

DNS GUARD



KEY BENEFITS

- Protects brand reputation
- Improves customer satisfaction and retention
- Reduces malicious traffic on the network
- Protects all client devices, including Internet of Things (IoT)
- Deploys without client software or additional network devices
- Prevents the loss of revenue from bandwidth piracy
- Prevents the theft of sensitive information via the DNS

KEY FEATURES

- Mobile and fixed line network support
- Real time updates
- Covers phishing, scam, botnet communication and malware distribution sites
- Blocks DNS tunnels
- High quality - extremely low false positive rate
- Multiple data sources ensure comprehensive coverage

Despite spending billions of dollars on endpoint security software, the world's security problem is getting worse. Existing endpoint security relies on consumers for proper management, a task that is either overlooked or too arduous for many consumers, especially across the variety of smart devices, including IoT, used in today's networks. Network-based security appliances add complexity and latency to the network while raising concerns about privacy.

Secure64 DNS Guard is a family of DNS-based security services that protects the network and its users from harm. Because it operates within the network, DNS Guard protects users without requiring installation of any software and protects all types of IP-enabled devices, including desktops, tablets, smartphones and CCTV's, refrigerators and routers.



Secure64 DNS Guard consists of the following separately purchasable services:

MalwareGuard - Protects users from sites that download malicious software such as viruses, trojans and worms. Blocks communication between bot-infected devices and their command and control centers so the bot is rendered harmless.

FraudGuard - Protects users from visiting sites known to conduct illegal activity, such as phishing, fraud or other online scams.

TunnelGuard – Blocks DNS tunnels that are used for data exfiltration, bandwidth piracy and evasion of regulatory controls.

Protecting customers is good business. Carriers can improve their reputation and reclaim lost bandwidth by eliminating denial of service and spam traffic from their networks. They can reduce customer support costs and churn by preventing device infections that can cause a poor end user experience. And they can protect revenue and improve security by eliminating DNS tunnel traffic that can be used to bypass data limits or exfiltrate stolen information.

