DoD AGENCY SECURES ITS SUPPLY CHAIN

> *"The Agency sought the most affordable, agile, secure, and high-bandwidth VPN tunneling and network intelligence solution for use at the edge."*

CLIENT PROFILE

An agency within the Department of Defense which has responsibility for protecting our country and its strategic interests, Allies and critical research & development.

CHALLENGE

As part of daily operations, the U.S. Government Defense Agency sends and receives communications from suppliers and partners across the globe. These communications contain sensitive information critical to the Agency's mission.

Eighty percent of all reported cyber breaches come through the supply chain. Remotely-located network devices and/or personnel using untrusted, unclassified, Internet based networks (public/free WiFi, foreign telco networks, etc.) are all vulnerable to network attacks and threats.

The Agency does not control supplier or partner equipment and relies on the end user to adhere to established security policies. Unfortunately, most suppliers do not have the security personnel or robust security systems to thwart sophisticated or nation state attacks.

Unclassified information systems remain a primary attack vector for cyber-adversaries, the results of which can translate into millions of dollars in losses, as well as posing a clear and present threat to our national security.

SOLUTION

Rather than restrict the use of Internet networks and lose the advantages of speed, convenience and security, the Agency sought an agile, simple and highly secure solution to modernize their legacy infrastructure. The GoSilent Firewall and VPN was determined to be the easiest-to-configure and most portable hardware VPN solution to secure the data transport and site-to-site network communications from suppliers' personnel in the field.

> *"The right solution had to secure unclassified network systems for the Agency's IT challenged supply chain constituents."*

ADVANTAGES

- **HIGHLY SECURE** - Top Secret level encryption, NIAP certification (pending), enterprise-grade firewall.
- **PLUG-AND-PLAY** - Works instantly with any IP-enabled device, ease of use for non-technical users.
- **PORTABLE** - Fits in the palm of your hand. (2.5x2x1 inch, 3oz).
- **INVISIBLE** - IP address obfuscation for all in and outbound data.
- **ISOLATED** - Full PC isolation from Captive Portal exploits.
- **AFFORDABLE** - Highly cost effective when compared to other solutions or device re-configuration.
- **DEPLOYMENT** - Via cloud or on-premise. Self-provisioning automatically applies enterprise policies to any device.

HOW THEY DID IT

The processing and sharing of information across unencrypted links from remote or offsite locations is a major concern for all Defense Industrial Base (DIB) partners. Internet based communications offer the advantage of speed and availability, but the channels carry an inherently unacceptable security risk.

Solutions to these challenges typically revolve around three scenarios:

1. Prohibit the use of unclassified network communications.
2. Issue devices re-configured to thwart cyber threat.
3. Implement an add-on solution.

Prohibition of use fails due to enforcement limitations in addition to the loss of a fast and convenient form of communication. Issuing newly configured devices is cumbersome, difficult to interoperate, manage and is cost prohibitive. With the market's rapid rollout and wide diversity of devices, aftermarket re-configuration will always lag behind.

With GoSilent, the Agency meets the criteria of implementing an out-of-the-box solution. The Agency also satisfied the demanding characteristics that government grade security must provide, such as:

- **PC Protection** – Filters all data traffic, unsolicited data request denied. Protection from cyber-attacks, identity theft & malware.
- **Commercial National Security Algorithm (CNSA) Suite (aka Suite B)** – Built-in Top Secret level cryptography.
- **Captive Portal Isolation** – Isolates PCs from malicious WiFi malware downloads.
- **IP Obfuscation** – Masks IP address of all in and outbound data traffic.

> *"Legacy and IoT equipment required an easy-to-configure and managed network security solution that can be retrofit and remain transparent to the systems they secure."*

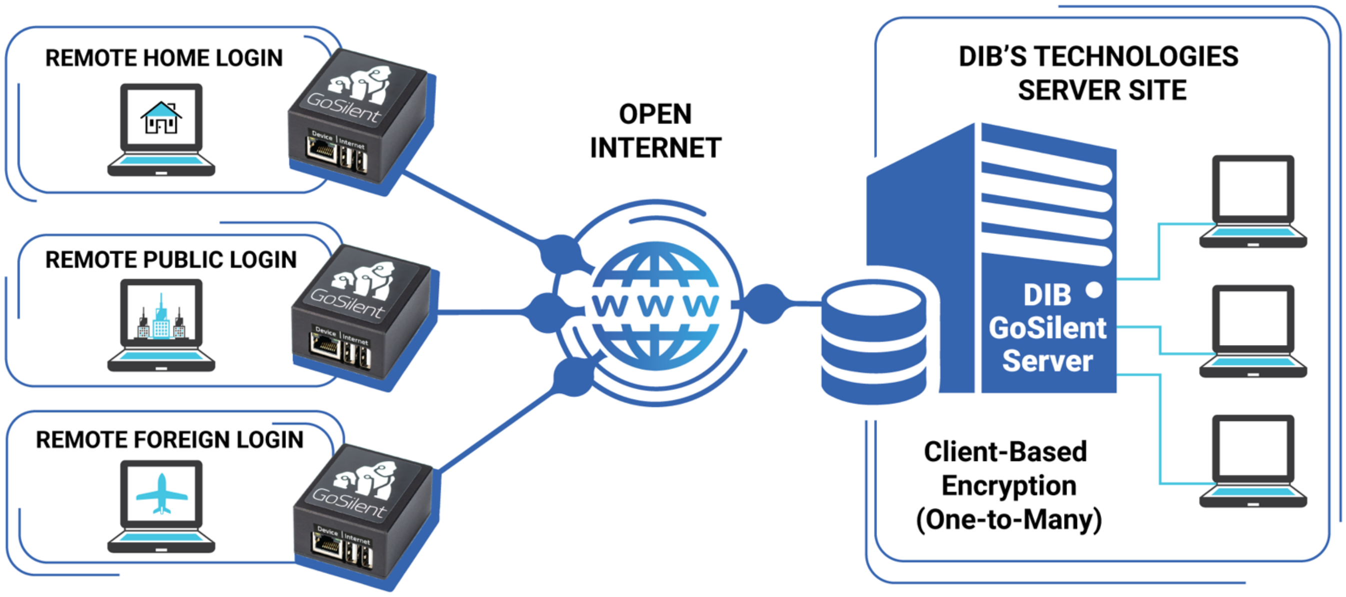
CONCLUSION

As the cyber attacks become more aggressive and sophisticated, government agencies require solutions that can be layered in quickly, work well behind the scenes, and offer the highest level of security.

As the GoSilent solution is deployed to DIB facilities, the Agency will seamlessly upgrade its entire network security footprint without compromising daily business operations. Furthermore, no DIB will be required to update their legacy equipment. With GoSilent, the U.S. Defense Agency choose an agile and robust response to cyber risks now and will remain confident in the security of its supply chain worldwide.

NOTES & DIAGRAMS

DIB Secure Transport



GoSilent solves a **major issue** common to DIB partners - Processing and sending technical data across unencrypted links from remote / off-site locations.

U.S. Defense Agency ultimately selected GoSilent based on the following key provisions:

1. CNSA (Suite-B) Quantum-Resistant Encryption - TS/SCI “quality” encryption for unclassified systems.

2. Satisfies 55% of NIST Cybersecurity Framework v1.1, as shown in the diagram below

GoSilent Cybersecurity Provisions

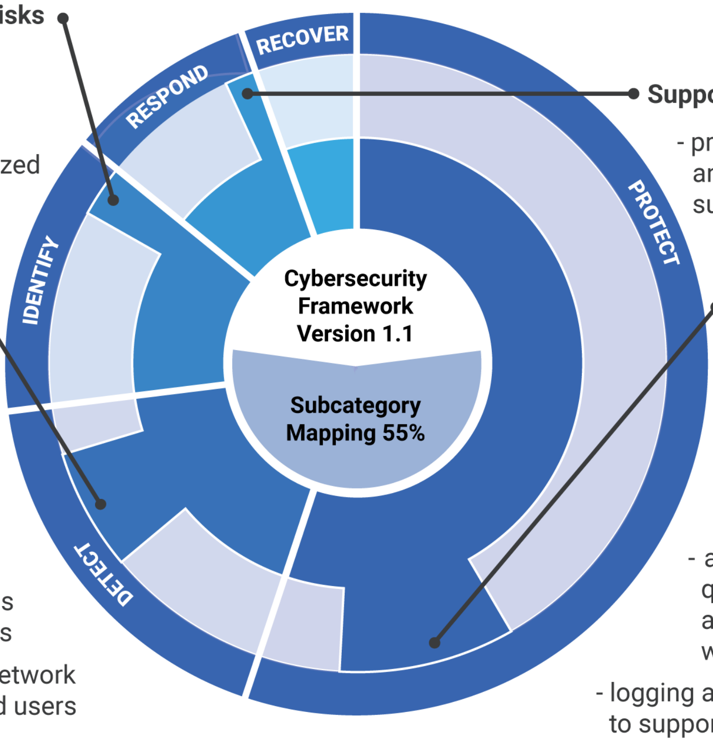
GoSilent Map to NIST 800-171 Controls

Minimizes cybersecurity risks by identifying [2]:

- organizational data flows from remote systems
- authorized and unauthorized connection attempts

Supports appropriate cyber defense response actions by [5]:

- providing an end point sensor for continuous monitoring of remote systems
- detecting attacks and potential attacks
- detecting authorized and unauthorized connections to organizational systems
- detecting unauthorized network activity performed by end users and/or malicious code



Supports response activities by [1]:

- providing analysts with logs and alerts of inappropriate, suspicious or unusual activity

Protects the confidentiality of data-in-transit by [7]:

- controlling remote access to authorized connections
- extending boundary protectionto the remote access system interface
- applying FIPS-validated, quantum resistant cryptography at the packet level to wired and wireless data transfers
- logging all network connections made to support auditing of system activity

GoSilent satisfies 15 of 107 NIST SP 800-171r1 security controls.
These controls map to 55% of NIST Cybersecurity Framework v1.1 subcategories

3. Industry leading performance per watt, 90 MegaBit/Sec Throughput

4. Captive Portal Bypass - Secure authentication through public WiFi access points (coffee shops, airports, hotels, etc.).

5. Over-the-Air Update - Push-button device firmware update.

6. Applies NSA and DoD – Top-secret level - Approved Best Practices.

7. NIAP and Common Criteria (CC) certification pending for the following Protection Profiles (PP) to appropriately cover Attila’s products for use by enterprise and government National Security Systems: Firewall - CPP_FW_V2.0E and VPN Gateway - EP_VPN_GW_V2.1.