SOLUTION BRIEF

Infoblox and McAfee for Unified Security

Pair real-time visibility with security automation, orchestration, and response

McAfee and Infoblox have partnered to improve holistic visibility, deliver comprehensive protection, and enable faster threat response. The solution redirects suspicious DNS traffic to the McAfee® Web Gateway Cloud Services and facilitates 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 provide workflow orchestration across solutions, gaining timely and effective protection for both the network and web-bound endpoints.

Infoblox was awarded the Most Innovative McAfee Security Innovation Alliance Partner in 2017.

McAfee Compatible Solution

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

Connect With Us

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 products. 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: 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 ActiveTrust Cloud with McAfee Web Gateway Cloud Service

Infoblox ActiveTrust Cloud detects and prevents DNS-based data exfiltration and DNS communications with command-and-control servers (C&Cs) and botnets. It automatically blocks access to content not in compliance with policy and shares aggregated threat intelligence and indicators of compromise (IoCs) with your existing security infrastructure for faster remediation. The solution leverages rich network context using on-premises DDI data for better visibility and prioritization, and enables unified policy management and reporting

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

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:

- Proactive and adaptive protection on various layers of a connection attempts, with increased web traffic inspection by McAfee Web Gateway for suspicious, but not yet convicted connections identified by Infoblox ActiveTrust Cloud
- Broader threat intelligence sharing by leveraging the combined capabilities of McAfee and Infoblox threat intelligence for better protection
- 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 and data exfiltration originating from infected endpoints or suspicious users, regardless of its location. The automatic re-direction by ActiveTrust Cloud to McAfee Web Gateway ensures that enterprise data are protected in real time.

Furthermore, Infoblox ActiveTrust Cloud is integrated with the premium McAfee endpoint management console, McAfee ePolicy Orchestrator (McAfee ePO™) software. McAfee ePO software can perform the centralized distribution and update and management of ActiveTrust Endpoint Agents running on endpoint computers, simplifying administration tasks that enhance the workflow of our joint solutions.

Infoblox DDI and ActiveTrust with DXL and 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 DDI and ActiveTrust publishes security and networking event topics, along with context, over DXL using outbound RESTful application programming interfaces (APIs). Data Exchange Layer (DXL) is a threat intelligence-sharing fabric for the entire McAfee product portfolio and its technology partner ecosystems. By sharing the security data, applications such as SIEM, user behavior analytics, vulnerability scanning, and mobile management solutions can take the high-value information into its own context and perform remediation, forming a well-orchestrated circle of protection. DXL topic subscribers can integrate DDI network changes and identified DNS threats within their solutions and trigger response to these events as needed. These networking and security events can also be pulled into McAfee ePO management via DXL, enabling remediation and policy actions.

McAfee and Infoblox Joint Solution Reference Architecture

Detection, automation, and orchestration

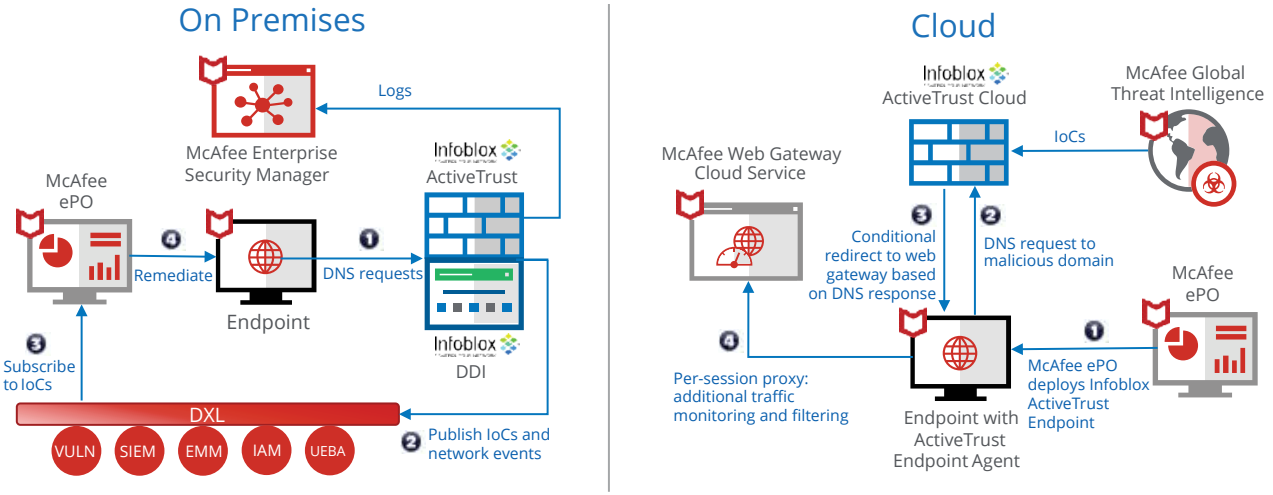

Figure 1. Solution reference architecture depicting the integration between Infoblox DDI, ActiveTrust and ActiveTrust Cloud, and McAfee security solutions.

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.

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 solution 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 existing security infrastructure for orchestration and faster remediation. 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

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.

.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com