DATASHEET

Infoblox Threat Defense™ Business Cloud

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

As modern networks expand across data centers, SD-WAN, cloud services and IoT infrastructure, maintaining consistent security coverage becomes more complex—but more critical than ever.

Infoblox Threat Defense™ Business Cloud delivers scalable, cloud-native DNS security that strengthens your posture from the ground up by securing your current environment and evolving digital initiatives without adding operational overhead. Whether protecting on-premises DNS, extending visibility into distributed branches or supporting remote users, Infoblox delivers DNS-layer enforcement where you need it.

KEY CAPABILITIES

- Preempt modern threats by blocking ransomware, phishing, exploits and malware using real-time threat intelligence.
- Prevent data exfiltration with analytics and machine learning, stopping DNS tunneling, domain generation algorithms (DGAs), DNSMessenger and fast-flux activity.
- Protect all devices, on or off-network, managed or unmanaged (bring your own device (BYOD), IoT, OT)—at the DNS layer.
- Enforce content policies with web filtering and user-based access controls.
- Protect your brand with Lookalike Domain Monitoring that detects and enables takedown of malicious domain impersonations.
- Accelerate investigations by up to three times with enriched DNS telemetry and threat context.
- Enhance visibility by correlating DNS activity with IP address management (IPAM) asset metadata for faster, more accurate incident response.
- Prioritize and respond faster to critical threats with SOC Insights and AI-driven investigation support.
- Integrate across your ecosystem by automatically sharing threat intelligence and logs with SIEM, SOAR, next-generation firewall (NGFW), IPS, endpoint and other security tools.

With real-time threat intelligence, unified visibility and integration with SOAR and SIEM tools, security teams can detect, prioritize and respond faster. This reduces time to resolution, improves the performance of your existing security stack and lowers the total cost of enterprise threat defense.

Delivered from the cloud, Infoblox Threat Defense Business Cloud scales effortlessly to match changing customer needs, without adding operational complexity. As demands grow across users, sites and workloads, security expands with you automatically.

THE INFOBLOX SAAS ADVANTAGE

Infoblox Threat Defense Business Cloud is a software-as-a-service (SaaS) solution that brings next-generation security capabilities to your existing on-premises infrastructure. Cloud-based and elastically scalable, the solution enables:

- Immediate improvement of a company's security posture
- Easy security coverage for all devices, everywhere
- Minimized IT overhead

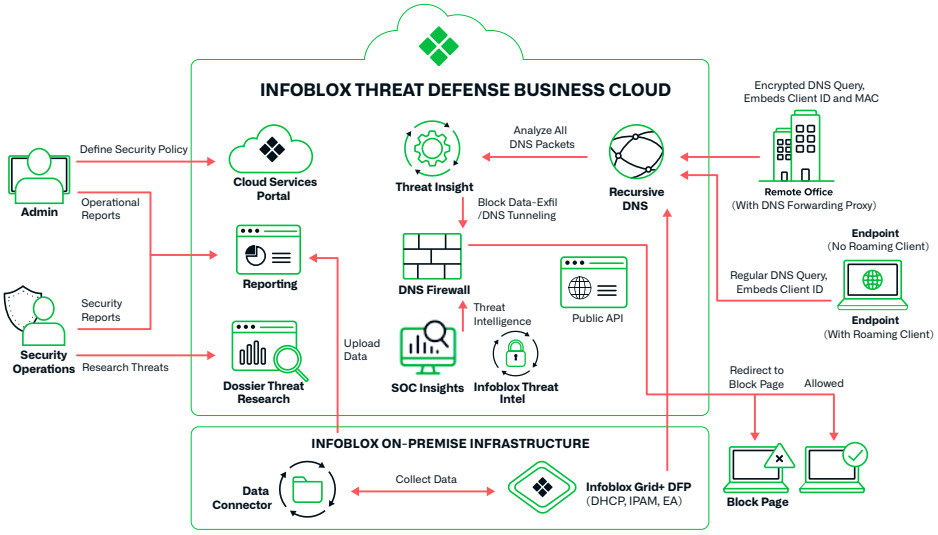

Figure 1. Workflow scenario for Infoblox Threat Defense Business Cloud

> *"In this day and age there is way too much ransomware, spyware and adware coming in over links opened by internet users. The Infoblox cloud security solution helps block users from redirects that take them to bad sites, keeps machines from becoming infected and keeps users safer."*
>
> **Senior System Administrator and Network Engineer, City University of Seattle**

DNS FORWARDING PROXY

For environments where installing an endpoint agent is not possible—such as IoT, printers or legacy systems—Infoblox provides a DNS Forwarding Proxy (DFP) to maintain device-level visibility and policy enforcement.

This lightweight virtual appliance embeds the original client IP into DNS queries before forwarding them to the Infoblox cloud. This ensures accurate source attribution, threat protection and consistent enforcement—without requiring local agents.

Integrated with Infoblox NIOS 8.3 and above, the proxy allows existing customers to activate cloud-based DNS security with no additional on-premises infrastructure or software deployments.

The Infoblox Endpoint Agent provides secure DNS-layer protection for roaming devices—ensuring visibility and control even when users work off-network.

This lightweight agent can be installed on laptops or workstations to ensure visibility and policy enforcement even when devices are off the corporate network.

- Redirects DNS queries to the Infoblox cloud for inspection and enforcement.
- Encrypts traffic and tags each query with device identity and user context.
- Enables user-level attribution for incident investigation and reporting.
- Automatically switches to bypass mode when the device is inside a protected corporate network.

Together with DNS Forwarding Proxy, the Endpoint Agent gives organizations full coverage across users, devices and environments—without gaps in visibility or protection.

BUILT-IN

Availability

Infoblox Threat Defense Business Cloud delivers 99.999% DNS uptime (excluding maintenance), with global Anycast delivery, daily backups and 24/7 monitoring.

Security

All DNS queries and stored data are encrypted in transit and at rest. Access controls support restrictions by role, IP and location.

Privacy

Infoblox follows security best practices—applying regular patching, code analysis and penetration testing. Customer data is logically separated, authenticated via unique API keys and never shared with third parties.

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

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

+1.408.986.4000
www.infoblox.com

Version: 20250723v1