SECURE64™

SECURE64 ENTERPRISE EDGE

The Always On Security Solution

FEATURING:

- Up to date lists delivered from the Secure64 Security team blocking Malware, Ransomware, Phishing and other inappropriate sites.
- Always on always protecting security solution
- Content Control platform to block inappropriate categories and sites on the internet.
- Cloud-based, constantly evolving, privacy-focused reporting engine.

SECURE64 ENTEPRISE EDGE

The Always On Security Solution

Simple protection for what matters the most

Secure64 Enterprise Edge is a solution to the issues of protecting any device in the network whilst maintaining low latency. Secure64 Enterprise edge is based on our carrier grade technology and delivers the same benefits and performance required in the largest of networks to the enterprise.

The key elements of the solution are:

- Caching DNS installed in the enterprise network to deliver low latency high performance caching DNS resolution.
- Automatically update feeds to prevent access to malware, phishing, and ransomware command and control sites.
- Automatic Data Exfiltration Blocking via DNS Tunnels.
- Content blocking by categories such as Alcohol, Gambling, Social Media, etc
- Simple to use, cloud based reporting GUI.
- A scalable solution from 1000 users to millions of users.
- DNS Anycast capable platform.

Security is at the heart of this platform, with an always-on, constantly updating list of sites hosting Command and Control for Malware, Phishing, and Ransomware. Every DNS query is evaluated against this list, and where a match is found, the site is blocked with a reason embedded in the DNS response using RFC8914. Lists are fed from geographically distributed Secure64 facilities around the world.

Simple to use GUI platform:

A simple to use cloud-based reporting GUI is included with the solution, and customers can opt to obfuscate the IP addresses logged at source and displayed in the platform.

The reports include:

- Number of queries
- Top ten talkers
- Security threats
- Top domains

As we create new reports these are automatically added to the platform for system administrators to benefit from.

Local SIEM integration:

Logs of threats being blocked can be exported to Kafka or Raw log files for integration with a locally provided SIEM platform that the customer already has.

Local blocking lists:

Where customers have a local list that needs to be blocked, this can be integrated with the solution using RPZ.

Work from anywhere:

With a Secure64 Enterprise Edge platform, your users can work from anywhere on their own devices. A simple client for Windows, Mac OSX, Android or iOS allows complete content control and protection irrespective of how or where they are connected. Protection can be in the home or on the road.

For enterprises that want to offer even greater protection, a simple in-home router can automatically connect any WiFi-connected device to the network and offer content control. Dynamic IP addressing is catered for with the solution allowing dynamic WAN connections. With this solution, the protection follows the user even if their internet IP address changes.

Questions? Contact Us:
1-303-242-5890
sales@secure64.com

Content blocking:

A simple network-wide policy can be deployed to block categories of the Internet. Over 57 different categories are available to be blocked or allowed, including:

- Gambling
- Alcohol
- Adult Content
- Tobacco

Safe Search for several search engines is an optional configuration redirecting the domains of Google, YouTube, Bing and other search engines. The results returned on searches are then altered by the search engine used.

Scalable performance:

Designed for customers with over 1000 users, the platform scales to millions of users using COTS hardware running Linux. The core of the system is installed in the network to ensure the highest performance. BGP Anycast is included to allow the enterprise to scaler and build a reliable platform.

Security updates:

Using an open accessible core, the system administrator controls security updates and when they should be applied.

Simple deployment

Available as a single ISO or QCOWS2 image, the platform is simple to install and deploy on COTS hardware in network with the reporting engine in a cloud environment. This ensures the highest performance with the lowest TCO. Privacy is preserved as IP addresses can be obfuscated in flight and at rest before being sent to the cloud. The benefit for a customer is that as reports are developed and insights are made into the traffic, the customer gains the benefits of a continuous development of the solution without costly upgrades.