DATASHEET

Infoblox Threat Defense™ Essentials

Protective DNS powered by predictive threat intelligence protects everything, everywhere—before impact

PROTECT BEFORE IMPACT WITH FOUNDATIONAL DNS SECURITY

Protecting infrastructure, data and users is more challenging than ever. Traditional, reactive security models can no longer keep up. Today's threats are faster, smarter and designed to bypass conventional defenses.

- AI-enabled attacks like lookalike domains, smishing, multi-factor authentication (MFA) bypass and targeted phishing are evolving too quickly for legacy tools to stop.
- The perimeter is gone. Users now connect directly to cloud apps from anywhere, leaving gaps traditional tools were not built to address.
- SD-WAN and branch locations often connect to the internet directly, bypassing centralized inspection points.
- IoT and unmanaged devices create blind spots that endpoint security alone cannot protect.
- Most legacy tools rely on detecting known malware or filtering content—reactive approaches that are too slow for today's attackers.

To stay ahead, organizations need **scalable, preemptive protection at the DNS layer.** Infoblox delivers foundational DNS security that identifies and blocks threats before they reach endpoints, cloud workloads or branch locations. With unmatched visibility, predictive intelligence and seamless integration into your broader security stack, Infoblox helps reduce alert noise, simplify operations and prevent attacks before they cause damage.

PROTECTIVE DNS SECURITY AT SCALE

Modern networks span across on-premises infrastructure, remote users, multi-cloud environments and distributed IoT. As your architecture evolves, your security needs to scale with it—without adding operational complexity.

Infoblox Threat Defense™ delivers centralized, DNS-layer security that adapts to wherever your users and workloads reside. Whether you are protecting data centers, securing cloud workloads or enabling SD-WAN and remote access, Infoblox applies consistent protection and policy enforcement across every location.

With lightweight deployment options and unified management, security teams can protect more, respond faster and reduce gaps across their infrastructure. Infoblox provides visibility and control across all environments, so you can confidently scale without compromise.

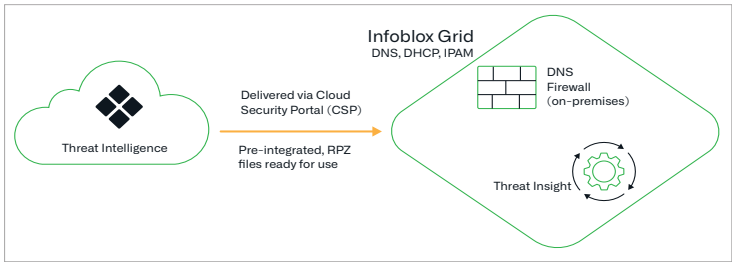

Figure 1. Infoblox Threat Defense Essentials architecture

KEY CAPABILITIES

Preempt Modern Malware Threats
Stop ransomware, phishing and other malware early by identifying attacker infrastructure and blocking threats before they reach endpoints or spread across your network.

Bolster Defenses Everywhere
Protect remote users, cloud workloads, branch offices and IoT devices using your existing DNS infrastructure, without agents or new security hardware.

Gain Visibility across Your Network
Correlate DNS activity with asset and IP address management (IPAM) data to surface threats faster, reduce false positives and improve response across hybrid environments.

Simplify Investigations
Leverage an easy-to-use threat lookup tool and enriched asset data.

Offload Strained Security Devices
Block threats before they hit your firewalls, IPSs and web proxies. Reduce traffic to perimeter tools by up to 60x using Infoblox DNS as your first layer of defense.

Integrate across Your Ecosystem
Automatically share threat intelligence and logs with next-generation firewall (NGFW), IPS, SIEM, SOAR, endpoint or other security tools.

UNLOCK THE POWER OF DNS-BASED THREAT INTELLIGENCE

The following curated threat intelligence feeds are included as part of the Infoblox Threat Defense Essentials package. These feeds enhance protection at the DNS layer by blocking known malicious domains and preventing common evasion tactics.

Infoblox Base: Delivers protection against known malicious or compromised domains, including those associated with malware, ransomware, APTs, exploit kits, sinkholes and malicious name servers. This feed enables foundational DNS-layer security and is recommended for blocking across all users.

Bogon: Blocks IP addresses from unallocated or reserved IP space—commonly referred to as "bogon space." These IPs are frequently observed as the source of distributed denial-of-service (DDoS) attacks and other spoofing threats. Because they serve no legitimate purpose, bogon IPs are often filtered by ISPs and security devices to eliminate unwanted traffic caused by misconfiguration or malicious intent.

DHS AIS IP and DHS AIS Hostname (Two Feeds): These feeds are based on indicators shared through the Department of Homeland Security's (DHS) Automated Indicator Sharing (AIS) program. They include high-velocity, unvalidated cyberthreat indicators sourced from both government and private sector participants. Infoblox classifies and normalizes this data to simplify consumption but does not alter the core content.

Use of this data is subject to the U.S. DHS AIS Terms of Use, available at www.us-cert.gov/ais. Prior to further distributing the AIS data, you may be required to sign and submit the Terms of Use. For more information, contact ncciccustomerservice@hq.dhs.gov.

DoH Public Hostnames and IPs Feeds (Two Feeds): These policy-based feeds include the domain names and IP addresses of public DNS over HTTPS (DoH) resolvers. Organizations that enforce security policies at the DNS layer may wish to block these to prevent users or endpoints from bypassing DNS security via third-party DoH services.

To learn more about the ways that Infoblox Threat Defense secures your data and infrastructure, please visit https://www.infoblox.com/products/threat-defense/.

> *"Sharing information among a user, community and getting collective intelligence on attack vectors and methods keeps victims from having to ask, 'Is it just us, or is someone else getting hit by this attack?' "*
>
> **Elderwood Data Breach**

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: 20250722v3