Delivering advanced content control for a large US Carrier

What was the solution delivered?

A large US carrier with over 125 million subscribers already saw the benefits of providing a content control and cyber security platform. This solution protects over 6 million subscribers from residential, businesses, libraries, schools and government organizations.

6 million Subs

The platform generally processes around 5.5 billion queries daily and blocks around 2 million cyber security threats every 24 hours.

The carrier had a relationship with Cisco and deployed Cisco Umbrella to provide this type of filtering. At the end of the contract, the customer faced a significant rise in costs for using Cisco Umbrella. The customer also wanted more reporting and API usage to allow the platform to become integrated into the customer support platform the CS Agents run.

Two million cyber threats per day

With the rising costs of the Cisco Umbrella solution, the carrier decided to explore alternate solutions and generate cost savings while maintaining the same service and blocking capabilities.

One fundamental consideration was integrating the solution quickly and without changes to how filtering was applied in the existing network.

What were the technical requirements of the solution?

The solution had to deliver content filtering at scale for around 6 million subscribers.

The platform had to filter based on both EDNS codes injected into the DNS query from the client by the gateway and fixed IP addresses as used by the forwarding DNS or the client. The policy needed to be flexible enough to recognize these EDNS codes and IP addresses, allowing total flexibility.

Different gateway vendors from significant equipment manufacturers can inject the EDNS code, and the solution must filter based on the code. The code relates to the policy and

groups of users that require a specific policy. Over 12 different policies from the same carrier have been used, and more are planned for the future.

Full reporting from the platform was required, along with an API interface for the carrier to integrate the solution into its own technologies. This would enable the call center agents to view policy settings at a glance within their existing solutions.

Critical to the deployment was the use of the Global LineGuard network to process this amount of traffic.

How quickly was the solution deployed?

1 million subs, 5 minutes to change

It took 6 weeks from the first live traffic to the complete rollout. Using automated tools, the last change window cut over 1 million subscribers in 5 minutes. The only change on the estate was repointing the DNS traffic from the in-network DNS servers to the LineGuard global Anycast addresses.

What financial benefits has the customer achieved in this change?

50% saving over 3 years

The primary benefit was the reduction in the cost of the service.
The costs more than halved over 3 years. On top of this, the customer has been able to generate savings as the number of in-network DNS servers has been reduced because LineGuard, unlike Umbrella, can filter on EDNS and Source IP from the same DNS server.

What latency benefits has the customer achieved in this change?

LineGuard in the region is around 1/3rd faster than Umbrella at the time of this paper. This means the latency for the solution has dropped significantly, benefiting every customer using it.

33% Faster

How many threats does the system block in a day?

100 million block actions daily

The solution blocks about 2 million threats and approximately 100 million block actions for content categories daily.

What are the next steps for the solution?

Secure64 collaborates with customers to analyse their network and operations, leveraging advances with LineGuard. We have already informed the customer about several benefits. For instance, AI category blocking can now be integrated for business customers, enhancing Lineguard with these additional features.

Secure64 pDNS vendor

Secure64 Guard platforms have been listed by the Cybersecurity and Infrastructure Security Agency as a vendor that can supply a Protective DNS platform : https://media.defense.gov/2025/Mar/24/2003675043/-1/-1/0/CSI-SELECTING-A-PROTECTIVE-DNS-SERVICE-V1.3.PDF

About Secure64

Secure64 brings trust to the internet through its suite of purpose-built, secure, DNS-based network security products. The company was built on a foundation of security, stability, and safety and has forged solutions that are self-protecting and not only immune to malware but also actively protect subscribers against Malware and phishing attacks. Secure64 secures the DNS infrastructures of leading service providers, government agencies, and enterprises globally.

Secure64 solutions
Our DNS supports a worldwide subscriber base of over 1.5 billion, representing over 20% of global mobile subscribers. Performing billions of DNS lookups every day across six continents, Secure64 lives up to its reputation for providing highly secure, safe, and stable DNS solutions.

Secure64 is a privately held company with deep technical and global experience in its leadership and technical staff. It is the only DNS solution provider that has authored a secure micro OS, automated the deployment of DNSSEC and built self-protecting DNS servers. For more information, visit www.secure64.com or contact sales@secure64.com

About Premier Systems Sales Ltd

Premier Systems Sales Ltd is a Woman Owned Small Business (WOSB/WBE) certified, ISO9001/2015, CMMC Level 1, DCAA Compliant Financials, with both federal and state contract vehicles.
Woman Business Enterprise (WBE), PA SDB Certified, PA-COSTARS Contract # 003-461, IT Hardware, Commonwealth of PA IT Contract, GSA Contract: GS-35F-0365U, Seaport-e (Prime Contractor)

NYC Vendor ID#: VC00203073. NASA SEWPV Prime (JV), NIH CIO-CS Prime (JV)

Premier Systems Sales Ltd is authorized supplier of Secure64 for DNS and LineGuard.

www.PremierSystemsLtd.com