UNISYS

How Financial Services Institutions Can Take Advantage of Unisys Stealth

Point of View

High profile security breaches, including recent attacks against several banks involving the messaging network those banks use to transfer funds, highlight the increasing risk facing the global financial system.

At the same time, Banks and other Financial Services entities are facing a perfect storm of competitive pressure that has the potential to disrupt core areas of their traditional business model.

Today's Security Challenges

High expectations for user-experience and mobile solutions are demanding greater IT agility and placing additional burden on security resources that are already stretched to the breaking point.

As these financial entities strive to maximize customer value and improve profitability - operational efficiency, cost reduction, customer data confidentiality and cybersecurity have become top priorities.

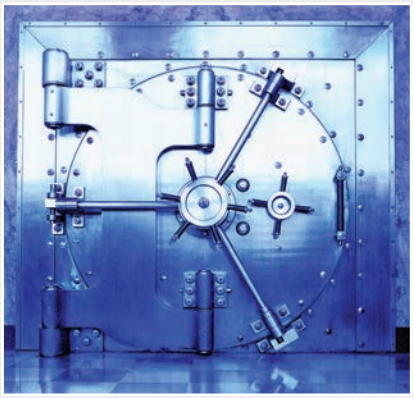
Unisys believes that security must be an **enabler of the business and NOT an obstacle.**

We believe a fresh approach to cybersecurity is necessary – one that recognizes that organizations aren't perfect, that employees sometimes work from home, that clouds and mobile are a necessary efficiency, that supply chains are integrated, and that adversaries have all the advantages – will tip the balance of power back to the good guys. This fresh approach is our future and is based on advanced technology coupled with an assumption the bad guys will get in somehow/somewhere/sometime, but the damage they do must be localized and limited so that it's not front page news.

Growing Cybersecurity Concerns within the Financial Services Sector

Financial Services entities are under attack by very sophisticated and persistent threat actors who are motivated by profit or malice and perpetrated by nation states and organized crime elements that have the means and methods to disrupt operations and commit cybercrime.

Client trust is critical as loss of trust can have a dramatic effect on the business and shareholder value. As a result, cybersecurity, information protection and maintaining customer privacy have become board-level issues.



Unisys Stealth enables "Zero Trust" - Initially proposed by Forrester, in Zero Trust, all network traffic is untrusted so all resources must be secured and access control must be limited and strictly enforced.

Stealth utilizes a Software Defined Network approach and micro-segmentation to enable Zero Trust. Stealth shrinks and minimizes the attack surface, limits and strictly enforces access, restricts lateral movement, obfuscates data assets, and has advanced encryption mechanisms for data-in-motion.

Unisys Stealth for Financial Sector

Attempts by IT to segment the network and ensure that a break-in to one segment of an enterprise doesn't affect the security of the other segments have largely failed. Traditional network security measures such as Firewalls and virtual local area networks (VLANs) are complex and costly to manage.

Unisys Stealth® delivers unparalleled security to Financial Services entities, while simultaneously lowering operational cost and complexity.

Stealth is a leading edge micro-segmentation security solution that protects information by cryptographically isolating data at the packet level and organizing it into functional communities that only authorized users can access.

Unisys Stealth Makes Financial Data Undetectable to Hackers

Unisys Stealth enables "Zero Trust" - Initially proposed by Forrester, in Zero Trust, all network traffic is untrusted so all resources must be secured and access control must be limited and strictly enforced.

Stealth utilizes a Software Defined Network approach and micro-segmentation to enable Zero Trust. Stealth minimizes the attack surface, limits and strictly enforces access, restricts lateral movement, obfuscates data assets, and has advanced encryption mechanisms for data-in-motion.

IT staff can easily and quickly segment physical networks into logical micro-networks without the traditional security management overhead. When done correctly, micro-segmentation will lower operating costs and allow control of the enterprise network without having to deal with complex firewall rules, outdated applications, remote users, cloud-based services and third parties that all have become attack vectors in today's world.

Select Use Cases, and how we're Helping Financial Services Entities

1. **Insider Threat Programs** - Traditional security measures have focused on external threats. The focus has shifted to insiders - individuals within the organization who leak information. Whether this is the result of negligence, social engineering or malice, the results can be the same and cause big problems.

   Strong security policies need to be in place for all employees and they need to be granular and such that users only have access to data they need, and not more. A security principal known as "Least Privilege"- where users only have privileges which are essential to their work - is a core tenet of every security program and nearly all compliance requirements.

Stealth provides end-to-end secure protection of business data and infrastructures from cyber-attacks. Stealth software can protect against payment fraud, data theft, malware and more. Installed on a network, with a single management console coupled with software agents that run on IP devices in the enterprise.

Stealth allows the system manager to establish controls that decide who gets to do what, and easily enforce those rules at the network packet level, without impacting existing applications, routers, firewalls and other infrastructure.

2. **Extending Enterprise Security to the Cloud** - NextGen technologies like cloud are too compelling to ignore. Stealth makes VMs in the cloud undetectable to unauthorized users. Stealth encrypts data-in-motion from the datacenter to the VM in the public cloud, and between VMs in the cloud. For additional information Unisys has recently announced partnerships with MS Azure and AWS.
3. **Securing Legacy Systems** - that are otherwise difficult / costly to secure. As an example, support for Windows XP ended in early 2014, and Microsoft no longer offers security patches, making XP extremely vulnerable to attacks. However, XP is still used in a multitude of critical systems (including many ATMs). The problem has been known for some time and in late 2013 the FFIEC (a U.S. regulator) issued a warning letter indicating that potential problems include degradation in the delivery of various products and services, application incompatibilities, and increased potential for data theft and unauthorized additions, deletions, and changes of data.
4. **Merger & Acquisition** - segregate / secure and reduce time to integrate the business. Protect and limit access to highly confidential information “prior to merger” and on a need-to-know basis.
5. **Data Center Consolidation** - Traditional network security zoning techniques are complex and expensive. Maintaining Firewall rulesets are labor intensive and network security devices are expensive. Stealth can speed consolidation efforts, lower costs and dramatically improve security.

Stealth is a leading-edge, software-based micro-segmentation security solution designed to make networks more secure and provide a cost-effective way to protect sensitive data from unauthorized access.

Stealth provides end-to-end secure protection of business data and infrastructures from cyber-attacks. Stealth software can protect against payment fraud, data theft, malware and more. Installed on a network, with a single management console coupled with software agents that run on IP devices in the enterprise.

Stealth allows the system manager to establish controls that decide who gets to do what, and easily enforce those rules at the network packet level, without impacting existing applications, routers, firewalls and other infrastructure.

Stealth has minimal impact on operations as a single change in the directory services system allows access to be granted or taken away in minutes, not months. Furthermore, Stealth reduces capital expense and allows a "flattening of the network" by eliminating traditional hardware security platforms (i.e. firewalls switches and routers). Stealth reduces operational costs by eliminating the maintenance on these hardware platforms, and by eliminating the need to maintain complex firewall rule-sets.

A Way Forward: Unisys Stealth

Unisys is helping today's leading financial institutions by enabling them to conduct business securely and with greater agility. Stealth provides Financial Services entities the following core security benefits:

- Shrink the Attack surface. Using Stealth's software micro-segmentation features, financial entities can logically separate sensitive systems from other systems and from unauthorized external, or internal access.
- Cryptographically secure and cloak systems. Using Stealth's advanced cryptography features, only users with the "key" have access and for all other users Stealth systems are "cloaked" and invisible to unauthorized traffic.
- Minimize lateral movement. In the event an attacker gains access to the network, Stealth mitigates their ability to move laterally, and finding Stealth enabled systems is virtually impossible as they are cloaked.
- Strictly manage and enforce which users have access to Stealth enabled systems, and control such access using commonly deployed directory services such as Active Directory (AD) or LDAP. Using Stealth, identity and access rights follow the user, rather than physical devices, so security moves with the user and is easier to manage.
- Not enough resources, or the right kind of resources, to manage the complexity. Stealth has minimal impact on operations as a single change in the directory services system allows access to be granted or taken away in minutes, not months. Furthermore, Stealth reduces capital expense and allows a "flattening of the network" by eliminating traditional hardware security platforms (i.e. firewalls switches and routers). Stealth reduces operational costs by eliminating the maintenance on these hardware platforms, and by eliminating the need to maintain complex firewall rule-sets.
- Reduced scope for Audit Scope, by restricting access to a business "need to know" basis and logically segmenting "in-scope" systems from other systems.

Contact:

Steve Migliore

Sr. Director Cybersecurity, Global Financial Services
Phone: 1 781.330.0803
E-mail: stephen.migliore@unisys.com

07/16 16-0318 (S)