

How Telos Ghost® helped a global financial services firm to proactively fight cybercrime.

Truly anonymous virtual private lines connecting locations around the world to a state-of-the-art threat intelligence center — with no discernable latency.

One of the world’s largest multinational financial services corporations with over \$10 billion in annual revenue faced increasingly sophisticated threats from cyber criminals. These escalating cybersecurity threats put millions of dollars in transactions at risk each day.

To thwart criminals, the company had two choices: one, lock down their system to make it safer, but less functional. Given the competitive nature of the financial services industry, less functionality and flexibility would be corporate suicide — a move their competitors would celebrate. Their second choice? Maintain their open system and their competitive edge — but stay one step ahead of the criminals.

Building a Proactive Threat Intelligence Center

In order to mitigate the significant risk posed by cybercriminals in the more than 200 countries where they do business, the company decided to build a state-of-the-art threat intelligence fusion center with very specific technical needs and requirements. However, they faced two major challenges in bringing this center to life.

Challenge #1: Finding an Affordable Solution

If you want to beat your enemy, you need to understand them. This means making sure you can gather real-time, uncompromised data — anonymously. Malware and attacks need to be studied and analyzed quietly without tipping off the enemy. Data needs to be returned to analysts quickly, without being traced.

However, doing this on a corporate network is risky. To mitigate risks, **any environment used to study malware needs to be completely technically and commercially separate from the corporate network.** This distinct network must also be set up quickly, with nodes available in short notice within any of hundreds of countries across the globe. Nodes that may ultimately be compromised and discarded, while new nodes are quickly created elsewhere.

However, the traditional way of setting up this kind of network – using private leased lines – is incredibly cost-prohibitive, making it impractical for all but the largest organizations.

Challenge #2: Uptime, Latency, Anonymization Requirements

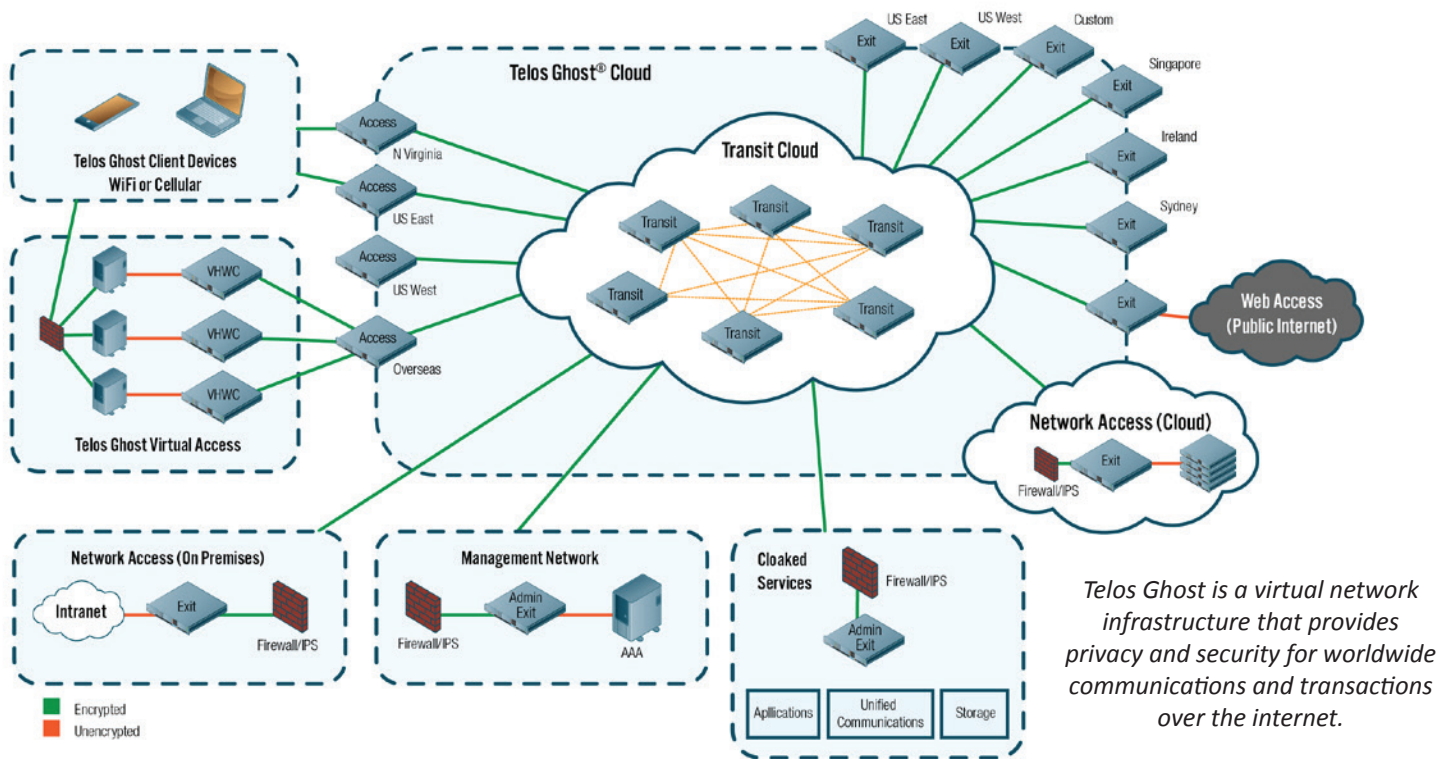
Not only does this network need to be separate and distinct, it also must meet **stringent performance requirements for uptime and minimal latency.** It must also be completely anonymous. Latency tips off the enemy. Downtime costs money. Easily traced sacrificial nodes compromise investigations and expose organizations and their computing assets. Because of this, traditional means of anonymization like Tor or one-hop proxies are inadequate. Why?

BUILDING A THREAT INTELLIGENCE CENTER

WHAT DOES IT TAKE TO BUILD A STATE-OF-THE-ART THREAT INTELLIGENCE CENTER?



Whether you are sending or receiving data, **Tor and similar products are notorious for latency, uptime issues, and identifiable nodes.** Identifiable nodes makes it obvious that you aren’t where you claim to be, while network latency and uptime issues slow your investigation to a crawl. This isn’t acceptable in a business where time can mean the difference between thwarting an attack and cleaning up after one.



The bigger issue is that Tor isn't really anonymous, and neither are competing products. It isn't hard for criminals to find published lists of their so-called anonymous nodes. Use these products, and you're easy to track. A threat intelligence center that isn't actually anonymous cannot gather the kind of data needed to justify its existence. Is there any way to meet these challenges within a realistic budget and timeframe?

Telos Ghost: A separate, flexible, anonymous network

These unique needs and costly challenges meant finding vendors with novel solutions to intelligence gathering and analysis. Enter Telos Ghost.

The Telos Ghost team built a custom network infrastructure to support the firm's extensive global reach, allowing them to have a presence in worldwide locations on short notice. This new infrastructure was sustainable and flexible, and most importantly it wasn't connected to the company or their new threat intelligence fusion center in any way.

Not only that, but the network was truly anonymous and surprisingly fast. That's because Telos Ghost network nodes appear to be part of the local cyber landscape, and cannot be traced back to their source. Minimal latency allows for rapid data collection and online activities. Proven uptime means users are always working, never waiting. Easily managed sacrificial nodes enable nimble data collection.

A fully automated deployment process allowed this customer's global network to be set up, configured and

operational in under two weeks, at a small fraction of the cost of setting up private leased lines, to say nothing of the real costs of a breach. The Telos Ghost network can be deployed worldwide, making it ideal for global security requirements.

Enhance your existing threat intelligence solutions

Not only can this affordable solution be put in place quickly, but **Telos Ghost can also be layered with other products to create a suite of robust and comprehensive threat intelligence tools.** Because Telos Ghost passes all ports and protocols, it can be used seamlessly in conjunction with a wide variety of tools and applications that require obfuscation or managed attribution.

This new Threat Intelligence Center is absolutely mission critical in this age of increasing number and sophistication of cyber attacks. Threats against the company's infrastructure are a threat to the life-blood of their business. It is imperative that they stay ahead of the cybercriminals.

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