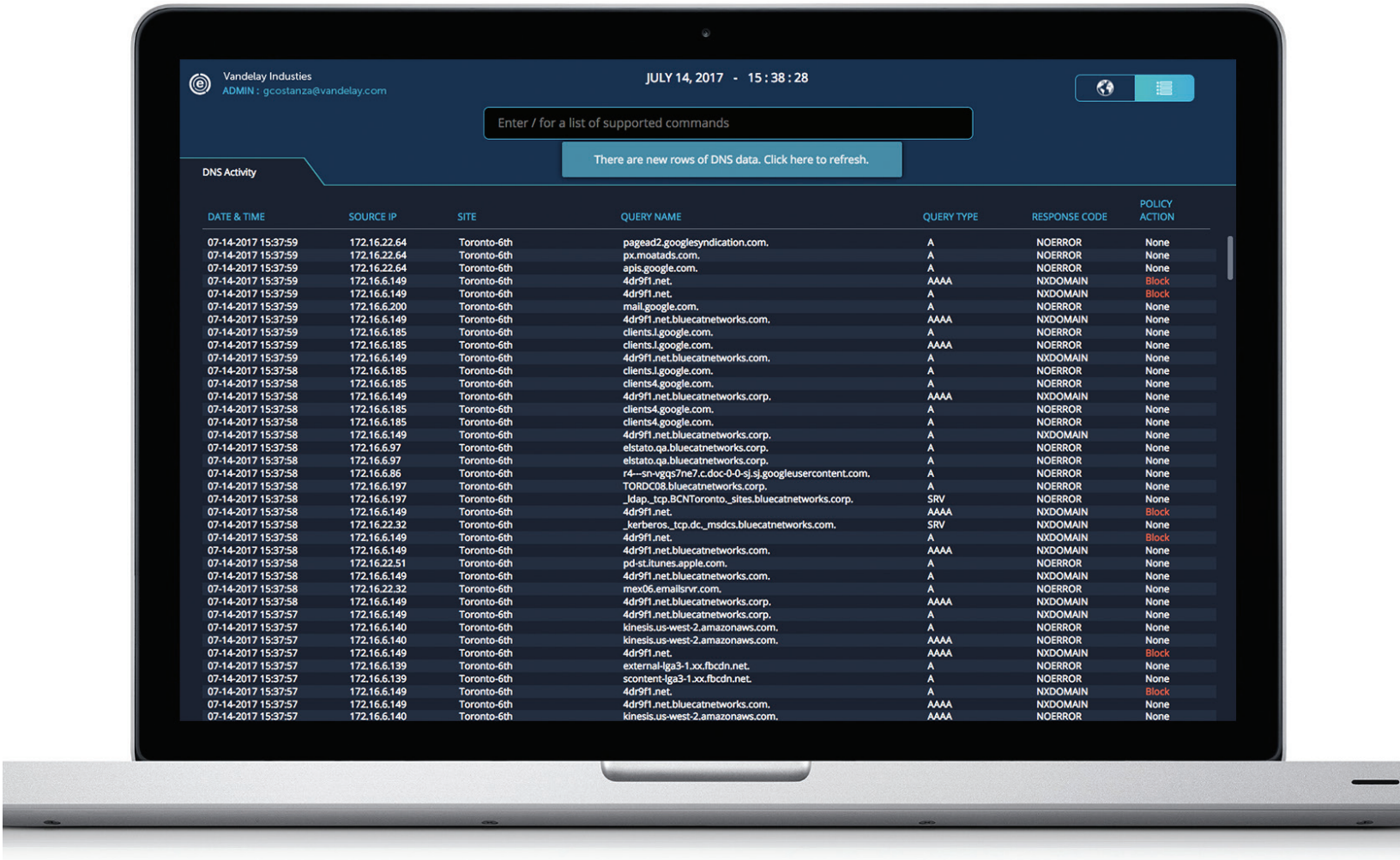
By collecting and analyzing query data from every client, BlueCat's enterprise DNS systems provide visibility into everything that happens on the network. Beyond mere visibility, the ability to implement policies to monitor or block malicious traffic will greatly minimize the cybersecurity risk highlighted by the SEC and the State of New York.

Collecting DNS data also creates a far more robust audit function in the event of an incident. Since most network security systems sit on the network boundary, they are unable to link network activity to a specific computer or user. BlueCat's position at the client level allows it to log network activity with a level of granularity which allows for association with individual users. In an audit situation, this client-level data saves weeks of poring through log files, allowing for real-time responses which in turn minimize cyber risk.

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, GET IN TOUCH

bluecatnetworks.com