STEALTH by UNISYS

Unisys Stealth for Financial Services

Strengthen Security *AND* Shrink Costs

Financial services executives must strike the perfect balance between cost and risk – it's easier than you think.

The highly sensitive, mission-critical information that financial services institutions are entrusted to protect is under relentless attack by sophisticated cyber criminals who have figured out how to penetrate the fortress of traditional security. Financial services executives know that an innovative approach to security must be embraced in order to sidestep the onslaught of external and internal security risks – one that not only helps strengthen security, but also reduces costs in today's budget-restricted, compliance-laden environment. Unisys Stealth™ is a software security innovation that eliminates the tradeoff between cost and risk and improves agility by strengthening data protection, simplifying management, and reducing reliance on physical technology infrastructure.

HIGHLIGHTS

- **Segment your data center based on users.** Define and control access to the mission-critical information you are entrusted to protect.
- **Go dark – conceal communication endpoints.** Make servers, devices, and other communication endpoints undetectable.
- **Secure data in motion.** AES-256 encryption secures data in motion.
- **Reduce reliance on physical infrastructure for security.** Consolidate physical networks and reduce costs.
- **Quickly respond to the needs of your business.** Easily update security access privileges through Active Directory.

Traditional Data and Network Security is Not Good Enough

Financial services executives are under intense pressure to protect their enterprises from APT, DDoS, insider threats, and other risks that jeopardize the security of highly sensitive company and client financial information. In addition:

- Regulations like Sarbanes-Oxley, BASEL III, and PCI are driving tightened security and controls, further squeezing limited budgets
- Mobile, cloud, social media, and other disruptive technologies are being integrated into the enterprise faster than they can be safeguarded
- Aggressive cost-cutting agendas are degrading security programs at a time when threats are escalating

According to the PWC 2015 Global State of Information Security Survey, the total number of security incidents detected by respondents climbed to 42.8 million in 2014, an increase of 48% from 2013.

Effective security requires an innovative approach. How can financial services leaders navigate today's converging pressures of escalating security risk, budget constraints, and regulatory compliance while increasing the security of critical financial transactions, systems, and networks?

Go Dark – Reduce the Attack Surface

Winning the battle over protecting mission-critical data demands a new, proactive security approach. Adding more layers of traditional security technology is not the answer. Reducing the attack surface is. Today's leading financial services executives are aligning with the trend towards software-defined networking and pursuing the ability to:

- **Limit data exposure** for the financial institution and users
- **Segregate data and transactions inside the network** so that only those with the right access even know the transaction is occurring, making it undetectable to others
- **Cloak servers and PCs** running sensitive applications in the data center, making servers undetectable to unauthorized users
- **Setup and secure new networks or devices** quickly based on emerging business requirements

Unisys Approach: You Can't Hack What You Can't See

Unisys Stealth is a software security innovation that makes data communication endpoints undetectable on a network, thereby helping to eliminate them as targets for hackers. In addition to increasing data protection and simplifying management, Unisys Stealth reduces reliance on physical technology infrastructure for security. Financial services leaders therefore no longer need to balance the traditional tradeoff between cost and risk – they can increase security and reduce costs. Leading financial services executives can benefit from the following approaches to implementing Unisys Stealth in their enterprises to help them strengthen security, reduce costs and increase agility:

- **Compartmentalize the data center and reclassify data based on need-to-know access**. Consumerization of IT, cloud computing, and breach attempts are driving financial services executives to segment their networks and data centers. Unisys Stealth is designed to securely segment data centers and protect data and systems by cloaking strategic assets.

> With Unisys Stealth there is no longer a tradeoff between cost and risk.

- **Protect local assets within designated regions while controlling access to assets from users in that region**. Unisys Stealth provides geographically dispersed data centers with secure access to the central data center in order to protect from untrustworthy governments or other rogue threats.
- **Help ensure only the right personnel have remote access to the enterprise or sensitive financial information**. Unisys Stealth is designed to cloak Stealth-protected endpoints from users or devices except those who are pre-identified as part of a secure Community of Interest (COI). You can manage access to sensitive information by establishing COIs and restricting members on a need-to-know basis.
- **Get more leverage from the cloud by cloaking public cloud provider servers**. Stealth-protected servers or virtual machines are cloaked from other tenants in the public cloud and from hackers attempting to infiltrate the cloud. This enables you to confidently deploy mission-critical workloads in the public cloud and take advantage of the associated cost savings.

For more information

contact us at: stealth@unisys.com
or visit us at: www.unisys.com/stealth

STEALTH by UNISYS

Printed in the United States of America 02/15 15-0080