INSIGHTS | SOLUTIONS BRIEF

Expose Hidden DNS Threats With WEI & Infoblox

DNS is one of the most commonly exploited layers in modern attacks—and one of the least inspected. While endpoint and network detection tools may catch known threats, DNS-layer visibility uncovers connections, and vulnerabilities those tools often miss.

As a Skilled to Secure Sapphire Partner with Infoblox, WEI delivers a low-lift, high-impact DNS Security Assessment that gives organizations the insights needed to strengthen posture, fast.

ASSESSMENT MODES

- **Gap Analysis:** Quantifies the additional protection Infoblox provides to your existing security stack, offering a side-by-side comparison of what's currently missed versus what's preventable.
- **Live DNS Analysis:** Examines your DNS queries to highlight security gaps and misconfigurations. No infrastructure changes required—data can be pulled from existing DNS logging or forwarding.

EXECUTIVE-READY REPORTING

- **Prioritized list of security gaps:** Risks are clearly categorized and ranked based on potential impact and ease of mitigation.
- **Devices showing threat activity:** Includes IP addresses and known indicators tied to infected or at-risk endpoints observed in your DNS logs.
- **Indicators of misused or misconfigured DNS components:** Highlights DNS hygiene issues such as stale records, unresponsive servers, and misaligned configurations that reduce effectiveness and increase attack surface.
- **Recommendations to block threats and strengthen posture:** Every issue comes with a vendor-agnostic fix, aligned with best practices—so action can be taken immediately, even before choosing a solution.

KEY ASSESSMENT FEATURES

No-Risk Security Insight With WEI

Discover hidden vulnerabilities without cost or commitment.

WEI offers a DNS-layer security assessment that provides deep visibility into network and infrastructure health—without any obligation to purchase.

This assessment is designed to take **15 minutes to run.** It is light on resources and focused on giving your team real insight into potential risks and misconfigurations that may be going undetected.

WHY CYBER LEADERS ENGAGE:

- Receive a detailed report exposing vulnerabilities and signs of active threat behavior
- No cost to participate
- No commitment to buy

View a sample report and request a DNS assessment

Inspect live DNS queries to reveal advanced threats and anomalies that may already exist in your environment:

- **Queries to known malicious or suspicious domains:** These domains are often tied to phishing campaigns, botnets, and ransomware delivery networks. Detection suggests that endpoints may be interacting with known threat actor infrastructure.
- **DNS tunneling used for covert data exfiltration:** DNS tunneling encodes information in DNS packets to bypass perimeter defenses and is often used for command-and-control communications or data theft.
- **Use of domain generation algorithms (DGAs) linked to malware:** DGAs are employed by sophisticated malware families to obscure communication with command centers.
- **Command-and-control communications:** These outbound connections help attackers maintain control of infected devices within your network, often operating undetected through traditional layers.
- **Lookalike domains and brand spoofing:** Spoofed domains impersonate trusted brands to deceive users and steal credentials. Their presence may reflect active phishing campaigns or reconnaissance efforts.

WHY WEI?

WEI brings technical depth and strategic perspective to every assessment we deliver. Our team supports clients from initial data capture through insight delivery—translating DNS-layer signals into real-world security improvements.

This is not a lab test. It's real telemetry, pulled from your actual environment, analyzed by expert engineers, and delivered back to you as a prioritized, actionable report. Whether you're looking to identify live threats, validate infrastructure hygiene, or uncover gaps in your current security stack, WEI makes the process easy to engage—and valuable from day one.

Contact WEI to schedule your assessment that takes just 15 minutes to run.

Request Assessment

EXAMPLE ROLLUP SUMMARY

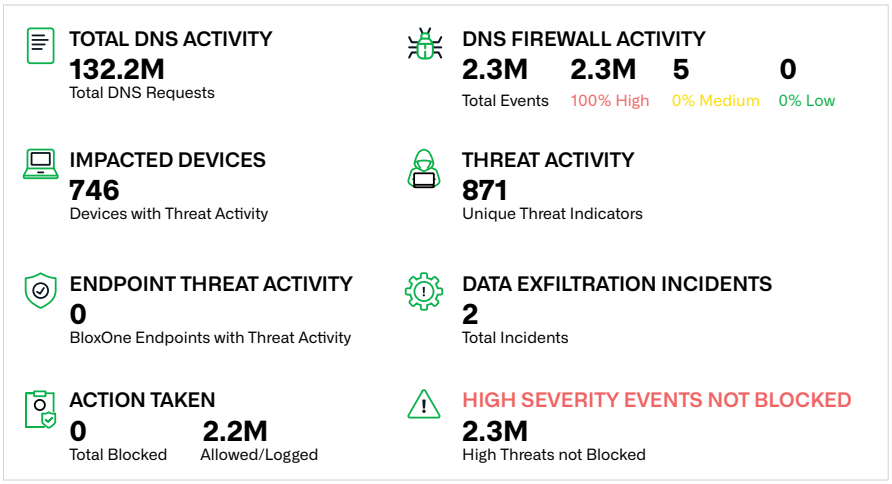

Figure 1: Summary example of identified threats