Infoblox
CONTROL YOUR NETWORK

ActiveTrust®

DATASHEET

Summary

Infoblox ActiveTrust bundles Infoblox DNS Firewall, Infoblox Threat Intelligence Data Exchange (TIDE) and Infoblox Dossier. The solution prevents malware C&C communications via DNS, centrally aggregates curated internal and external threat intelligence, distributes threat data to the customer's existing security infrastructure, and investigates for rapid threat context and prioritization.

Key Features

- Infoblox Threat Intelligence Data Exchange (TIDE): Collect curated threat intelligence data from internal and external third-party sources.
- Simple integration into Infoblox DDI infrastructure: Apply ActiveTrust threat intelligence data to DNS Firewall to block endpoint communications to C&Cs and botnets.
- Distributing TIDE: Push threat intel data selectively to internal infrastructure and cybersecurity ecosystem.
- Dossier tool for easier threat investigation: Use a Google-like threat indicator investigation tool to get immediate threat context and analyze threats rapidly.

Security Challenges

Internet communications, including malware, rely on DNS. Attackers are taking advantage of DNS as a malware control point. Over 91% of malware uses DNS to communicate with the command and control (C&C) server 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 which 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 makes response slow 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 malware. 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 purpose built, highly efficient, scalable solution that offers DNS Firewall for malware containment, automatically prevents device communications with C&Cs/botnets, and helps accelerate remediation by informing the existing security infrastructure.

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. The 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, academics, several premier Internet infrastructure providers, and law enforcement. The end result is a highly refined feed with a very low historical false-positive rate.

ActiveTrust also includes the Infoblox Dossier threat indicator investigation tool that provides rich threat context to prioritize incidents and respond quickly.

The following table shows the three ActiveTrust bundles.

	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
Zones (RPZs)	Standard (4)	Standard (4) + Advanced (5) + SURBL (2)	Standard (4) + Advanced (5) + SURBL (2)
Infoblox Data via Threat Intelligence Data Exchange	Not available	One of: □ Hostnames □ IP Addresses □ URLs	All of: ☑ Hostnames ☑ IP Addresses ☑ URLs
Dossier	No (threat lookup via Cloud Services Portal only)	32,000 queries/year (supports 2 analysts)	65,000 queries/year (supports 4 analysts)
3rd Party Data via Threat Intelligence Data Exchange	Not available	Available a la carte	Available a la carte

Hardware Requirements	If you will 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, and IB-4000 • PT Series: PT-1400, PT-2200, and PT-4000
Software Requirements	• If you will NOT deploy ActiveTrust threat intelligence data on 3rd party infrastructure, then buy an ActiveTrust Standard license, which is based on the Trinzic appliance model(s). • If you will deploy ActiveTrust threat intelligence data on 3rd 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 # 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 # of annual Dossier threat indicator queries that can be transacted.
Optional Services	• Infoblox Threat Insight - for protection against DNS tunneling and sophisticated data exfiltration techniques - Note: this only works on the following Infoblox Trinzic models: IB-1400 or higher, PT-1400 or higher. • Infoblox Security Ecosystem license - enables integration of Infoblox DNS RPZ / Firewall with 3rd 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 • 3rd party marketplace threat feed(s) - 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 usage by Infoblox DNS Firewall. The Infoblox ActiveTrust and SURBL data sets 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, customers get Actionable Network Intelligence (ANI) with flexible threat intelligence integrated into their DDI enthronement. Customers can therefore proactively detect, investigate, prioritize, remediate, and prevent cyberthreats.

Confidently Act on Threats with Trusted Data

With Infoblox, you can stop attacks and address the most damaging threats to your network using high-quality, accurate, reliable, and up-to-date threat intelligence. Infoblox distills data from thousands of sources, processes, and services, and our threat intelligence team works around the clock to verify threat indicators and curate machine-readable threat intelligence.

Every data entry includes an appropriate expiration and a verified data set of threat indicators with a false-positive rate of <.01 percent. We also provide information on the nature of each threat and related indicators, in a wide variety of formats that are easy to use.

Proactively Detect and Prevent Malware C&C Communications via DNS

With Infoblox DNS Firewall, you gain proactive network protection against fast-evolving, elusive malware threats that exploit DNS to communicate with command and control (C&C) servers and botnets.

Ease Consumption of Threat Intelligence from Various Data Sources

Infoblox TIDE enables customers to aggregate, normalize, and manage internal and multiple third-party threat intelligence data, for distribution to your existing security infrastructure.

Build Intelligence Rapidly into Your Existing Security Infrastructure

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, RPZ for your infrastructure.

Readily Deploy Trusted Data to Mitigate Threats

Deploying trusted threat intelligence directly to the Infoblox DNS Firewall and other security technologies can help prevent or disrupt an attack by blocking malicious access to resources in the network. Threat intelligence can also be used to detect and alert on malicious activity. Furthermore, ActiveTrust threat intelligence data enriches security event data found on security systems such as next-generation firewalls, SIEMs, and others.

Quickly Obtain Rich Threat Context and Prioritize Threats

Use the Infoblox Cloud Security Portal and Dossier research tool to 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, 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.

Why Infoblox ActiveTrust?

- Acquire curated threat intelligence from internal resources and third-party vendors and selectively distribute data
- Apply threat intel data to DNS Firewall, preventing malware communications with C&C hosts
- Quickly investigate threat indicators for context and prioritization
- Easily deploy threat data using pre-built integrations with your existing cybersecurity infrastructure to remediate threats and prevent future attacks

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.