SOLUTION NOTE

Data Protection and Malware Mitigation

SUMMARY

The Data Protection and Malware Mitigation Solution from Infoblox leverages infrastructure you rely on every day, DNS, as the first line of defense to block data exfiltration, DGA threats, malware activity and more. The solution also automates response and provides "crime scene DNA" to the rest of the ecosystem for faster remediation.

Malware Attacks Are Costly and Impact Brand

Ransomware attacks and data breaches can negatively impact a company's brand and stock price. In addition, digital transformations create significant security challenges. Organizations can meet these challenges by leveraging the unique security capabilities residing in core network services such as DNS. DNS is the common denominator in all modern network interactions, making it the ideal foundation for security. Ubiquitous in networks, DNS is located close to the endpoint and is as scalable as the Internet itself.

Motion of malware through a network follows a "PIE" model—penetration, infection and exfiltration (Fig. 1). In the penetration stage, the infected endpoint queries malicious domains and reports to the command and control (C&C) site. In the infection stage, the C&C server downloads additional malicious software, such as ransomware, to the infected host. In the exfiltration stage, the data is copied or removed from the network and transported offsite. All of these stages require DNS interaction, most commonly DNS lookups.

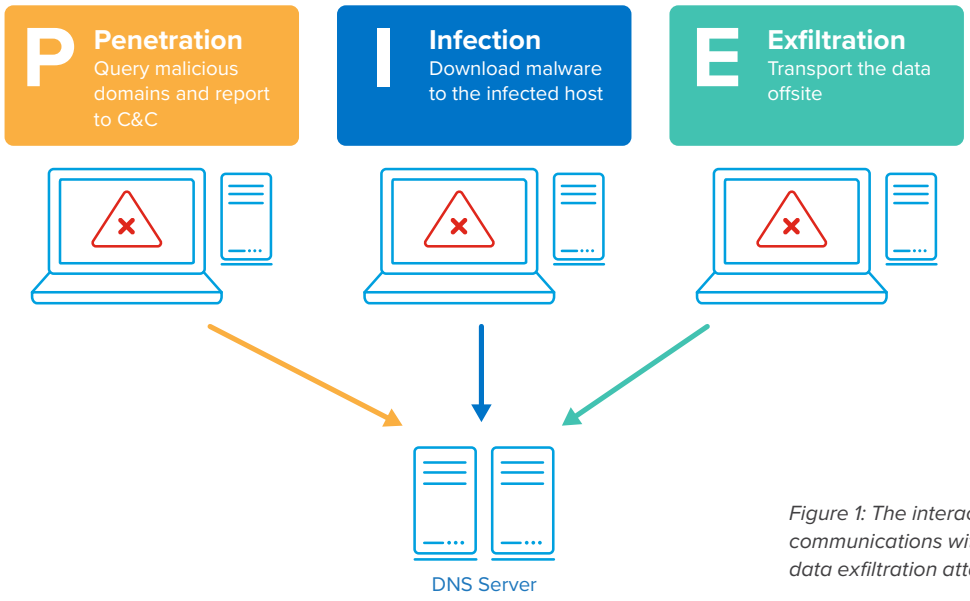

Figure 1: The interaction of malware communications with DNS during a data exfiltration attack

Raising Security to the Next Level with Infoblox Data Protection and Malware Mitigation

Infoblox reduces risk and secures your existing networks as well as digital transformations like SD-WAN, IoT and the cloud leveraging architecture that you already rely on—DNS. Critical to the fabric of the internet and any IP-based communication, DNS is the common denominator that can serve as the ideal foundation for security. Security teams are focused on stopping lateral, internal threats before any exfiltration can even begin, and the best way to accomplish this is through Internal DNS.

The Infoblox solution:

- Blocks DNS Data Exfiltration, DGA threats, malware and more using machine learning based analytics
- Detects and blocks malware activity
- Secures digital transformations including SD-WAN, cloud and IoT
- Is ubiquitous and uses a scalable hybrid security architecture that spans on-premises and cloud infrastructure
- Automates response by blocking threats and providing data to rest of ecosystem for investigation, quarantine and remediation
- Reduces remediation time and the costs associated with data breaches

Block Data Exfiltration, DGA and Malware

The Infoblox solution for Data Protection and Malware Mitigation uses a multi-pronged approach that combines reputation, signature and and machine-learning-based analytics. It detects data exfiltration via DNS and the DGA family of threats. It also proactively contains malware such as phishing, ransomware and more and stops C&C communications at the DNS choke point. It enables security teams to automatically enforce policy using the industry's most extensive and up-to-date threat intelligence—aggregated, verified and curated by the Infoblox threat research team.

Secure Digital Transformations

Digital transformations like SD-WAN introduce new security challenges. For example, SD-WAN branches directly connect to the Internet without the ability to access the full headquarters security stack, exposing remote and branch locations to risk. In addition, the rise of IoT has led to an explosion in the numbers of non-standard devices running non-standard security protocols, vastly expanding attack surfaces that can't easily be protected. Infoblox secures existing networks as well as digital transformations like SD-Wan, cloud, IoT digital transformations through a ubiquitous, scalable, hybrid architecture that spans on-premises and cloud environments.

Optimize Perimeter Security

With Infoblox, organizations can use DNS as the first line of defense to block known security risks. As a result, they can reduce the amount of junk traffic sent to perimeter defenses, such as next-gen firewalls, secure web gateways, and intrusion detection and prevention systems, preserving their processing power for more urgent tasks.

Extending Protection across the Entire Security Infrastructure

The Infoblox solution enables network-wide remediation. It automatically shares indicators of compromise using more than 30 API-level integrations with multi-vendor security ecosystem tools, including next-generation endpoint protection, Network Access Control (NAC), vulnerability scanners and SIEM.

Unified Reporting and Data Mining

With Infoblox, organizations can bolster their security response and operational efficiency through detailed and centralized reporting and by tapping the treasure trove of insights contained in historical DNS data. Available as part of on-premises and cloud-delivered Infoblox solutions, reporting and data mining capabilities enable organizations to:

- Harness rich network data to gain actionable insights that improve security responses
- Stay on the alert by continuously monitoring and analyzing networks, devices and applications for potential security events

Conclusion

With the Data Protection and Malware Mitigation solution from Infoblox, organizations can reach a higher plane of network security. Through its unique combination of advanced DNS security, centralized visibility, up-to-date threat intelligence, automation and security ecosystem integration, security teams can more easily and effectively protect devices and data inside and outside the network perimeter.

Learn more about the solution at https://www.infoblox.com/solutions/network-security.

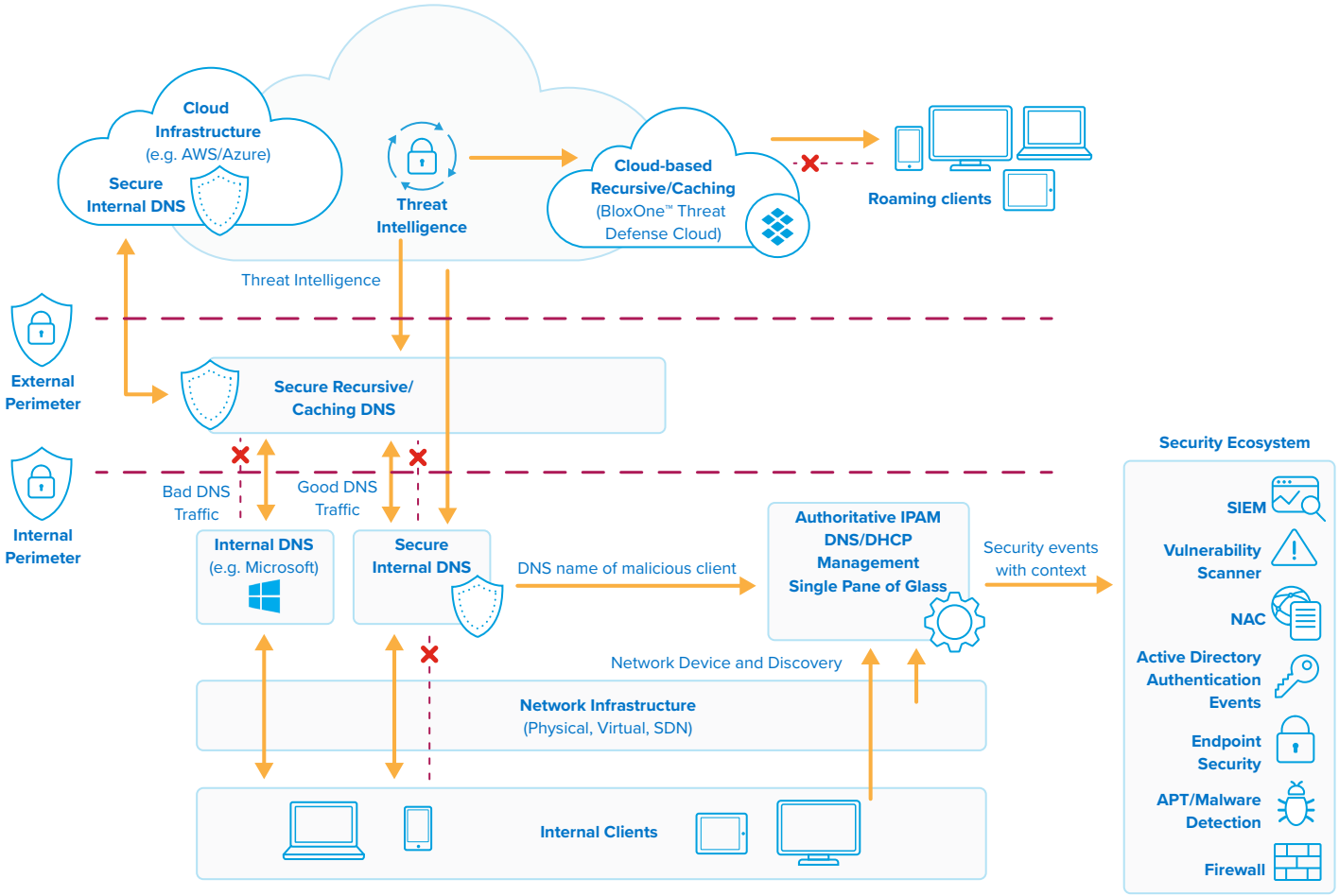

Figure 2: Key elements that comprise the Infoblox Solution for Data Protection and Malware Mitigation

Infoblox
NEXT LEVEL NETWORKING

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.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com

© 2019 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). SN-0231-00 1902