Infoblox
NEXT LEVEL NETWORKING

ActiveTrust® Cloud

DATASHEET

Key Features

- Threat Insight: Detect and block DNS-based data exfiltration, DGA, DNSMessenger, fast flux and using analytics and machine learning
- DNS Firewall/DNS Response Policy Zones (RPZs): Disrupt malicious communications to C&Cs and prevent malware from propagating
- Content Categorization: Restrict access to objectionable content (e.g. social media, adult content and other restricted categories) and review content activity
- Threat Intelligence Data Exchange (TIDE): Collect and manage curated threat intelligence from internal and external sources and distribute threat intel data to third-party security systems for remediating threats rapidly
- 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
- Ecosystem notifications using public APIs or on-premises integrations: Respond to threats faster by pulling security event data into ecosystem tools using public APIs or on-premises Infoblox
- 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 lightweight agent using automated solutions such as SCCM or McAfee ePO for faster and mass rollout
- DNS Forwarding Proxy: Forward DNS queries to Infoblox Cloud without need for endpoint agents, embedding client IP; also integrated with NIOS 8.3+ eliminating need for installing additional software
- Reporting and Analytics: Get deep visibility and rich network context including IPAM metadata (e.g. MAC address, source IP) for correlation of events

The Challenge and Corporate Landscape

Most Internet communications rely on DNS. Attackers know that DNS is often not sufficiently secured, and DNS continues to be a leading vector for data exfiltration. 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.

There are additional challenges in today's dynamic environment – increasingly mobile workforce, distributed offices and increased adoption of IoT. 81% of mobile knowledge workers connect to free public WiFi network using their work devices, causing security concerns. Roaming users don't always use VPN and often rely on antivirus products that do not secure DNS.

In addition, today's corporate landscape is changing. Organizations are increasingly consuming services from the cloud for the following reasons:

- They want easy, fast, reliable, high value implementations with lower upfront costs
- They do not want to deploy/make changes to architectural components or manage more solutions internally
- They lack dedicated IT resources (especially in remote/branch offices) to manage infrastructure on-premises
- They want to leverage the scale of the cloud and expanded use cases (anywhere protection – on and off premises).

Solution: Protecting Devices Anywhere with ActiveTrust Cloud

Infoblox ActiveTrust Cloud is a subscription service that blocks DNS based data exfiltration, stops malware communications with command-and-control servers, automatically prevents access to content not in compliance with policy, and shares intelligence and IOCs with your existing security infrastructure for orchestration and faster remediation.

The solution leverages rich network context using on-premises DDI data for better prioritization, consolidates and distributes curated, timely and accurate threat intelligence, and enables unified policy management, reporting for hybrid deployments.

Delivered as a subscription service, it is easy to configure and use without dedicated IT resources, and protects devices everywhere—on the enterprise network, roaming, or in remote office/ branch offices.

- *...continued* Key Features

- Smart cache: Enable end user to connect to destination domain using cached entry if it times out
- Recursive DNS services w/ EDNS: Get geo-location response on the premises with highly available recursive DNS service
- Granular policy management: Ability to apply different policies for different user segments; set policy precedence to customize enforcement for threat feeds, content category filters
- Data Access via S3 Bucket: DNS query log export to Amazon S3 buckets with support for common formats including CSV, JSON, and CEF

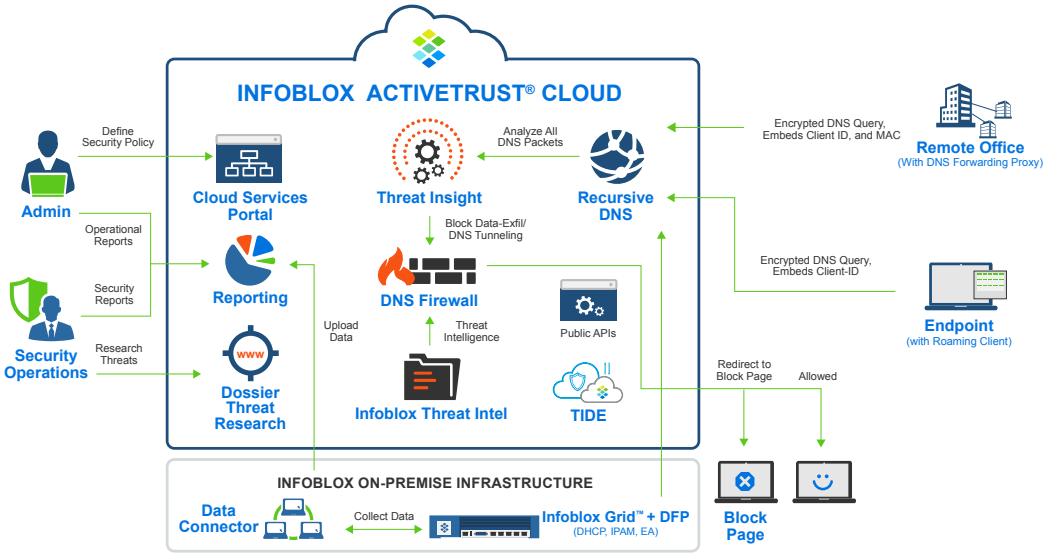

Figure 1: Workflow Scenarios

Key Benefits

Prevention of DNS-based Data Exfiltration That Other Systems Can't Detect
ActiveTrust Cloud automatically stops data exfiltration through DNS using unique behavioral analytics, machine learning, and artificial intelligence. It also detects zero day threats using behavioral analytics and adds domains associated with DGA, DNSMessenger and fast flux to Response Policy Zone (RPZ) blacklists.

Content Categorization and Policy Enforcement
ActiveTrust Cloud allows security admins to restrict access to certain types of content (e.g. social media, adult content and other restricted categories) and to review content activity in the organization.

Integrated into DNS for Early Detection of Malware 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.

Leverage cloud to scale threat detection for enforcement anywhere
ActiveTrust Cloud allows customers to leverage the scale of the cloud to perform large scale analytics and leverage threat intelligence to detect more threats.

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.

Improve Security Posture by Sharing Curated Threat Intelligence Data

Combine threat data from all your sources, use contextual metadata to select the relevant subset, and leverage the right format(JSON, STIX, CSV, CEF, and RPZ) to distribute the data to your existing security ecosystem such as NGFW, web proxy and SIEM. This greatly improves the security posture and situational awareness.

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 Public APIs and On-premises Ecosystem Integrations

ActiveTrust Cloud enables faster response to threats by providing easy access to security events through public APIs or by leveraging on-premises Infoblox infrastructure. The event data can be sent to a SIEM, or to other tools like vulnerability scanners, network access control, endpoint remediation and more.

What Customers Say

"In this day and age there is way too much ransomware, spyware, and adware coming in over links opened by Internet users. The Infoblox cloud security solution helps block users from redirects that take them to bad sites, keeps machines from becoming infected, and keeps users safer."

— Senior System Administrator and Network Engineer, City University of Seattle

Get Started on Evaluation

It is 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.

Appendix:

Tiers and Additional Capabilities

	ActiveTrust Cloud Standard	ActiveTrust Cloud Plus
Recursive DNS Firewall (RPZ Zone)	Threat Intel Feeds Standard (6 reputation datasets) • Base • Anti-malware • Ransomeware • Bogon • Automated Indicator Sharing (AIS) data (2)	Threat Intel Feeds Standard (6) + Advanced (7) + SURBL (3) • Base, anti-malware, ransomware, bogon, AIS (2) • Malware IPs, bots IPs, exploit kit IPs, malware DGA hostnames, Tor Exit Node IPs, US OFAC Sanctions IPs, EECN IPs • SURBL multi-domains, SURBL fresh domains, SURBL Multi Lite
Content Categorization	Not included	Restrict access to objectionable content in the cloud
Dossier (Threat Investigation Tool)	Not included (Basic threat lookup via Cloud Services Portal only)	32,000 queries/year
Public APIs (for ecosystem) • Threats APIs • Custom list APIs	Not included	• Included - Security events available in CEF or JSON format via Cloud APIs– with enhanced security reports • Ability to create custom threat feeds via Cloud APIs
Threat Insight (DNS Tunneling/Data Exfiltration, DNSMessenger, DGA, Inline DGA, Dictionary DGA, Fast Flux)	Not included	Machine learning based analytics included
TIDE Infoblox Threat Intelligence Data Exchange (TIDE) license – enabling use in third party security solutions	Not included	Licensed use for ONE of the following: (for use in any non-Infoblox security solution) • Hostnames or • IP Addresses or • URLs
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 • Inclusion of IPAM metadata for correlation of events
ActiveTrust Endpoint (Client Agent - can be deployed using SCCM or McAfee ePO)	Included	Included
DNS Forwarding Proxy	Included	Included
Hosted Recursive DNS with Geo-Location Response (Using EDNS)	Included	Included

Infoblox
NEXT LEVEL NETWORKING

ActiveTrust® Cloud

DATASHEET

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, or McAfee ePO.

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 DNS Forwarding Proxy is also integrated with NIOS 8.3 and above, eliminating the need for Infoblox customers to install additional software on-premises.

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.

About Infoblox

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

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