Balancing Security and Privacy with DoT and DoH

DNS is fundamental to the Internet. But it wasn’t built with security and privacy in mind. So it’s more important than ever to balance user privacy with security.

Two new developments are improving DNS privacy: DoT and DoH.

Both encrypt communication between the endpoint and recursive resolver.

But there’s a catch: they allow people to sidestep enterprise DNS controls.

That could lead to:
- Exposure to data exfiltration and malware proliferation
- Loss of visibility

Both are designed for privacy.

Endpoint communications are not encrypted, making them open to:
- Snooping
- Interception
- Data theft

Third parties and bad actors can learn a lot, simply based on what sites people access.

47% of organizations in a recent survey experienced DNS phishing.

7 in 10 employees struggle with cyber awareness.

64% of organizations say the “last mile” is the data security area they need to focus most on.

Circumventing the internal DNS infrastructure is a bad idea.

The right best practices can help you solve the “last mile problem.” Without compromising security.

The solution?
- Block access to unauthorized DoT/DoH servers
- Use internal DNS resolvers to retain control and security

It’s time to get proactive about DNS security.

Read the Solution Note