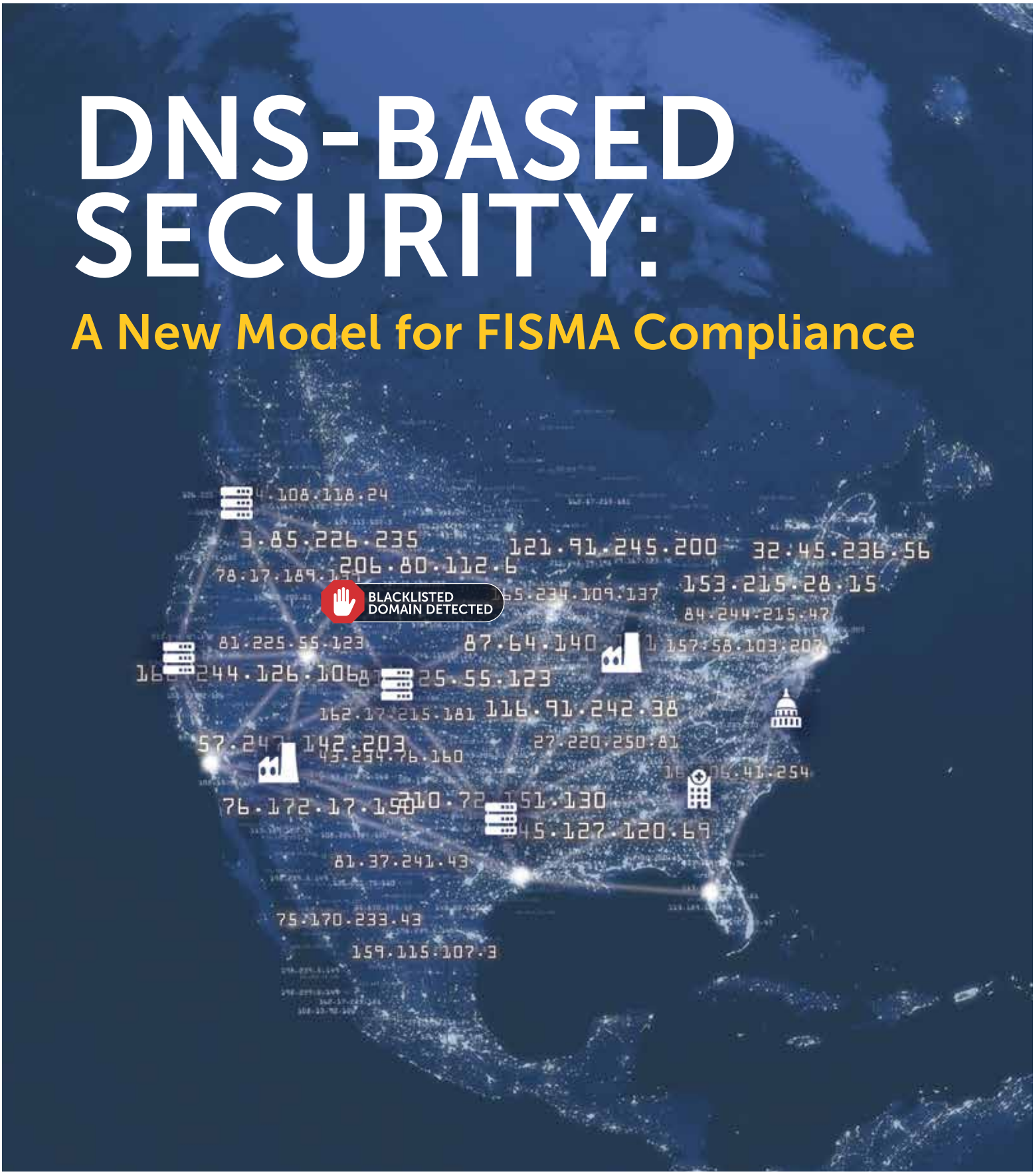
DNS-BASED SECURITY:

A New Model for FISMA Compliance



BLUECAT™

bluecatnetworks.com

FISMA (Federal Information Security Management Act) compliance criteria are designed to evolve in reaction to changing network security threats. This creates a moving target for agency IT security and IT management personnel. Maintaining accurate and reliable data on an ever-changing series of targets is a monumental, resource-intensive task. IT staff are constantly altering their data collection methods to fulfill FISMA reporting requirements.

With the FISMA criteria shifting slowly but perceptibly every year, Federal IT security and management staff are always looking for ways to collect and report on the data they need. Security Information and Event Management (SIEM) software is increasingly popular in the Federal space precisely because it provides a "single pane of glass" which can process any new data stream, allowing IT staff to quickly and easily monitor FISMA-relevant information even as requirements change.

Yet there is a marked difference between compliance and security. In the FISMA metrics document, DHS (Department of Homeland Security) notes that the requirements should be more than just a "cyber security compliance checklist". Monitoring data streams is one thing, but actually doing something about that data is what FISMA is really trying to encourage.

Federal IT administrators need tools that promote an active security posture while fulfilling the FISMA compliance requirements. FISMA provides a valuable framework for cyber security, but Federal administrators need something deeper – insight into the core of network functionality, user activity, and the relationship between the two.

"Agencies should view target levels for FISMA metrics as the minimum threshold for securing their information technology enterprise, rather than a cyber security compliance checklist.

In other words, reaching a performance target for a particular metric means that an agency has taken meaningful steps toward securing its enterprise, but still has to undertake considerable work to manage risks and combat ever-changing threats."

– DHS FISMA CIO Metrics

DNS Security – A New Model

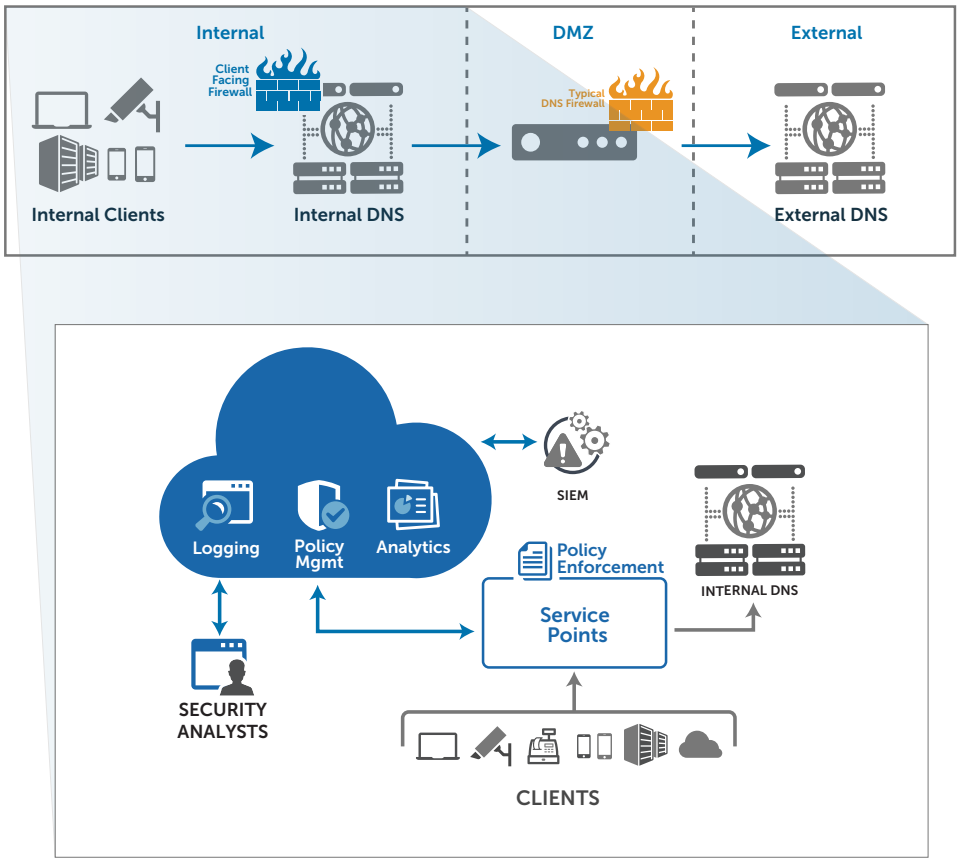
DNS data represents an extraordinarily valuable – and surprisingly underutilized – data stream which gets to the heart of FISMA compliance.

No single information source can create the active defenses and situational awareness across the network which FISMA envisions. Yet some data feeds naturally provide more utility and insight than others. As a service which touches every part of the network by definition, DNS naturally speaks to the core security requirements captured in FISMA, and therefore to the cyber security strategies of every Federal agency.

Typical approaches to network security rely on boundaries and filters to identify and block abnormal activity. The FISMA requirements are emblematic of this approach, requiring agencies to build strong external barriers and plan for responding to anomalous activity and breaches. There are two primary underlying assumptions in this model, neither of which are borne out in practice.

The first assumption is that effective boundaries can be created in the first place. Since the dawn of the digital age, IT administrators have deployed firewalls and filters to protect the network from incoming threats. Over that same period, firewalls and filters have repeatedly failed to deter or block malicious actors. Today's cyberattacks are more sophisticated and powerful than ever, consistently overwhelming even the most sophisticated boundary protection defenses.

The second assumption is that once an effective separation between the "inside" and the "outside" has been created, network traffic within the security boundary can be trusted. Yet the recent pattern of cyberattacks demonstrates that threats from inside the network, not external attacks, are the more potent threat. It usually isn't deliberate – one wrong click on a phishing email can provide enough access to compromise a network. Yet the effects can be devastating – outages, downtime, and stolen data.



DNS-based security represents a unique approach to FISMA compliance. Because it underpins every part of network architecture, DNS-based security transcends the traditional idea that security barriers are effective against network intrusions. By monitoring and controlling every part of the network – and casting equal suspicion on abnormal activity regardless of where it originates – DNS-based security covers the entire enterprise with strong, enforceable policies that dramatically minimize the operational space for malicious activity.

Taking FISMA to the Next Level

A quick look through the FISMA compliance categories provides some illustration of how a DNS-based security posture gets to the active security and situational awareness Federal agencies require by fulfilling FISMA requirements in a unique way:

Identify

FISMA requires agencies to keep inventories of information systems, devices, and endpoints connected to the network. While a useful baseline of how the network is constructed and what demands might be placed on it, any inventory is bound to be a snapshot in time.

DNS data provides more than just an inventory of network devices. It provides a richer stream of information which encompasses what those devices are actually doing. Rather than merely monitoring the existence of a network user, DNS data can monitor the impact of that user.

Protect

FISMA uses credentials as a firewall of sorts, ensuring that every user and device on the network is authorized.

DNS data gives Federal agencies deeper insight into the activity of each client. This helps not only for everyday detection of anomalies, but also in helping investigators identify "patient zero" quickly and easily in the event of a breach.

Detect

FISMA uses filters, intrusion detection systems, and quarantines to create a boundary between protected networks and the outside world.

DNS-based security recognizes that any attempt to wall off a network is likely to be unsuccessful in today's pervasive threat environment. By monitoring and acting on malicious activity at every point in the network, DNS-based security treats all threats – whether from inside or outside the network – with the same urgency.

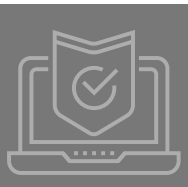
Respond

FISMA requires agencies to have a concrete plan in place to react to an ongoing incident.

DNS data allows agencies to quickly react to breaches by identifying and then shutting down any malicious activity. From the network's core to its periphery, active management of DNS gives agencies the ability to act with a targeted, proportionate response which mitigates against network outages.

Recover

FISMA uses resilience as the metric of an effective recovery strategy, requiring that all agencies have concrete measures in place to quickly return to normal operations after an incident.



Active DNS management gives IT administrators the power to re-route network traffic in response to an incident, minimizing the scope of a breach and restoring normal operations to the widest extent possible.

Owning Your DNS

If DNS data is such a powerful tool for both FISMA compliance and network security, why aren't more IT administrators using it? The answer lies somewhere between familiarity and prestige.

FAMILIARITY

Familiarity is one of the prime reasons that DNS falls through the cracks. Since it is such a basic part of how the internet works, the Domain Name System and the data it produces are taken for granted by many IT departments. Fading into the background of day-to-day network administration, DNS is seen as something to be maintained, not something to be leveraged.

DNS-based security demonstrates the true value of this underappreciated, overlooked data. By bringing this fundamental source of information out into the open, DNS-based security also turns the familiarity most IT administrators have with DNS into a demonstrable security asset.

PRESTIGE

Prestige is another reason many IT departments fail to recognize the power of DNS.

In most agencies, DNS is seen as a day-to-day operational burden assigned to the network operations team, which contributes to the idea that it has minimal value. By relegating DNS to the category of grunt work, IT departments ignore its potential as a security asset. CISOs are frequently unaware of the possibilities that DNS-based security can provide simply because it doesn't appear on their radar.

When security teams do begin to see the value of DNS data, conflict often follows. System administrators claim DNS as part of their territory, and an intra-departmental spat frequently breaks out. Without strong leadership to bridge the gap, the prospect of DNS-based security can easily fall through the cracks.

Vision is the critical factor in DNS-based security. Reclaiming overlooked DNS data requires network and security staff to work together, seeing through the everyday tasks of maintenance and administration to leverage information for a new purpose. CIOs and CISOs should jointly recognize the value of this data set for FISMA compliance, making it a core piece of their security platform.

TAKING THE FIRST STEP

As a core network service, DNS represents a prime opportunity to exceed FISMA standards and move toward a comprehensive approach to network security. How then can network administrators, CISOs, and IT organizations take the first step towards a DNS-based security regime?

Centralize

In order to get a handle on DNS data and put it to work, the first step is to centralize administration of DNS. Many organizations use spreadsheets and other manual, pieced-together tools which they have developed over time to manage DNS. Automating these functions and routing the flow of DNS data through a single, robust, and manageable infrastructure provides the foundation of a DNS-based security system, all while eliminating the uncertainty and risk associated with jerry-rigged solutions.

Analyze

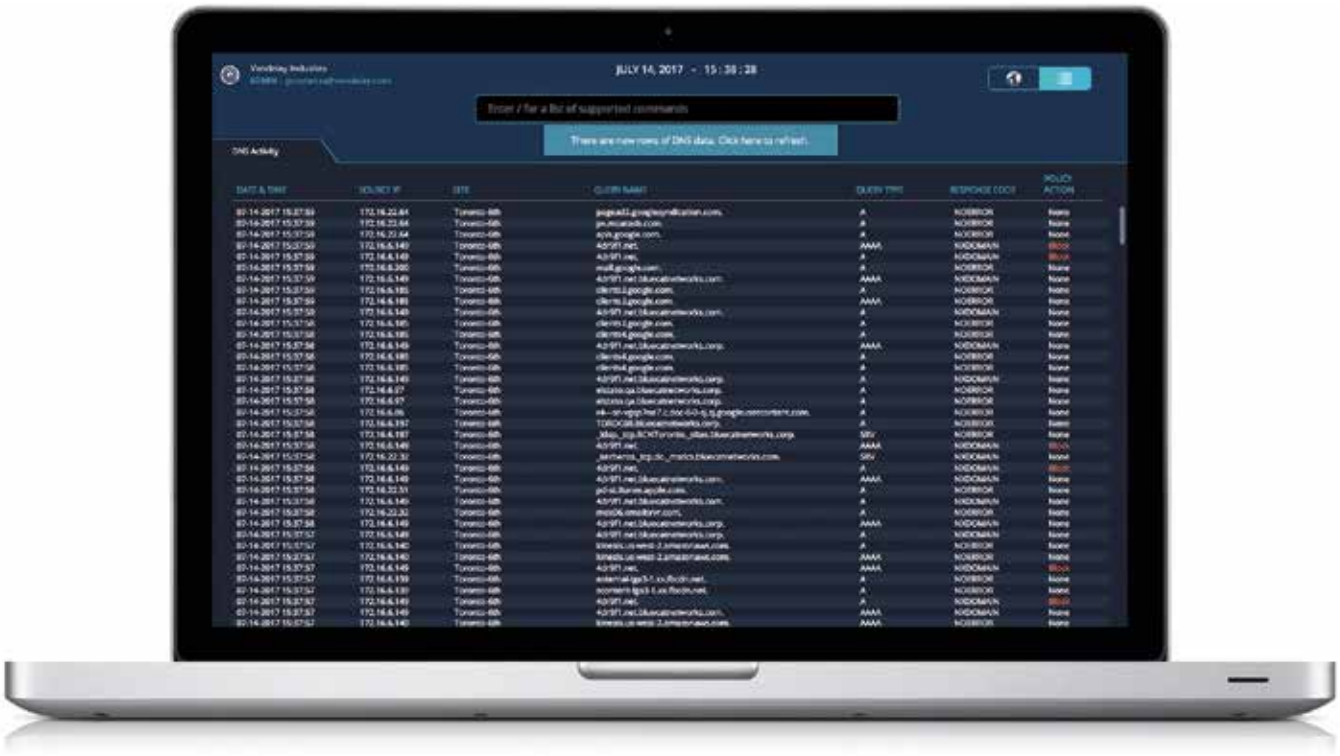
Once the centralized administration tools are in place, network administrators can start to analyze DNS patterns. Setting a baseline of "normal" network activity over time provides the information necessary to detect future anomalies in DNS traffic, both for the network as a whole and for individual users of that network.

Apply

Armed with a centralized system and the tools for analysis, IT administrators are then empowered to apply DNS-based security policies to their normal network operations. Whether viewed in a DNS management platform or through a SIEM implementation, administrators will have the visibility they need to detect malicious activity as well as the tools to respond effectively. Leveraging DNS-based policies allows network administrators to centrally manage their security posture.

Report

DNS-based security makes FISMA reporting easier and more substantive. With DNS administration tools in place, IT personnel can quickly identify the number of IP address enabled hardware devices are on the network (FISMA criteria 1.3). Quarterly reports on attempts to access large volumes of data are a snap (FISMA criteria 3.19). The answer to FISMA questions about coverage – for blocking unauthorized connections and data exfiltration – becomes a simple 100% (FISMA sections 2-3).



BLUECAT™

The Standard for DNS-based Security

As the Enterprise DNS Company™, BlueCat is committed to bringing the power of DNS-based security to all of its Federal customers who struggle with the evolving challenge of FISMA compliance.

Through its DNS Edge and DNS Integrity products, BlueCat offers the full range of DNS security and management tools for cyber security professionals. BlueCat works with agencies across the U.S. government to centralize and analyze their Domain Name Systems, providing them with the information they need to apply strong security policies that easily meet FISMA compliance standards.

BlueCat products are easy to deploy, simple to maintain, and cost-effective.
With available cloud, private cloud, and on premise options, BlueCat has a solution to meet the needs of any network architecture.

Contact us to learn more about BlueCat's approach to DNS-based security.