SOLUTION NOTE

BLOXONE ON-PREM HOST OS HARDENING SECURITY IMPLEMENTATION

PRODUCT PORTFOLIO:

INFOBLOX DELIVERS FOUNDATIONAL PROTECTION TO EMBED SECURITY EVERYWHERE, AUTOMATE RESPONSES AND REDUCE SECOPS WORKLOAD.

Infoblox delivers foundational protection to embed security everywhere, automate responses and reduce SecOps workloads. Automatically detect and stop the widest range of DNS attacks—attacks that many other security providers often miss—to protect your network, minimize disruptions and maximize uptime. Gain visibility, enrich your data with contextual ecosystem insights, improve threat analyst productivity, speed remediation and lower costs. With Infoblox, you can leverage industry best security practices for hardware and software design, eliminate vulnerabilities, secure systems, monitor alerts, enhance threat intelligence, and accelerate response for greater core network security visibility, control and automation. With over two decades of expertise in delivering global, reliable, enterprise-grade DNS, DHCP and IPAM (DDI), Infoblox is the industry leader in core network and security services for the data center, hybrid multi-cloud and the network edge. Over 12,000 customers in every major industry and vertical, including 70 percent of the Fortune 500, trust Infoblox to power their core network, cybersecurity, and cloud network automation services because company revenue, operations, employees, partners and—most of all, customers—depend on all of these things running reliably. Infoblox delivers modern, cloud-first networking and security services from on-premises to cloud-native solutions so you can reliably automate and secure access to apps and services anytime, anywhere.

Infoblox also offers extensive, market-leading cybersecurity ecosystem integrations with leading security vendors to automate SecOps response and efficiency. For organizations with SaaS initiatives, BloxOne® Threat Defense quickly deploys hybrid DNS-layer security everywhere to protect the data and infrastructure of the distributed enterprise. Infoblox also supplies advanced threat intelligence for better DNS and contextual and multi-sourced threat intelligence to empower your entire security stack. By establishing foundational security throughout the network, Infoblox simplifies security administration, delivers unparalleled visibility and boosts the productivity of your security staff and resources. Infoblox embeds security everywhere to automate responses and reduce the burdens on SecOps teams. Beginning with core DNS, DHCP and IPAM and extending throughout the operating system, physical and virtual layers, applications, distributed appliance deployments, security integrations, threat intelligence and ongoing support operations, Infoblox delivers foundational protection for anytime, anywhere defense.

CORE SERVICES:

Infoblox enables core network services based on the package ordered and installed on each appliance. The Infoblox software architecture uses industry best practices found in leading firewall and security solutions.

BLOXONE:

BloxOne DDI is the industry's first cloud-managed solution that enables you to centrally control and automate DNS, DHCP and IP address management (DDI) for hybrid and multi-cloud networks. Built on the cloud-native BloxOne® Platform and available as a SaaS service, BloxOne DDI eliminates the complexity, bottlenecks and scalability limitations of traditional DDI implementations. The solution delivers secure, reliable, and centrally managed DNS, DHCP, and IPAM services at each location. You can deploy BloxOne DDI across thousands of sites and reduce the total cost of ownership by leveraging low-cost hardware, virtual appliances, license pooling, and license portability. BloxOne DDI provides a secure environment for IPAM and integrated cybersecurity protection against DDoS, data exfiltration, and other DNS attacks.

BLOXONE ON-PREM SECURITY:

Infoblox Engineering performs security assessments on each release of the Infoblox product library. These assessments include vulnerability scanning, code scanning, penetration testing and other controls to detect security issues. Infoblox is committed to continual security improvements and maintains an active program to respond to product vulnerabilities and issues reported by customers or identified by our own teams.

All source code is analyzed using static code analysis, and any potential defects are resolved. All code is reviewed prior to a production deployment. For code identified as security sensitive, the review is done by both the project team and a relevant security specialist. Post-compilation security assessments are performed on the product binaries.

The BloxOne Onprem Host employs several security best practices to ensure reliability, performance, and resilience against potential security threats, including:

- Access Control:
  - By default, both local console root access and remote SSH access are disabled, ensuring stringent control over system entry points. Interacting with OS file systems or console sessions is not possible under normal circumstances.
  - For initial configuration, the web console is accessible but under strict restriction, requiring a robust password. Once configuration is complete, the web console is automatically disabled, reducing potential attack vectors.
  - Debug CLI access is similarly restricted, with a fortified password requirement. Access is limited to executing pre-approved commands, focused on essential operations like firmware upgrades and network diagnostics. For additional information, see our documentation.
- OS Hardening
  - Interactive shell access for all OS users is eradicated, bolstering security measures. BloxOne Onprem services operate within a locally hosted K3S cluster, adhering closely to Kubernetes security best practices.
  - Any superfluous Linux services, daemons, or background services are either removed or disabled, minimizing potential vulnerabilities. Additionally, unwanted SUID and SGID binaries are either eliminated or rendered inert.
- Data Protection
  - The BloxOne host environment is devoid of customer data, mitigating any risk associated with unauthorized access.
- Software Upgrades and Hotfixes:
  - BloxOne is a Software as a Service (SaaS) offering. OS kernel upgrades and hotfixes are regularly administered remotely, ensuring the system's resilience and staying ahead of potential vulnerabilities.

- Data Communication
  - All data transmitted to and from the Application Host is meticulously encrypted, utilizing HTTPS and Secure gRPC connections, fortifying the integrity of data in transit.
  - The BloxOne Onprem host fortifies its defenses against network-based attacks by employing a meticulously crafted network firewall implementation grounded in iptables. This robust setup serves as a formidable barrier, strategically configured to thwart any unauthorized access attempts and malicious activities traversing the network.
- Vulnerability Management and Security Hotfixes
  - Infoblox vulnerability management program is diligently maintained, complemented by routine penetration testing to uncover and mitigate potential weaknesses. Any identified security hotfixes are promptly deployed to BloxOne OnPrem hosts remotely, preserving system integrity.

infoblox

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

Version: 20240628v1