Infoblox DNS Firewall for Carbon Black

Key Benefits

- Know where malicious DNS traffic is originating and which endpoints are infected.
- Dramatically reduce dwell time by automating endpoint incident response using DNS based detection.
- Leverage Carbon Black and Infoblox DNS Firewall to automatically ban malicious files, processes and domains from future execution or connection.
- Protect remote users by extending Infoblox protection beyond the network perimeter.

Supported Products

- Cb Response
- Infoblox DNS Firewall 7.0 +

"To enhance their protection, organizations should unify network and endpoint security to provide 'closed-loop' protection. DNS security plays a critical role in defending against advanced persistent threats (APTs) and malware. This integration will vastly improve an organization's security posture."

- Craig Sanderson, Senior Director for Security Products, Infoblox

Unifying Endpoint and DNS Security

Carbon Black, in partnership with Infoblox, is introducing the world's first 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/responses associated with APTs, malware or data exfiltration. This integration will automatically prevent any endpoint, whether they are inside or outside the network, from connecting to malicious domains and will automatically remediate infected endpoints by terminating the originating process.

Together this integration enables organizations to:

- Gain important context into where malicious DNS traffic is originating and which endpoints are infected.
- Dramatically reduce dwell time by automating endpoint incident response using DNS based detection.
- Automatically leverage Carbon Black and Infoblox DNS Firewall to ban malicious files, processes and domains from future execution or connection.
- Provide management and executives with greater visibility into infected devices, high-risk users and sources of infection for improved reporting and analysis.
- Significantly improve organizational security by extending Infoblox DNS Firewall protection to off-network devices and mobile users.

Prioritize Malware Alerts and Automate Incident Response

By integrating DNS security and endpoint threat detection and response, organizations can for the first time correlate malicious DNS traffic alerts from an Infoblox DNS Firewall to Carbon Black's continuous endpoint recorder to automatically identify and take action against the infected devices, whether they are on or off the corporate network.

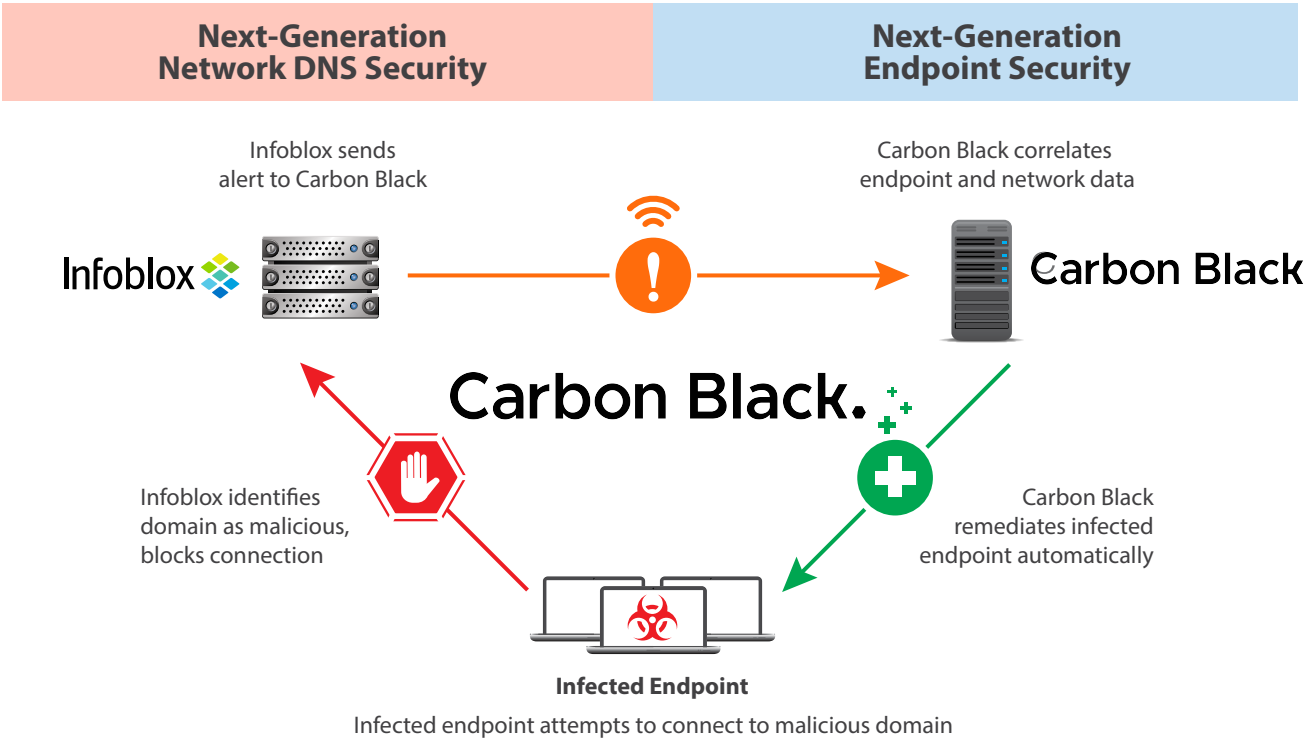
This is delivered through two unique and powerful use-cases:

- When malicious DNS traffic is identified by an Infoblox DNS Firewall, it sends an alert to Carbon Black where this information is correlated against Carbon Black's real-time endpoint data to instantly identify all infected endpoints and processes connecting to that domain. Once identified, an organization can either automatically or on-demand kill any malicious processes running on those systems. Once this is complete, an organization can then use Carbon Black to institute a process ban, preventing those malicious processes from ever running again anywhere in the organization's environment.
- When an endpoint is outside the corporate network, Carbon Black extends Infoblox DNS Firewall protection by automatically terminating any processes known to be connecting to a malicious domain.

Together, this integration enables organizations for the first time to dramatically reduce endpoint response and remediation times associated with DNS Firewall alerts and extend the power and security of Infoblox DNS Firewall protection to off-network devices.

Carbon Black.

Infoblox
CONTROL YOUR NETWORK



Infoblox DNS Firewall

Infoblox DNS Firewall is the leading DNS-based network security solution that protects against APTs and malware that use DNS to communicate with command-and-control (C&C) sites and botnets. DNS Firewall works by employing DNS Response Policy Zones (RPZs) and timely threat intelligence for effective protection.

About Cb Response

Cb Response is the first and only endpoint threat detection and response platform that enables SOC and IR teams to prepare for a breach through continuous endpoint recording, customized detection, live response, remediation, and rapid attack recovery with threat banning. Built entirely on open APIs, Carbon Black delivers unparalleled security operations development capabilities for best-of-breed detection and response tailored for your organization.

About Infoblox

Infoblox delivers network control solutions, the fundamental technology that connects end users, devices, and networks. These solutions enable more than 8,100 enterprises and service providers to transform, secure, and scale complex networks. Infoblox helps take the burden of complex network control out of human hands, reduce costs, and increase security, accuracy, and uptime. Infoblox (www.infoblox.com) is headquartered in Santa Clara, California, and has operations in over 25 countries.

About Carbon Black

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security. Carbon Black serves more than 4,300 customers globally, including 35 of the Fortune 100. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV). Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black solutions enable customers to defend against the most advanced cyber threats, including malware, ransomware, and non-malware attacks. Deployed via the cloud, on premise or as a managed service, customers use Carbon Black solutions to lock down critical systems, hunt threats, and replace legacy antivirus.