Infoblox
CONTROL YOUR NETWORK

ActiveTrust® Cloud

DATASHEET

Summary

Infoblox ActiveTrust Cloud provides visibility into infected and compromised devices on or off the premises, prevents DNS-based data exfiltration, and automatically stops device communications with C&Cs/botnets. Infoblox ActiveTrust Cloud provides these benefits with automated, high-quality threat intelligence feeds and unique behavioral analytics. Delivered as a service, it is easy to use, deploy, and maintain without dedicated IT resources. It provides rapid time to value and enables unified policy management, analytics, and reporting for on-premises/cloud hybrid deployments. It protects users everywhere—on the enterprise network, roaming, or in remote office/branch offices.

Key Features

- Threat Insight: Detect and block DNS-based data exfiltration using behavioral analytics.
- DNS Firewall/DNS Response Policy Zones (RPZs): Disrupt malicious DNS-based communications to C&Cs and prevent malware from propagating.
- Threat intelligence data: Stay on top of evolving malicious domains and IPs using real-time machine-readable threat intelligence curated for low false positives.
- Infoblox Dossier for easier threat investigation: Use a Google-like threat indicator investigation tool to get immediate threat context and analyze threats rapidly, shortening attack windows.
- Cloud Services Portal: Intuitive portal with unified management, analytics, and reporting on the premises and in the cloud. Customize policy based on business needs without DNS expertise, and investigate threats for actionable context.
- ActiveTrust® Endpoint Client: Lightweight agent to protect roaming devices by redirecting DNS requests from endpoints to Infoblox cloud
- Reporting and Analytics: Get deep visibility and rich network context around infections and compromised devices on or off the premises
- Recursive DNS services: Highly available recursive DNS services delivered as a service

The Challenge

Most Internet communications rely on DNS. Attackers know that DNS is often not sufficiently secured, and use it for data exfiltration and as a malware control point. Over 91 percent of malware uses DNS to communicate with the command-and-control (C&C) server, exfiltrate data, or redirect traffic to malicious sites. Existing security controls, such as firewalls, email proxies, and web proxies, rarely focus on DNS and associated threats.

Moreover, today's workforce is increasingly mobile, and the number of employees working from multiple and remote locations is rising. According to Gartner, by 2019 57 percent of workers **will not** be deskbound in the office. According to a recent remote and mobile user study, 70 percent of organizations are concerned with data loss when users are off the enterprise network, and 75 percent worry that malware will infiltrate the network due to the increase in roaming or off-network access.

Challenges in protecting users off the network are driven by a combination of the following:

- Roaming users (home workers, consultants, field sales, transient users) often relying on antivirus products that do not secure DNS, and users not always using VPN for all traffic
- Remote/branch offices lacking resources or finding it expensive to deploy and manage security infrastructure on-premises
- Companies backhauling all traffic to the datacenter, which introduces latency and geo-location issues, such as not knowing where the DNS requests are originally coming from

The Infoblox Solution

Infoblox ActiveTrust Cloud provides visibility into infected and compromised devices on or off-premises, prevents DNS-based data exfiltration, and automatically stops device communications with C&Cs and botnets. Delivered as a service, it is operationally easy to use, deploy, and maintain (without dedicated IT resources). Infoblox ActiveTrust Cloud provides rapid time to value, and enables unified policy management, analytics, and reporting for on-premises/cloud hybrid deployments. Infoblox provides actionable network intelligence with highly accurate threat intelligence to prioritize, protect, and predict threats.

Infoblox is changing the model of how security is delivered. It is the industry's first and only DDI vendor that provides a hybrid approach for security—on-premises solutions for central offices and cloud-based security for roaming users, remote and branch office users, and customers that have

a cloud-first strategy. Customers get seamless integration of the cloud service and the on-premises solution for:

- Unified policy management with an easy to use Cloud Services Portal
- Deep context and visibility for assessing risk profile (including User ID, MAC address, device type, device OS, DHCP lease history, etc.)
- Reporting and Analytics

Key Benefits

ActiveTrust Cloud is an ideal solution for organizations that want to consume services from the cloud, or are concerned with extending protection to remote or branch office users and roaming users.

Prevention of DNS-based Data Exfiltration That Other Systems Can't Detect

ActiveTrust Cloud automatically stops data exfiltration through DNS by using unique streaming analytics, and automatically adds domains associated with the data exfiltration to the Response Policy Zone (RPZ) blacklist. The software examines every DNS query and applies several analytical heuristics such as entropy, lexical analysis, and time series to detect anomalies.

Integrated into DNS for Early Detection without Any Disruptive Changes

ActiveTrust Cloud is a purpose-built solution integrated into DNS for early detection of malware without the need to deploy infrastructure everywhere. It automatically contains and controls malware by disrupting device communications with malicious Internet destinations using advanced threat intelligence. The threat intelligence is regularly updated with malicious Internet destinations and is curated by a dedicated threat intelligence team for low false positives.

Faster Threat Investigation

ActiveTrust Cloud allows threat analysts and security researchers to investigate threats easily using threat context and inputs from multiple sources, enabling them to quickly decide on action in minutes, not hours. This significantly shortens the attack window for cybercriminals.

Unified Policy Management, Analytics, and Reporting

ActiveTrust Cloud, when used in a hybrid deployment model with the on-premises ActiveTrust solution, enables administrators to set policy once for each user, seamlessly manage policy, get a complete lifecycle view of user activity while moving between on-premises and roaming states, and get enriched reports with on-premises Infoblox Grid™ data using Data Connector virtual utility.

Improved Visibility and Rich Network Context

ActiveTrust Cloud helps identify devices attempting malicious communications by leveraging an on-premises Data Connector or Infoblox Grid™ to get DHCP fingerprint including IP address, MAC address, device type, device OS, and DHCP lease history. With this deep visibility, admins get valuable network context to prioritize threats for remediation.

Accelerated Remediation with On-premises Ecosystem Integrations

ActiveTrust Cloud, when used in a hybrid deployment model with the on-premises ActiveTrust solution, can share indicators of compromise in real time with existing security infrastructure including endpoint security, NAC, vulnerability scanners, and SIEMs for automated incident response to quarantine, scan, or kill malicious process running on a suspicious device.

ActiveTrust Cloud Tiers

	ActiveTrust® Cloud Standard	ActiveTrust® Cloud Plus
Hosted recursive DNS	Available	Available
DNS Firewall (RPZ Zone)	Standard (4 reputation datasets) • Base • Anti-malware • Ransomeware • Bogon	Standard (4) + Advanced (5) + SURBL (2) • Base, Anti-malware, Ransomware, Bogon • Malware IPs, bots IPs, exploit kit IPs, malware DGA hostnames, Tor Exit Node IPs • SURBL Multi-domains, SURBL Fresh domains
Dossier (threat investigation tool)	Not included (Basic threat lookup via Cloud Services Portal only)	32,000 queries/year
Threat Insight (DNS tunneling/data exfiltration, DGA, fast flux)	Not included	Included
Reporting	Basic—malware blocked, number of hits	• Integrated reporting with on-premises Grid, enabled by Data Connector virtual utility • Enhanced visibility with drill-down reports to identify exact user and device
ActiveTrust® Endpoint (client agent)	Included	Included

Infoblox ActiveTrust® Endpoint

In order to use the Infoblox ActiveTrust Cloud service, users can install the roaming client—ActiveTrust Endpoint on the end user's device. This small lightweight client agent does the following:

- Redirects the endpoint's DNS to Infoblox DNS in the cloud
- Encrypts and embeds the client identity in DNS packets
- Automatically switches to bypass mode when it is on a corporate network protected by on-premises ActiveTrust

ActiveTrust Endpoint can be installed on Windows (7/8/10) and Mac OSX 10.10 – 10.12. Support for Linux, iOS, and Android is expected in 2017.

An alternative to installing the agent is to manually configure the local resolver to point to the Infoblox service. However, visibility into the end client will be lost if this approach is used.

The Infoblox SaaS Advantage

ActiveTrust Cloud delivered as a service leverages an advanced next-generation platform with containerized architecture. This allows the solution to horizontally scale every component and handle requests as the user base and number of devices grow. The service enables:

- Immediate improvement of a company's security posture
- Immediate access to next-generation features for trial
- Minimized IT overhead

Availability (anytime, anywhere access)
The Infoblox service is designed for always-on, anywhere access with reliable service delivery, with Infoblox service-level terms that include 99.999 percent uptime for DNS infrastructure, not including scheduled maintenance. Infoblox provides disaster recovery (anycast) and leverages worldwide datacenters. Infoblox NOC continuously monitors the service, and configurations, policy, and user data are backed up daily.

Security and Privacy
Infoblox protects your data and access to the service by encrypting DNS queries during transmission, encrypting all databases and stored data, restricting access based on location, IP addresses and role, and putting controls in place for movement of data.

Infoblox also adheres to best practices for security like making sure all software is patched, and performing penetration testing, static and dynamic code analysis.

Data Privacy: Infoblox SaaS solutions protect the privacy of customer data with logical separation of customer data and unique API key for authentication. Infoblox doesn't share any customer data with any third-party vendors.

Why Infoblox?

- Market leading DDI vendor with a hybrid model for delivering security to protect users everywhere: on-premises, roaming, or in remote and brand offices
- Single-pane-of-glass to provide unified reporting, analytics, and management
- Comprehensive solution scope with protection against various types of DNS threats, including data exfiltration, malware containment, and attacks
- Unique position in the network to provide Actionable Network Intelligence
- Market Leader in DDI (DNS, DHCP, IPAM) with 50 percent market share according to IDC

Easy to Try and Buy
With no upfront hardware to buy and install, Infoblox SaaS solutions reduce upfront technology purchasing costs. It is also easy to try the service before making the purchase decision. To request a free full-featured 30-day trial, please go to http://www.infoblox.com/activetrustcloudsignup

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

