TABLE OF CONTENTS

Enabling the Digital Workforce Generation................................................3
Growing Cost, Risk, and Intensity of Cyber Attacks .................................3
Future Evolution of the Perimeter ..............................................................3
Redirect Security Investments to Four Pillars ..........................................4
Unisys Stealth™: Digital Security for Digital Government ......................5
Features and Benefits Offered by Unisys Stealth™ ...............................5
Conclusion...............................................................................................6
ENABLING THE DIGITAL WORKFORCE GENERATION

Security in the digital environment will be increasingly fine-grained, broad-based, targeted, convenient, and intrinsic to products and applications. As government agencies expand digital capabilities and draw upon a new generation of tech-savvy workers so too will cybersecurity threats grow—in number, sophistication, and intensity. Chief Information Security Officers (CISOs) are recognizing that their traditional security models, primarily based on threat prevention and detection, are no longer effective and a new paradigm is emerging. Agencies are no longer bound by what they own but rather by what technologies, such as the cloud and mobile, their employees use and own. In today’s digital world, they must secure data and assets within an IT ecosystem that extends well beyond their agency walls.

GROWING COST, RISK, AND INTENSITY OF CYBER ATTACKS

The number of security incidents reported by government agencies has skyrocketed in recent years, growing from 5,503 in fiscal year 2006 to 67,168 in 2014.¹ The Pentagon alone gets 10 million hacking attempts every day. A data breach at the Office of Personnel Management (OPM) resulted in more than 20 million stolen records of current and former employees, while an Internal Revenue Service (IRS) data breach netted scammers tens of millions of dollars in fraudulent tax refunds.² No agency is safe from attack. Many struggle to implement cost-effective security. In 2014, 19 of the 24 federal agencies covered by the Chief Financial Officers (CFO) Act reported “cybersecurity as a significant deficiency or material weakness for financial reporting purposes,” the U.S. Government Accountability Office (U.S. GAO) said.

The growing use of digital technologies will only exacerbate the security challenge. Social, mobile, analytics and cloud, and other digital technologies give agencies the ability to collect, share, and analyze huge stores of data for insights that can increase operational efficiencies and mission performance across every agency. However, many of these new digital activities will occur outside an agency’s firewalls. In fact, remote and mobile users—government employees, businesses, and citizens—are already accessing government applications and data any time, anywhere and from multiple devices. Consequently, the traditional model of perimeter security, which was already growing obsolete, has become even more untenable in a digital environment with a seemingly limitless attack surface. Among the key digital technologies that are driving innovation, as well as disrupting legacy security approaches are:

Social Media – Government enterprises are sharing more information and services within and across agencies, including the military services; law enforcement; and intelligence, homeland security, and health and human agencies. The increased information sharing enhances mission capabilities but also increases security risks.

Mobility – Increased mobile use expands the number and types of devices to be secured. In 2014, mobile overtook desktop in Internet usage. Not only are more government workers using mobile devices to carry out their responsibilities but increasing numbers of citizens are engaging with government through mobile devices. Together smart phones and tablets account for 35 percent or more of traffic on federal websites, according to analytics.usa.gov, which collects web traffic from 400 executive branch government domains across over 4,000 total websites.

Analytics – The explosion of data due to the Internet of Things (IoT), especially unstructured data collected and analyzed in real time, has expanded the attack surface for data theft, malware, and sabotage. Security experts increasingly think of data as a “liquid,” capable of seeping into unexpected, unsecure areas. This view further diminishes the emphasis on securing the perimeter in favor of greater containerization of data, even micro-segmentation of data designed to enable users to gain the slimmest access strictly according to need.

In addition, more and more data is going straight from end users’ mobile devices to the cloud, entirely bypassing the perimeter.

Cloud Computing – As agencies move applications away from traditional computing infrastructure and toward public, community, and hybrid clouds, hardening the dissolving perimeter becomes expensive, cumbersome, and uncertain. Despite security anxieties government agencies are increasing cloud investments while moving more and bigger workloads to both public and private clouds. Research firm, International Data Corporation (IDC), predicts that cloud spending will eventually grow to about 50 percent of all government IT spending by 2018.³

FUTURE EVOLUTION OF THE PERIMETER

The IoT will provide endless opportunities to exploit weak links. IoT devices will become increasingly enabled (i.e., capable of much more functionality and connectivity) and increasingly autonomous (i.e., setting in motion a series of interactions without user intervention)—thus immensely attractive to cyberthieves. A study by Business Insider Intelligence predicts the IoT will be “the largest device market in the world, more than double the size of the smartphone, PC, tablet, connected car, and the wearable market combined.”⁴

The IoT in government has already begun. Government “smart buildings” use real-time measures of water, gas, solar power, and


UNISYS
energy consumption, along with diagnostic tools, to help buildings perform more efficiently. Agencies use sensors to track vehicles and other government assets. The military attaches sensors to soldiers’ protective gear to monitor their movement and health. The perimeter security challenges are obvious when billions of devices are connected together, creating new vulnerabilities by offering hackers a potential door inside. According to Gartner, by 2020, enterprises and governments will fail to protect 75 percent of sensitive data and will declassify and grant broad public access to it.5 That leaves a great deal of highly sensitive data that must be protected more rigorously than ever. Government agencies will have to put more intelligence into classifying their various streams and stores of data, and providing targeted, differentiated security as appropriate to each.

**REDIRECT SECURITY INVESTMENTS TO FOUR PILLARS**

Since perimeter security is already failing and future technologies and threats will make perimeter security even more porous, government agencies need to switch to a new approach. We recommend that agencies adopt four main pillars of action to secure their data and networks in the new digital environment:

**Move away from an over reliance on firewalls and other perimeter defenses, and redirect security budget toward a new and advanced technology called micro-segmentation.**

Micro-segmentation severely restricts the movement and damage of attackers that get in. The normal behavior of most malware once it gets in is to enable the attacker to move laterally through the network with the goal of finding and then exfiltrating high value assets. But with micro-segmentation, an attacker that gets in is contained in a tiny compartment. Once they are in, they are stuck which dramatically reduces access to your high-value assets. Cost-effective and easy to manage, micro-segmentation is an essential component of robust, multi-layered cybersecurity.

**Switch from a device-based to identity-based security scheme.**

This seems simple, but the reality is that devices like firewalls, routers, and other assets have all been stitched together into a complex security stack in an attempt to protect the agency. In many cases, agencies have hundreds of thousands of firewall rules alone. The rules are often unduly complicated and expensive to maintain and control. Ultimately, there’s no way agencies can possibly keep up with or understand all of their multiplying firewall rules. Agencies can dramatically reduce dependence on firewalls by switching from a device-based security approach to one based on identity coupled with micro-segmentation. The identity-based security concept scales limitlessly and is cost-effective in terms of deployment and operation, because it uses a common identity scheme that’s already in place, such as Microsoft Active Directory or common access cards as in the military. Whatever the ID system, it can be used as the foundation for a security approach. The advantages are lower costs, less risk, and higher security.

**Rеevaluate current digital enterprise security approach.**

The concept of the perimeter firewall as the key security control was great back when government enterprises existed wholly within four walls, but now it includes entire ecosystems (e.g., cloud providers, mobility, suppliers, etc.). In many cases, it also includes citizen services that interact with systems on a regular basis. Securing the extended ecosystem with a four-wall security approach will cost a lot of money without delivering necessary results. What’s needed is security that works and flows actively through all devices and is delivered in a way that meets security and compliance requirements. All of this is possible when the switch is made to an identity-based micro-segmentation security system.

**Ensure security is operationally feasible.**

It may sound odd that one would build something that isn’t feasible but too often security people have, in fact, designed systems they knew would not be completely effective. Government agencies need to redesign their systems to operate more transparently, cost-effectively, and within the skill sets that are available to the organization.

---

**UNISYS STEALTH™: DIGITAL SECURITY FOR DIGITAL GOVERNMENT**

Recognizing the challenges of securing government networks and data in today’s digital environment, Unisys built a better way for dealing with advanced cyber threats. By substituting traditional hardware based security for software-defined security, our Unisys Stealth™ micro-segmentation solutions make endpoints invisible to unauthorized users, thereby preventing unauthorized access to sensitive information and reducing the attack surface. The Unisys Stealth™ software suite delivers consistent, inimitable security for global enterprises focused on protecting data in their data center, cloud, and mobile infrastructures.

**FEATURES AND BENEFITS OFFERED BY UNISYS STEALTH™:**

- **Endpoint and Data Cloaking.** Unisys Stealth™ drops any network packets except those formatted with Unisys Stealth™ community of interest (COI) specific encryption. This provides security from external and internal threats by rendering data, servers, and users as undetectable on the network to users and devices that do not belong to the same COIs.

- **Virtual Communities of Interest.** Unisys Stealth™ maintains secure COIs of users and servers by segregating the network on a “need-to-know” basis. This enables the network to be cryptographically virtualized based on user or device identity rather than on physical location.

- **Execution Low in the Protocol Stack.** Unisys Stealth™ operates below the application layer in the network stack (i.e., between levels 2 & 3). This renders Unisys Stealth™ transparent to applications so no application code changes are required.

- **Integration with Identity Management Systems.** Unisys Stealth™ COIs are managed by Active Directory or other Lightweight Directory Access Protocol (LDAP) based identity stores. This simplifies COI management and enables administrators to make changes quickly (e.g., by adding or deleting users or changing COI privileges).

- **Perfect Forward Secrecy (PFS).** Unisys Stealth™ is designed so session keys will not be compromised even if the private key of the server is compromised. This protects against malicious insiders. For example, one member in a COI can’t read messages sent between two other members of the COI.

- **Enterprise Manager.** This Unisys Stealth™ management tool provides a single interface for configuring, monitoring, and managing the Unisys Stealth™ environment.

The Unisys Stealth™ security package can be deployed in multiple environments and operating systems, such as Unisys Clear Path Forward, Amazon Web Services (AWS), and FedRAMP approved security providers. For example, with Unisys Stealth™, agencies can “cloud burst” into AWS because Unisys Stealth™ can easily be configured in the AWS cloud.

**Ready for Government**

The Unisys Stealth™, software received the National Information Assurance Partnership’s (NIAP) coveted Evaluation Assurance Level 4+ (EAL4+) certification, a Common Criteria international standard in effect since 1999. NIAP’s Evaluation Assurance Levels are now superseded by National Security Agency’s (NSA) new Common Criteria Protection Profile certifications and, as of January 15, 2015, all product versions evaluated and validated by NIAP were migrated to the NIAP Validated Archived Products List.

The current version of Unisys Stealth™, which added the ability to leverage the industry standard Internet Protocol Security (IPsec) protocol suite, as well as other key enhancements, conforms to NSA’s Protection Profile for IPsec virtual private network (VPN) and will soon complete validation. It uses Suite B encryption and also appears on the Commercial Solutions for Classified (CSfC) Components List. This NIAP Common Criteria Protection Profile is also the basis for inclusion in North Atlantic Treaty Organization’s...
(NATO) Information Assurance Product Catalogue, while CSfC enables Unisys Stealth™ to be used to protect classified National Security Systems (NSS) data.

Unisys Stealth™ has been sold and installed by the United States Department of Defense (DoD) and allied defense forces as well as in a variety of local and federal governments and commercial entities around the world.

CONCLUSION

Federal agencies are transitioning—steadily and inexorably—to digital environments that facilitate easy and widespread access to government services and data, as well as support data analytics and other advanced tools. These new virtual, cloud, and mobile environments offer unprecedented value in terms of cost savings; agile development and deployment of new services; and enhanced mission capabilities. They also extend an organization’s IT ecosystem beyond the walls of its traditional security perimeter. Consequently, agencies should move away from an over reliance on firewalls and other perimeter-based defenses and instead adopt a new security approach that extends security to wherever the data, devices, and users are operating.

Unisys Stealth™ delivers the security required for the new digital government environment. It tightens access control by focusing on user identity rather than physical devices, so security moves with the user and is easier to manage. Unisys Stealth™ conceals endpoints by making them undetectable to unauthorized parties inside and outside the enterprise, and it protects sensitive data in motion from potential compromise through encryption. Because it uses micro-segmentation, Unisys Stealth™ quickly contains unauthorized intruders and prevents them from accessing critical networks or data. It can also strengthen management controls; scale to growing needs; and reduce costs by allowing agencies to consolidate and virtualize networks, servers, and cloud architectures. Unisys Stealth™ is designed to meet the evolving security requirements and needs of government agencies.

ABOUT UNISYS

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. To find out more about how our solutions can work for you, please visit http://www.unisys.com/offerings/security-solutions.

ABOUT THE AUTHOR

Mark Cohn is a Vice President of Engineering and Chief Technology Officer for Unisys Federal Systems. In this role Mark leads technology strategy and solutions development for major U.S. Federal government programs. He and his team bring innovation to expand the mission impact of IT, design capabilities that enable secure business operation and implement mobility-enabled and cloud-driven enterprise services transformation. Mark represents Unisys for government-industry liaison on Defense Industrial Base cybersecurity and critical infrastructure protection and sits on AFCEA International’s Technology Committee serving the defense, homeland security, and intelligence communities.

© 2016 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.