infoblox

TOP 7 REASONS WHY DNS MTTRs TO SECURITY PROS

YOU'RE FACING CRITICAL SECURITY CHALLENGES

With breaches averaging $4 million,[1] the stakes have never been higher. Infoblox Protective DNS stops threats before they hit users, endpoints or data—giving security teams the early advantage they need to reduce risk and stay ahead.

Threats are getting more sophisticated.

Adversaries constantly evolve to evade traditional defenses. DNS enables preemptive detection at the earliest stages, helping neutralize threats before they escalate.

Security teams are overwhelmed.

With limited resources and growing alert fatigue, teams need smarter, earlier signals. DNS provides early insights that reduce noise and help security teams focus on what matters most.

Hybrid work expands the attack surface.

Remote users, cloud apps and unmanaged devices make visibility and control more difficult. DNS provides a consistent, preemptive layer of protection across environments.

Point tools create blind spots.

Siloed solutions leave exploitable gaps. DNS helps unify visibility and control, enabling early-stage threat detection and faster response.

270+
DNS can detect and block over 270 types of threat indicators providing broad, early-stage coverage across the kill chain.

92%
DNS-layer security can reduce time to detect and remediate threats by up to 92%, helping teams act faster and more decisively.

82%
DNS-layer security can protect against 82% of threats before impact.

68.4 DAYS
DNS can detect threats on average 68.4 days before other tools.

0.0002%
DNS-layer security has a false positive rate of just 0.0002%.

TOP 7 REASONS WHY DNS MTTRs TO SECURITY PROS

1. **DNS is a Strategic Control Point:** DNS is foundational to how users and devices connect to the internet. It offers a unique vantage point to detect and block threats earlier in the attack chain before they **reach endpoints or networks.**

2. **Preemptive Threat Detection:** DNS identifies malicious activity at the earliest stages before a full connection is made. This enables security teams to act preemptively, reducing dwell time and limiting exposure.

3. **Fills Visibility Gaps:** DNS provides visibility into traffic that other tools may miss, especially in hybrid and remote environments. It helps uncover shadow IT, rogue devices and evasive threats that bypass traditional defenses.

4. **Accelerates Threat Investigation:** DNS logs offer rich context for threat hunting and incident response. Security teams can quickly trace malicious domains, map attacker infrastructure and correlate events across the kill chain.

5. **Reduces Risk Without Adding Friction:** DNS-layer security operates silently in the background, protecting users without impacting performance or requiring endpoint agents. It's a lightweight, high-impact layer of defense.

6. **Enhances Existing Security Investments:** DNS security integrates with SIEM, SOAR and XDR platforms to enrich alerts and automate responses. It strengthens the efficacy of your broader security ecosystem.

7. **Supports Zero Trust and SASE Strategies:** DNS plays a critical role in enforcing policy and verifying trust before access is granted. It aligns with Zero Trust principles and supports secure access in cloud-first, hybrid environments.

1. "Cost of a Data Breach" Report 2025, IBM, 2025.

See and stop threats earlier, reduce the burden on SecOps, accelerate your MTTR and give your company the DNS strategic security advantage it deserves.

LEARN HOW AT
infoblox.com/dns-mttrs

Read the Forrester Total Economic Impact study.

Discover the hidden potential of DNS in security.

See how Infoblox Threat Defense™ helps you reduce MTTR.