

SOLUTION NOTE

INFOBLOX SUPPORTS PCI DSS COMPLIANCE WITH SECURE DNS MANAGEMENT

Automated DNS Solutions to Safeguard Cardholder Data

SUMMARY

Leveraging DNS for Secure and Efficient Network Management as Part of Your PCI DSS Compliance Requirements

Infoblox DDI (DNS, DHCP and IP address management) and DNS Detection and Response solutions are critical tools to assist with your Payment Card Industry Data Security Standard (PCI DSS) compliance. These solutions help ensure secure, automated and efficient management of network services, which is essential for protecting cardholder data. Infoblox enables organizations to reduce the risk of data breaches, maintain continuous compliance and enhance overall security posture.

OVERVIEW AND CHALLENGES

The PCI DSS is a set of security standards designed to protect cardholder data. It applies to all entities that store, process or transmit cardholder data. Compliance with PCI DSS is mandatory for organizations handling payment card information to prevent data breaches and fraud.

Because of the critical nature of PCI DSS, organizations face numerous challenges including:

- Ensuring continuous compliance with evolving standards
- Managing and securing complex network infrastructures
- Protecting cardholder data from cyberthreats
- Automating compliance processes to reduce manual effort and errors

Domain Name System (DNS) is a critical component in solving these PCI DSS challenges. In simple terms, DNS is the internet's phonebook, translating human-friendly domain names into IP addresses. If an attacker manipulates this system, they can redirect traffic, intercept sensitive data or launch malware attacks. In the context of PCI DSS, a compromised DNS can undermine the entire security posture of an organization handling payment card information, leading to severe consequences, such as:

- **Interruption of Services:** DNS is crucial for website and application availability. Attacks like distributed denial of service (DDoS) targeting DNS servers can bring down a merchant's online payment systems.
- **Data Breaches and Theft:** Increased risk of data breaches and loss of sensitive cardholder information through DNS spoofing/cache poisoning, lookalike domains, phishing attacks, malware distribution and data exfiltration via DNS tunneling.
- **Financial Penalties:** Non-compliance can result in fines ranging from \$5,000 to \$100,000 per month as well as other costs relating to solving downstream effects of non-compliance.
- **Reputation Damage:** Loss of customer trust and damage to the organization's reputation
- **Operational Disruptions:** Increased manual effort and potential for human error in managing network configurations.

DNS can play a critical role in PCI DSS compliance, serving as a fundamental component of network security and data protection, and Infoblox offers solutions to help keep you in compliance.

KEY CAPABILITIES

Infoblox supports PCI DSS compliance with:

Centralized Management: Provides a centralized platform for managing DDI to simplify administration and ensure consistent security policies across the network

DNSSEC Support: Ensures the integrity of DNS responses and preventing DNS spoofing

Visibility and Control: Granular visibility into DNS traffic allows organizations to monitor for suspicious activity and quickly identify and respond to threats

DNS Security: Offers advanced DNS protection against a wide range of attacks, including DDoS attacks, DNS spoofing/cache poisoning, lookalike domains, phishing attacks, malware distribution and data exfiltration via DNS tunneling

Threat Intelligence Feeds: Identify and block known malicious domains and IP addresses. Protect against phishing attacks and malware distribution

THE INFOBLOX SOLUTION

Infoblox DDI and DNS Detection and Response solutions can help organizations meet the stringent requirements of PCI DSS and bolster their overall security posture. Our solutions provide comprehensive protection and management of network services through:

- **Automated Network Discovery:** Continuous discovery and monitoring of network devices to ensure compliance
- **Role-Based Access Control:** Enforcing secure access to network devices and configurations
- **Configuration Management:** Automated configuration and change management to maintain secure network settings
- **Threat Detection and Response:** Real-time detection and mitigation of DNS-based threats

Here's how Infoblox DDI and DNS Detection and Response solutions impact several PCI DSS requirements:

PCI DSS Requirement	How Infoblox Supports
Build and Maintain a Secure Network and Systems <i>Requirement 1: Install and Maintain Network Security Controls</i>	Infoblox provides advanced DNS firewall capabilities that help in segmenting and protecting networks where cardholder data is processed. By controlling and monitoring DNS traffic, Infoblox supports the establishment of a robust firewall configuration.
Maintain a Vulnerability Management Program <i>Requirement 5: Protect All Systems and Networks from Malicious Software</i>	Infoblox DNS security solutions can detect and block DNS-based threats, preventing malware from communicating with command-and-control servers—a common method attackers use to infiltrate networks.
Maintain a Vulnerability Management Program <i>Requirement 6: Develop and Maintain Secure Systems and Software</i>	Infoblox offers seamless software updates and patches for our DNS services, to help ensure that vulnerabilities are addressed promptly, which is crucial for maintaining secure systems.
Regularly Monitor and Test Networks <i>Requirement 10: Log and Monitor All Access to System Components and Cardholder Data</i>	Infoblox has comprehensive logging features to allow organizations to track DNS queries and activities. This visibility is essential for auditing purposes and for detecting any unauthorized access or anomalies in real time.
Regularly Monitor and Test Networks <i>Requirement 11: Test Security of Systems and Networks Regularly</i>	Infoblox provides tools that facilitate security testing of DNS infrastructure, including ecosystem integrations with top vendors for regular vulnerability assessments.

CONCLUSION

Infoblox DNS-focused network and security solutions are essential tools to help with the challenges of achieving and maintaining PCI DSS compliance. By automating network management and enhancing security, Infoblox helps organizations protect cardholder data, reduce the risk of breaches and support PCI DSS compliance.

INFOBLOX BENEFITS

 Scalability to Meet Growing Demands	 Visibility and Control, Ease of Management	 Enhanced Security and Threat Detection
Infoblox scales seamlessly with your organization's growth, ensuring robust security and compliance as your network expands.	With centralized management interfaces, Infoblox simplifies the oversight of DNS services, helping reduce the complexity and potential for configuration errors.	Infoblox secures DNS infrastructure to prevent data breaches and protect cardholder data from cyberthreats.

DISCLAIMER : The information provided in this document is for general informational purposes only and does not constitute legal advice. Our solutions are not PCI "Compliant Products" themselves but are intended to assist customers in enhancing their security as part of their own PCI compliance activities.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com