

# TOP 7 REASONS WHY DNS MTTRs TO SECURITY PROS



## DNS is not just for networking anymore.

DNS is increasingly vital as a first line of defense to secure your expanding network infrastructure and reduce your Mean Time To Respond (MTTR).

## YOU'RE FACING CRITICAL SECURITY CHALLENGES:



### Expanding attack surface

As WFA and multi-cloud needs grow, there are more opportunities for malware, C2, lookalikes and other threats to bypass current defenses.



### User and device blind spots

Security has no unified, real-time view of all network users and devices, including multi-cloud and IoT/OT.



### Lack of vital resources

The security skills gap and resulting burden on SecOps means critical alerts are being missed on a daily or weekly basis.



### Slow investigation & remediation

Delayed access to user and device forensics bottlenecks investigations and extends threat dwell times, exposing your business to more damage.

# \$4M

Average cost of a data breach

# 270+

Hours on average to identify and contain threats

# 92%

Of malware leverages DNS for command and control

## HOW DNS DETECTION AND RESPONSE HELPS YOU SOLVE THESE CHALLENGES AND MORE:

# 1

### Identify threats sooner

Map DNS queries to user and device activity in real-time using IPAM DNS-based application discovery.

# 5

### Shut down lookalikes

Use AI/ML analytics on DNS queries to more quickly detect DGAs, data exfil and sophisticated Lookalike domains.

# 2

### Stop attacks faster

Use advanced threat intel to block phishing, ransomware, malware, C2, DGA, data exfil and others sooner.

# 6

### Automate security ROI

Automate ecosystem integrations to share DNS data with SOC tools and allow SecOps to better prioritize alerts and minimize efforts.

# 3

### Protect systems anywhere

Safeguard your expanding attack surface by defending across clouds and on the edge, including IoT/OT.

# 7

### Use less resources

Unite networking and security information to see and stop threats sooner, and enable SecOps to do more with less.

# 4

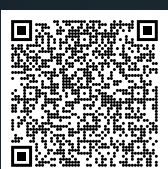
### Block emerging threats

Leverage global threat hunting to detect emerging suspicious domains and block them up to 3 months sooner.

# DNS MTTRs

## Learn more about how Infoblox DNS Detection and Response

drives huge economic benefits by improving your proactive security and accelerating Mean Time To Response across your enterprise.



Read the **Forrester Total Economic Impact™ study today**

