SECURING SURVEILLANCE CAMERAS

When your Security Cameras are sharing too much

> *The end result was significantly better …but there was a hidden cost – compromised network security*

CLIENT PROFILE

A Fortune-100 enterprise with thousands of retail locations.

CHALLENGE

This enterprise initiated a multi-year, multi-million dollar video surveillance system upgrade. The end result was significantly better for surveillance capturing and management functionality, but there was a hidden cost – compromised network security. Many retail location camera installation contractors had purchased cameras using the provided video system specifications, without realizing that these cameras often included firmware and chipsets with a weak security posture.

CHALLENGE

The enterprise found itself under attack by an organized Far East adversary who exploited firmware vulnerabilities in these camera systems and rapidly compromised nearly every camera on the network. Without firmware updates being extracted from the different camera manufacturers and then painstakingly applied to every installed camera, the enterprise would have to consider a complete hardware and installation re-deployment with updated acceptable cameras. Even worse, the new secure cameras had much higher price points, so overall installation cost would be significantly higher!

> *The enterprise found itself under attack by an organized Far East adversary … [who] rapidly compromised nearly every camera on the network.*

Those responsible for maintaining the digital security of surveillance systems typically consider three ways of overcoming these challenges:

1. Prohibiting the use of unclassified network communications;
2. Issuing devices re-configured to thwart cyber threats; or
3. Implementing an add-on solution.

Prohibiting the use of unsecured Internet networks impedes workflow and reduces productivity. Issuing new secure devices is cumbersome, difficult to manage, cost prohibitive, and poses interoperability problems. Aftermarket device re-configurations, on the other hand, cannot keep up with changing requirements.

THE ARCHON SOLUTION

The enterprise can mitigate the threats to its video infrastructure by implementing an agile, simple and highly secure solution: GoSilent. This multiple-award-winning device has been widely recognized as the most portable and easiest-to-configure hardware VPN solution for securing network communications to and from remote locations, no matter what IP device is connecting to it.

> *GoSilent filters all internet and data traffic and denies unsolicited data requests.*

GoSilent filters all internet and data traffic and denies unsolicited data requests. It offers protection from cyber attacks, identifies theft and malware. It offers the following key advantages:

- **HIGH SECURITY**—Offers enterprise-grade protection, with top-secret-level encryption and NIAP certification (in process).
- **EASE OF USE**— Works instantly with any IP-enabled device, offering "plug-and-play" ease for non-technical users.
- **PORTABILITY**—Fits in the palm of a hand (2.6 x 1.9 x 1.2 inches; 3 ounces).
- **INVISIBILITY**—Obfuscates IP addresses for all in-and outbound data.
- **ISOLATION**—Completely isolates IP devices.
- **AFFORDABILITY**—Highly cost effective compared to other add-on solutions or device re-configurations.

CONCLUSION

We demonstrated that GoSilent could support video requirements, had the network security features needed to lock out the adversary and had low enough power requirements that there was no need to re-run new power cables to all systems.

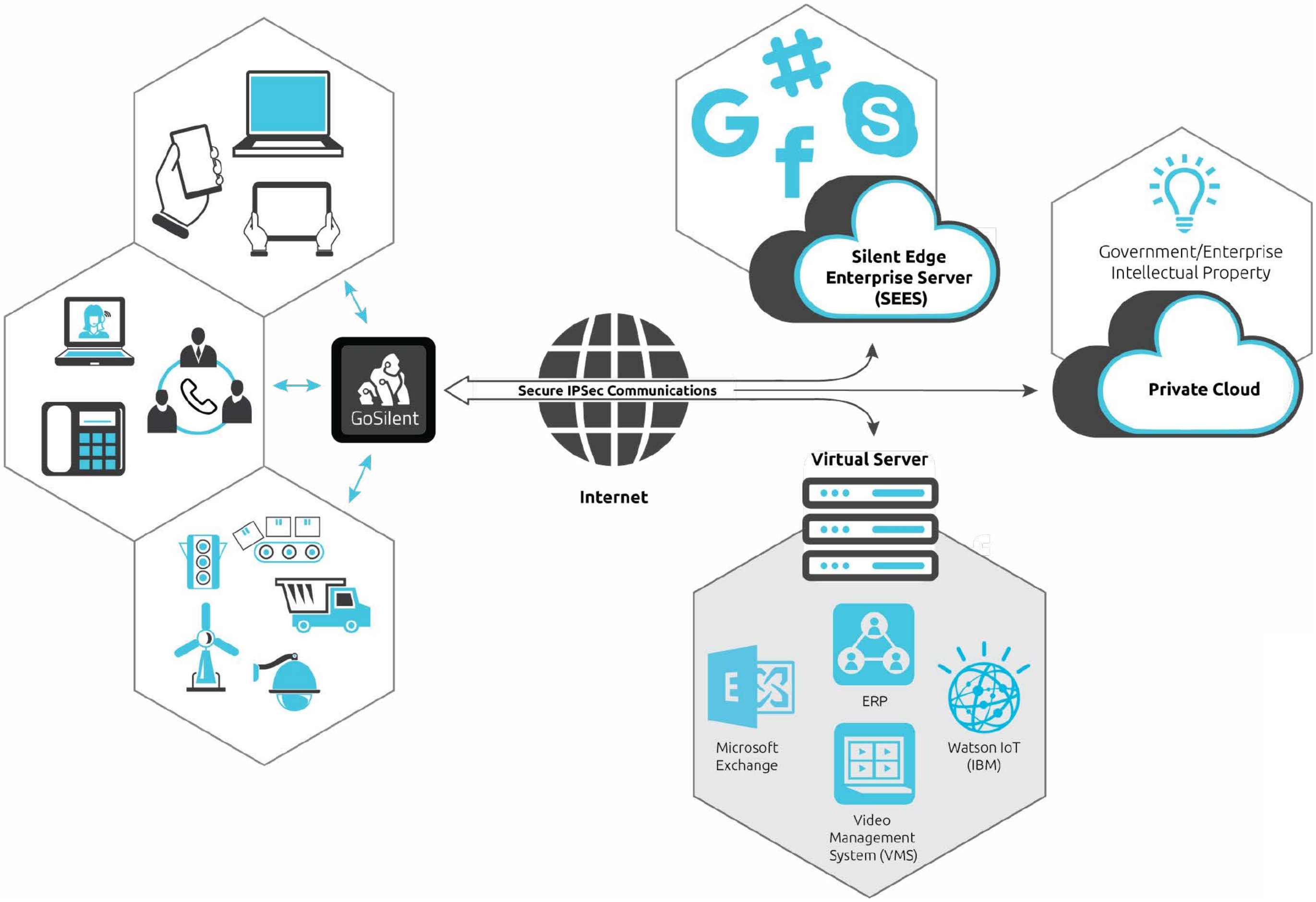
Today the customer has implemented GoSilent and restored the security of its surveillance camera live streams. No new threats have been introduced, and live streams and other information have ceased making its way to unknown adversaries.

Want to Learn More?

CONTACT US

NOTES AND DIAGRAMS

GOSILENT IOT ARCHITECTURE



ARCHON
A CACI Company