Security to Give you Freedom to Focus on What Matters Most – Your Public Sector Mission

Safeguard the Critical Information your Mission and Citizens Depend on

Public sector organizations must navigate a multitude of security, budget, and compliance challenges that are drawing focus and resources away from their missions. Whether it's equipping first responders with critical information to help protect citizens, leveraging cost benefits through cloud deployment, safeguarding sensitive data, or sharing information securely in crisis situations, federal, state, and local public sector leaders are entrusted to deliver.

In today's sophisticated threat environment, the traditional approach to security is no longer effective. A fresh approach is needed as today governments and their agencies are transforming their public services—and many are moving toward digital channels. Securing data in the clouds while enabling mobile access is a necessary efficiency as supply chains are integrated, and adversaries are both skilled and motivated to attack. Unisys brings expertise and insight to address the critical security needs unique to public sector organizations.

- IDC forecasts that around $37Bn will be spent on IT security products worldwide by 2016[1]
- Estimated to hit approximately $46Bn by 2019[1]
- Regulatory compliance, vulnerability exploits and Target breaches are key security drivers for CISOs[2]
- 77.9% of CISOs had to assume responsibility for a breach[2]

Public Sector Organizations are Uniquely Vulnerable

2015 was known as "The Year of Cybersecurity Incidents." However, this isn't much different from what we saw in 2014, and 2013 and 2012. Each time the public is exposed to a "massive breach," it is bigger and more destructive than the

1. Source: IDC, Worldwide IT Security Products Forecast, 2015–2019
2. Source: IDC's State of the "C" in CISO Survey, 2015

previous. In June 2015, the U.S. government's Office of Personnel Management (OPM) reported that background check data for millions of Americans had been compromised. For decades, the rapid expansion of technology and its integration into every part of public sector agencies has contributed to improved service delivery and efficiency – most recently through cloud and mobile. But this rapid technology integration comes at a cost – as indicated by Operation Shady RAT, where an APT attack stole intellectual property from 70 government agencies across 14 countries.

As threats continuously evolve and become more sophisticated and targeted, traditional methods of using firewalls, intrusion detection and prevention systems can't a guarantee of full protection. Across all of the recent attacks, there is one common thread: the bad guys always get in. Today's attacks get in, then move around, and then start doing damage. The attack vectors vary greatly, from social engineering to Advanced Persistent Threats to something as simple as an unpatched server or a lost laptop. Public sector leaders know that an innovative approach to security is needed – not only to combat converging risks, but also to help control costs. How can public sector leaders improve security while also reducing costs?

Micro-Segment Everything; with Precision

There is a better way to approach security, but it requires a fresh approach - Micro-segmentation. Micro-segmentation is based on software loaded onto the network devices, with a single management console coupled with bits of code that run on IP devices in the enterprise. It embraces new technologies like clouds and new business models like integrated supply chains, and delivers real results that are cost-effective in terms of both money and security resources.

Micro-segmentation allows public sector enterprises to quickly and easily divide their physical networks into hundreds or thousands of logical micro networks, or microsegments. Installed and running quickly, Micro-segmentation is a simple way to take back control of an enterprise network without having to deal with firewall rules, outdated applications, remote users, cloud-based services, and third parties that all have become attack vectors in today's world.

Unisys Stealth – Identity Drive Security that can Facilitate Revenue Growth

Unisys Stealth™ is designed on the principles of micro-segmentation at the packet level, ultimately concealing the networks from prying eyes and malware. Stealth software-defined security portfolio delivers a consistent security methodology across the range of environments public sector enterprises need to secure - data center, cloud and mobile. It employs software-based cryptography instead of traditional hardware topology to prevent unauthorized access to sensitive information, reducing the attack surface by making endpoints invisible to unauthorized users (including DBA's). Public sector leaders can create secure communities of interest based on customer value, allowing them to apply varying levels of security to specific users. Unisys Stealth offers:

Protecting Legacy Systems: The reality today is that many public sector organizations don't necessarily operate with the latest, most secure operating systems. How does one protect legacy systems? The most secure strategy that can enable public sector firms to still use legacy operating systems such as XP and Windows 2003 is to isolate them from the production network using their own micro-segmentation. Unisys Stealth does just that.

Cryptographically Secure Information: Stealth works at the Internet packet level, cryptographically sealing each packet in such a way that only packets that are within the approved microsegment will be processed. For every packet, not only is the data portion completely encrypted, but the routing information (headers) is cryptographically sealed so that only authorized users within communities of interests can send and receive packets for their respective groups.

Adopt Identity Driven Management: Stealth enables definition of access control policies through roles and identities, rather than IP addresses, making them simpler to manage thus reducing the risk of any unintentional configuration errors. It facilitates identity driven Micro-segmentation, straight from existing Active Directory (AD) or LDAP systems already in place. A single change in the AD and access can be granted or taken away. In minutes, not months.

Leverage the Clouds: Yesterday's security schemes were holding back public sector enterprises' migration to public and private clouds. Unisys Stealth (cloud) provide an extra layer of security to sensitive applications running in the Amazon Elastic Compute Cloud (EC2) platform or Microsoft Azure Virtual Machines (VM), while maintaining a logical segregation of these applications. It uses encryption cloak both EC2 instances and VMs from non-authorized users and restrict communication between other unauthorized EC2 instances and VMs in the VPC.

Integrate Supply Chains: With suppliers now becoming fully integrated components of an enterprise, Micro-segmentation is a much better approach to providing just the right amount of access (least privilege) they need to do their job, while not allowing them to even see outside of their authorized community. With Stealth, public sector enterprises can rest assured that whatever suppliers try to do outside of what is asked of them, will be stopped at the network packet level through Micro-segmentation.

Embrace BYOD: While public sector enterprises can certainly leverage the cost benefits associated with employees using personal devices for work from the comforts of their homes, it has been historically offset by the cost of security. With Stealth Micro-segmentation, an additional level of security can be deployed to enforce additional access based on location. When inside the office premises, they may have access to sensitive competitive information, but when accessing information from elsewhere, they get only limited access.

"While several peer vendors are more focused on developing and implementing solutions that allow log management systems and detect and alert systems, Unisys is more focused on making information-rich targets invisible in the networks. Unisys Stealth not only strengthens data security but also enables effective controls for endpoint access."

Frost & Sullivan, 2015

Advanced Technology for Today's Global Threats

The Unisys Stealth product family continues to win both industry awards and customer accolades. Called 'groundbreaking' by Frost & Sullivan, the Stealth software-defined security family of solutions helps eliminate the threat of a cyber-attack and prevents an enterprise's highly sensitive data, systems, and intellectual property from being compromised.

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

Unisys is a global information technology company working with government clients across the globe to drive innovation and transform citizen-centric services through leading-edge digital initiatives, including cloud deployments, applications modernization, security solutions, and advanced data analytics. Supporting more than 300 government organizations around the world, Unisys provides IT consulting services and delivers innovative solutions that facilitate the transition to Digital Government. For more information on Unisys' Public Sector solutions and impact, visit www.unisys.com/publicsector.

For more information visit www.unisys.com

Printed in the United States of America 02/16 16-0089