STEALTH™

SAIC®

Exclusive Federal Reseller

Accelerating the ATO Process with Unisys Stealth®

White Paper

Value Statement (Bottom Line Up Front)

A major barrier to achieving the enhanced capabilities and efficiencies of modernized Federal Information Systems quickly is the Assessment and Authorization (A&A), Authority to Operate (ATO) process. As organizations adopt Agile applications development capabilities, their ability to quickly update systems based on evolving business requirements is outpacing Federal agency ability to rapidly comply with A&A requirements. Unisys' Stealth, a proven technology, directly addresses several challenges on the path to accreditation by streamlining multiple steps throughout the ATO process. It reduces the scope and simplifies how security controls can be applied.

Introduction

The Federal Government needs Information Technology (IT) systems for mission success. Agency IT governance and security requirements for these IT systems must be well documented and tested, prior to operation, through the A&A process. A process that must be performed correctly, to result in an IT system achieving an ATO. Organizations must modernize their aging IT systems by leveraging innovative approaches without exceeding risk tolerance thresholds to effectively enhance their mission capability.

Every government facet relies on IT to achieve positive mission outcomes. Thus, maintaining the IT system's Confidentiality, Integrity, Availability (CIA) is paramount. Given the criticality of these systems, the US Federal Government has established IT governance that is based, in part, on legislative authority from the Privacy Act of 1974, the Information Technology Management Reform Act of 1996 (ITMRA), and the Federal Information Security Management Act of 2002 & 2014 (FISMA). Direction and execution is overseen by several organizations including the Office of Management and Budget (OMB), Department of Homeland Security (DHS), United States Computer Emergency Readiness Team (US-CERT), and the National Institute of Standards and Technology (NIST).

Processes with Challenges

The first A&A step is one of the most difficult – Categorization, as defined in FIPS 199/ SP 800-60. A key requirement within Categorization is defining the scope of the security perimeter (as known as the security boundary) of the information system. Defining the security boundary of the Information System requires identification of the information types to include:

- All the information types that are input, stored, processed, and/or output from each system
- All applicable sub-systems for Mission Information System
- All Support and Management Information sub-systems of the Information System

Defining the system boundary grows in complexity year after year due to the distributed nature of information systems spread across multiple platforms, networks, and geographically separated users. With the increasing adoption of cloud computing services by Federal agencies, portions of systems remain on premise while other portions are hosted in approved commercial cloud environments.

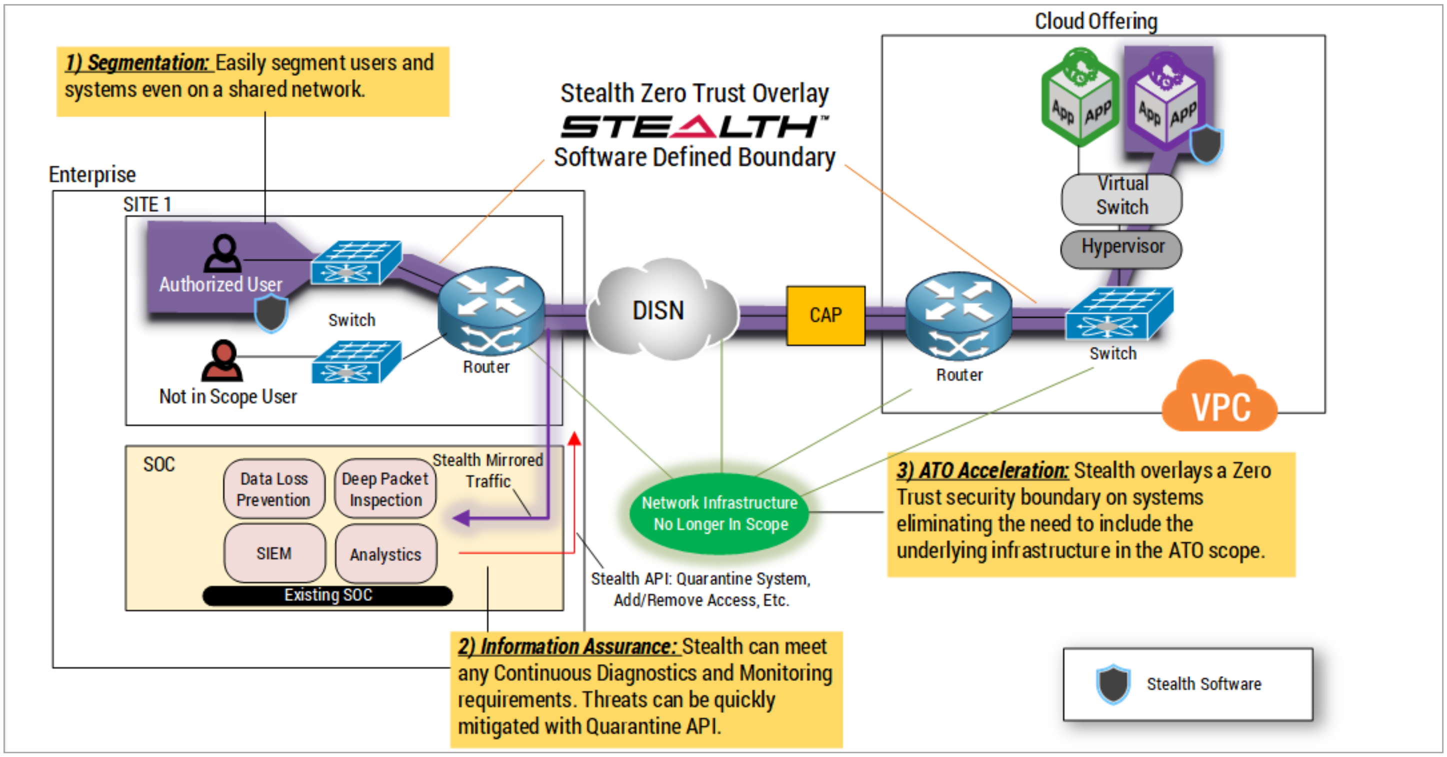
Unisys Solution: Keep It Simple

Unisys Stealth is a software-based microsegmentation capability that overlays on or across infrastructures (on-premise, enterprise and cloud) to secure and segment users and workloads. The Stealth software, installed on the user workstations and servers, allows creation of a trusted security boundary between systems. Establishing trust end-to-end between systems without having to trust the underlying network is a core principle to establishing a Zero Trust Architecture. Stealth uses NIST FIPS compliant cryptography to enforce the segmentation. And it runs low in the OSI networking model remaining transparent to systems with low impact on the end user experience, server or application administration.

The core features of Stealth for streamlining the ATO process are:

- **Segmentation**: Provide a simple way to segment the in-scope components from the rest of the environment; without complex network reconfiguration through additional VLANs or firewalls.
- **Information Assurance**: Provide the customer end-to-end visibility and immediate threat isolation capability of all Stealth systems.
- **ATO Acceleration**: Accelerate the Assessment and Authorization (A&A)/Authority to Operate (ATO) process by significantly reducing the scope of the environment through the use of Stealth as a security boundary overlay. Stealth employment eliminates the need to ensure that every router, switch, firewall, platform, etc. is compliant because trust is formed end-to-end with Stealth software – both User-to-Server and Server-to-Server. This concept is depicted in below in Figure 1.

Stealth can be implemented quickly, providing benefit of immediate cost avoidance by not reconfiguring networks, buying new firewalls, or physically separating network equipment. Stealth overlays on the existing network infrastructure establishes cryptographically isolated communities on the same physical network backbone. Stealth can easily segment systems on the same shared network without the need for new VLANs, re-IP addressing of systems, or creating new firewall policies. This streamlined approach allows mission owners and Information Assurance (IA) teams to easily define, document, and enforce the security boundary of the environment regardless of where systems and users are located throughout the Enterprise. Stealth empowers an organization to rapidly deploy the capabilities securely because all systems in scope are in a cryptographically isolated boundary. A boundary that the Security and IA teams can monitor with existing security tools. Security Operations personnel can respond to any threat by using Stealth to remove or isolated a user, resource, or system access from the environment.



1) Segmentation: Easily segment users and systems even on a shared network.

3) ATO Acceleration: Stealth overlays a Zero Trust security boundary on systems eliminating the need to include the underlying infrastructure in the ATO scope.

2) Information Assurance: Stealth can meet any Continuous Diagnostics and Monitoring requirements. Threats can be quickly mitigated with Quarantine API.

Figure 1.

Mapping to NIST RMF

To achieve an ATO, information systems need to implement NIST security controls to secure and protect the information, people, and assets that interact with the system. Achieving compliance through a software-defined boundary expedites this process by providing end-to-end network security and segmentation, mitigating risk in multiple NIST RMF Control Families. Figure 2 depicts a sample of the NIST RMF Controls that Stealth addresses without the complexities of network re-design.

NIST 800-53	Control Family	Requirements	Stealth Applicability
AC-3	Access Control	**Access Enforcement** Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Stealth provides access enforcement through identity/role/attribute based policies that are cryptographically enforced. Stealth creates trusted security boundaries between systems, applications, and users called Communities of Interest (COIs). Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.
AC-6	Access Control	**Least Privilege** Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	Stealth employs "Least Privilege" by ensuring that only authorized users are able to access the least amount of systems and resources required to perform their duty. This enforcement take place in as a software overlay, eliminating the need to reconfigure the underlying network. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.
SC-13	System and Communications Protection	**Cryptographic Protection** Control: The information system implements organization-defined cryptographic uses and the type of cryptography required for each use in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, and standards.	Stealth supports FIPS/NSA approved and validated cryptography.
SC-7	System and Communications Protection	**Boundary Protection** Control: The information system: Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;	Stealth supports all inspection and monitoring requirements to allow Information Assurance and Security Operations personnel to peform Continous Diagnostics and Monitoring and mitigate threats through the use of the Stealth Management API.
SC-8	System and Communications Protection	**Transmission Confidentiality and Integrity Control:** The information system protects the confidentiality and integrity of transmitted information.	Stealth protects transmission confidentiality and integrity where needed and implemented by the organization with the use of Communities Of Interest (COI). Communities of Interest (COIs) enable cryptographically secure, virtual networks based on user-id. Only users within the same COI are able to communicate with each other. Users not part of a particular COI are not able to see each other's systems on the network nor communicate. This segments and isolates users within the network based on policy. COIs change dynamically based on Active Directory/LDAP User or Group membership. The result is a much simpler network infrastructure, increased agility to react to new requirements, and enhanced security of your network data.

Figure 2. Sample of Stealth Mapping to NIST RMF Controls

Proven Technology

Stealth's strength is demonstrated by the evaluations and validations it has achieved, including from National Security Agency's (NSA) National Information Assurance Partner (NIAP). Stealth is approved for use with an ATO by the DoD Information Security Risk Management Committee (ISRMC), the Defense Security/Cybersecurity Authorization Working Group (DSAWG), Cross Domain Technical Advisory Board (CDTAB), and is built into the NSA's approved Cross-Domain Separation Solution for Cross Domain Access.

Conclusion

Stealth's software-based approach allows rapid implementation, incrementally enabling Federal Agencies to deliver new capabilities securely while protecting legacy environments from multiple threat vectors that can result in data breaches or denial of service. Stealth's ability to provide a single pane of glass view across multiple platforms (on-premise or cloud) directly aligns with the needs of Federal Government organizations to continue current operations, while modernizing/transforming to cloud architectures. Stealth is the solution for next generation security in a hybrid enterprise, solving the challenge of obtaining and maintaining an ATO for evolving IT technology and mission needs.

Learn more about how you can quickly achieve ATO with Stealth at www.SAIC.com/stealth and contact us at www.SAIC.com/stealth-contact.

SAIC is the exclusive reseller of Unisys Stealth to the federal government.

For more information visit www.unisys.com

05/20 20-0229