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 command-and-control servers (C&Cs) and botnets. The solution provides these benefits using automated, high-quality threat intelligence feeds, behavioral analytics, and machine learning to catch even zero-day threats. 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 and reporting for on-premises/cloud hybrid deployments. It protects devices everywhere—on the enterprise network, roaming, or in remote office/branch offices.

Key Features

- Threat Insight: Detect and block DNS-based data exfiltration, DGAs, and fast-flux threats
- DNS Firewall/DNS Response Policy Zones (RPZs): Disrupt malicious 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
- Dossier tool 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: With an intuitive portal with unified management, analytics, and reporting, customize policy based on business needs without DNS expertise
- ActiveTrust Endpoint Client: Deploy a lightweight agent that using automated solutions such as SCCM to redirect DNS requests from endpoints to Infoblox Cloud
- DNS Forwarding Proxy: Use a virtual appliance that enables agentless deployment, embedding client IP into DNS queries before forwarding to Infoblox Cloud
- Reporting and Analytics: Get deep visibility and rich network context around infections and compromised devices
- Recursive DNS services with EDNS: Get geo-location response on the premises with highly available recursive DNS service

The Challenge

Most Internet communications rely on DNS. Attackers know that DNS is often not sufficiently secured, and hence use it for data exfiltration and as a malware control point. Over 91 percent of malware uses DNS to communicate with C&C servers, lock up data for ransom (ransomware), or exfiltrate data. Existing security controls, such as firewalls and proxies, rarely focus on DNS and associated threats.

Challenges in protecting devices in today's dynamic environment are driven by a combination of the following:

- Low-cost IoT devices are not built with security in mind and are prone to hacks and botnet formation. In addition, even if a vulnerability is identified, IoT devices are seldom patched and continue to remain prone to cyberattacks.
- Today's workforce is increasingly mobile. According to Gartner, by 2019, 57 percent of workers will not be deskbound in the office. A recent remote and mobile user study showed that 70 percent of organizations are concerned with data loss when devices are off the enterprise network. Roaming users (home workers, consultants, field sales) often rely on antivirus products that do not secure DNS, and users don't always use VPN.
- Remote/branch offices lack resources or find it expensive to deploy and manage security infrastructure on the premises.

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 provides actionable network intelligence to prioritize, protect, and predict threats in your network.

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 and cloud-based security for protecting devices everywhere. 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.)
- Detailed reporting and analytics on infections and activity

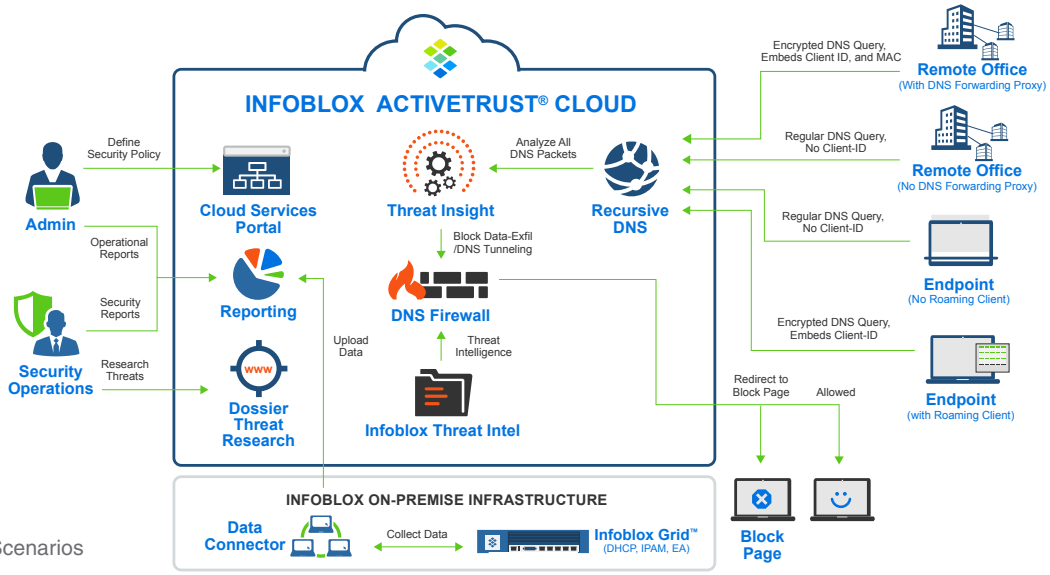

Figure 1: Workflow Scenarios

Key Benefits

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

ActiveTrust Cloud automatically stops data exfiltration through DNS using unique streaming analytics, machine learning, and artificial intelligence to detect the presence of data in queries. It automatically adds domains associated with data exfiltration, DGAs, and fast flux to Response Policy Zone (RPZ) blacklists.

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 regularly updated and curated threat intelligence.

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 take action in minutes, not hours. This significantly shortens the attack window for cybercriminals.

Unified Policy Management, Analytics, and Reporting

ActiveTrust Cloud, when used in hybrid deployment with the on-premises ActiveTrust solution, enables administrators to seamlessly manage policy, get complete lifecycle views of device activity, and get enriched reports with on-premises Infoblox Grid™ data using the Data Connector virtual utility.

Improved Visibility and Rich Network Context

ActiveTrust Cloud helps identify infected devices by leveraging an on-premises data connector or Infoblox Grid to get DHCP fingerprints including IP address, MAC address, device type, device OS, DHCP lease history, etc. 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 hybrid deployment 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 such as quarantine, scan, or killing of malicious processes running on suspicious devices.

ActiveTrust Cloud Tiers

	ActiveTrust Cloud Standard	ActiveTrust Cloud Plus
Hosted Recursive DNS with Geo-Location Response (using EDNS)	Included	Included
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 virtual Data Connector utility • Enhanced visibility with drill-down reports to identify exact user and device
ActiveTrust Endpoint (client agent)	Included	Included
DNS Forwarding Proxy	Included	Included

Infoblox ActiveTrust Endpoint

In order to use the ActiveTrust Cloud service, admins can install the roaming client—ActiveTrust Endpoint—on the devices or workstations. This small lightweight client agent:

- Redirects the endpoint's DNS to Infoblox DNS in the cloud
- Encrypts and embeds the client identity in DNS packets
- Sends information on the logged-in user to ActiveTrust Cloud for reporting
- 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 and can be mass deployed using automated solutions such as SCCM.

DNS Forwarding Proxy

In cases where installing an endpoint agent is not always desirable or possible (certain IoT devices), DNS forwarding proxy can be used. It is a virtual appliance that embeds client IP into DNS queries before forwarding to Infoblox cloud. As with the endpoint agent, the communications are encrypted and client visibility is maintained.

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 and 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 such as making sure all software is patched and performing penetration testing and 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 devices everywhere: on premises, roaming, or in remote and branch offices
- Single-pane-of-glass control 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 up-front hardware to buy and install, Infoblox SaaS solutions reduce up-front 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

