Infoblox

PARTNER SOLUTION BRIEF

Extending Infoblox Intelligence for Endpoint Remediation

OVERVIEW

With the Infoblox and Carbon Black partnership, security and incident response teams can leverage the integration of next-generation endpoint and DNS security to improve threat detection, protection and response. BloxOne™ Threat Defense provides a consolidated view into malicious domains and DNS queries and responses associated with malware and data exfiltration. Integration with Carbon Black enables Infoblox customers to dramatically reduce endpoint response and remediation times associated with BloxOne Threat Defense alerts, boosting security operations efficiency.

Background and Challenges

CARBON BLACK
ARM YOUR ENDPOINTS

By 2020, 75 percent of enterprises' information security budgets will be allocated for rapid detection and response approaches, up from less than 10 percent in 2012, according to recent security research. Organizations will continue to invest in multiple security technologies and products as part of an in-depth defense strategy.

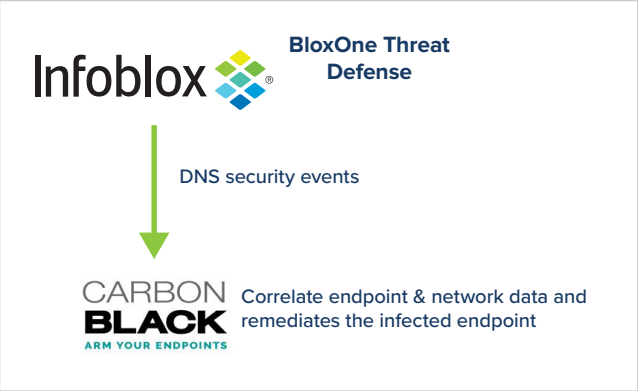
In particular, BloxOne Threat Defense plays an important role in defending networks against advanced malware and data exfiltration by disrupting communications of endpoints to malicious domains. However, BloxOne Threat Defense alone cannot identify or stop a malicious process from running on the infected endpoint. Integration of BloxOne Threat Defense with next-generation endpoint security can help organizations achieve "closed-loop" protection, from detection to remediation.

Key challenges include:

- Black hats are always looking for new areas to attack. Today, DNS, which is essential to all network connectivity, is now among the most common areas for infiltration.
- Once malware or other security threats compromise an endpoint, the ability to quickly identify and remedy the breach is paramount.
- Most organizations lack the ability to automatically respond when infected endpoints make DNS queries to command-and-control (C&C) servers, botnets and malicious sites.
- Because endpoints are increasingly connecting from outside, not just inside an organization's perimeter, maintaining visibility and controlling risk regardless of location are essential.

Infoblox–Carbon Black Solution

Together, 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 and enabling organizations to raise network security to the next level (Fig 1).



How the Solution Works

Infoblox and Carbon Black provide the world's first integration of DNS security and next-generation endpoint security to improve advanced threat detection, protection and response. By integrating BloxOne Threat Defense and the Carbon Black Enterprise Response's continuous endpoint recorder, we've made it possible to automatically 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, BloxOne Threat Defense uses an automated threat intelligence feed to identify the infected endpoint.
- When BloxOne Threat Defense detects an endpoint query to a malicious domain destination, it sends an alert, essentially an indicator of compromise, to Carbon Black Enterprise Response's continuous endpoint recorder. Using this information, Carbon Black then automatically identifies the infected endpoint and either eliminates the malicious process or isolates that device until the security team can investigate it further
- BloxOne Threat Defense 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

The solution combines the leading Infoblox DNS solution with the industry's most advanced endpoint threat prevention, detection and response solution from Carbon Black, enabling organizations to reduce security risks in the following ways:

Identifying and Preventing DNS-Based Endpoint Communications to Malicious Domains

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

Automatically Responding to Endpoint Threats, Reducing Dwell Time

Once Infoblox identifies an infected endpoint, Carbon Black acts immediately. The security operations team no longer needs to schedule a maintenance window and spend time remediating the endpoint. The results are a shorter dwell time for the threat and more efficient security operations.

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

Infoblox

Infoblox is the leader in next generation DNS management and security. More than 12,000 customers, including over 70 percent of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-first world. Learn more at https://www.infoblox.com.

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com

© 2022 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).