SECURE64™

Secure64® DNS GUARD™

Reduce churn through user protection

DATA SHEET

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
- Complements other security efforts

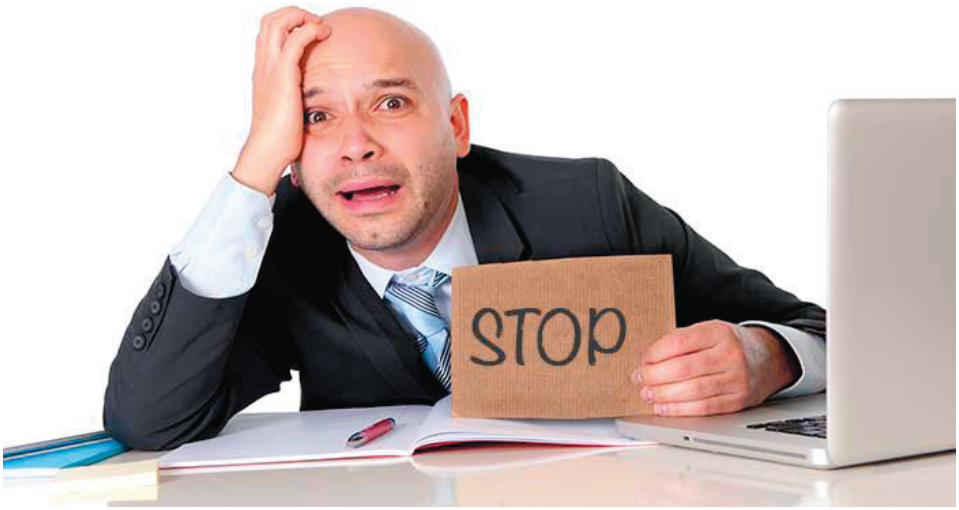
KEY FEATURES

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

D N S G U A R D

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 CCTVs, refrigerators and routers.

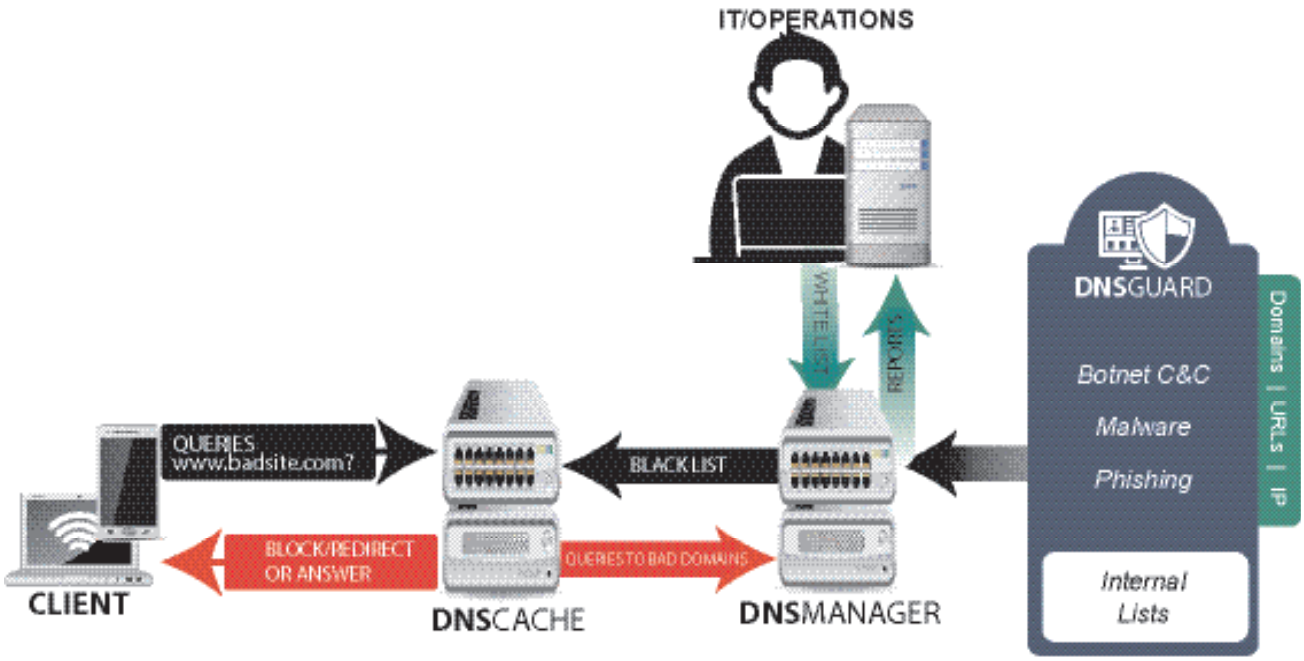


Secure64 DNS Guard consists of the following separately purchasable services:

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.

Protecting customers is good business. Carriers' reputations can be damaged by allowing their networks to be used for distributed denial of service attacks or conveying spam traffic. They can be unfairly blamed by users with infected devices for poor performance, and infected devices can consume valuable bandwidth to perform illicit activities. By preventing these infections from occurring in the first place or by neutralising bot communications, carriers can improve the customer experience, reduce churn and optimise network efficiency.



c-cor 2 Anzed Court Mulgrave VIC 3170 Australia | T: +61 3 8542 0600 sales@c-cor.com.au | www.c-cor.com.au