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

Government Use Case

Securing a Broad Mission

The mission of Government is very broad and involves protecting, providing for and investing in developing its citizens. In the U.S., hundreds of Federal agencies and commissions manage the country's space program, protect its forests, and gather intelligence, for example. Government agents often travel into foreign countries, and must continue to be productive in proximity to well-funded, sophisticated agents of foreign powers. Military equipment and devices must function in environments with unique characteristics—in a Humvee, onboard a fighter jet, remote locations at sea—and must be rugged enough to continue to function, sometimes for years unattended, and maintain security.

State and local governments strive to become "smart cities," moving more business to the edge via ecommerce sites, social media platforms, embedded sensors, and streaming services. The move to the edge promises multiple benefits of greater citizen engagement, improved network performance and speed, and new revenue opportunities.

However, this move also leaves them vulnerable to an increase in security attacks. The rise and escalation in ransom demands have heightened security concerns. Additionally, the government workforce is becoming more mobile and carrying with them IT assets with confidential or classified information that could be lost or stolen.

Governments at all levels are increasingly under attack. Cyberattacks are becoming the most common form of aggression between hostile nations. As economies become increasingly digital with utilities, banking systems, and supply chains all being managed with computers, a nation's private and public sector computer networks are becoming bigger targets for attacks. With the increasing threats to the private and public sector, governments around the world are heavily investing in their cybersecurity.

The Challenge

Founded 20 years ago to develop military grade and classified encryption solutions for the United States Government, SPYRUS is the only vendor offering a complete cryptographic approach, delivering authentication access, end point management, and data protection using encryption. SPYRUS is the preferred trusted software and hardware vendor across many government agencies, including the IRS, DoD, DHS and State Department.

For various government agiencies, SPYRUS helps secure their network and devices used by officials, employees and contractors. In general, the most widely deployed solution must meet the following criteria:

- Verified Security: Solution must protect data-at-rest, in-motion, and in-process while also being “tamper-proof” and 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.

The SPYRUS Solution

To meet these requirements, SPYRUS typically recommends its comprehensive DevicePatrol™ Platform comprised of a Device Management server, encrypted and hardened tokens, and the NcryptNshare application.

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” SPYRUS devices remotely. Additionally, each time the user is connected to the Platform, 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 firm 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” drive. Secured by an embedded SPYRUS Rosetta security module built on a EAL 5+ microprocessor 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.

The SPYRUS NcryptNshare application facilitates secure collaboration. With NcryptNshare, files and/ or folders can be encrypted and authenticated while shared with third parties. Permissions can be set including read-only, access timers, and auto-destroy to prevent files orfolders being modified or removed by recipients. In the case that the primary Rosetta key is lost or stolen, an enterprise recovery agent can be used to support continuity of operations.

The Results

The SPYRUS DevicePatrol™ Platform with the Device Management Server, encrypted tokens and NcryptNshare application protect the mission of Federal, State and Local Governments from hostile attacks by providing the following capabilities:

- 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 “zeroed” remotely.
- Cost-effective: SPYRUS deployments dramatically reduce CAPex and OPex. Paired with SPYRUS’ Device Management Software, 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.