The role of DNS in CMMC compliance

In January 2020, the US Department of Defense released version 1.0 of the much-anticipated Cybersecurity Maturity Model Certification (CMMC) standard. DOD is already projecting that CMMC requirements will appear in contracts as early as June 2020.

In a departure from related government cybersecurity guidelines, DNS security is an explicit requirement of several CMMC controls.

This datasheet provides a quick overview of how DNS security plays into the CMMC controls, and how BlueCat promotes compliance.

Capability 039 – Control communications at system boundaries

Level one (SC.1.175) requires organizations to "monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of information systems." BlueCat provides the unique ability to monitor and control not only external, "north-south" traffic, but also internal, "east-west" traffic. This ability to place DNS controls anywhere and everywhere on the network gets to the "key internal boundaries" requirement in particular.

Level three (SC.3.192) adds a level of specificity, requiring implementation of "DNS filtering services" to reduce attack surface. BlueCat's DNS security solutions filter out known bad domains and allow for the creation of custom security policies. Since they can be applied to both internal and external traffic, those policies cover the entirety of a network, not just requests which reach the network boundary.

Level four (SC.4.199 and SC.4.229) explicitly requires the use of threat intelligence to define known bad domains. BlueCat addresses this requirement in two ways: through our "standard" threat feed, and through an integration between BlueCat and Cisco Umbrella. Together, these represent an unmatched source of operational intelligence to fulfill this control.

Level five (SC.5.208) requires implementation of "organizationally defined and tailored" protections. BlueCat's unique position as the "first hop" of any network query allows this kind of security control to be put in place without the need for an on-device agent. With the ability to tag devices according to any factor or typology you want, BlueCat makes the creation of customized, targeted security controls simple to implement across the enterprise.

Capability 037 – Implement threat monitoring

Level four (SA.4.173 and SA.4.171) of this control requires the implementation of a system for threat hunting which allows security personnel to quickly identify and disrupt anomalous activity. It then looks for a system to leverage, integrate, and share indicators of compromise across the organization.

DNS data is an essential tool for threat hunters, demonstrating the critical link between device-level activity and boundary-level indicators of compromise. The CMMC explanation of these controls specifically mention DNS data as a valuable source of actionable intelligence for threat hunters. Unfortunately, many organizations don't collect comprehensive DNS logs because their DNS architecture is decentralized and virtually impossible to monitor at scale.

BlueCat provides a single source of truth for DNS data, automating collection and dissemination of core infrastructure information across the enterprise. Using this comprehensive source of intelligence on network activity, BlueCat's government customers have cut their response time from over a week to hours or less. They can also use BlueCat's control over DNS traffic pathways to consistently apply security policies across the enterprise simply and easily.

Move At The Speed of Business

You need your DNS to enable your business and customer transactions and BlueCat can help you make it fast, resilient, and secure. Whether you need to centralize control of core DDI services, accelerate application performance, deliver networking for branch offices, or to integrate with hybrid and multi-cloud environments, we have you covered.

Want to get into the details? Contact BlueCat today to learn more about our DNS security solutions for CMMC compliance.

United States Headquarters
1000 Texan Trail, Suite #105, Grapevine, Texas 76051
+1.817.796.8370 | 1.833.BLUECAT

Canada Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
+1.416.646.8400 | 1-866-895-6931

bluecatnetworks.com

Next Steps

Get in touch with a BlueCat representative to future proof your network.

Visit bluecatnetworks.com/contact-us/