SOLUTION BRIEF

VULNERABILITY MANAGEMENT + BLOXONE® THREAT DEFENSE — A WINNING COMBINATION

Enhance defense-in-depth of both solutions through seamless integration

THE CHALLENGE

Vulnerability management is the process of identifying and remediating security weak points lurking in networks and applications. In today's dynamic threat environment, automation is crucial to modern vulnerability management. Using automated vulnerability scanners, SecOps teams can readily detect security flaws, insecure configurations and other issues in network infrastructure and connected assets. Despite all the capabilities of modern scanners, however, even the best ones are not designed to detect significant vulnerabilities that exploit DNS pathways.

ELEVATE VULNERABILITY MANAGEMENT EFFECTIVENESS WITH INTEGRATED DNS DETECTION AND RESPONSE

The DNS protocol plays a central role in all network communications. It is also inherently insecure, which is why it is the vector for more than 90 percent of malware and is also invoked in pervasive ransomware, data exfiltration and distributed denial of service attacks. DNS Detection and Response (DNSDR) expands the defense-in-depth of vulnerability management by identifying and remediating DNS threats that elude other security measures.

The industry's leading DNSDR solution, Infoblox BloxOne Threat Defense, integrates with top vulnerability management platforms, enhancing the capabilities of each solution and elevating overall SecOps effectiveness. It delivers these benefits by:

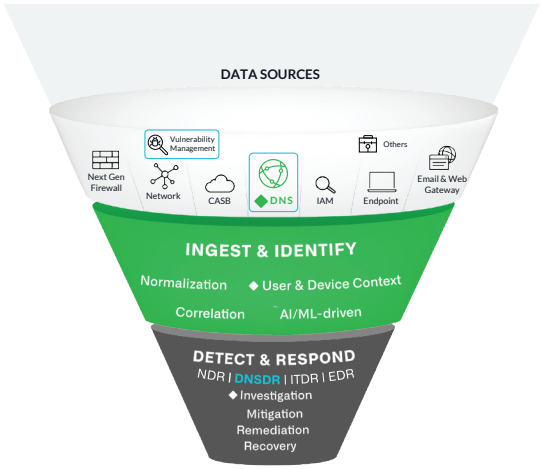
- Eliminating blindspots and empowering SecOps to perform more thorough vulnerability and compliance assessments with near real-time visibility into devices, servers and users that reveal the presence of suspect or malicious DNS-based threat activity
- Automatically notifying vulnerability management platforms when new devices and virtual workloads become active, enhancing policy enforcement
- Detecting and blocking DNS-based communications and triggering alerts for vulnerability assessments in compromised assets
- Supplying historical DNS data for troubleshooting and to automate and streamline compliance by providing up-to-date information about network devices, including non-compliant hosts

TOP VULNERABILITY MANAGEMENT PLATFORMS INTEGRATE WITH INFOBLOX

RAPID7 · Qualys. · tenable

DNSDR ENHANCES VULNERABILITY MANAGEMENT AND THE ENTIRE XDR ECOSYSTEM

DNS Visibility and Vulnerability Management Work Hand-in-Hand in the XDR Framework

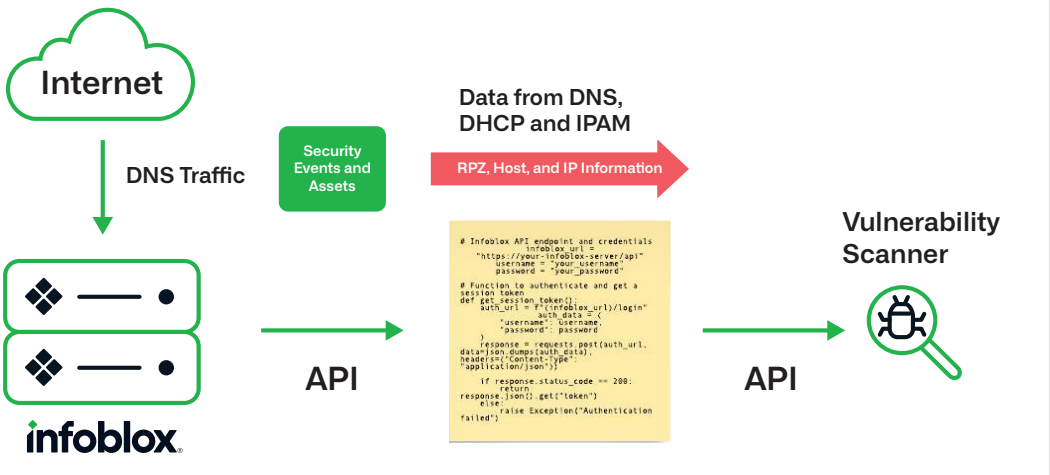


DNSDR and vulnerability management platforms are essential components of extended detection and response (XDR) solutions. DNSDR implementations like BloxOne Threat Defense improve the performance and efficiency of not only vulnerability management, but of core XDR capabilities across the security ecosystem. Through APIs and pervasive automation, BloxOne Threat Defense shares indicators of compromise (IoCs) and other verified threat intelligence with other tools and systems, enabling SecOps to reduce Mean Time to Respond (MTTR) for fast-moving cyber threats.

TOP 10 REASONS CUSTOMERS CHOOSE BLOXONE THREAT DEFENSE

1. Accelerate Time to Value
2. Detect Threats Other Solutions Miss
3. Achieve Anywhere, Hybrid Visibility and Control
4. Stop Attacks Earlier in the Attack Chain
5. Boost SecOps Efficiency
6. Speed Investigation and Response by 3X
7. Unlock the power of DNS Threat Intel
8. Optimize the Security Ecosystem
9. Get More from Security Investments
10. Gain Greater Context by Merging IPAM with DNS

HOW INFOBLOX AND VULNERABILITY MANAGEMENT INTERACT



To learn more about the benefits of our Cybersecurity Ecosystem visit https://www.infoblox.com/products/cybersecurity-ecosystem/

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