SOLUTION NOTE

GREATER SECOPS EFFECTIVENESS THROUGH ENHANCED 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 evolving complexity 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, these capabilities enable Infoblox customers to 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, with attacks growing increasingly advanced. And unsanctioned devices and applications continue to find their way onto the enterprise network. All of tthese factors complicate 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 investigating threats 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 appraoch 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).

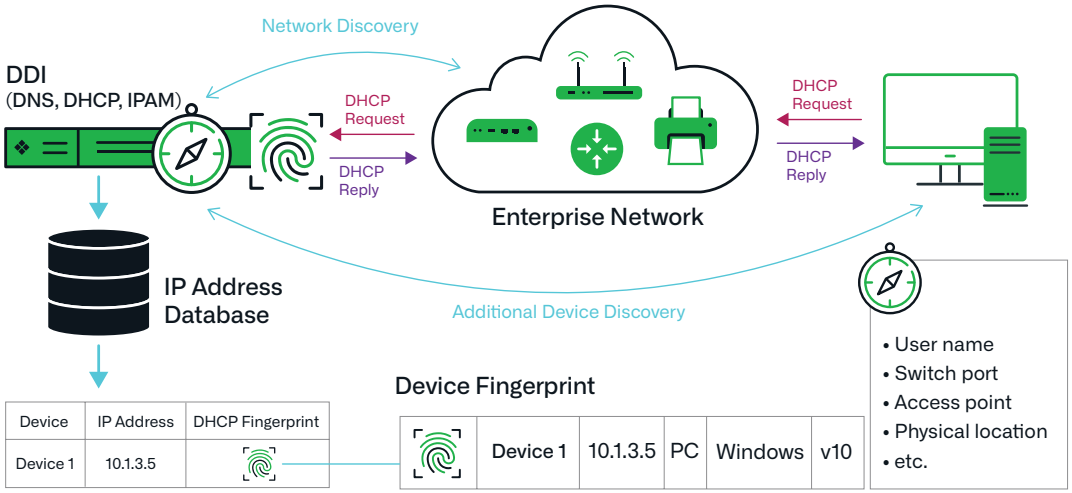

Figure 1: Leveraging DHCP, network discovery, and IPAM for greater device visibility

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 common vulnerabilities and exposures (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 you to 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.

Contextual network visibility is critical in today’s hybrid multi-cloud environments. 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 correlation can reduce threat investigation by as much as two-thirds, and provide incident responders with the details they need to confidently execute an optimally effective response.

Infoblox discovery for the Cloud Services Portal (CSP) allows hybrid on-premises NIOS to BloxOne cloud migration and single control plane visibility by sending network data discovered by Network Insight (or NetMRI) to the CSP for visibility through the BloxOne platform. This means that BloxOne customers can use a small Network Insight Grid (or NetMRI) and gain all the visibility of on-premises discovery in their BloxOne deployment.

In addition, Infoblox further raises visibility and enables cloud migration with the ability to deploy Reporting and Analytics members in AWS and Microsoft Azure public clouds. The Infoblox Reporting and Analytics solution is built on Splunk, a market-leader in data search, monitoring, visualization and SIEM solutions. This capability both simplifies the migration of physical data centers to the cloud and delivers single and multi-site visibility into DDI metadata for historic audit/compliance, real-time alerting and security, network performance and capacity planning. As a result, the solution helps organizations simplify compliance reporting and ensures complete visibility and detailed audit of DNS and IP address information for hybrid, multi-cloud resources across networks and geographic regions.

DNS SECURITY CLOSES SECURITY GAPS

Malware depends on DNS for communications, which provides an opportunity to detect threat activity other solutions miss. Even evasion techniques—such as 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 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 Infoblox 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

Infoblox Network Insight and Cloud Network Automation

Discover and view all assets across your hybrid, multi-cloud network

Network Insight and Cloud Network Automation ensure that you see every network asset through a single control plane. With extensive discovery, visibility, automation and management capabilities, you're empowered to establish authoritative IPAM, identify rogue devices, manage endpoints and automate device lifecycle, security and compliance.
Learn more (Network Insight)
Learn more (Cloud Network Automation)

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, improves 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 Reporting and Analytics

Gain on-demand network visibility for audit/compliance, real time alerting, network performance and capacity planning.

Built on the Splunk reporting and visualization engine, Infoblox Reporting and Analytics gives you the big picture you need to make fast, accurate decisions that profoundly affect performance, security and availability—even as your network extends across distributed onpremises, virtual and cloud infrastructure.
Learn more

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

+1.408.986.4000
www.infoblox.com

Version: 20230918v1