Securing Cyber Red Teams on the Internet

Telos Ghost protects cyber researchers by masking their identities, misattributing their locations, and hiding their presence on network resources.

As the frequency and sophistication of cyber attacks increase, more organizations are using red teams to gather intelligence on threats and vulnerabilities as part of their cyber defense planning. This yields a more realistic understanding of how well their systems will withstand, and how well their people will respond to, an actual emergency.

The Challenge: Working Securely on the Internet.

Red teams and other cyber threat researchers perform their job using the public internet. They must leave the relative safety of the enterprise network to investigate threats coming from the internet. And, they need to use the internet as a jumping-off point for their attempts to break into the enterprise network being tested.

This work can unintentionally reveal their presence on the internet, their geographic location, and even their identities, as well as inadvertently open up attack surfaces for bad actors to exploit. To work safely and effectively, these teams need to disguise their presence on the network – just as soldiers wear camouflage to mask their presence and undercover police try to blend in with their surroundings.

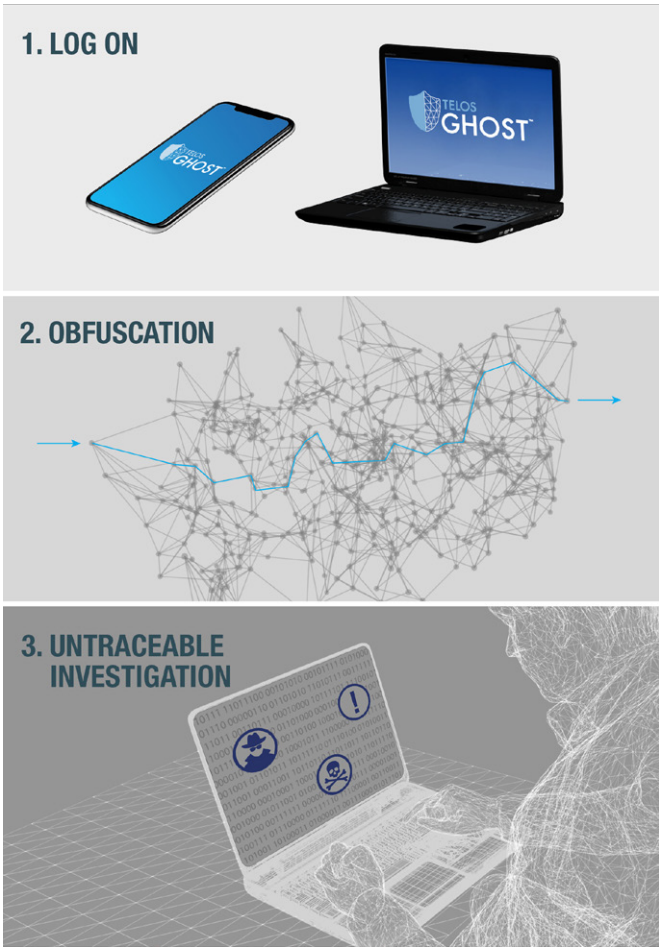
The Risk: A Single Exposure Means the Wargame Is Up.

To achieve this level of secrecy, dedicated network resources must be configured specifically for each mission. A single error can set off alarms and leave digital footprints that not only jeopardize the mission, but also threaten the safety of the operatives themselves. Worse, such failures can create new exposures for actual adversaries to exploit.

One-hop proxies such as anonymous VPNs and using the Tor network are common ways to disguise cyber research activities. However, these methods are easily tracked and traced, and suffer from predictable performance challenges. They are inadequate for truly sensitive and high-risk endeavors. The success of red teaming, penetration testing, and other forms of cyber threat research require you to get it right 100% of the time. There is no margin for error.

The Solution: Protect Your Red Teams and Other Researchers with Telos Ghost.

Cyber threat research requires an isolated networking infrastructure that enables red team members to operate securely and privately without bringing unwanted attention to themselves. The starting point for assuring red team security is an integrated digital environment that's purpose-built as a cloak for untraceable anonymity on the public internet.



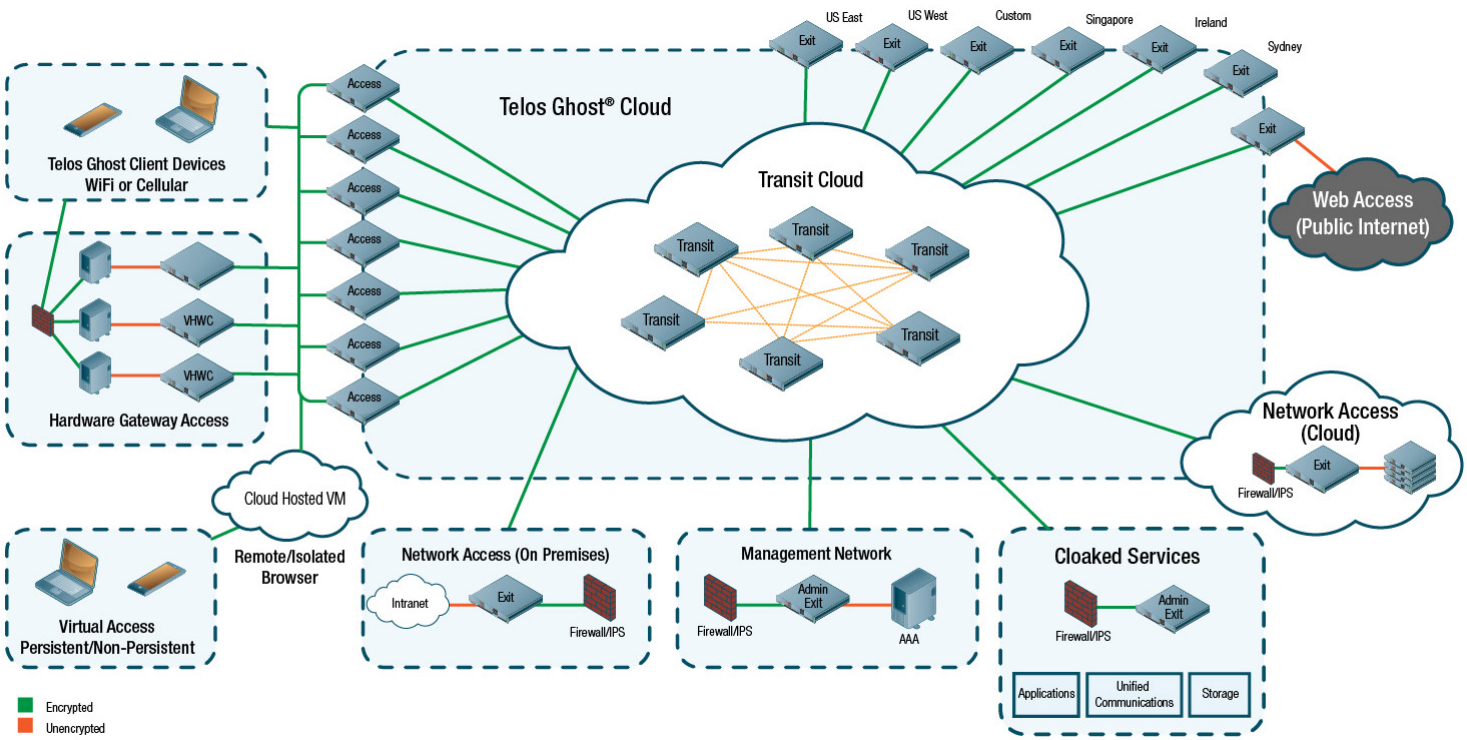
Telos Ghost is a cloud-based obfuscation and non-attribution network that lets red team members securely log on wherever they have an internet connection and instantly blend into the background as nondescript web traffic. Telos Ghost hides their network resources, masks their identities, and misattributes their locations.Its unique set of integrated capabilities includes:

Dynamic IP routing – hide your team members in a labyrinth of network nodes. Telos Ghost is made up of a mesh of secure routers that make it impossible to determine the source or direction of network traffic. User data is sent through a seemingly random number of virtualized cloud-based nodes to the exit node, eliminating source and destination IP addresses from node to node.

Multi-layered encryption – make your data impenetrable throughout your mission. Telos Ghost applies up to four layers of AES 256 encryption to your dataas it traverses the network to ensure the critical information sent and retrieved in your cyber research missions is kept hidden from friend and foe alike.

TELOS GHOST®

Telos®



Key capabilities:

- **Web access –** private, anonymous worldwide access to the public internet
- **Network access –** secure cloud- or premises-based network connectivity
- **Cloaked services –** Secure unified communications, applications, and storage

Obfuscation:

- Dynamic IP routing – random circuits generated for each new session
- Eliminate source and destination IP addresses
- Swapping points of presence
- On-demand exit node IP swap

Managed attribution:

- Completely anonymous (non-attribution)
- Masked identity (misattribution)
- VDI access for managing personas (managed attribution)

User authentication:

- Active Directory-based username and password
- Certificate-based circuit creation

Managed attribution – shape your team members' personas to match the cover story for their mission. Technical attribution lets you specify your location, swap end-point IP addresses, and change your point of presence on demand. Personal attribution establishes a convincing online persona and ensures all of your activities are consistent with it.

Virtual desktop interface – isolate your device by remoting your browser operating environment to a virtual instance. Telos Ghost lets you set up virtual machines that enable you to control both the technical and personal attributes involved in online investigations. Any information "leaked" from the VMs will support the authenticity of the persona you need to establish. This persona can then be used on future sessions, or can be taken down to eliminate that persona.

Virtual network – spin up the pre-configured environment you need for mission requirements. As a software-defined network, Telos Ghost consists of virtual resources designed to work together, hosted in and dispersed across a variety of highly secure cloud regions. Telos Ghost supports the tools and techniques you use for accomplishing your cyber research mission.

Contact Telos for More Information

If you would like further information or a demonstration of the capabilities of Telos Ghost, please contact Telos Sales:

1-800-70-TELOS or sales@telos.com. We look forward to learning more about your requirements for anonymous networking and sharing how Telos Ghost can help protect your people and information.

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