OneGuard

The Ultimate OnNetwork cybersecurity Protection

Key Features

- Comprehensive protection against DNS attacks
- Robust defense against online threats to subscribers
- Complete content control by device/account
- Continuously updated threat databases
- Comprehensive reporting

Key Benefits

- Protect subscribers from phishing, malware, and other attacks.
- Allow subscribers to block objectionable content
- Generate new revenue
- Reduce subscriber churn
- Increase customer satisfaction
- Reduce network capital expenses
- Improve brand value

Generate New Revenue

Improve Brand Value

Increase Customer Satisfaction

Offer comprehensive security to your subscribers, protecting your network and driving new revenue

As the world grows more connected and the role of service providers continues to evolve, opportunities for new services and revenue streams have emerged. Offering value-added services like content filtering and advanced subscriber security features represents a major boost to your bottom line, while significantly decreasing networking costs and increasing customer satisfaction.

Backed by our proprietary database and filtering tools, Secure64 OneGuard eliminates malicious traffic from your network and protects opt-in subscribers from the ever-increasing number of threats online. In addition, it provides subscribers with complete control over other potentially objectionable traffic.

Whether it's parents looking to block adult content from their children or businesses seeking to enforce Acceptable Use policies on employee devices, Secure64 OneGuard makes it possible. The dark corners of the internet are too easy to access but easy to protect against. Your subscribers are ready to pay for these solutions, and they trust you, their service provider, to provide them. Don't miss out on this opportunity.

Industry-Leading DNS Security

Secure64 OneGuard protections are delivered through Secure64 DNS Cache, a secure DNS resolver deployed in tier one carrier environments around the world and processing queries from over 1 billion subscribers. Running on SecureOS, a security hardened operating system, DNS Cache provides built-in protections against the variety of attacks that are waged against DNS servers today, including direct, reflected, and amplified flood DDoS attacks, cache poisoning attacks, PRSD (water torture) attacks, spoofing attacks, DNS tunnels and many others. And because DNS Cache is not based on BIND, it is not vulnerable to any BIND-specific vulnerability exploits.

Unmatched Subscriber Protection

Global Threat Intelligence

Secure64 OneGuard uses a combination of third party and proprietary threat intelligence feeds to provide the most comprehensive threat protection available. The proprietary threat intelligence feed is powered by a distributed infrastructure located in over 200 data centers around the globe. This infrastructure utilizes web crawlers and analyzers that process over one trillion data requests and meta data every month - identifying, analyzing, and categorizing new domains as they appear on the internet.

Feedback Loop

If a user-generated query contains a domain that has not been seen before, the domain is sent to the security research team for analysis and categorization, and the threat intelligence database is quickly updated with this information and synchronized with all customers. As attacks are becoming more targeted against a specific region or country, this fast feedback loop protects against unknown, fast-moving attacks and greatly reduces the amount of time that bad actors have to utilize newly registered domains for malicious purposes.

Robust Content Filtering

Domains are assigned to one of over 40 categories. End users or company administrators can easily select categories to block while also being able to allow or deny specific domains regardless of category.

Comprehensive Protection With Real-Time Updates

The threat intelligence feed contains over 300 million entries that are continuously updated as new threats are discovered. Customers receive updates at a maximum of every 4 hours.

Visibility

Every query that is blocked or redirected is captured, stored, and made visible to both opt-in subscribers and communication service provider teams. Opt-in subscribers can see exactly what was blocked, when it was blocked and why it was blocked through a simple web portal or through an app on their device. Internal CSP teams can access information across one or more subscribers through a robust web portal.

Simple Management

The Secure64 OneGuard solution includes DNS Manager, which greatly simplifies operational tasks such as DNS monitoring and alerting, server configuration management, software version management, and threat intelligence feed management, reducing the burden on your engineering and operational teams.

Secure64 Software Corp.
2900 S College Ave. #2A
Fort Collins, CO 805254
1-303-242-5890
www.secure64.com