Infoblox
CONTROL YOUR NETWORK

Infoblox Solution for Data Exfiltration Prevention

SOLUTION NOTE

Data is as Good as Cash. Keep Yours Safe from Thieves.

Data theft is one of the most serious risks for modern business. Intruders often use DNS as a pathway for data exfiltration because it is commonly overlooked by security solutions such as firewalls, IDS, and proxies. data loss prevention technologies are traditionally focused on web and email traffic and SIEM-based methods may not catch DNS-based data exfiltration in real time. The cost associated with a data breach can be staggering. According to Ponemon Institute's study in 2015, the average consolidated cost of a data breach is $3.8 M, which includes investigative and forensic efforts, resolution, and consequences of customer defection. Beyond a major financial hit on your bottom line, successful attacks can lead to legal woes and irreversible damage to your brand and reputation.

Keep Your Valuable Data Where It Belongs—Safe from Cybercriminals

Infoblox solution for Data Exfiltration Prevention uses actionable network intelligence and streaming analytics to detect and block DNS-based data exfiltration attempts. The solution scales enforcement to various parts of the network and shares contextual threat information with leading security technologies to help expedite threat response.

The High Price of Poor Protection:

- **Time**: spent dealing with the fallout from a breach
- **Lost revenue:** capital spent on mitigating the effects
- **Productivity:** teams focus on fixes, not core functions
- **Customer trust:** consumers avoid unsafe enterprises
- **Brand prestige:** it only takes one breach to ruin your reputation

Benefits

Lock the DNS Back Door

- Utilize tools to detect and block data breaches through DNS
- Use streaming analytics built into the market-leading DNS infrastructure to detect zero day threats
- Protect data by blocking communication from infected endpoints to malicious destinations
- Secure data without endpoint software or additional network infrastructure changes
- Scale enforcement across the network with Grid-wide updates

Connect the Dots

- Gain visibility into data exfiltration events
- Link exfiltration activity with other security events using network context
- Stay ahead of the curve with intelligence on new and evolving tunneling methods

Create a Unified Front

- Seamlessly integrate with existing security tools already in place
- Enable a stronger, more effective incident response
- Combine the power of Infoblox with the leading security technologies such as NAC, endpoint security, and SIEM
- Gain flexibility and interface with REST API, STIX™, and Cisco pxGrid

| www.infoblox.com

Infoblox
CONTROL YOUR NETWORK

Infoblox Solution for Data Exfiltration Prevention

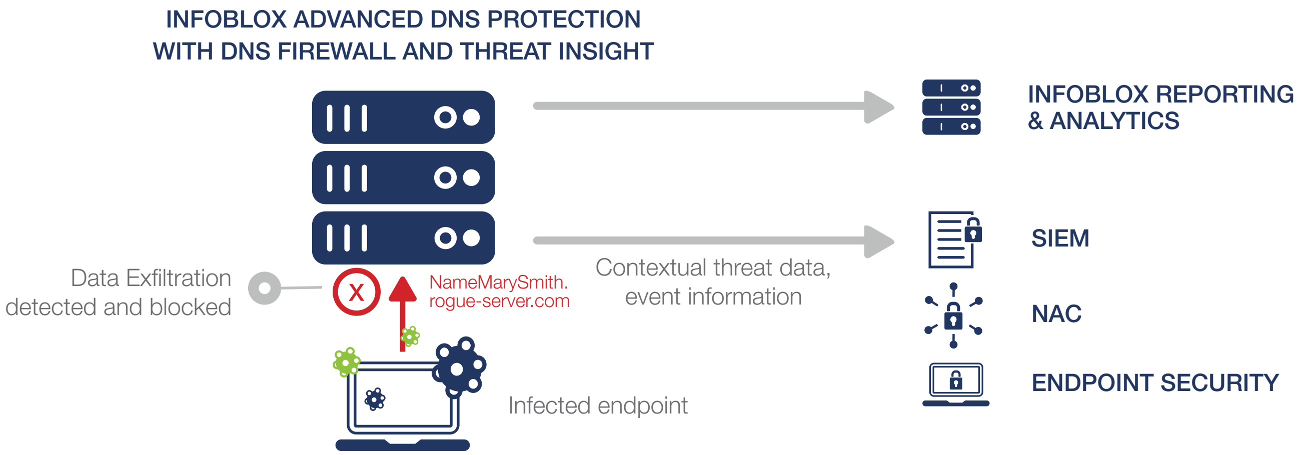
SOLUTION NOTE

Security for Your Data from the Core

Using Actionable Network Intelligence, Infoblox detects and automatically blocks attempts to steal sensitive data via DNS—without the need for endpoint agents or additional network infrastructure—leveraging real time streaming analytics and signature rules. Our platform provides protection against both DNS tunneling and sophisticated zero-day data exfiltration techniques.

In addition, the Infoblox platform shares indicators of compromise with leading security technologies to automate and accelerate threat responses. Infoblox is the only vendor to offer a DNS infrastructure with built-in streaming analytics for the protection of your data.

How It Works


INFOBLOX ADVANCED DNS PROTECTION
WITH DNS FIREWALL AND THREAT INSIGHT
INFOBLOX REPORTING & ANALYTICS
SIEM
NAC
ENDPOINT SECURITY
Contextual threat data, event information
Data Exfiltration detected and blocked
X
NameMarySmith.rogue-server.com
Infected endpoint

COMPONENTS

Infoblox Products

Threat Insight

- Detects zero-day data exfiltration attempts with machine learning and streaming analytics
- Leverages RPZ feed entries in DNS Firewall to block communications with malicious destinations
- Scales protection with Grid-wide updates to all Infoblox members

DNS Firewall

- Blocks communications from infected endpoints to malicious destinations associated with data exfiltration
- Shares contextual threat information with other security technologies to accelerate remediation and enhance security

Advanced DNS Protection

- Uses automated threat intelligence and signature rules to detect and block data exfiltration that uses standard DNS tunnels
- Keep protection updated with intelligence on new and evolving tunneling methods

Cybersecurity Ecosystem

- Infoblox's flexible third-party system interfaces support REST API, STIX™/TAXII™, Cisco pxGrid, Syslog, etc.
- The solution simplifies integration with third-party security products.
- SIEM and UBA integration enables Infoblox to share security events as part of a comprehensive threat view, allowing for automation of response workflows.

Reporting and Analytics

- Provides visibility (including devices) into data exfiltration attempts
- Identifies threat information like device IP, user name, MAC address, and device type using Infoblox DHCP fingerprinting and Identity Mapping
- Enables operators to quickly understand current threats using detailed threat context

Ecosystem Products

SIEM

- Gathers, analyzes, and correlates data, alerts, and logs from network, security, and other sources

Endpoint Security

- Protects the corporate network when accessed via remote devices, such as laptops or other wireless and mobile devices

NAC

- Unifies endpoint security, user authentication, and network security enforcement

About Infoblox

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox (www.infoblox.com) reduces the risk and complexity of networking.

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