infoblox.

Infoblox Threat Defense Package Tier Comparison

The information in this comparison highlights key differences in the Infoblox Threat Defense product line to help you understand which package can best meet your unique visibility and security needs and priorities.

Features & Capabilities	DNS FW w/NIOS 9.x on X6	Essentials	Business On-Premises	Business Cloud	Advanced
On-Premises DNS Firewall	Per Appliance	Per Appliance	Grid Wide		Grid Wide
Cloud-based DNS Firewall[3]				X	X
DNS Forward Proxy				X	X
DNS over HTTPS risk management		X	X	X	X
Block DNS Data Exfiltration, DNS Tunneling		X	X	X	X
Zero Day DNS™					X
Block Malicious Domains *(malware, C2, phishing, etc.)*		X	X	X	X
File-less Malware *(i.e. DNSMessenger)*		X	X	X	X
Detect Inline DGA, Dictionary DGA, etc.[3]				X	X
Block inappropriate or unwanted websites[3]				X	X
Lookalike Domain Monitoring[1,3]					X

Continued...

Features & Capabilities	DNS FW w/NIOS 9.x on X6	Essentials	Business On-Premises	Business Cloud	Advanced
Application Discovery[3]					X
SOC Insights – Configuration/ Health[3]				X	X
SOC Insights – Security[3] *(add-on option)*				X	X
Threat Insight		X	X	X	X
Infoblox Threat RPZ feeds (On-Premises)[2,4]		Base feeds, DOH, Bogon, DHS	Base feeds, Base IP feeds, Informational feeds, DOH, Bogon, DHS, EECN, US OFAC Sanctions, cyrptocurrency, TOR Exit		Base feeds, Base IP feeds, Informational feeds, DOH, Bogon, DHS, EECN, US OFAC Sanctions, cyrptocurrency, TOR Exit, High risk, Medium risk, Low risk
Infoblox Threat Feeds (Cloud)[2]				Base feeds, Base IP feeds, Informational feeds, DOH, Bogon, DHS, EECN, US OFAC Sanctions, cyrptocurrency, TOR Exit	Base feeds, Base IP feeds, Informational feeds, DOH, Bogon, DHS, EECN, US OFAC Sanctions, cyrptocurrency, TOR Exit, High risk, Medium risk, Low risk
TIDE[3] *(ingest & distribute custom feeds)*					X
Ecosystem *(data sharing and response automation)*		Available	Grid Wide	Cloud Data Connector Only	Grid Wide

Continued...

Features & Capabilities	DNS FW w/NIOS 9.x on X6	Essentials	Business On-Premises	Business Cloud	Advanced
Threat Lookup to research attacker data		"a la carte"	X	X	X
Dossier for contextual & detailed threat intelligence (queries per year)		X	32,000	32,000	64,000
Infoblox Endpoint[3] *(Mac, Windows, & Chromebook; Mobile: iOS & Android)*				X	X

1 - Also available as a standalone product. Refer to the Lookalike Domain Monitoring Solution Note.
2 - A complete breakdown of available threat feeds available for each package is available in the Infoblox Threat Intel Solution Note.
3 - This feature requires a cloud or hybrid deployment.
4 - For those considering a pure on-premises deployment, the physical appliance may limit the total number of RPZs/feeds that can be supported.

On-Premises vs Cloud/Hybrid Deployment Considerations

Infoblox offers a range of appliances to support on-premises or hybrid deployments. However, for purely on-premises deployments, customers should be aware of capabilities that are unavailable without the cloud.

- **Cloud-dependent features:** Endpoint security, SOC Insights, Lookalike Domain Monitoring, Application Discovery, Threat Intel Data Exchange (TIDE), and the ability to control unwanted or inappropriate websites.
- **Cloud-dependent threat detection capabilities:** Zero Day DNS, DGA detection (both static and dynamic), and unique detections available through SOC Insights analytics. (Spearphishing, Botnet Discovery, NXDomain, Outlier, Open Resolvers, Major Atack, and Lookalike Threat)
- **RPZ/Feed support limitations** based on physical appliance specifications. In determining which appliance to purchase, it is critical to assess the requirements of desired RPZs/feeds and identify the appliance(s) that will support immediate and long-term plans. It is important to note that the number of threat indicators/feeds in the Infoblox solution continues to grow significantly monthly as we identify new threat actors and their extensive networks. So, when choosing a pure on-premises deployment, purchasing an appliance with future-proofing capacity in mind is critical.

NIOS 9.x on Trinzic X6 Use Cases for the On-Premises DNS Firewall

The latest Trinzic X6 appliance platform runs NIOS 9 or higher and includes a license for the on-premises DNS Firewall with RPZ (Response Policy Zones) support. This license primarily provides customers with a simple redirection capability to support use cases such as standards enforcement during M&A activities or redirecting public cloud/multi-cloud API calls to preferred or more trusted locations. The use of RPZs makes redirection setup and management easy while helping to mitigate the human errors common with more manual approaches.

For a pure security use case, customers can provide their own threat intelligence to the DNS Firewall, using it as a first line of defense to block access to malicious domains. For a more robust DNS Detection and Response solution, customers should consider one of the Infoblox Threat Defense packages. In addition to expanded, managed threat intelligence, Threat Defense customers can benefit from behavioral analytics (Threat Insight), proactive threat intelligence (such as Zero Day DNS), data tunneling/exfiltration detection, lookalike domain monitoring, AI-driven analytics (via SOC Insights), the Dossier threat research portal, and much more.

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: 20250203v4