Authoritative IP and DNS/DHCP management as a single pane of glass and a "hub" for sharing actionable intelligence and data enrichment with the security ecosystem.

Advanced DHCP service that fingerprints endpoints to provide context and lease history.

Infoblox Internal DNS (recursive and authoritative) with security capabilities based on reputation, signatures, and behavioral analysis. Can be deployed in public or private cloud infrastructure.

Recursive Infoblox DNS (for Internet name resolution) with security capabilities based on reputation, signatures, and behavioral analysis.

Infoblox provides consistent, high-quality threat intelligence information and feeds for consumption not only by Infoblox products, but by any component that form part of your security ecosystem. For Data Protection and Malware Mitigation, this will focus on reputation, signatures, and heuristics that disrupt the kill chain.

ActiveTrust® Cloud provides an advanced cloud-based DNS resolution service that incorporates threat intelligence, reputation, and behavioral analytics.

Infoblox Solutions

Cloud Infrastructure e.g. AWS/Azure

Secure Internal DNS

Internet Authoritative DNS

Cloud-based Recursive/Caching (ActiveTrust® Cloud)

External Perimeter

Internal Perimeter

Proxies and Secure Gateways

DNS Traffic

Good DNS Traffic

Bad DNS Traffic

Communication Flow

Threat Intelligence

Cloud service used for threat intelligence

Threat data feeds for use across the security ecosystem, including SIEM, NGFW, proxies, etc.

Advanced threat data from ATP/Malware detection

Actionable Intelligence

Security events with context such as syslog messages and outbound API notifications

Data Enrichment

Authenticated user data (from NAC and AD)

DNS name of malicious client

DHCP fingerprinting, MAC, etc.

Contextual network data (including DNS, DHCP, IP, L3/L2, and User Data) via APIs

Network Discovery

Discovery of switches, routers

Discovery of attached endpoints

Discovery of virtual infrastructure