Infoblox

SOLUTION NOTE

Greater SecOps Effectiveness Through Greater Network Visibility

OVERVIEW

The role of SecOps has become increasingly complex as the users and devices they protect continue to evolve in the face of business, workplace, and digital transformations. This challenges the team's ability to eliminate blind spots, control rogue IT, reduce noise/false alerts, proactively recognize areas of risk, and execute timely investigation and response activities.

Organizations that have overcome these challenges embrace the security value found in core DNS, DHCP, and IPAM services (collectively DDI). Infoblox IPAM and DHCP help SecOps know who and 'what' is on the network and provide extensive context around security events to help drive more efficient proactive and reactive security capabilities. Combined with BloxOne® Threat Defense, Infoblox customers can significantly elevate their security profile and SecOps effectiveness.

The Challenge

Every organization's unique blend of users and devices is constantly changing, driven by the business, workplace, and digital transformations around us. Threats continue to adapt to leverage these changes, growing increasingly advanced. And unsanctioned devices and applications continue to find their way onto the enterprise network. All of this complicates every aspect of SecOps, from proactive security monitoring, compliance, and protection to breach detection, investigation, and response.

However, by leveraging core network data from DNS, DHCP, and IPAM (collectively 'DDI') services, innovative SecOps teams are finding new ways to be more proactive, eliminate blind spots, speed threat investigations, and respond more effectively.

Knowing What is on the Network is Half the Battle

Being able to associate a security incident to a user has long been key to threat investigation and making response decisions. But in a world with more devices on a network than users, including BYOD and IoT/OT, it has become just as crucial for SecOps to have access to device details.

In alignment with modern best practices, Infoblox provides DHCP and network discovery capabilities to identify sanctioned and unsanctioned (rogue) devices on the network, supporting a dual-method approach to asset discovery. This allows both security and networking teams to collect basic device details and extensive metadata, which are then stored in the Infoblox IPAM solution for fast, on-demand access by either network or SecOps personnel or automatically sharing the data with SIEM, SOAR, or other tools (see Figure 1).

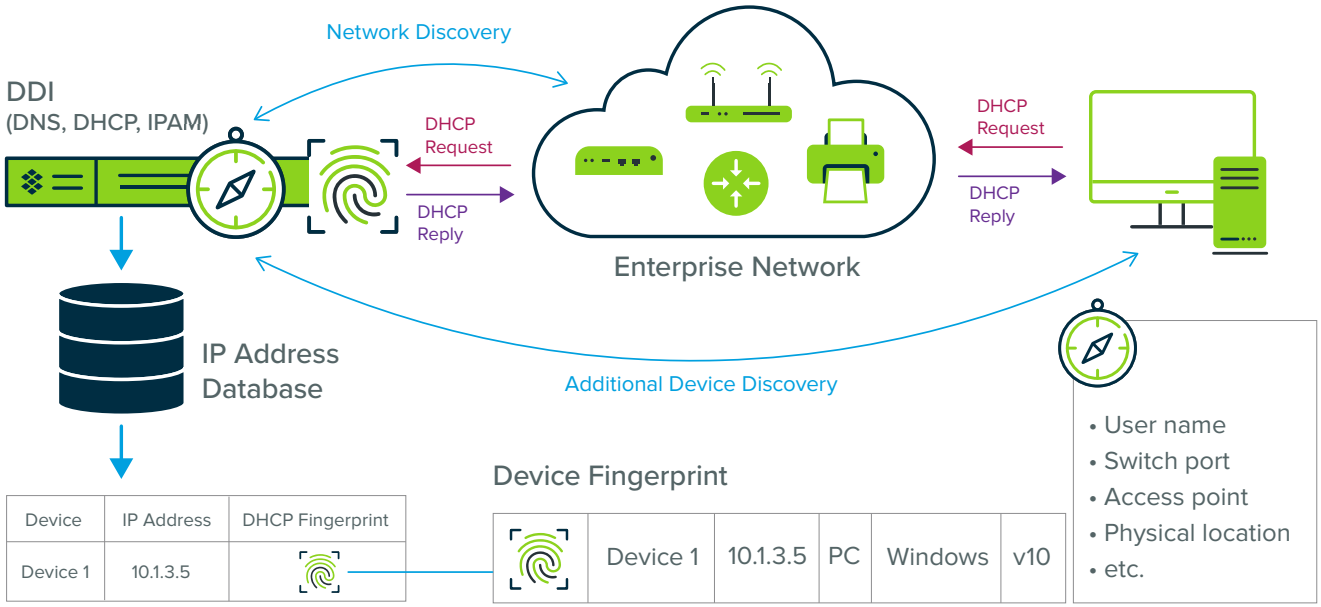

Figure 1: Leveraging DHCP, network discovery, and IPAM for greater device visibility

Visibility Opens Proactive Security Opportunities

One of the most obvious benefits of a dependable asset management capability is the ability to identify unsanctioned or 'rogue' devices on the network. From an innocent baby-cam device consuming bandwidth to something presenting a more direct threat, SecOps cannot measure risk and respond appropriately without information and context at the device level.

But vulnerabilities continue to be at the heart of many large breaches. The extensive metadata that can be available within Infoblox IPAM includes firmware details that can help SecOps proactively monitor devices that may require a patch or update. Infoblox can even use CVEs to automatically highlight affected devices that may require more urgent attention or simply to support compliance reporting.

Context Speeds Investigation and Response

SecOps teams have struggled with managing their workloads for years, and Infoblox DDI solutions can help provide the valuable context that can help reduce tens of thousands of alerts to only a few dozen that require attention. From device-aware security policies to enabling SIEM and SOAR solutions with more data, Infoblox does more than just another 'alert priority' portal.

With the extensive data available through Infoblox IPAM, SecOps teams save time with on-demand access to the latest information. Combined with BloxOne Threat Defense, this data can be correlated with security events to further refine the data for analysts. This can reduce threat investigation by as much as 2/3rds, and provide incident responders with the details they need to confidently execute an optimally effective response.

DNS Security Closes a Common Security Gap

Like everything else, malware depends on DNS for communications, which provides an opportunity to detect threat activity other solutions miss. Even evasion techniques like malicious tunnels, Lookalike URLs, or Demand Generation Algorithms (DGA) can be exposed at the DNS layer. And some threats specifically use DNS for malicious activities like C2 communications, to exfiltrate data, or receive ransomware encryption keys.

Infoblox BloxOne Threat Defense detects threat activity at the DNS layer but also offers a platform for sharing threat intelligence across the entire security stack to uplift your defenses. It includes the "Dossier" threat research tool to help analysts investigate threats and can integrate Active Directory, IPAM, and other contextual sources into one place to speed threat investigation and incident response.

Referenced Infoblox Products

Infoblox IPAM & DHCP

Simplify IPAM and DHCP management to increase efficiency and responsiveness

With Infoblox IPAM (IP address management) and DHCP, you can automate and centralize all aspects of IP address provisioning and DHCP server management in conjunction with DNS. Our integrated platform enables you to confidently handle your most challenging IPAM and DHCP requirements in every type of network environment, data center and hybrid cloud environment.

Learn more

BloxOne Threat Defense

Improve security effectiveness and resiliency and elevate SecOps efficiency

BloxOne Threat Defense operates at the DNS level to see threats that other solutions do not and stops attacks earlier in the threat lifecycle. Through pervasive automation and ecosystem integration, it drives efficiencies in SecOps, uplifts the effectiveness of the existing security stack, secures digital and work-from-anywhere efforts, and lowers the total cost of cyberdefense.

Learn more

Infoblox NetMRI

Smartly manage your multi-vendor network with automation, visibility and continuous insight

NetMRI is Infoblox's off-Grid network change and configuration management solution that automates routine workflows such as device and configuration discovery and provisioning, policy monitoring and enforcement and security operations, enabling tighter compliance, quicker app development, and faster incident response.

Learn more

Infoblox

Infoblox is the leader in next generation DNS management and security. More than 12,000 customers, including over 70% of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-firs world. Learn more at www.infoblox.com.

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

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