SPYRUS®

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

Implementing a Zero Trust Architecture

In a previous article (SPYRUS Strategic Vision paper, "New Approaches to Protecting Against Future Cyber Attacks") SPYRUS asserted that consistency in the application of cyber security is the path to successful protection. And, a 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—is critical. This article examines how to apply these concepts that may be new to the cybersecurity models that has evolved over the past 15 years but are basic to the Information Security objective of 25 years ago.

Birth of Zero Trust Architecture

Early in 2020 the National Institute of Standards and Technology (NIST) and National Cybersecurity Center of Excellence (NCCoE) published a draft report titled ***Implementing a Zero Trust Architecture***. In this document the authors' wrote:

> *The proliferation of cloud computing, mobile device use, and the Internet of Things has dissolved traditional network boundaries. Hardened network perimeters alone are no longer effective for providing enterprise security in a world of increasingly sophisticated threats. Zero trust is a design approach to architecting an information technology environment that could reduce an organization's risk exposure in a "perimeter-less" world.*
>
> *A zero trust cybersecurity approach removes the assumption of trust from users and networks. It focuses on accessing resources in a secure manner regardless of network location, user, and device, enforcing rigorous access controls and continually inspecting, monitoring, and logging network traffic.*
>
> *This requires data-level protections, a robust identity architecture, and strategic micro-segmentation to create granular trust zones around an organization's digital resources. Zero trust evaluates access requests and network traffic behaviors in real time over the length of open connections while continually and consistently recalibrating access to the organization's resources. Designing for zero trust enables enterprises to securely accommodate the complexity of a diverse set of business cases by informing virtually all access decisions and interactions between systems.*

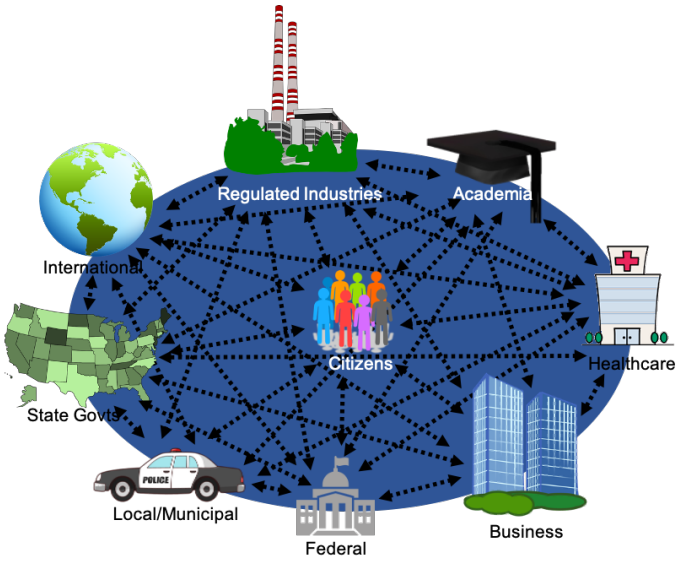
However, long before the proliferation of cloud computing, mobile device use, and the Internet of Things (IoT), the concepts defined in this 'new' zero trust cybersecurity approach had their roots in the early days of the USG's concerns about securing the Internet—which was the inspiration of the SPYRUS solution suite. Between the early 90's through 2004, E-Government legislation and regulation had promised the U.S. citizenry security for:

- Electronic Records to replace Paper Records
- Electronic Transactions to replace Paper Transactions
- Electronic Signatures to replace Wet Signatures

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

Evolution to Information Assurance

During this same period we moved from using the term *Information Security* to *Information Assurance* and began socializing that ***Today Information Assurance is based on who & what, not where***—understanding the identity of the people, devices, servers, objects, code (and now IoT)—must be accurate to achieve strong mutual authentication and enable relying parties to only trust an entity for what it should be trusted.



To date, the promise of a ***Citizen-focused, secure E-Government*** remains a promise rather than a reality in the United States even though the technology to achieve success has been deployed and matured. Unfortunately, it has been largely ignored or poorly implemented. During this same period the USG and industry partners spent $100's of million building strong cryptographic identity authentication and encryption systems. These systems were intended to be normalized across USG services, absorbing the heavy lifting and costs of early adoption, in order to proliferate across our on-line ecosystem. Unfortunately, the USG was never able to establish a market for those services among Federal agencies. Perhaps this has been a 'not invented here' push back? This is evidenced by an easily federated technology being deployed in numerous silos within the USG causing an unsurmountable obstacle for wide-spread adoption.

Some believe arguments about the need to immediately achieve a 100% solution precipitated the delay of implementing a 98% or better solution. Regardless of the reasoning, the lack of securing our citizenry in a growing online ecosystem has only resulted in exponentially increasing vulnerabilities allowing fraud and waste to be the largest threats to our nation's economy and security. Since there has been no market for a citizen-focused strong cryptographic encryption, identification, authentication, and authorization services championed by E-Government services envisioned by the existing statutory and regulatory environment, neither the urgency nor understanding of this need has materialized.

A "Perimeter-less World"

A "*perimeter-less world*" has existed for decades. As have the tools to achieve the concepts of a Zero Trust Architecture. SPYRUS has been an innovator and thought leader in the design, manufacture and implementation of these tools since the early 90's. With data moving at increasing speed, to and through so many endpoints that are inconsistently protected, the myriad of incompatible solutions that hamper productivity and foster short cuts that exacerbate vulnerabilities are no longer adequate. Without a true end-to-end security approach to manage user and device multifactor authentication (MFA) for access; and, authenticated encryption to protect data at rest (in use and in transit) with asymmetric technology and private key protection that is easy for the user and translates all computing devices, attended and unattended are essential to achieving a successful Zero Trust Architecture. Only with the highest levels of confidence in the identity and cryptographic processing of each endpoint can Zero Trust be achieved. Stacking symmetric solutions has proven ineffective without some confidence in the initial mutual authentication transaction. For enterprises, the ability to manage the keys of those endpoints is also essential.

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

SPYRUS: Protecting Endpoints

SPYRUS protected endpoints are managed with enterprise-driven policies to enforce 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 solutions leverage military grade MFA and encrypted token expertise that allows an organization to start with a low-cost solution to enable Zero Trust. Because one size does not fit all, our solution works from a user and enterprise perspective exactly the same. This is also very convenient to the user and cost effective to the enterprise to achieve repeatably consistence, enhanced security and productivity. SPYRUS solutions make security a business enabler, not an obstacle. SPYRUS has matured its solutions from the early days of Information Security through Information Assurance and now in the age of Cybersecurity. We are addressing tomorrow's challenges with quantum technology and blockchain security needs, but most importantly, the security necessary for day to day life in our *"perimeter-less" world.*

The USG is soon to challenge industry again by setting minimum requirements via the Cybersecurity Maturity Model Certification (CMMC) program. To protect our national interests, the CMMC-Accreditation Body has been established to manage CMMC certification audits starting with the Defense Industrial Base. As this promulgates throughout the USG, the message is clear, if not already, that it is not enough to create a security plan or roll-out a solution, all organizations must take a broad view of what needs protecting and how. That means considering technology, people and processes required for a wholistic security approach. SPYRUS' mature solutions are easily implemented to address the many specific technical controls necessary to protect data and access. SPYRUS continues to maintain our commitment to certified hardware and cryptography that allows individuals and enterprises to have ultimate control of the keys that enable encryption, authentication and access control with the highest level of confidence and with an ease of use that protects against malicious use and human error. Our Rosetta security chip offers physical security mechanisms with proven anti-tamper/response circuitry that zeroes all plaintext security information and can be embedded pre- or post-market in modern computing endpoints.

SPYRUS is well-prepared to help you meet the security challenges of today and of tomorrow. Whether you are planning to improve your security infrastructure or preparing to meet new compliance requirements such as the CMMC or other stringent regulations including the General Data Protection Regulation (GDPR) and the Gramm-Leach-Bliley Act (GLBA) that expose you to financially and reputationally damaging fines, contact us at sales@spyrus.com to engage with a SPYRUS security expert.

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.