Infoblox
CONTROL YOUR NETWORK

Extending Infoblox Intelligence for Endpoint Remediation

PARTNER SOLUTION BRIEF

CARBON BLACK
ARM YOUR ENDPOINTS

Infoblox and Carbon Black have partnered to enable security and incident response teams to leverage the integration of next-generation endpoint and DNS security to improve advanced threat detection, protection, and response. Infoblox DNS Firewall provides visibility into malicious domains and DNS queries and responses associated with malware and data exfiltration. Integration with Carbon Black enables Infoblox customers for the first time to dramatically reduce endpoint response and remediation times associated with DNS Firewall alerts.

Background

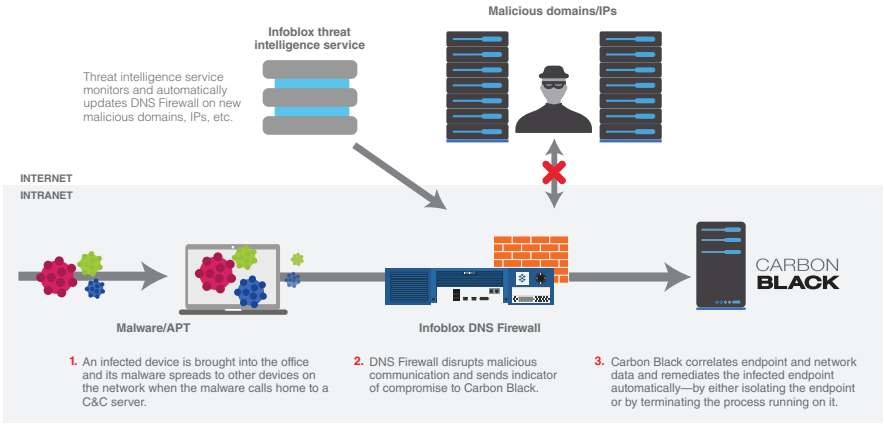
By 2020, 75% of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10% in 2012, according to recent security research. Organizations will continue to invest in multiple security technologies and products as part of a defense-in-depth security strategy. In particular, Infoblox DNS Firewall plays an important role in defending the network against advanced malware and data exfiltration by disrupting communications of endpoints to malicious domains. However, it cannot identify nor stop a malicious process from running on the infected endpoint. Integration of Infoblox DNS Firewall with next-generation endpoint security can help organizations achieve "closed-loop" protection, from detection to remediation.

Challenges

1. Black hats are always looking for new areas to attack and today DNS, which is essential to all network connectivity, is that new area for infiltration.
2. Once an endpoint is compromised by malware or other security threats, the ability to quickly identify and remedy the breach is paramount.
3. It's difficult to automatically take action on infected endpoints as soon as they make DNS queries to command-and-control (C&C) servers, botnets, and malicious sites.
4. Because endpoints are increasingly connecting from outside, not just inside the corporate perimeter, maintaining visibility and controlling risk regardless of location is essential.

Solution

Infoblox and Carbon Black automatically prevent endpoints, from connecting to malicious domains, and remediate infected endpoints by terminating the originating process, dramatically reducing attack dwell time.



Infoblox
CONTROL YOUR NETWORK

Extending Infoblox Intelligence for Endpoint Remediation

PARTNER SOLUTION BRIEF

How It Works

Infoblox and Carbon Black have partnered to provide the world's first integration of DNS security and next-generation endpoint security to improve advanced threat detection, protection, and response. By integrating Infoblox DNS Firewall and the Carbon Black Enterprise Response's continuous endpoint recorder, we've made it possible to mitigate the impact of malware infection in three simple steps:

- If an infected endpoint (aka device) tries to contact a C&C server or malicious site via DNS, Infoblox DNS Firewall uses an automated threat intelligence feed to identify the infected endpoint.
- When Infoblox DNS Firewall detects an endpoint query to a malicious domain destination, an alert, essentially an indicator of compromise (IoC), is sent to Carbon Black Enterprise Response's continuous endpoint recorder. Using this information, Carbon Black then automatically identifies the infected endpoint and either kills the malicious process or isolates that machine until further investigation can be conducted by the security team.
- Infoblox DNS Firewall continuously monitors new risks via an automated threat intelligence service and sends this information periodically to Carbon Black so it can take action.

Key Capabilities of the Solution

By combining the leading Infoblox DNS solution with the leading advanced endpoint threat prevention, detection, and response solution from Carbon Black, you can reduce security risks in these ways.

Identify and Prevent DNS-based Endpoint Communications to Malicious Domains

Infoblox automatically monitors known malicious domain destinations (C&C sites and botnets), so that you can identify impacted endpoints before malware spreads inside the network to other hosts or causes further harm, such as data exfiltration.

Automatically Respond to Endpoint Threats, Reducing Dwell Time

Once Infoblox identifies an infected endpoint, Carbon Black takes immediate action, reducing the time to response. Operational efficiency is increased, since there is no longer a need for the security operations team to schedule a maintenance window and spend time remediating the endpoint, which can take hours or days.

To learn more, visit www.infoblox.com/securedns

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