

2025 Forrester Opportunity Snapshot

Embrace DNS Security And Overcome Hurdles Of Cloud Adoption



Traditional Security Approaches are Unsuitable in a Cloud-driven World

Complex cloud environments are outpacing perimeter-based security models & tools

New Risks

Wider Attack Surfaces

More DNS-based Attacks

71%

security leaders struggle with complexity of hybrid cloud environments

DNS Security is Viewed as Core Pillar of Overall Cybersecurity Strategy

91%

security leaders prioritize DNS Security to protect hybrid environments

90%

view DNS Security as important as firewalls for monitoring suspicious activity

DNS is a Multifaceted Threat to Critical Assets

95%

orgs have experienced DNS-related incidents in the past year

Phishing Ransomware DDoS Attacks

Average cost per attack: **\$1.1M**

67% of orgs lack visibility into DNS traffic, deep DNS analytics, and intelligence

Business Impacts of DNS Attacks are Severe:

62% disruptions to system availability

61% financial impacts

59% brand damage

Security Strategies Are Evolving From Reactive to Proactive to Strengthen Resilience

84%

Boost identity and access management by enforcing multifactor authentication or Zero Trust Architecture

85%

Perform regular audits of DNS configuration to identify and mitigate vulnerabilities

Key Takeaways

- 1 Adapt** your security strategy to ease cloud complexity
shift toward new automated solutions to respond to evolving threats
- 2 Embrace** DNS security as frontline defense
enhance visibility / threat detection / policy enforcement
- 3 Invest** in strategic pillars for strengthening resilience
threat intelligence / AI-driven technology

GET THE FREE FORRESTER STUDY

