

Infoblox BloxOne Threat Defense helps protect users on and off the network from malware, advanced threats, DNS attacks, and more. It is designed to [integrate with the security solutions you already have](#) using a [large partner ecosystem](#) and REST APIs for custom integrations with 3rd party products. And it [works with your current network architecture](#), without modification, through on-premises, cloud, and hybrid deployment options. BloxOne Threat Defense is a scalable, reliable platform that can help unify your defenses with shared threat intelligence, [response automation](#), and more to realize the benefits of next level networking.

The information in this comparison highlights key differences in the BloxOne Threat Defense product line, which your sales representative can help you understand, personalize, and prioritize for the best options.

Features & Capabilities	Essentials	Business On-Premises	Business Cloud	Advanced
DNS Firewall	Per Appliance	Grid Wide		Grid Wide
Cloud-based DNS Firewall			X	X
DNS over HTTPS risk management	X	X	X	X
Block DNS Data Exfiltration, DNS Tunneling	X	X	X	X
Block Malicious Domains <i>(malware, C2, phishing, etc.)</i>	X	X	X	X
File-less Malware <i>(DNSSmessenger)</i>	X	X	X	X
Detect Inline DGA, Dictionary DGA, etc.		X	X	X
Block inappropriate or unwanted websites			X	X
Custom Lookalike Domain Monitoring				X
Threat Insight On-Premises	Per Appliance	Grid Wide		Grid Wide
Threat Insight in the Cloud		X	X	X
Infoblox Threat (RPZ) feeds	Basic (9)	Intermediate (20)	Intermediate (20)	Advanced (27)
TIDE <i>(Ingest & Distribute custom feeds)</i>				X
Ecosystem <i>(data sharing and response automation)</i>	Available "a la carte"	Grid Wide	Cloud Data Connector Only	Grid Wide
Threat Lookup to research attacker data	X	X	X	X
Dossier for contextual & detailed threat intelligence <i>(queries per year)</i>		32,000	32,000	64,000
BloxOne Endpoint (Mac & Windows)			X	X



BloxOne™ Threat Defense Solution Comparison

July 2020

One of the most important factors when selecting a security solution is understanding the [threat intelligence](#) behind it. BloxOne Threat Defense offers a wide range of threat feeds, curated by the [Infoblox Cybersecurity Intelligence Unit](#), and the TIDE feature provides the ability to ingest additional feeds so customers can leverage their own custom blend of feeds to meet personal, industry, regional or other requirements. TIDE can also distribute the resulting ‘super feed’ across the security stack to further help customers enjoy a stronger, more unified defense without affecting your current security investment. Here are the threat feeds available directly from Infoblox for each BloxOne Threat Defense solution.

BLOXONE THREAT DEFENSE ESSENTIALS (9)				
<ul style="list-style-type: none"> • Base Hostnames • Anti-malware • Ransomware 	<ul style="list-style-type: none"> • Bogon • DHS_AIS_IP • DHS_AIS_Hostname 	<ul style="list-style-type: none"> • DHS AIS NCCIC Watch list Hostnames and Domains 	<ul style="list-style-type: none"> • DHS AISNCCIC WatchlistIPs 	<ul style="list-style-type: none"> • DoHPublic IPs and Hostnames
BLOXONE THREAT DEFENSE BUSINESS ON-PREMISES AND BUSINESS CLOUD (20)				
<ul style="list-style-type: none"> • Base Hostnames • Anti-malware • Ransomware • Bogon • DHS_AIS_IP 	<ul style="list-style-type: none"> • DHS_AIS_Hostname • DHS AIS NCCIC Watch list Hostnames and Domains • DHS AISNCCIC WatchlistIPs 	<ul style="list-style-type: none"> • DoHPublicIPs and Hostnames • Malware IPs • Bot IPs • Exploit KitIPs 	<ul style="list-style-type: none"> • MalwareDGA hostnames • TORExitNodeIPs • SURBLMulti domains • SURBL Multi Lite domains 	<ul style="list-style-type: none"> • SURBLFresh domains • USOFACSanctions IPs • EECN IPs • Cryptocurrency hostnames and domains
BLOXONE THREAT DEFENSE ADVANCED (27)				
<ul style="list-style-type: none"> • Base Hostnames • Anti-malware • Ransomware • Bogon • DHS_AIS_IP • DHS_AIS_Hostname • DHS AIS NCCIC Watch list Hostnames and Domains 	<ul style="list-style-type: none"> • DHS AISNCCIC WatchlistIPs • DoHPublicIPs and Hostnames • Malware IPs • Bot IPs • Exploit KitIPs • MalwareDGA hostnames 	<ul style="list-style-type: none"> • TORExitNodeIPs • SURBLMulti domains • SURBL Multi Lite domains • SURBLFresh domains • USOFAC Sanctions IPs • EECN IPs 	<ul style="list-style-type: none"> • Cryptocurrency hostnames and domains • Extended Base & anti-malware Hostnames • Extended malware IPs • Extended TOR Exit Node IPs 	<ul style="list-style-type: none"> • Extended Ransomware IPs • Extended Exploit Kits IPs • SpamBot IPs • SpambotIPsDNSBL

Refer to the Infoblox [Threat Intelligence Solution Note](#) for more information on threat feeds.