MAJOR US CARRIER DEPLOYS LINEGUARD

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 agencies and saved 50% of the cost of the alternate solution over 3 years

REPLACING CISCO UMBRELLA

Why did the carrier take this step?

The US carrier was facing mounting costs for using Cisco Umbrella and needed to look at alternatives. Secure64 LineGuard has been designed to replace Umbrella and integrate into an existing deployment. This this case, the customer needed the EDNS features for policy decision to be available. Secure64 LineGuard supports policy decision making using EDNS as well as source IP network ranges.

What was the benefit for the customer?

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.

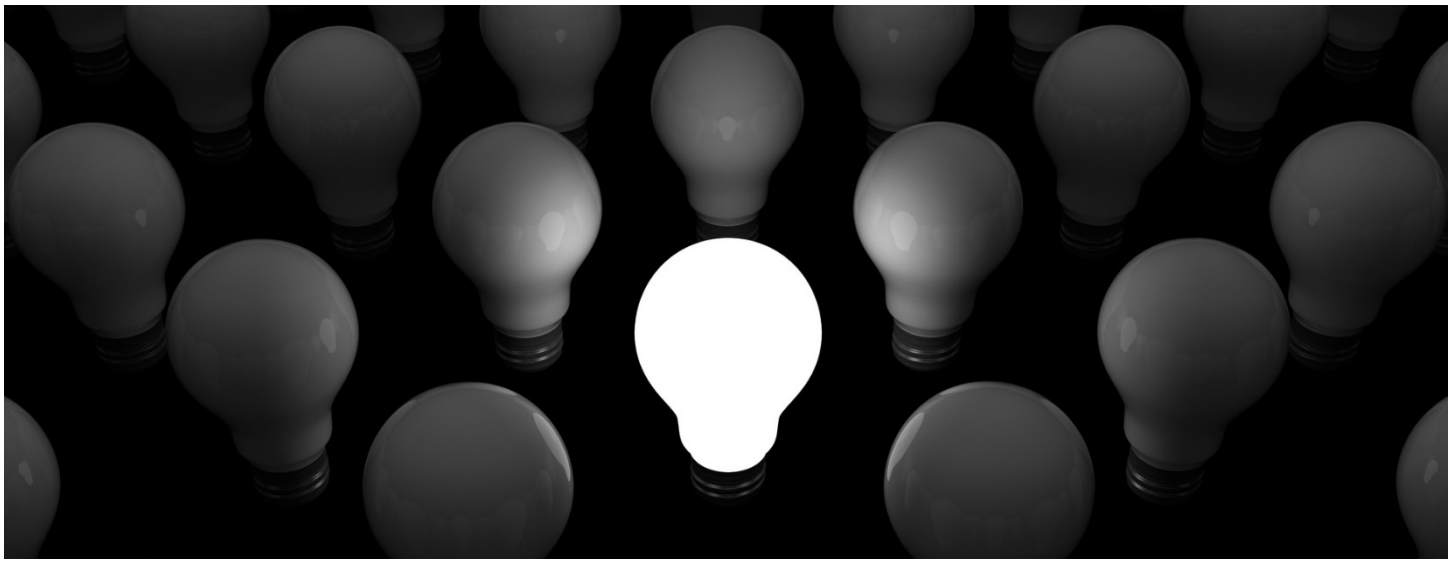


Figure 1

What else improved with this new deployment?

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.

Additionally, the customer how has more reporting capabilities and they utilize the included API with the platform to generate their own reports, provision users, search the database and number of other functions to help the customer agents provide reduced time to resolution for customer queries.

How many threats does the system block in a day?

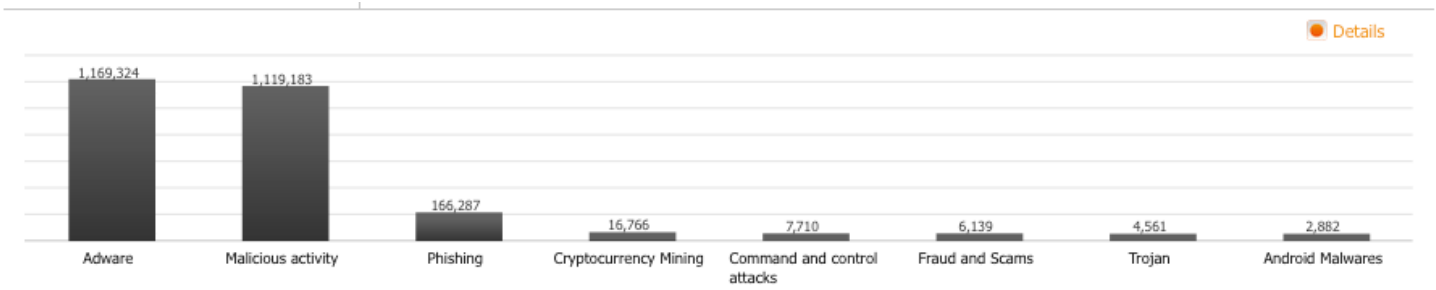
The platform performs around 100 million block actions every day for cyberthreats and content blocks. Overall the platform for this one customer processes close to 6 billion queries every 24 hours from around 6 million subscribers.

BLOCKING MALICIOUS TRAFFIC

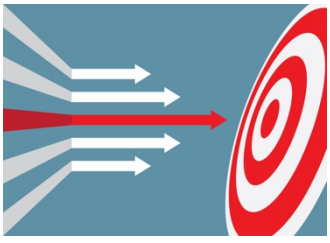
Secure64 LineGuard in this deployment blocks a large number of threats, cyber attacks and malicous traffic every day for this customer. This has benefits to the end user.
In a 24 hour period, the platform processes almost 5.8 Billion queries

Threats detected	Blocked requests	NX - Not existing	Total DNS requests
2,148,285	119,809,121	297,991,585	5,751,976,096

There is a wide spread of Threats. The graph below shows an example of the type of threats seen in a 24 hour period.



Malware	Requests	Malware	Requests	Malware	Requests
Adware	1,169,324	Android Malwares	2,882	Riskware	267
Malicious activity	1,119,183	Trojan Downloader	1,721	Virus Hoax	150
Phishing	166,287	Backdoor	1,322	Remote Access Trojan	78
Cryptocurrency Mining	16,766	Spyware	1,084	Ransomware and Cryptowall	12
Command and control attacks	7,710	Exploit	476	Trojan Dropper	5
Fraud and Scams	6,139	Botnet	462		
Trojan	4,561	DGA - Domain generation algorithm	456		



LineGuard protects every device type of this ISP, regardless of the operating system.
Utilizing an AI-generated list for protection and site classification backed by Human resources ensures up-to-date protection.

6 Million subscribers gain the benefit of an always on protection with an always up to date list.

LINEGUARD DEPLOYMENT

LineGuard is a cloud-based solution and can be deployed at scale quickly for customers. Secure64's Customer Success Managers worked with the customer to map the policies from the existing solution to the new platform. As the Secure64 team has many years of experience in this type of solution, the deployment time was greatly reduced to a few weeks.
Another benefit of the solution was that the customer didn't have to deploy more network DNS servers, as LineGuard supports EDNS and network mapping to a policy from the same source IP address. This limitation in the existing deployment would have resulted in the customer eventually having to deploy more internal DNS servers to work around this limitation.

Mapping Categories to Policies

Policies are the solution's fundamental construct and define what categories, sites, and apps the platform blocks. In the Carrier network, traffic is tagged by the various manufacturer gateways to assign a policy via an EDNS field.
Secure64 collaborated with the customer to map the policies and enhance them to leverage the more granular categories and app blocking features available within LineGuard, compared to the existing platform.

Deployment timeframe

The solution was gradually transitioned from the existing system to LineGuard, which took a total of six weeks. This timeframe allowed for thorough testing and ensured that deployment increased in line with the customer's schedule. During the final change window, one million subscribers were migrated to the platform in five minutes without any issues.
Secure64 customer success managers were involved every step of the way, and they delivered reports after every changeover.

KEY PROJECT OBJECTIVES

The key objectives of the project were met during the upgrade to Secure64 LineGuard:

Reduce the TCO for operation of the platform

This was more than achieved as the service provider was able to generate addition revenue saving with a reduction in hardware over the life time of the project

Seamless Migration with no disruption to service or features

This was achieved as the solution was able to be deployed reutilizing the existing policy ID's, Server addresses and policy configurations.
Once deployed the customer has taken advantage of the additional features the platform has to offer to improve the customer experience.
6 Million subscribers were migrated in a few weeks

Improve the performance of the platform.

The customer has taken advantage of the API and is integrating the solution with their infrastructure to improve the customer agent interface.
A key difference is the lower latency the solution offers over the existing deployment. This has reduced the time for every query thus improving the customer experience