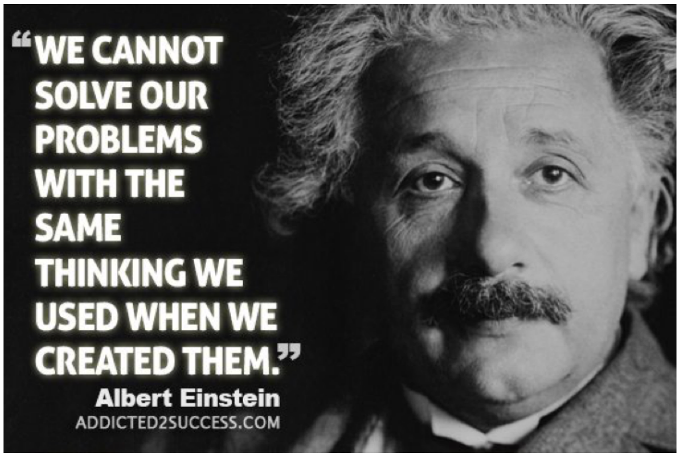
SPYRUS®

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

New Approaches to Protecting Against Future Cyber Attacks

Flawed Thinking

The notion that there is no immediate preventative strategy which can curtail future cyber-attacks is fundamentally flawed. Enforcing strong cyber-policy and best practices without complicating the user experience has the best potential to remove the opportunity for compromising mishaps. Communities of interest concerned with privacy and security can no longer be defined by location. Today’s Information Assurance/Cyber Security solutions must address access to multi-level secure resources and message traffic based on identity, roles, and privileges.


“WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING WE USED WHEN WE CREATED THEM.”
Albert Einstein
ADDICTED2SUCCESS.COM

In today’s society, everyone is doing business online from various locations. Unfortunately, our network architectures continue to be based on decades old theories that result in access challenges and complicated solutions that foster security workarounds. Phishing is successful because of these user challenges. Data is moving at increasing speed, to and through so many endpoints that are inconsistently protected.

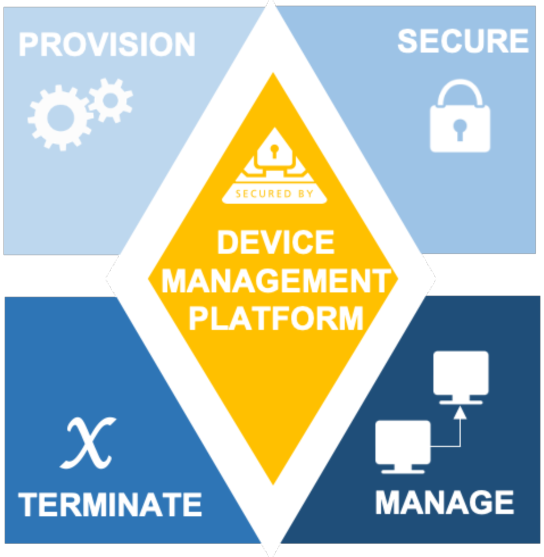
Layered approaches to security (focus on the locking down of large data centers, on premise or in a cloud) have created a myriad of incompatible solutions that rarely provide adequate security and always hamper productivity and foster short cuts that exacerbate vulnerabilities.

A New Approach to Cyber Security

SPYRUS believes consistency in the application of cyber security is the path to successful protection. Our solutions do not look to protect a specific mode of communications, or approach cyber security differently for each specific device. Our solutions focus on a common tool set that protects the endpoints and enterprise resources in a consistent and repeatable experience—providing the ability to achieve a zero-trust model, dramatically reducing the opportunity for human error, and building a level of confidence in an enterprise’s cyber security posture.

At the heart of the SPYRUS solution is the Device Management Platform, also known as the SPYRUS Enterprise Management System (SEMS). The platform extends a true end-to-end security approach to manage user multifactor authentication (MFA) for access; and, protect data at rest, in use and in transit within a single deployed solution. While many enterprises are struggling with different schemas to address different security function and controls, SPYRUS enables the enterprise to comply with all applicable laws and regulations while providing its endpoints with a common experience. Logging onto an enterprise edge through each application server, the SPYRUS solution provides users with a single repeatable experience. Whether using enterprise-unique credential/keys or the

SPYRUS embedded credential/keys managed with our partner Sectigo, the enterprise can be confident they are protected at the highest level by our tamper proof tokens that are verified/ certified at FIPS 140-2 Level 3.



With the SPYRUS Device Management Platform enterprise administrators can centrally register, block/unblock, revoke, set policies, integrate 3rd party applications for secured access, audit, and “kill” the SPYRUS hardware encrypted tokens. The platform provides a high-security and productivity solution for any organization.

It is offered on premise or as a hosted enterprise management service with auditability, accountability and control of all SPYRUS solutions, electronically enforcing enterprise controls.

Each component in the SPYRUS solution can be managed with enterprise-driven policy that enforces data protection controls, removing the ability for users and administrators to 'work-around' data protection security controls, whether maliciously or in error, on-premise or from any remote location:

- Our embedded Rosetta cryptomodule with smartcard and PKI features (USB or MicroSDHC) ensure, at the highest levels of protection, that ONLY authorized users and/or devices obtain data access and protects data in motion;
- Our family of USB 3.0 storage and bootable live drives, hardware encrypted tokens, add the highest levels of protection for data at rest;
- Our NcryptNshare suite of applications leverage the SPYRUS hardware root of trust to ensure, at the highest levels of protection, that data sharing is only allowed between authorized personnel on authorized devices; and,
- The SPYRUS Device Management Platform

Our solution allows an organization to start with a low cost, military grade MFA and encrypted token and add a more elegant booting token which allows mobile workers to travel, work at home or from anywhere with confidence that their operating system and data are well protected. And, because one size does not fit all, all of our tokens work from a user and enterprise perspective exactly the same. This is also very convenient to the user and cost effective to the enterprise when a user needs to change token type. Repeatably consistence enhances security and productivity.

The SPYRUS NcryptNshare suite of applications allow file encryption and control access in the cloud or wherever they are stored. The patented ‘seal’ of the encrypted file can detect if a file has been tampered with (for instance by malware), and by owning the key, the tampered file will not decrypt. By separating access to specific data objects, NcryptNshare can encrypt any file format and ensure that only the persons who should have access to a user’s private data may obtain access. SPYRUS NcryptNshare securely wraps all data, only accessible to the destination device and/or individual, so that the cloud or other unsecured communication paths can be used with the highest levels of confidence.

SPYRUS supports secure anywhere, anytime, anyplace access to live and stored data from fixed or wireless locations supporting mobile and ad-hoc configurations that can operate over a wide range on environmental conditions. As an example, responders on the US nationwide public safety broadband network can securely access live views and streaming video with confidence, promoting enhanced situational awareness, personnel safety, and force multiplication as well as protecting citizen privacy.

The SPYRUS Vision

As the SPYRUS vision expands to all online entities our platform is poised to provide a single integrated that allows any enterprise to manage all of its endpoints via a common Device Management Platform. Today, that is being realized with software and hardware integration partnerships within the evolving industrial IoT industry that will transition to software and hardware OEM relationships. SPYRUS will also apply its unique technology, evident in more that 90 patents, to satisfy emerging use cases. For example, our patented K of N scheme supports the requirement for multiple shares that will allow the activation or shut down of remote unmanned devices based on any number of or combination of external/ environmental attributes that is capable of providing confidence in action based on artificial intelligence (AI) decisions.

Our method by which a hardware security module can attest remotely to its measure of Level of Assurance without a human element will allow our platform to “rekey” in accessible devices with a high level of confidence. Lowering the maintenance burden and extending the useful life of these components. With such unique technologies, the SEMS Platform will go beyond the Orchestration of individual devices and endpoints and evolve into include a comprehensive cradle to grave supply chain management tool for their online resources and data.

From IT to IoT

As enterprises across many industries embrace IoT in the manufacturing floor, the office or the store front, their IT departments must be concerned with device identification, authentication and establishment of trust. Ten to fifteen years ago we were concerned about the vulnerability of a few billion users. IoT is rapidly moving towards relying on an order of magnitude more endpoint for decision making. Whether using AI or labor rich monitoring, IoT devices are flooding our critical infrastructure with end points that are not designed with security in mind.

We are pushing our functional capability without understanding how we can trust their input with confidence. To answer this, SPYRUS has instantiated its high-grade security solutions that support both after-market and future embedded authentication and data protection functionality. Military grade and commonly managed so that your IT team can focus on one method to manage and audit secure endpoints across your user and IoT ecosystem.

In Summary

In short, the SPYRUS solution offers enterprise-wide consistent secure MFA access, protection of data at rest and in motion and trusted asset management Orchestration Platform. With the highest level of security protecting identity and encryption credentials/keys for people, devices and things, the SPYRUS solution enhances enterprise security and productivity with the Power of Simple.

About SPYRUS

SPYRUS develops and deploys cryptographic solutions 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.