PRODUCT OVERVIEW

LogRhythm and Infoblox: Integrated Enterprise Security

The Security Intelligence Company

LogRhythm and Infoblox have developed an integrated solution for comprehensive enterprise security intelligence and continuous threat protection. Today's targeted attacks pose threats to data and systems across the distributed enterprise. Increasingly, the Domain Name System (DNS) is being leveraged to execute such attacks, making it imperative to detect malicious activities that exploit DNS, including command-and-control (C&C) communications and data exfiltration attempts. Infoblox DNS Firewall, which is based on Infoblox DDI (DNS, DHCP and IP address management) Appliance, prevents advanced malware and attacks from exfiltrating data by disrupting the ability of infected devices to communicate with C&C sites and botnets. DNS Firewall provides protection by employing DNS response policy zones (RPZs), timely threat intelligence, and optional Infoblox DNS Threat Analytics to prevent data exfiltration. Infoblox DDI also offers extensive network context that can be used by LogRhythm to take action. LogRhythm's Security Intelligence Platform automatically contextualizes and analyzes both security events and related endpoint data (e.g., IP, MAC address) it receives from Infoblox in real-time. By combining this information with other security, system and event data that LogRhythm collects from across the distributed IT environment, LogRhythm enables security teams to rapidly detect, prioritize and respond to high-risk incidents and anomalous network activity.

LogRhythm and Infoblox leverage DNS Threat Visibility for Enhanced Incident Response

- ☑ Reduce detection time for network-based attacks
- ☑ Uncover advanced malware and data exfiltration via DNS
- ☑ Pinpoint infected devices by user, IP, and more
- ☑ Streamline and automate threat response

The Infoblox and LogRhythm integration allows organizations to:

- Continuously analyze DNS activity against established behavioral baselines to detect intermittent or suspicious activity over time and quickly identify compromised endpoints and user accounts
- Increase enterprise-wide visibility by automatically associating internal and external internet activity with users and devices for accurate incident recognition and rapid response
- Detect and prevent communication with command-and-control servers, advanced attacks, and phishing attempts by associating DNS activity with other threat intelligence sources
- Automate and streamline incident response to prevent the spread of malware and reduce organizational risk

Combining Infoblox's DNS Firewall with industry-leading security intelligence and analytics from LogRhythm enables the rapid detection and remediation of attacks in progress for immediate threat neutralization.

LogRhythm

LogRhythm empowers organizations to detect, respond to and neutralize cyber threats early in the threat lifecycle to prevent damaging data breaches and cyber incidents. LogRhythm solutions also deliver rapid compliance automation and assurance, and enhanced IT intelligence.

LogRhythm's award-winning Security Intelligence Platform integrates next-gen SIEM and log management with network forensics, endpoint monitoring and multidimensional security analytics. Its collaborative incident response orchestration and patented Smart**Response**™ automation framework help security teams perform end-to-end threat lifecycle management. LogRhythm's unified solution powers the next-gen SOC, accelerating the detection and response to emergent threats across the holistic attack surface.

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 reduces the risk and complexity of networking.

LogRhythm and Infoblox are tightly integrated, bridging the value of Infoblox's DNS Firewall with the threat management and incident response capabilities of LogRhythm's Security Intelligence Platform. The combined offering empowers customers to accurately detect DNS-based threats, mitigate attacks, extend network visibility, and reduce security vulnerabilities.

Stop DNS-based Data Exfiltration Attempts

Challenge In large enterprises, high-volume, global communication is common but makes it difficult for IT administrators to identify and prevent unauthorized or suspicious data transfers outside the organization. Manually monitoring network traffic to prevent data exfiltration via DNS is inefficient and time consuming.

Solution LogRhythm can incorporate data on malicious DNS-based communications and data exfiltration attempts shared by Infoblox's DNS Firewall and Infoblox DNS Threat Analytics, including data embedded directly in DNS queries, and correlate that data against all other machine and event data from across the environment to model behavioral baselines for users, endpoints, and the network. LogRhythm can trigger a prioritized alarm when activities deviate from established baselines across multiple dimensions, such as access to confidential file servers followed by a spike in outbound web traffic.

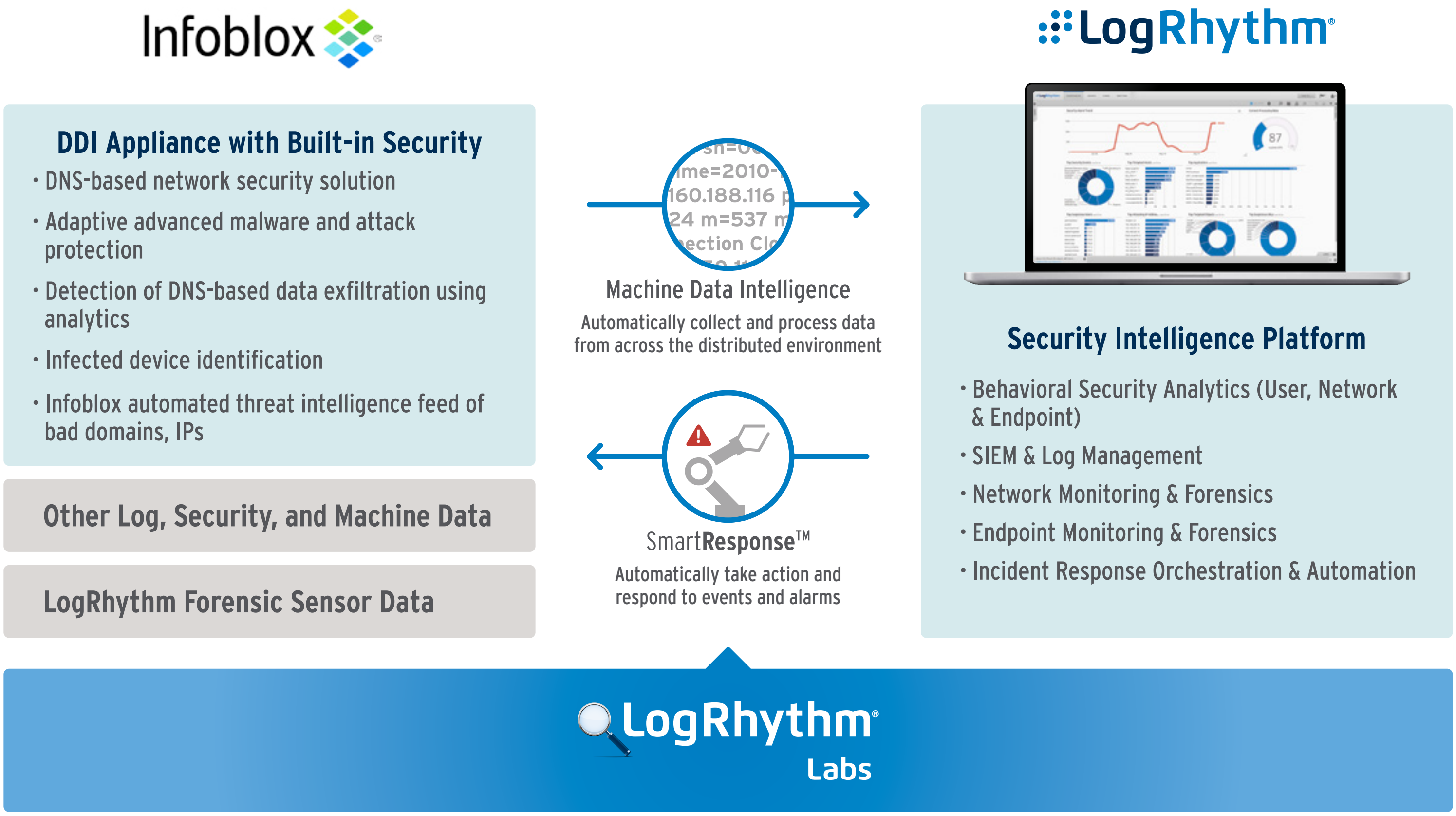
Additional Benefit From the alarm, administrators can execute a LogRhythm Smart**Response**™ countermeasure to automatically quarantine and lock down a compromised endpoint to reduce the risk of data exfiltration until further investigation can verify the legitimacy of the data transfer.

Expedite Incident Response

Challenge An IP address is dynamic and over time may be allocated to different users and systems, making it difficult for security teams to identify the end user associated with network activity, impeding the rapid investigation of security incidents. Since even one compromised device or user account can act as a starting point for an enterprise-wide breach, organizations need to be able to quickly and accurately detect and pinpoint any compromised system or account.

Solution LogRhythm collects Infoblox DHCP lease history, device IP, MAC address, user and other device data, and correlates all of that data against additional logs and event data to expose malicious activity and accurately identify compromised devices or users.

Additional Benefit LogRhythm's fully integrated Case Management capability enables analysts to build a case by aggregating corroborated evidence in a cyber-evidence locker. The case can then be shared with other analysts to facilitate collaboration with extended teams to rapidly investigate potentially compromised user accounts or devices on a prioritized basis and drive down the mean time required to respond to and remediate incidents.



Infoblox

DDI Appliance with Built-in Security

- DNS-based network security solution
- Adaptive advanced malware and attack protection
- Detection of DNS-based data exfiltration using analytics
- Infected device identification
- Infoblox automated threat intelligence feed of bad domains, IPs

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data

Machine Data Intelligence

Automatically collect and process data from across the distributed environment

Smart**Response**™

Automatically take action and respond to events and alarms

LogRhythm

Security Intelligence Platform

- Behavioral Security Analytics (User, Network & Endpoint)
- SIEM & Log Management
- Network Monitoring & Forensics
- Endpoint Monitoring & Forensics
- Incident Response Orchestration & Automation

LogRhythm Labs