Infoblox

WHITE PAPER

Adopting NIST Cyber Security Framework

Using Foundational Network Infrastructure

Introduction

With the explosion of mobile devices, software-as-a-service (SaaS) applications hosted in public/private clouds, advent of SD-WAN, and the growing number of internet of things (IoT), IT organizations are struggling to effectively secure all of these scenarios using existing network security architectures.

As companies of all sizes go through digital transformation to increase the “speed of doing business”, CIOs/CISOs are held accountable for securing the business infrastructure and protecting the reputation of the company. But it’s easier said than done. Security teams add more and more security tools to combat cyber threats, but that causes operational overload and a mountain of security alerts to review. As networks grow more complex, they are struggling with maintaining a real-time view of what is on their network, quickly isolating/quarantining end-points compromised by malware and blocking back doors to sensitive data.

Foundational network infrastructure services such as Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and IP Address Management (IPAM), collectively called as DDI, is the “dial-tone” of any network, essential in maintaining integrity, connectivity and availability of business infrastructure and applications. DNS can also become the most vital component of your cyber security strategy. It often has the front row seat to malware activity and data exfiltration attempts initiated by compromised hosts.

The National Institute of Standards and Technologies (NIST) Cyber Security Framework (CSF) is a set of best practices and standards that CISOs in both government and private companies are increasingly adopting to improve their overall cyber security posture. Organizations overlook the fact that they can leverage robust DDI services, to satisfy some of the guidelines described in the NIST CSF framework to reduce their overall business risks. This white paper briefly describes the relevance of DDI services, how they can help secure your critical infrastructure and data, and how NIST CSF can be applied to improve any organization’s cyber security posture using the top 10 must haves in the foundational network infrastructure services you choose to deploy.

Primer to NIST Cyber Security Framework (CSF)

Why NIST CSF?

NIST Cyber Security Framework (CSF) seeks to address the lack of standards when it comes to security. It defines a set of best practices that enables IT organizations to effectively manage cyber security risks regardless of size, degree of cyber risk or sophistication. Organizations can voluntarily use this framework to determine their current level of cyber risks, set goals for cyber security that are in sync with their business environment, and set plans for improving or maintaining their security posture over time.

The increasing adoption rate of NIST by most IT organizations can be attributed to the following.

- NIST applies to both public and private sectors with an appeal beyond the US
- It can co-exist, take advantage of existing frameworks such as ISO, COBIT, FFIEC, as well as form the basis for compliance programs such as FedRAMP
- It depicts an information security lifecycle that is typically followed and understood by IT

organizations

- It provides a common taxonomy that can be applied across a wide variety of IT infrastructure components (network, endpoints, applications, and data)

Key Elements of NIST CSF

The NIST CSF is broken down into 3 components – the core, the implementation tiers, and profiles.

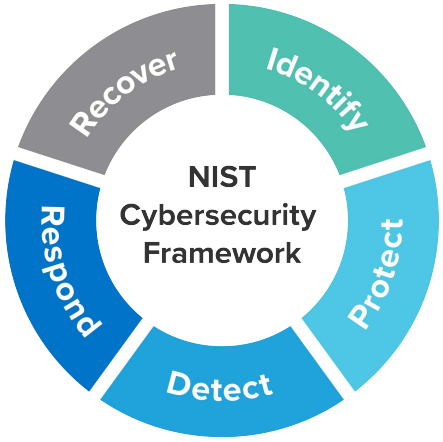

Figure 1: Core Functions of the NIST Cyber Security Framework

- **Core:** Contains the array of activities, desired outcomes, and references, which are applicable across all IT infrastructure components. It consists of the following 5 high-level functions as shown in Figure 1, which are further divided into 23 categories, and 108 subcategories.
    - **Identify:** Gain organizational understanding of risks to systems, people, assets, data, and capabilities. The key components here include taking asset inventory and performing a risk assessment to understand and prioritize business risks based on an organization's policies and procedures.
    - **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. This includes implementing protective technologies for identity management, access control, and data security.
    - **Detect:** Implement the appropriate activities to identify security events/incidents that escape the protective controls you have in place. This includes 24/7 monitoring, anomaly detection, and forensics analysis, using threat intelligence.
    - **Respond:** Implement activities to act-on and contain security events/incidents detected in the previous phase. It includes incident response planning, security orchestration, automation and response (SOAR) run-books, to mitigate the risk.
    - **Recover:** Implement appropriate activities to maintain plans for resilience and restore any services or capabilities that were impaired due to a cyber security

event/incident. It includes recovery planning, process improvements and communications.

- **Implementation Tiers:** Provide context on how an organization views its cyber security risks and the processes in place to manage those risks. Tiers help organizations characterize their practices in each of the Core functions and Categories and prioritize the findings into these 4 tiers – Partial (1), Risk Informed (2), Repeatable (3), and Adaptive (4). For example, if the finding from risk assessment indicates that all wireless assets (laptops, mobile devices) are not in the asset database, this risk is registered under implementation tier 1 (Partial) and prioritized for improvement using profiles below.
- **Profiles:** Define the outcomes based on business needs that an organization has selected from the framework categories and subcategories. Profiles can be used to prioritize opportunities for improving an organization's cyber security posture by comparing a "current" profile with a "target" profile (to be state).

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
What assets need to be protected to reduce risks?	What safeguards are in place to protect them?	What techniques can detect incidents that escape safeguards?	What processes can mitigate impact of security incidents?	What techniques can restore services?
Asset Management	Identity Management, Authentication, and Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environ.	Awareness Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Information Protection Procedures		Mitigation	
Risk Mgmt. Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technologies			

Primer to Foundational Network Security

Using DNS for Improving Security Posture

IT organizations can leverage a highly integrated DDI platform which includes DNS, DHCP and IPAM services, to gain precise visibility across their physical, virtual, cloud, container and IoT environments. They can also leverage DNS as a first line of defense to detect and block activity related to most modern malware like ransomware, exploits, phishing, C&C callbacks, data exfiltration, DGAs, APTs and more using latest threat intelligence and ML based analytics.

DNS Security augments the existing security stack and can actually offload blocking of threats from perimeter security, reducing the amount of malicious traffic sent to these tools and preserving their processing power. Here are the 3 ways DNS security can be leveraged.

- **DNS Resolution:** When a compromised endpoint attempts to resolve the domain name of a C&C server, the DNS server could block that name resolution and send that connection request to a sink-hole. This will prevent data exfiltration or new malware downloads from these C&C sites.

- **DNS Tunneling:** Hackers use DNS payloads as means to exfiltrate data on port 53, to circumvent next-generation firewalls, IDS/IPS rules. Enhancing DNS to detect such exfiltration attempts will prevent data exfiltration via DNS.
- **Volumetric DNS Requests:** Botnets could be used to launch a distributed denial of service (DDoS) attack on external DNS servers and make them unavailable to resolve name resolution of genuine domains. In 2016 the Mirai malware launched a massive DDoS attack on the DNS server operated by Dyn, by using millions of IoT devices as bots to generate fake DNS requests. A robust DNS service should be able to detect such fake DNS requests in large volume.

Role of DDI in SecOps

Over and above the standard role that DNS, DHCP and IPAM play in providing connectivity, they are also a gold mine of data that can be leveraged by SecOps teams.

- **Domain Name System (DNS):** DNS provides critical audit trail of any domain/hostname lookups. This audit trail can be leveraged to quickly map out services and resources that have been accessed by compromised devices. DNS and domain registration data are also key data sets in making threat intelligence actionable.

- **Dynamic Host Configuration Protocol (DHCP):** is used to dynamically assign reusable IP addresses to devices on the network, every time when a device (e.g. laptop) joins a network. DHCP data also helps correlate disparate security events related to the same device under investigation especially in dynamic environments.

- **IP Address Management (IPAM):** Begins with IP address discovery, tracking, and allocation of data pertaining to all devices on the network. It maintains a centralized repository of data associated with devices, networks, and services in one clear and easy to manage interface. Every time an IoT device is connected to the physical network, virtual machine is provisioned, or a laptop leaves a network, the IPAM database is updated, making it the single source of truth for IT asset inventory.
    - Example: If a host is generating excessive network traffic, the IPAM database could be searched to discover the switch port it is connected to, the VLAN it is on, and triangulate on the device that has been compromised. DHCP fingerprinting can enrich the database with

the device type and integrate with a network access control (NAC) solution to enforce policies to isolate or quarantine the compromised machine.

Empowering SOAR: Once the cyber threat is detected, the DDI platform should be able to send valuable network context to the deployed security orchestration automation and response (SOAR) solution and automate response to the attack.

- Example: It could enable the following types of integrations for rapid response.
    - Vulnerability Management (VM) solutions, such as Tenable Nessus, to run a scan on the compromised host to determine what patches to apply.
    - Network Access Control (NAC) solutions, such as Cisco ISE, to quarantine the infected endpoint so that the malware does not spread laterally on the local area network.
    - Endpoint Detection and Response (EDR) solutions, such as Carbon Black (Bit9), to kill the rogue process that is spawned by the malware just downloaded from an email attachment.
- Event Correlation: DNS name resolution and DHCP lease logs can be sent to 3rd party security information and event management (SIEM) systems to track detect anomalous name resolutions of C&C domains or MAC spoofing on DHCP servers.
-

Top 10 Must Haves to Satisfy NIST CSF

1. Asset Management: Use of IPAM database as the authoritative source of asset inventory of all systems on the network, virtual machines, mobile and IoT devices.
2. DHCP Fingerprinting: Use of DHCP request packet to “fingerprint” the device and enrich IP Data with device type, physical location, OS/application running on the device, in addition to network configuration data (IP address, host name, network gateway, netmask, switch port, and VLAN) is necessary.
3. Risk Assessment: Enable automated discovery and scanning of all devices on the network to identify and prioritize vulnerabilities that need to be patched to reduce business risks and reduce attack surface.
4. Threat Intelligence: to the detect the latest set of attack vectors using threat data curated from internal and external sources (e.g. malware, endpoint, C&C sites).
5. Detection of Anomalous Events: to detect MAC Spoofing, Volumetric DNS requests, DNS tunneling and exfiltration of sensitive data.
6. Rapid Mitigation: Enable security orchestration automation and response (SOAR) through APIs for rapid mitigation and response via partner solutions – endpoints detection response (EDR), network access control (NAC).
7. Security Continuous Monitoring: ability to forward DNS requests and DHCP lease logs to 3rd party SIEMs for continuous monitoring and event correlation to detect complex threats.
8. Centralized Management: Consolidate DDI services into a single platform, centrally managed using common dashboard/console to provide centralized visibility into all devices and services running on the network.
9. Diverse Infrastructure Support: DDI should function across diverse infrastructure – on-premises, SaaS applications in private/public/hybrid clouds, mobile and IoT devices.
10. Customizable reporting: to meet audit and compliance requirements of varied compliance regulations and industry standards including the NIST Cyber Security Framework.

Mapping DDI Solution to NIST CSF Core Functions

A DDI platform should enable validating/auditing the following core functions and categories of version 1.1[(2)] of the NIST Cyber Security Framework as shown in Table 2.

TABLE 2: Mapping of DDI Solution to Core functions/categories in NIST CSF

NIST Core Function	NIST Core Category	Category Identifier	DDI Solution
Identify	Asset Management	ID.AM	IPAM used in the following capacity: As the single source of truth for network assets. For automated device discovery Integration with vulnerability scanners for scanning when a device joins the network
Identify	Risk Assessment	ID.RA	Network automation tool for automated discovery and scanning of all devices on the network to identify misconfigured devices. Integration with vulnerability Management (VM) tools when something anomalous is detected
Protect	Access Control	PR.RC	Integration with Network Access Control solutions to isolate/quarantine compromised devices and prevent them from joining the network.
Detect	Anomalies and Events	DE.AE	Detect DNS tunneling and exfiltration of sensitive data.
Detect	Security Continuous Monitoring	DE.CM	Ability to forward DNS requests and DHCP lease logs to 3rd party SIEMs and other SecOps tools for continuous monitoring
Detect	Detection Processes	DE.DP	DNS Firewalling & Malware Detection using aggregated threat intelligence Detect volumetric DNS attacks DGA detection, data exfiltration, Fast flux, file-less malware using ML based analytics
Respond	Mitigation	RS.MI	DNS Firewalling and automatic incident response via ecosystem integrations using STIX, REST APIs. Rapid mitigation with ecosystem partners (e.g. NAC, Endpoint Detection and Response)
Respond	Analysis	RS.AN	DDI data and threat intel context, automated threat investigation using aggregated search tool

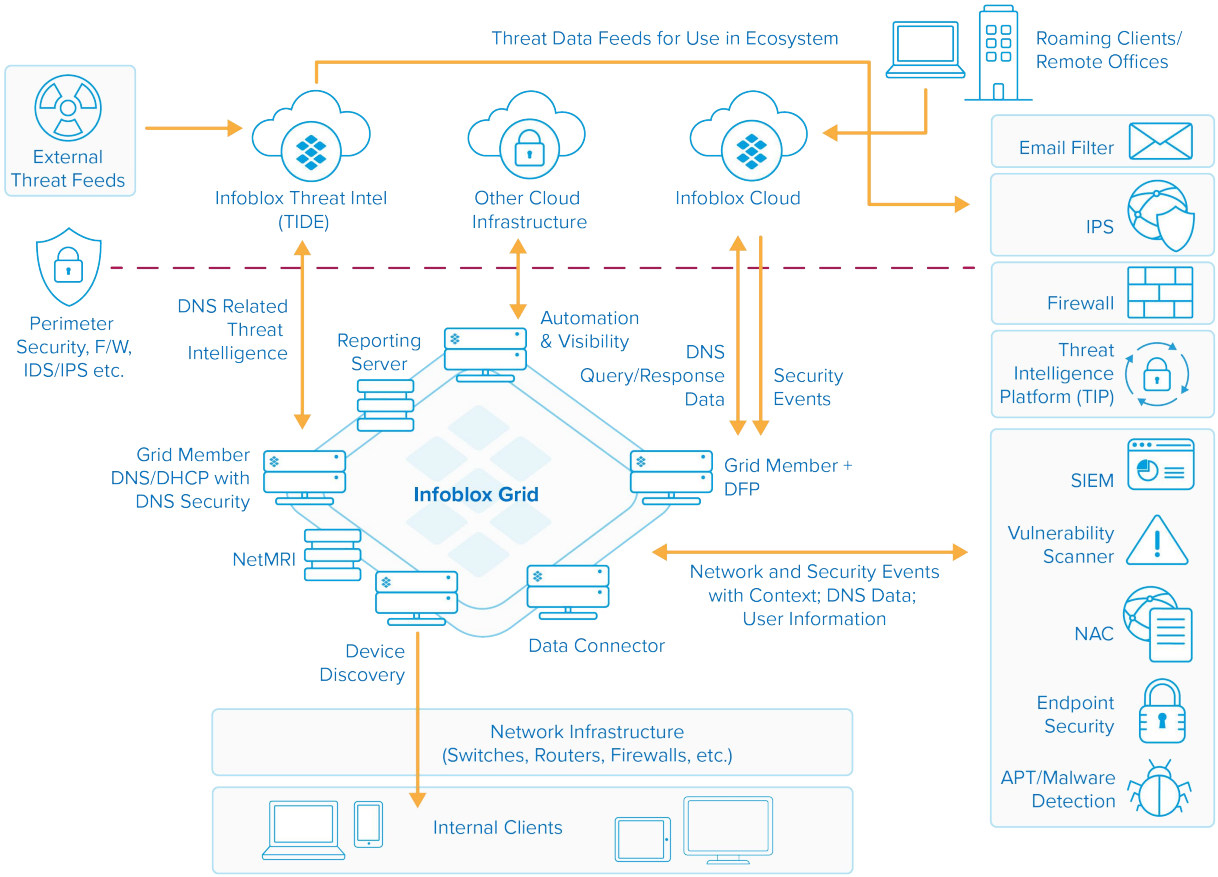

Figure 2: Integrated DDI platform to help satisfy NIST requirements from asset management to detection to mitigation.

Simplify NIST CSF Compliance with Infoblox

As CIOs/CISOs are increasingly held accountable by the board for securing their business infrastructure, they are looking for ways to simplify assessing business risks by adopting industry standard best practices, such as the NIST Cyber Security Framework. Hence, 73% of IT organizations are already implementing or planning to implement NIST CSF in the next 18 months, to measure the security posture of their business infrastructure.

In summary, foundational network infrastructure services such as DDI solution offered by Infoblox, plays a critical role in satisfying the following core functions in the NIST CSF.

- Identifying what is on your network in real-time by using the IPAM service that provides a single source of truth of your asset inventory.
- Protecting your network by rapidly isolating endpoints (using integrations with NAC solutions) compromised by malware that bypasses your perimeter defenses.
- Detecting cyber threats that use DNS tunneling to exfiltrate sensitive data and preventing backhaul traffic to malicious C&C servers.
- Responding to and mitigating cyber-attacks by providing API-level integrations with NAC, endpoint detection and response providers.
- Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management.

REFERENCES

1. The NIST Cyber Security Framework 1.1 – Top Customer Concerns, Khushbu Pratap, Gartner Security and Risk Management Summit, June 2019.
2. Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, NIST Publication, dated April 16, 2018.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054

+1.408.986.4000 | info@infoblox.com | www.infoblox.com