SPYRUS®

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

Financial Services Use Case

SPYRUS Enables Secure Work from Home

Protecting Employee and Client PII Outside the Office

Work from Home Challenges

Most of the Financial Services industry operates large offices in major cities where all employees must work. This traditional model creates a cyber environment which is easier for the IT departments to protect. Employees and guests can have separate networks managed by the IT department that create federated access to company resources, ensuring guests cannot access sensitive information with some level of confidence. In addition, these networks are operated by the IT department, allowing for quick security patches, instantaneous alerts for breaches, and adequate visibility of endpoints on the network.

However, the workspace is increasingly becoming more mobile with efficient processors, proliferation of faster networking, and 82% of all workers wanting to work from home one day a week according to a LinkedIn study (“The Future of Work Could be at Home”). Mobile workers, whether with company computers or personally owned, present a tremendous challenge for a company’s IT department. The security of home Wi-Fi routers and computers may be out-of-date or missing critical security patches, public Wi-Fi may be scanned by third parties, and employees often fall for sophisticated phishing schemes—especially in familiar and comfortable environments. According to a 2019 survey conducted by Apricon (https://apricorn.com/), almost half of the surveyed businesses experienced data loss or breach as a direct result of mobile working.

The Financial Services industry is one that traditionally has been unable to support remote workers due to government privacy regulations.

Customer Challenges

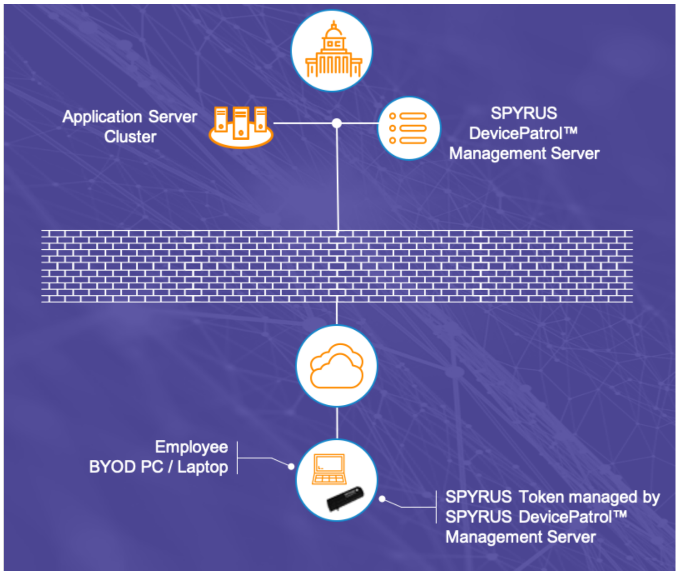
The Financial Services industry is especially concerned due to their handling of personal identifiable information (PII) of their clients, trade secrets and the movement of large sums of money. Mishandling this data can result in violation of stringent regulations including the General Data Protection Regulation (GDPR) and the Gramm-Leach-Bliley Act (GLBA), opening the firm to financially and reputationally damaging fines.

SPYRUS is working with several international Financial Services companies. These companies were looking for solutions to support remote workers facing “shelter in place” orders due to the global pandemic. The solutions had to meet strict criteria, including:

- Verified Security: Solution must protect data-at-rest, in-motion, and in-process while also being “tamper-proof”, with the ability for IT departments to “destroy” the data on devices remotely.
- Cost-effective: Solution must reduce both CAPex and OPex, particularly with regards to set-up, turn-down time, and security enforcement.
- Flexibility: Works with any existing device online and offline.

SPYRUS Solution

To meet these requirements, SPYRUS provides a comprehensive DevicePatrol™ Platform comprised of its Device Management Server and SPYRUS encrypted and hardened tokens.


Application Server Cluster
SPYRUS DevicePatrol™ Management Server
Employee BYOD PC / Laptop
SPYRUS Token managed by SPYRUS DevicePatrol™ Management Server

The SPYRUS Device Management Server provides enterprise management capabilities that enable administrators to centrally register, block/unblock, revoke, set polices, integrate 3rd party applications for secured access, audit, and "kill" all data SPYRUS devices remotely. Additionally, each time the user is connected to the server, the audit functionality is synchronized, allowing the enterprise to monitor user actions as well as control access to the use of the devices in the ecosystem. By capturing log-on and log-off activity, device disabling, and enabling and activation code recovery actions, the Financial Services company can monitor users and devices from structured data that allows the determination of patterns of use and detection of suspect operational behavior, informing corrective action; with the highest level of confidence.

SPYRUS hardened endpoints are the only Microsoft-certified Windows-to-Go endpoints and offer military-grade cybersecurity to the private sector. They are able to boot on any standard computing device (including Apple), come in a variety of storage sizes, ensuring data and operating environment security in a FIPS 140-2 level 3 certified "tamper-proof" solid state drive. Secured by an embedded EAL5+ SPYRUS Rosetta security microcontroller with software that provides precise protection and management of all key material and algorithms necessary to achieve the highest levels of encryption and strong multi-factor authentication (MFA) managed by an easy to use, central, web-based interface for controlling and monitoring all secured endpoints. The tokens meet all Federal and Military standards necessary to ensuring the highest level of encryption security and support in-house or third-party PKI implementations. Additionally, the SPYRUS Windows to Go tokens solve the security challenges related to teleworkers connecting with Virtual Desktop Infrastructure (VDI) desktops or applications.

The Results

The SPYRUS DevicePatrol™ Platform with the Device Management Server and WorkSafe Pro drives provides international Financial Services companies with a solution to securely enable employees to work from home at the highest levels of confidence. Unlike company issued laptops, these customers have indicated SPRYUS tokens are less likely to be lost or stolen unlike company issued laptops. In addition, the SPYRUS solution has proven to be:

- Secure: FIPS 140-2 level 3 validated, SPRYUS tokens provide the highest-grade data protection and key protection for MFA in the commercial market. No data is stored on the host computer and the device can be "zeroized" remotely.
- Cost-effective: SPYRUS deployments dramatically reduce CAPex and OPex. Paired with SPYRUS' Device Management Platform, IT departments can manage the devices remotely, reducing call center costs and downtime associated with changing permissions and wiping data.

- Flexibility: Preloaded with the corporate operating system and user MFA/SSO, the SPYRUS tokens can be plugged into any device. Unlike VDI solutions, SPYRUS tokens provide secure offline work that synchronizes when connectivity is available eliminating agent downtime protecting against data compromise.

About SPYRUS

SPYRUS develops and deploys cryptographic operating systems in innovative ways, providing the strongest protection for data in motion, data at rest and data in process. For more than 20 years, SPYRUS has delivered encryption, authentication, and digital content security products to government, financial, and healthcare enterprises. SPYRUS solutions enable customers to meet stringent regulatory requirements for data protections across industries.