Telos®

Telos Ghost® for Financial Services

The Secret Weapon in Your Security Strategy: Network Obfuscation for Financial Services

Endpoint security is important and ZTNA is a step forward, but you can do more to protect your crown jewels. You can hide them from the internet entirely with network obfuscation.

Financial services organizations are not new to risk management. They know their crown jewels, and they've invested heavily in protecting them. Yet they continue to fall victim to hackers and other cyber criminals. And when businesses as savvy and well-protected as Equifax and Capital One can be hacked, CIOs and CISOs in other financial businesses may feel like they are just waiting for their turn in the cross hairs.

They wouldn't be wrong. The first half of 2020 saw a 238 percent spike in attacks[1] against these organizations – and along with that came a 141 percent increase in regulatory fines.[2] It's time for CIOs and CISOs to find a better way to keep their data out of the hands of criminals.

300x

How much more likely finserv firms are to be attacked than businesses in other sectors.

— Boston Consulting Group

Old or new, all are at risk.

Most finserv organizations are still using decades-old legacy core systems, with others integrated with them following mergers and acquisitions. These systems, designed before the internet was even conceived, are inherently vulnerable, and may not even be supported with fresh patches.

And while those that have made the move to the cloud are in a better position in some ways, they face their own set of security concerns. Many organizations are reliant on a few leading vendors for critical services, so one virtual machine breakout or similar type of attack at the vendor level can open the door for attackers to move laterally in order to learn where key assets are located and how to exfiltrate them.

Beyond endpoints and conventional enterprise security.

Before the rise of digital transformation, the gold standard of cybersecurity approaches was the castle-and-moat defense, which focused on protecting the perimeter. Today, the perimeter is obsolete and the focus has shifted to endpoints.

But endpoints aren't the goal of an attack. They're just the first stage. Attackers breach them in order to get inside a network and find stored assets they can sell or use to conduct extortion or fraud.

70%

of finserv organizations have experienced a security incident.

— Ponemon Institute

The SEC's Division of Examinations has warned financial services organizations that they need to do a better job of securing their storage systems, whether on premises or in the cloud. New regulations are emerging to encourage better protection of records in storage, but many of these organizations are still figuring out how to handle this effort. Zero Trust is a step forward, but Zero Trust alone is not the final answer. BYOD, third-party apps, and remote workforces are pushing finserv organizations toward a decentralized trust model that is hard to secure, even when Zero Trust is in use.

$5.85 million

Average total cost of a data breach in the financial services sector in 2020.

— Banking Exchange

[1] *VMWare and Carbon Black, 2020 study of the finserv attack landscape*

[2] *Fenergo, 2020 study of global financial institution fines*

The ultimate security is invisibility…with Telos Ghost.

Threats are proliferating. Costs of breaches continue to grow. Regulatory fines and reputation damage add to the pain. It's time to think differently about security.

Traditional cybersecurity focuses on protecting the infrastructure through its endpoints, firewalls, and applications. But despite all the tools and technologies devoted to these efforts, finserv organizations continue to leak data. It's enough to make a CIO or CISO wish they could take their most valuable assets off the internet entirely.

And now, they can – virtually.

Hide your crown jewels from the internet with network obfuscation. Telos Ghost hides your assets from the internet, so while they remain fully accessible to authorized users, malicious actors won't even know they exist.

How network obfuscation protects your most valuable assets.

A bank has locks and alarms on the doors, protective teller windows, and surveillance cameras throughout the facility. Yet with all that security, they still have a vault in the back to protect cash, valuables, records, and other critical assets.

Think of Telos Ghost as an impregnable vault that contains your most critical digital assets in addition to the conventional security you use on the enterprise network. Network obfuscation hides servers, applications, and unified mobile communications from the network, so even if attackers were able to enter parts of the environment through a compromised web app, stolen laptop, or firewall misconfiguration, they wouldn't be able to find your crown jewels.

This is a different approach from traditional cybersecurity, which focuses on protecting the enterprise and its perimeter. Instead, network obfuscation focuses on the internet itself.

Proven in the toughest environments.

Members of the U.S Intelligence Community and the military have been using the network obfuscation capabilities of Telos Ghost for years to preserve the lives of their people and the confidentiality of their movements – and now, the same technology is available to you. Network obfuscation ensures your most valuable information remains secure, even if your endpoint security fails or your policies are misconfigured.

Telos Ghost: The secret weapon in your security strategy.

Telos Ghost is a robust, scalable, secure communications network-as-a-service that privatizes the public internet to hide network resources and mask the identity and location of users to ensure total protection on the organization's network.

Telos Ghost uses network obfuscation, multiple layers of encryption, and proprietary-based mesh algorithms to dynamically route IP traffic among cloud transit nodes. Advanced managed attribution makes users and their locations completely anonymous, which is a particularly compelling case for banks, insurance companies, and investing, financial planning, and accounting firms.

To learn more, please contact us.

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 | info@telos.com | www.telos.com