Infoblox
CONTROL YOUR NETWORK

ActiveTrust®

DATASHEET

Summary

Infoblox ActiveTrust® proactively detects and prevents cyberthreats. ActiveTrust bundles Infoblox DNS Firewall, InfoBlox Threat Insight in the Cloud, Infoblox Threat Intelligence Data Exchange (TIDE), and Infoblox Dossier. The solution prevents data exfiltration and malware command-and-control (C&C) communications via DNS, centrally aggregates curated internal and external threat intelligence, distributes validated threat data to the customer's security ecosystem for remediation, and enables rapid investigation to identify context and prioritize threats.

Key Features

- Infoblox Threat Insight in the Cloud detects DNS based data exfiltration and newer threats such as DNSMessenger, DGA, and Fast Flux. Threat Insight is the only DDI solution that leverages reputation, signatures and behavioral analytics to detect DNS based data exfiltration
- Infoblox DNS Firewall executes administrator-defined policy action (block, redirect device to a walled garden site, and/or log event) to help stop devices anytime, anywhere from communicating with C&Cs or botnets via DNS
- Infoblox Threat Intelligence Data Exchange (TIDE) collects and manages curated threat intelligence from internal and external sources in a single platform. It enables security operations to remediate threats more rapidly by sharing normalized TIDE data in real time with third-party security systems such as Palo Alto Networks, SIEM, etc
- Infoblox Dossier is a threat investigation tool that provides immediate threat context and allows threat analysts to save precious time, shortening the attack window for criminals
- Integration with Security Ecosystem Integration with third-party security systems extends the unique visibility we have into DNS to other security systems such as Qualys and Carbon Black

Security Challenges

Internet communications, including malware, rely on DNS. Attackers are taking advantage of DNS as a data-exfiltration and malware control point. Over 91 percent of malware uses DNS for data exfiltration and to communicate with C&C servers or redirect traffic to malicious sites. Existing security controls such as firewalls, email proxies, and web proxies rarely focus on DNS and associated threats.

Using unverified threat data residing in silos in your cybersecurity infrastructure is like trying to pick out instruments in an orchestra that is playing outdoors in the midst of rush-hour traffic. The noise blocks out everything you really want to hear. Low-quality data creates nuisance red flags that threat analysts still must track down. They can easily be swamped by false-positives, leaving them unable to detect and prevent genuine threats.

To research information and gather context about threats, analysts must go to multiple tools. The process is manual and time consuming, which slows response and often requires high levels of expertise. In addition, they often lack a centralized tool for threat investigation that aggregates threat and indicator data from multiple sources and quickly shares context.

The Infoblox Solution

Intercepting DNS traffic is an ideal approach to counter DNS-based data exfiltration and malware communications with C&C sites. In addition, it is an ideal approach for devices on which endpoint agent software cannot be deployed (e.g. POS, medical equipment, certain IoT devices, etc.). ActiveTrust is a highly efficient, scalable solution that offers:

Infoblox DNS Firewall for prevention of malware communications with C&C sites and botnets

In**foblox Threat Insight in the Cloud** prevents (with DNS firewall) DNS-based data exfiltration by uniquely leveraging reputation, signatures, and behavioral analytics. It is also able to block (using DNS firewall) newer threats such as DNSMessenger, DGA, and Fast Flux. Threat Insight in the Cloud is offered as a service to scale in the cloud and is bundled with ActiveTrust Plus and ActiveTrust Advanced.

Infoblox
CONTROL YOUR NETWORK

ActiveTrust®

DATASHEET

Infoblox Threat Intelligence Data Exchange (TIDE) leverages highly accurate machine-readable threat intelligence (MRTI) data to aggregate and selectively distribute data across a broad range of security infrastructure. Our threat intelligence team curates, normalizes, and refines the high-quality threat data to minimize false positives. Our threat feeds begin with information gained from native investigations and harvesting techniques. We then combine them with verified and observed data from trusted partners including government agencies, academic institutions, several premier Internet infrastructure providers, and law enforcement. The end result is a highly refined feed with a very low historical false-positive rate.

Infoblox Dossier threat indicator investigation provides rich threat context to prioritize incidents and respond quickly.

	ActiveTrust Standard	ActiveTrust Plus	ActiveTrust Advanced
Annual Subscription Licensed by	Appliance by model	Organization-wide by number of protected users	Organization-wide by number of protected users
Infoblox DNS Firewall Zones (RPZs)	Standard (6)	Standard (6) + Advanced (7) + SURBL (3)	Standard (6) + Advanced (13) + SURBL (3)
Infoblox Threat Insight in the Cloud	Not available	Included	Included
Infoblox Data via Threat Intelligence Data Exchange	Not available	One of: ☐ Hostnames ☐ IP Addresses ☐ URLs	All of: ☑ Hostnames ☑ IP Addresses ☑ URLs
Infoblox Dossier	No (threat lookup via Cloud Services Portal only)	32,000 queries/year (supports 2 analysts)	65,000 queries/year (supports 4 analysts)
Third-party Data via Infoblox Threat Intelligence Data Exchange (TIDE)	Not available	Available a la carte	Available a la carte
Hardware Requirements	If you intend to use Infoblox DNS Firewall for RPZ-based policy enforcement, you need to buy: One or more Infoblox Trinzic (physical) or vNIOS (virtual) appliances with DNS with recursion enabled. Trinzic models: IB Series: IB-800, IB-1400, IB-2200, IB-4000, and IB-4030 PT Series: PT-1400/1405, PT-2200/2205, and PT-4000 TE Series (physical and virtual appliances): TE-100, TE-810/815/820/825, TE-1410/1415/1420/1425, TE-2210/2215/2220/2225, and TR-4010/TR-4010-10GE		
Software Requirements	• If you want Threat Insight in the Cloud, then you can purchase either ActiveTrust Plus or ActiveTrust Advanced license. If you will NOT deploy ActiveTrust threat intelligence data on third-party infrastructure, then buy an ActiveTrust Standard license, which is based on the Trinzic appliance models. • If you intend to deploy ActiveTrust threat intelligence data on third-party infrastructure (e.g. next-generation firewall, SIEM, Web proxy), then you can buy either ActiveTrust Plus or ActiveTrust Advanced license. The license is based on total number of protected users' organization-wide (Grid-wide license). The two products vary based on the amount of data sets that can be applied and total number of annual Dossier threat indicator queries that can be transacted.		

Optional Services	• Infoblox Threat Insight (on premises) for protection against DNS tunneling and sophisticated data exfiltration techniques is available as a separate standalone option for purchase for all AT customers.
	  - Note: this only works on the following Infoblox models: PT-1405, TE-1415/V1415, TE-1425/V1425, TE-2210/v2210, 2215/v2215, TE-2220/v2220, 2225/v2225, PT-2200, PT-2205, IB-4010/v4010, V4015, TE-V4010/V4015, PT-4000, IB-4030-DCAGRID-AC/DC, IB-4030-DCAGRID-T1-AC/DC, IB-4030-DCAGRID-T2-AC/DC, and IB-4030-DCAGRID-T3-AC/DC.
	• Infoblox Security Ecosystem license enables integration of Infoblox DNS RPZ/Firewall with third-party security systems: FireEye, Qualys and threat intelligence platforms.
	• Infoblox Dossier (portal, 65,700 queries package) 1-year subscription
	  - ActiveTrust Standard customers can purchase if they want to perform threat investigation, since Dossier is not bundled with ActiveTrust Standard.
	  - ActiveTrust Plus and ActiveTrust Advanced customers that need additional queries beyond what is provided in the base product can also purchase this:
	  - Third-party marketplace threat feeds
	  - Prerequisite: ActiveTrust Plus or ActiveTrust Advanced must be purchased in order for customers to purchase and subscribe to one or more 3rd party marketplace threat feeds
	  - Does NOT Include Maintenance/Support
	• Infoblox Reporting and Analytics (appliance) – provides rich reporting on Infoblox DNS Firewall (top RPZ hits, top malicious hostnames, users)

Note: The SURBL (an Infoblox premium threat intelligence data partner) OEM license is bundled with the ActiveTrust Plus and ActiveTrust Advanced bundles for use by Infoblox DNS Firewall. The Infoblox ActiveTrust and SURBL data sets (Multi-domain and Multi Lite domain) are complementary and if used together, can enable increased threat coverage. To learn more about the Infoblox threat intelligence data, please refer to the solution note "Overview of Infoblox Threat Intelligence for ActiveTrust" on the Infoblox website.

Key Benefits

With Infoblox ActiveTrust, you get actionable network intelligence with flexible threat intelligence integrated into your DDI enthronement. this enables you to proactively detect, investigate, prioritize, remediate, and prevent cyber threats.

Prevent DNS-based Data exfiltration at Scale in the Cloud

With Threat Insight in the Cloud, you can detect and block (with DNS Firewall) DNS-based data exfiltration using a combination of reputation, signature, and behavioral analysis.

Detect and Block DNSMessenger, DGA, and Fast Flux

Offered as a service, Threat Insight in the Cloud can also detect and block (with DNS Firewall) new threats such as DNSMessenger, DGA, and Fast Flux.

Stop DNS-based Malware C&C/botnet Communications

With Infoblox DNS Firewall, you gain proactive network protection against fast-evolving, elusive malware threats that exploit DNS to communicate with C&C sites.

Infoblox
CONTROL YOUR NETWORK

ActiveTrust®

DATASHEET

Collect and Manage Curated Threat Intelligence from Internal and External Sources in a Single Platform
Infoblox TIDE enables you to aggregate, normalize, and manage internal and multiple third-party threat intelligence data in a single location, preventing siloed and disjointed threat intel.

Improve Security Posture by Sharing Curated Threat Intelligence Data in Real Time with Security Ecosystems
Creating custom API data feeds built for specific use cases is quick and easy. Combine threat data from all your sources, use contextual metadata to select the relevant subset, and leverage the right format such as JSON, STIX, CSV, CEF, and RPZ to RPZ to improve the security posture and situational awareness of your existing security ecosystem, such as NGFW, IPS, web proxy, and SIEM.

Extend the Unique Visibility Infoblox Provides into DNS such as Indicators of Compromise (IoCs) to Other Security Systems
Infoblox provides the unique visibility into DNS data as the market-leading vendor of DDI that other vendors cannot match. DNS data such as indicators of compromise (IoC) can be shared with other security systems such as vulnerability scanners (Qualys and Rapid7) to kick off a scan when a new device comes on the network to determine whether it is malware infected.

Expedite Threat Investigation to Free Up Security Personnel and Provide Timely Access to Context for Threat Indicators
Use the Infoblox Dossier research tool as a single source of truth to rapidly understand the types of threats happening on your network, where they are coming from, and the risks they pose to your organization, including understanding the data source, threat severity, and priority. Gain insight into questionable activities related to inbound or outbound network communications. Furthermore, quickly learn about and understand what a variety of trusted sources report about the indicator in question to improve the operational efficiency of scarce security operations resources, saving you time and effort.

About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

Corporate Headquarters: +1.408.986.4000 1.866.463.6256 (toll-free, U.S. and Canada) info@infoblox.com www.infoblox.com