SOLUTION BRIEF

SECURE WEB GATEWAYS + INFOBLOX THREAT DEFENSE—A DYNAMIC COMBINATION

Enhance defense-in-depth of both solutions through seamless integration

THE CHALLENGE

A secure web gateway (SWG) protects organizations, networks, users and devices from internet-related threats. Sitting between the user and the internet, SWGs filter out unsafe content from web traffic and block risky or unauthorized user behavior. Enterprises deploy these filters to protect employees and users from accessing or being infected by malicious websites and web traffic, internet-borne viruses, malware and other cyber threats and to help ensure regulatory compliance.

In today's dynamic threat environment, however, SWGs and other perimeter defenses can become overwhelmed by the task of scrutinizing web traffic for potential threats. In addition, SWGs are not designed to see certain malicious payloads hidden in DNS queries.

SECURE WEB GATEWAYS THAT INTEGRATE WITH INFOBLOX

zscaler™

ELEVATE SECURE WEB GATEWAY EFFECTIVENESS WITH INTEGRATED DNS DETECTION AND RESPONSE

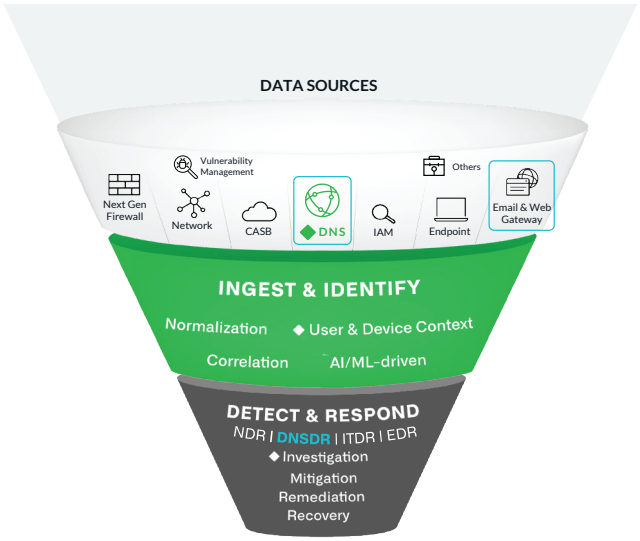
The DNS protocol plays a central role in all network communications. It is also inherently insecure, which is why it is the vector for more than 90 percent of malware and is also invoked in pervasive ransomware, data exfiltration and distributed denial of service attacks. DNS Detection and Response (DNSDR) expands the defense-in-depth of secure web gateways by identifying and remediating DNS threats that elude other security measures.

The industry's leading DNSDR solution, Infoblox Threat Defense, integrates with SWG platforms, extending the capabilities of each solution and elevating overall SecOps effectiveness. It delivers these benefits by:

- Reducing overall malicious traffic to SWGs by blocking threats at the DNS level before they reach these solutions, thereby extending the life of the web gateway investment and/or reducing the number of gateways needed, resulting in cost savings
- Unifying domain blocking and HTTP security for broader security protection
- Speeding the detection of malicious traffic originating from infected endpoints, regardless of the endpoint's location (on-prem, remote and cloud)
- Complementing web gateway content filtering capabilities by restricting user access to certain web content categories based on DNS threat intelligence for more efficient policy enforcement
- Complementing the SWG policies with researched-backed DNS-based threat intelligence

DNSDR ENHANCES SECURE WEB GATEWAYS AND THE ENTIRE XDR ECOSYSTEM

DNS Visibility and Secure Web Gateways Work Work Together in the XDR Framework

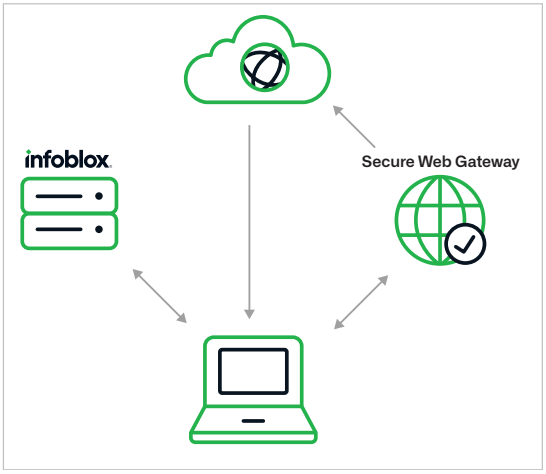


DNSDR and secure web gateways are essential components of extended detection and response (XDR) solutions. DNSDR implementations like Threat Defense improve the performance and efficiency of not only secure web gateways but also core XDR capabilities across the security ecosystem. Through APIs and pervasive automation, Threat Defense blocks threats at the DNS level, protecting users with verified threat intelligence and enabling SecOps to reduce Mean Time to Respond (MTTR) for fast-moving cyber threats.

TOP 10 REASONS CUSTOMERS CHOOSE THREAT DEFENSE

1. Accelerate Time to Value
2. Detect Threats Other Solutions Miss
3. Achieve Anywhere, Hybrid Visibility and Control
4. Stop Attacks Earlier in the Attack Chain
5. Boost SecOps Efficiency
6. Speed Investigation and Response by 3X
7. Unlock the Power of DNS Threat Intel
8. Optimize the Security Ecosystem
9. Get More from Security Investments
10. Gain Greater Context by Merging IPAM with DNS

HOW INFOBLOX AND SECURE WEB GATEWAYS INTERACT



To learn more about the benefits of our Cybersecurity Ecosystem visit https://www.infoblox.com/products/cybersecurity-ecosystem/

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054