SOLUTION BRIEF

Infoblox and McAfee for Unified Security

Automated triage and remediation.

McAfee and Infoblox have partnered to improve holistic visibility and deliver comprehensive protection and faster threat response. The solution redirects suspicious DNS traffic to the McAfee® Web Gateway Cloud Services and enables deep levels of content inspection, including malware scanning and SSL inspection. In addition, by sharing intelligence among ActiveTrust and Data Exchange Layer (DXL), organizations can break through the silos of security tools and enable workflow orchestration across solutions, gaining timely and effective protection for both the network and endpoint domains.

McAfee Compatible Solution

- Infoblox ActiveTrust
- Infoblox ActiveTrust Cloud
- Infoblox DDI
- McAfee® Web Gateway
- McAfee Enterprise Security Manager
- Data Exchange Layer

McAfee™ COMPATIBLE

Infoblox® CONTROL YOUR NETWORK

The Business Problem

Companies have invested in various security tools, and yet malware enters the network, steals data, and bypasses the existing security infrastructure. DNS traffic is not investigated or filtered by firewalls and thus is a gap that is most commonly exploited by malicious actors. Today, 91% of malware uses DNS to carry out campaigns once it has breached the perimeter. In a recent *SC Magazine* survey, 46% of survey respondents said they experienced DNS-based data exfiltration.

Being able to detect and respond in real time to network events and threats seen by the DNS protection platform greatly accelerates incident response. However, the lack of easy access to network data inhibits taking the right action based on context.

Furthermore, the various security tools that organizations have today work in silos. The lack of interoperability and inability to share threat intelligence inhibits an organization's capability to respond effectively to ever-increasing numbers of attacks.

Solving the above challenges requires the following:

- Visibility into DNS traffic
- Plugging the DNS security gap with a multipronged approach to threat detection
- Integration between DNS security and other security tools that are part of the ecosystem

The integrated solution from Infoblox and McAfee provides visibility into DNS and web traffic, plugs the DNS security gap in organizations, and automates data sharing between Infoblox DNS, DHCP, IPAM, (DDI), and McAfee product suites. Not only does the interoperability provide enhanced protection against attacks through DNS traffic, the combined solution simplifies the administrative burden of agent distribution and enables automated workflows that quickly remediate infected endpoints managed by McAfee.

McAfee and Infoblox Joint Solution

Infoblox ActiveTrust Cloud with McAfee Web Gateway Cloud Service

Infoblox ActiveTrust Cloud prevents DNS-based data exfiltration, automatically stops DNS communications with command-and-control servers (C&Cs) and botnets, and pinpoints infected and compromised devices on or off premises.

The integration of Infoblox ActiveTrust Cloud and McAfee Web Gateway Cloud service unifies domain blocking and HTTP security to provide broader protection for mutual customers. Capabilities include:

- Protection on various layers of a connection attempts
- Enhanced content filtering technology to manage access to cloud applications and the content therein by scanning any uploads for possible DLP violations

This integration enables faster detection of malicious traffic originating from infected endpoints, regardless of its location. The automatic re-direction by ActiveTrust to McAfee Web Gateway ensures that enterprise data are protected in real time.

Infoblox and McAfee: DNS and Web Security, Data Sharing, and Orchestration

Infoblox and McAfee offer customers the choice of deploying a solution that is on premises, cloud-based, or a combination of both to protect devices and users everywhere.

Infoblox DDI and ActiveTrust with DXL and McAfee® ePolicy Orchestrator® (McAfee ePO™)

Infoblox DDI provides device discovery and single source of truth for devices and networks. It knows when there are changes in the network, such as new devices joining the network, virtual workloads being spun up, or malicious activities detected by the DNS security solution.

Infoblox publishes security and networking event topics, along with context over DXL using outbound RESTful application programming interfaces (APIs). This enables DXL topic subscribers to integrate DDI network changes and identified DNS threats within their solutions and trigger response to these events as needed. Infoblox also sends these networking and security events directly into McAfee ePO software, enabling remediation and policy actions.

The sharing of intelligence among solutions enables the security ecosystem to work together in unison to contain threats faster.

Infoblox DDI and ActiveTrust with McAfee Enterprise Security Manager

Infoblox shares networking events and DNS security events/alerts with McAfee Enterprise Security Manager (SIEM) solution to allow for comprehensive threat data correlation and detection. Infoblox also shares valuable network context and actionable intelligence (IP address, DHCP fingerprint, lease history, and more) to help assess risk and prioritize alerts. This enables more efficient incident response based on real risk.

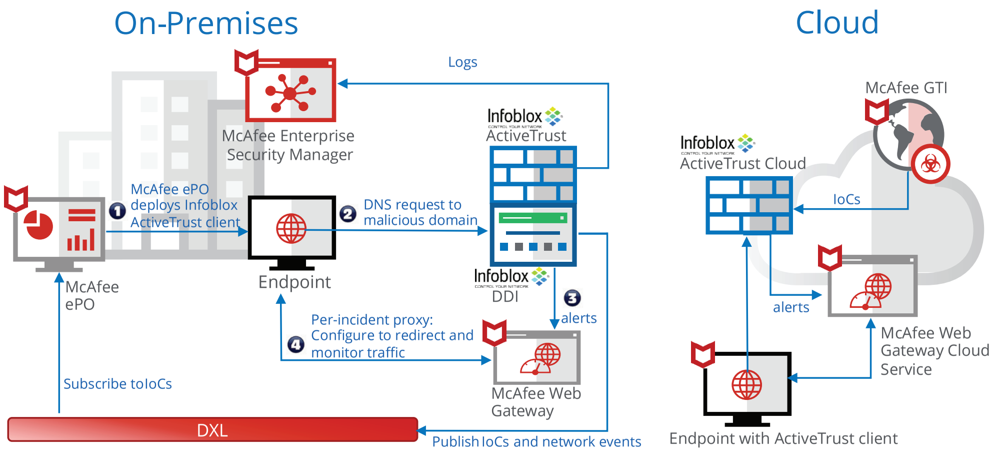
On-Premises
Cloud
Logs
McAfee Enterprise Security Manager
Infoblox
ActiveTrust
McAfee ePO
1 McAfee ePO deploys Infoblox ActiveTrust client
Endpoint
2 DNS request to malicious domain
Infoblox
DDI
3 alerts
Per-incident proxy:
4 Configure to redirect and monitor traffic
McAfee Web Gateway
Subscribe to IoCs
DXL
Publish IoCs and network events
McAfee GTI
Infoblox
ActiveTrust Cloud
IoCs
alerts
McAfee Web Gateway Cloud Service
Endpoint with ActiveTrust client

Figure 1. Solution reference architecture depicting the integration between Infoblox DDI, ActiveTrust and ActiveTrust Cloud, and McAfee security protection solutions.

About McAfee Web Gateway Cloud Service

McAfee Web Protection uses secure gateway technology to protect every device, user, and location from sophisticated threats.

McAfee Web Protection is a unified solution combining the on-premises McAfee Web Gateway and cloud-delivered McAfee Web Gateway Cloud Service. When deployed together, both on-premises and cloud solutions can be managed with a single console and with a single shared policy that is applied to devices wherever they travel.

About McAfee ePolicy Orchestrator

McAfee ePolicy Orchestrator is the endpoint management console and the foundation of the McAfee management solution. More than 30,000 customers use McAfee ePO software on more than 60 million nodes to manage security, streamline and automate compliance processes, and increase overall visibility across security management activities. With its scalable architecture, fast time to deployment, and optimization for enterprise systems, McAfee ePO software is the most advanced security management software available.

About Data Exchange Layer

The Data Exchange Layer (DXL) communication fabric connects and optimizes security actions across multiple vendor products, as well as internally developed solutions. Enterprises gain secure, real-time access to new data and lightweight, instant interactions with other products.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

About Infoblox ActiveTrust Cloud

Infoblox ActiveTrust Cloud is a SaaS service that provides visibility into infected and compromised devices on or off premises, prevents DNS-based data exfiltration, and automatically stops DNS communications with 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.

About Infoblox ActiveTrust

Infoblox ActiveTrust is an on-premises DNS security solution that prevents data exfiltration and malware C&C communications via DNS, centrally aggregates curated internal and external threat intelligence, distributes validated threat data to the customer's security ecosystem for remediation, and enables rapid investigation to identify context and prioritize threats.

About Infoblox DDI

Infoblox DNS, DHCP, and IPAM (DDI) services maximize uptime, reduce security risks, and help control operating expense (OpEx), both in traditional networks and mixed cloud environments. Unlike "zero dollar" DNS/DHCP solutions, Infoblox DDI supports your current and evolving needs while achieving the highest standards for performance, optimization, and manageability.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com