Virtual Obfuscation Network: Technical Overview

Dynamic IP routing, multiple layers of encryption, and managed attribution techniques keep personnel, information, and digital resources secure and private.

Telos Ghost is a virtual obfuscation network-as-a-service that provides privacy and security for worldwide communications and transactions over the internet. Telos has integrated various technologies to provide high levels of network obfuscation, multiple layers of encryption, and managed attribution capabilities to:

- Obscure and vary network pathways;
- Use encryption not only to protect the information but to allow removal of source and destination IP addresses, thereby eliminating network paths back to the source;
- Hide critical network resources using cloaked capabilities for email, storage, applications and unified communications

Telos Ghost provides three foundational capabilities that can be tailored and integrated to your specific requirements:

Private Web Access: Secure anonymous Internet access. Disguises the identity and location of personnel when using the public web for cyber threat intelligence and competitive research. It provides users with dynamic access for every session and assures that your traffic securely traverses the virtual private lines of the Telos Ghost network. Scalable and flexible, Telos Ghost Private Web Access allows users multiple points of international or domestic egress to the public internet based on customer requirements. Traffic mixing and misdirection techniques ensure your activity remains anonymous and private.

Private Network Access: Leased-line security with VPN flexibility. Allows authorized users to work with mission-critical enterprise information without being seen or discovered. It enables the establishment of sustainable cybersecurity infrastructure, providing multi-layered secure tunnels for all data traffic and obscuring the correlation between the entry doorways and the client cloud from external observers. Software and system agnostic, and accessible from any device and location, Telos Ghost Private Network Access provides a full security solution while maintaining your existing encryption and software services.

Cloaked Services: Hidden unified mobile communications, storage, and applications. Provide remote users with the ability to securely talk, text, email, store information, and use video and applications over any mobile device. They include fully encrypted geo-masked hidden mobile communications for device-agnostic voice, video, chat, and data; hidden storage to store, analyze, and collaborate privately and securely within Telos Ghost; and hidden email and applications that let you cloak your email and application servers for access only by Telos Ghost users.

The Telos Ghost network-as-a-service offers enterprises the availability and performance needed for their secure voice, video, network, and web access requirements on a subscription-based model. Network node virtualization allows allocation of resources based on your users' changing needs.

- When you need to protect cyber researchers on the public internet, Telos Ghost disguises them so they can work without fear of discovery.
- When you need to shield critical business and financial transactions from view, Telos Ghost clads them in multiple layers of encryption and hides them in an impenetrable thicket of anonymous network nodes.
- When you need to limit access to critical servers and applications, Telos Ghost makes them invisible to all but authorized users.
- When you need to talk, text, email, and share video without fear of compromise, Telos Ghost offers a private as-as-service network for unified communications over any device.

Telos Ghost capabilities include:

Obfuscation with dynamic IP routing and encryption. Telos Ghost sends user data through a seemingly random number of virtualized cloud-based nodes to the exit node, with random circuits generated for each new session. Data is also protected with up to four layers of AES 256 encryption. Layers added and removed as data traverses between access and exit nodes. As layers are removed, source and destination IP addresses are removed, eliminating ability to track back to source. Users' data is protected and their location and identity cannot be tracked.

Key capabilities

- Web Access
- Private Networks
- Cloaked Services

Telos-patented methodologies

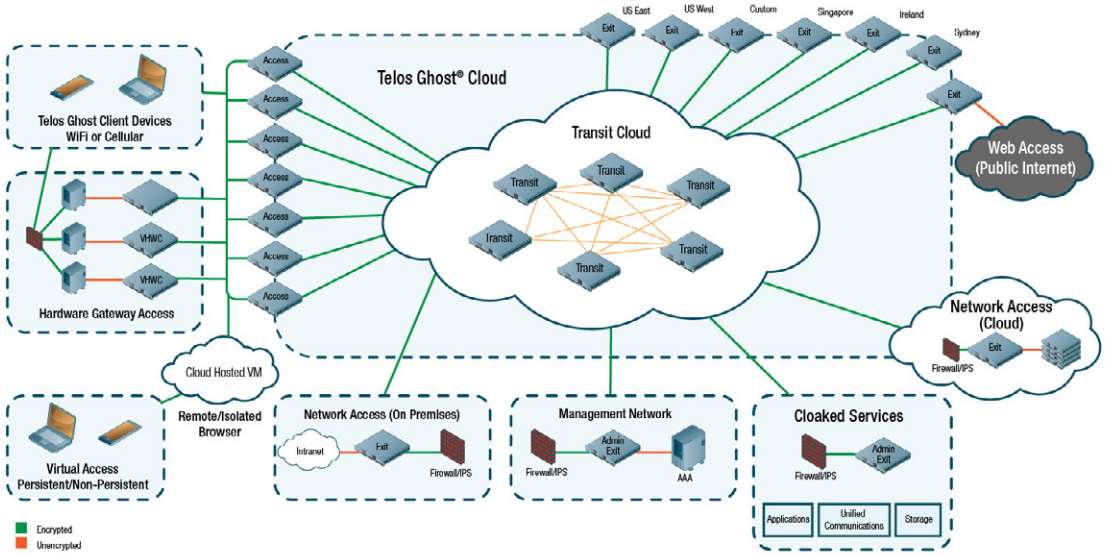
- Secure Geo-location
- Secure Obfuscation
- SIP Diverter

Key network components

- Access Methods
- Transit Cloud
- Exit Options

Offerings

- Shared Network
- Hybrid Network
- Dedicated Network



Managed attribution allows the user to select the level of attribution necessary to meet their mission or operation. It provides the ability to create various personas for specific tasks and missions in order to maintain a "digital cover story" that lets you blend into the background while working on line. You can work completely anonymously (non-attribution) or with a masked identity (misattribution). You can build your persona on your device or in a virtual machine.

- **Technical attribution** — Lets you control all technical details including specifying your location, swapping end point IP addresses, change your point of presence on demand.
- **Personal attribution** — Supports the creation of a convincing online persona and ensures all of your activities are consistent with this persona.

Dual path authentication provides the assurance of protecting user credentials. This unique method of access control and authentication provides a separate path through the obfuscation network to the hidden authentication server. Once the user is authorized on the network, a second path through the obfuscation network is create from the access and point of presence exit selected by the user.

Engineered to Eliminate Your Presence on the Internet.

Telos Ghost uses patented methodologies to integrate various technologies that vary network pathways, swap exit node IP addresses, and eliminate source and destination IP addresses, thereby eliminating the presence of the user on the internet and ensuring that none of their internet activity can be traced back to them.

Methods of access include software client, hardware client, and virtual machine. The user can access the network via an open VPN client on their workstation, laptop, tablet, or mobile phone. Alternatively, multiple users can be funneled through a centralized server from a secure location. Lastly, a user can remote and isolate their browsing and internet activity in a persistent or non-persistent virtual instance. These various access methods provide maximum flexibility for users to architect the best solution for their needs.

You can take full use of these capabilities with an annual license to the Telos Ghost Shared Network. You can also create a hybrid environment by using the shared network and adding capabilities unique to your operation, such as dedicated access/exit pairs located anywhere in the world, and various types of cloaked services, including voice, video, chat, file storage, and email. For customers with special purpose needs, a completely dedicated network can be implemented just for their use. These dedicated networks can be established, eliminated and re-established in various locations worldwide.

Learn more at www.telos.com/telos-ghost

Telos® Solutions that **empower** and **protect** the enterprise.™

Telos Corporation | 19886 Ashburn Road, Ashburn, VA 20147-2358 | 1.800.70.TELOS | 1.800.708.3567 | Fax 703.724.3865 | www.telos.com