A NEW SECURITY APPROACH FOR GOVERNMENT

Micro-Segmentation as a Strategy to Secure the Government Enterprise

A Digital Government Series by Unisys Corporation

UNISYS | Securing Your Tomorrow™

TABLE OF CONTENTS

INTRODUCTION

While cybersecurity has come a long way, the journey has been slow with starts and restarts. National, state, and local governments have made progress toward safeguarding their enterprises against cyber threats; however, the continued development of Internet of Things (IoT), mobility, smart cities, and new digital channels, among several other additional factors, have added complexity and more risk along the path toward securing the government enterprise. There are new dimensions and challenges, which are just becoming known and today's solutions and approaches are lagging far behind.

A fresh approach to security—one that understands government enterprises aren't perfect; government employees are often in the field or could be more efficient working from home; clouds and mobile are the new norm; and adversaries are both skilled and motivated to attack—is needed. This fresh approach is based on advanced technology that assumes bad guys will get in—or more likely they are already there. Yet damage can be localized and minimized so that it's not front-page news. For government entities and Chief Information Security Officers (CISOs) and Chief Information Officer (CIOs) who are often held accountable, a breach is far more damaging and controversial because trust is eroded and difficult to regain. Breaches aren't just devastating to the integrity of the institution but possibly damaging to the citizens of whom governments serve. While information integrity and data privacy are critical issues, perpetrators who are inside can plan an attack that significantly disrupts government operations and creates vulnerabilities.

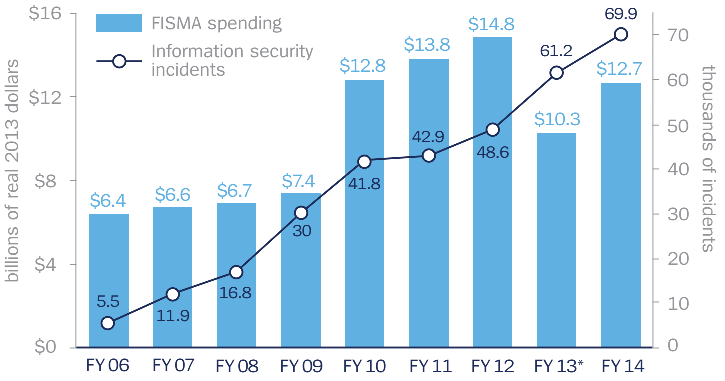
This white paper explores the power of a new security strategy, micro-segmentation, to effectively address this challenge for today's governments.

BACKGROUND

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

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. Such occurrences aren't slowing down despite billions of dollars invested in cybersecurity. Simply put, current strategies aren't working. Without taking drastically different measures, we will continue to be vulnerable.

Federal Cybersecurity Spending &
Total Reported Federal Information Security Incidents



Data note: **OMB calculation methodologies of total Federal Information Security Management Act (Fisma) spending changed in indicated years.*

Sources: *Congressional Research Service. "Cybersecurity issues and Challenges: In Brief," December 16, 2014; Government Accountability Office. "Information Security: Federal Agencies Need to Enhance Responses to Data Breaches." April 2, 2014;*
Office of Management and Budget, "FISMA Annual Report to Congress," February 27, 2015.
Produced by Eli Dourado, Andrea Castillo, and Rizqi Rachmat, Mercatus Center at George Mason University, March 2015.

ELIMINATING THE THREATS IS NOT THE ANSWER

Government CISOs and CIOs are facing tremendous pressure as governments are under constant attack and scrutiny. Today's—let alone tomorrow's—security issues can't be solved with the same type of thinking and approaches. The scope of threats—both known and unknown—pose a multitude of new risks for government organizations, especially as they have expanded their reliance on cloud computing and as employees access information through their own mobile devices. Threats come from all perimeters. They are often caused by poorly configured settings, permissions, or by ineffective data governance, access management, or usage policies.

The larger or more complex the enterprise, the bigger the attack surface and higher amount of entry points. Those entry points can differ in nature—from digital assets or the end users themselves who might succumb to social engineering; expose their passwords; or inadvertently provide access by losing or failing to destroy their hard drives. With a big enough target on a long enough timeline, the odds of patching every portion of an attack surface drops to zero. There will always be vulnerabilities.

Today's attackers get in, move around, and then start doing damage. It's now time to stop them from moving around—particularly "East-West" movement across platforms, which has farther-reaching risks and consequences.

...firewalls are a failed premise and have become outdated or obsolete with respect to security. Their modern-day purpose continues to keep perpetrators out, while ***today's cyber criminals have already gotten in.***

FIREWALLS ARE NOT THE ANSWER

From "air gaps" that physically separate networks into different spaces, to expensive firewalls with too many back doors, and local area networks (LANs) or virtual local area networks (VLANs) that still fail to keep up with the risk load, the cyber landscape is riddled with inconsistency and failed promises.

Today's CISOs and CIOs, however, are still under massive pressure to manage risk while reducing costs. Most governments are moving or have moved into hybrid architectures on the path toward modernization and also as enablers of digital government. The hybrid architecture or hybrid network is now commonplace as governments are migrating to the cloud. Yet this introduces more complexity from a security perspective as there is a mix and match of resources, configurations, tools, and controls—all very difficult to unify under a common and consistent environment. This is where segmentation comes in.

According to the U.S. Office of the Director of National Intelligence (ODNI), and many other global security experts, segmentation can effectively secure an enterprise. Break-ins will occur, but boundaries through segmentation can contain or reduce the risk. To that end, for the last few years, organizations have begun attempts at segmenting their enterprise based on this vision.

The primary focus of segmentation is that it recognizes perpetrators are already inside the network. They are unwelcome guests who have already arrived. It is critical to point out that firewalls are not the mechanism to achieve advanced security via segmentation. In fact, firewalls are a failed premise and have become outdated or obsolete with respect to security. Their modern-day purpose continues to keep perpetrators out, while today's cyber criminals have already gotten in. Segmentation by firewall achieves segmentation but not necessarily security, as failures have pointed out.

A NEW APPROACH: IDENTITY-BASED MICRO-SEGMENTATION

There is a better way to approach security—micro-segmentation. Micro-segmentation takes on the mission of the old style segmentation with an entirely new approach that makes it easier to implement and manage and is much more secure and inclusive. It embraces clouds and new business models such as integrated supply chains, and delivers real results that are cost-effective in terms of both money and security resources.

Micro-segmentation allows enterprise managers to quickly and easily divide their physical networks into hundreds or thousands of logical micro networks, or microsegments. Micro-segmentation can be described as having a safety deposit box "room" within a vault. Establishing different microsegments to keep different parts of an organization logically separate dramatically lowers risk. When a perpetrator does succeed in getting inside, they only can see what's in a one tiny little box (segment).

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. It can be effectively implemented and managed through a single management console coupled with bits of code that run on Internet Protocol (IP) devices within the enterprise. The system manager can layer on controls that decide who gets to do what and easily enforce those rules at the network packet level.

MICRO-SEGMENTATION: CRYPTOGRAPHICALLY SEALED PACKETS

Micro-segmentation 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 (payload) completely encrypted but also the routing information (headers) is cryptographically sealed to ensure only authorized delivery. That way users within your communities of interest can only send and receive packets for their group.

By implementing micro-segmentation at the packet level, organizations avoid the need for tinkering with applications that are often either too old to modify; too rushed to secure; or from third parties that don't allow access. The packets still flow normally through your existing routers and equipment, but each packet that flows through the extended enterprise is cryptographically sealed.

MICRO-SEGMENTATION: IDENTITY-DRIVEN MANAGEMENT

One of the key failures of trying to segment networks with firewalls and VLANs is the rules required to secure the physical topology. These old devices are built to manage flow from point A to point B, and those points must be hard coded. When an individual needs to be given access to something at point B, new rules must be created and propagated across the entire network. Often these rules number in the tens of thousands, if not hundreds of thousands. This has introduced unacceptable error rates due to missed or faulty rules and has driven the time to make simple changes from minutes to months.

Micro-segmentation can be identity driven straight from existing Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) systems already in place. A single change in the AD access can be granted or taken away. This can be achieved in minutes, not months.

One of the largest security issues is that firewall rules are almost never removed. The fear of breaking something has often overwhelmed network engineers. With identity-based rules, that fear no longer exists. When a user is removed from AD or the LDAP, their access is automatically removed with no additional work on the part of the network engineers. This is known as mandatory access controls.

MICRO-SEGMENTATION: LEVERAGE THE CLOUDS

Clouds are cost-effective, agile, and here to stay. Yesterday's security schemes were holding back migration to public and private clouds, but software-based micro-segmentation is topology and network hardware independent, so enterprises can have one security model that works as easily in local data centers as it does in the public cloud. Now with micro-segmentation you can extend your enterprise security model natively to the cloud while retaining control of your data in motion and the keys that secure it. This can be done while still leveraging all of the cost savings and flexibility that the cloud provides. Micro-segmentation can quickly and easily be implemented within virtual machines (VMs) to defend against side-channel attacks and other cloud-specific risks.

CYBER SUPPLY CHAIN SECURITY

One of the biggest holes in the cyber system is in the area of supply chain security, especially hardware and key infrastructure components. In the past, the "edge" of a network was well defined and well protected, however, today the boundaries of where a network ends are often not well defined. The lines of responsibilities are often blurred across unclear boundaries. This is exactly why a successful micro-segmentation solution must present itself to be easily deployable across disparate networks and different hardware and operating systems while maintaining security from endpoint to endpoint.

MICRO-SEGMENTATION AND THE MOBILE WORKFORCE

Government agencies are moving quickly to enable mobile strategies for improved service to citizens. From enabling access to criminal justice information, any time; anywhere; and from any device, to providing access to health and human services information, government agencies understand the importance of what mobility can do for their missions, citizens, and employees.

Micro-segmentation, with its topology independent model, enables the same security system to work at the office, in the field, or from home. With micro-segmentation, an additional level of security can be deployed. Additional access rules can be deployed based on location. If an employee is inside the "building" they can be granted higher levels of access than when they are in the field and they may only be granted access to lower levels of "released" information.

MICRO-SEGMENTATION: PROTECTING YOUR LEGACY SYSTEMS

Regardless of where a government enterprise is in its modernization journey, the reality is that today most agencies are running and dependent upon both legacy and modernized systems. But security doesn't need to be compromised because micro-segmentation enables legacy operating systems, such as XP and Windows 2003, to be isolated.

The technology of today and tomorrow is already demanding a new wave of security. Government organizations are under constant attack. When it is implemented properly and deployed in an identity-based model, micro-segmentation protects the entire government enterprise ecosystem.

Today's government organizations can achieve powerful benefits through micro-segmentation including:

- Lower operating costs
- More secure data centers
- Rapidly improved security of high-risk environments
- Stop the Advanced Persistent Threat (APT) in its tracks—threat kill chain
- Compliance with government policies

THE UNISYS SERIES ON DIGITAL GOVERNMENT

Becoming a digital government organization

The transition to digital government is not an all-or-nothing proposition. Agencies will continue to optimize and leverage their legacy environments while they identify opportunities to implement new hosting models; strengthen data collection, integration, and analytics; and expand their digital capabilities throughout the enterprise. The hallmark of a digital organization is its ability to leverage free flowing information through an interconnected world.

The next step for government agencies is to build on their experimentation and initial deployments to create a digital government roadmap. The lessons learned from earlier programs will help agency leaders establish priorities and identify the benefits they want to achieve. This planning will also help them create the governance mechanisms to manage their digital programs and keep them moving forward.

Digital government organizations will enjoy many benefits. Agencies will realize cost savings and operational efficiencies to help them meet expanding mission requirements even as budgets tighten. And the ability to collect and analyze the enormous amounts of data will generate insights for improving the mission capabilities of warfighters, civilian employees and government systems. Overall, digital government will empower employees to bring forward the most advanced and innovative solutions for spending taxpayer dollars wisely, serving citizens, and performing governments' many missions.

For more information on Digital Government visit: www.unisys.com/digital-government

ABOUT UNISYS

Unisys is a global information technology company that specializes in providing industry-focused solutions integrated with leading-edge security protocols to clients in the government, financial services and commercial markets. Unisys offerings include security solutions, advanced data analytics, cloud and infrastructure services, application services and application and server software. For more information, visit: www.unisys.com