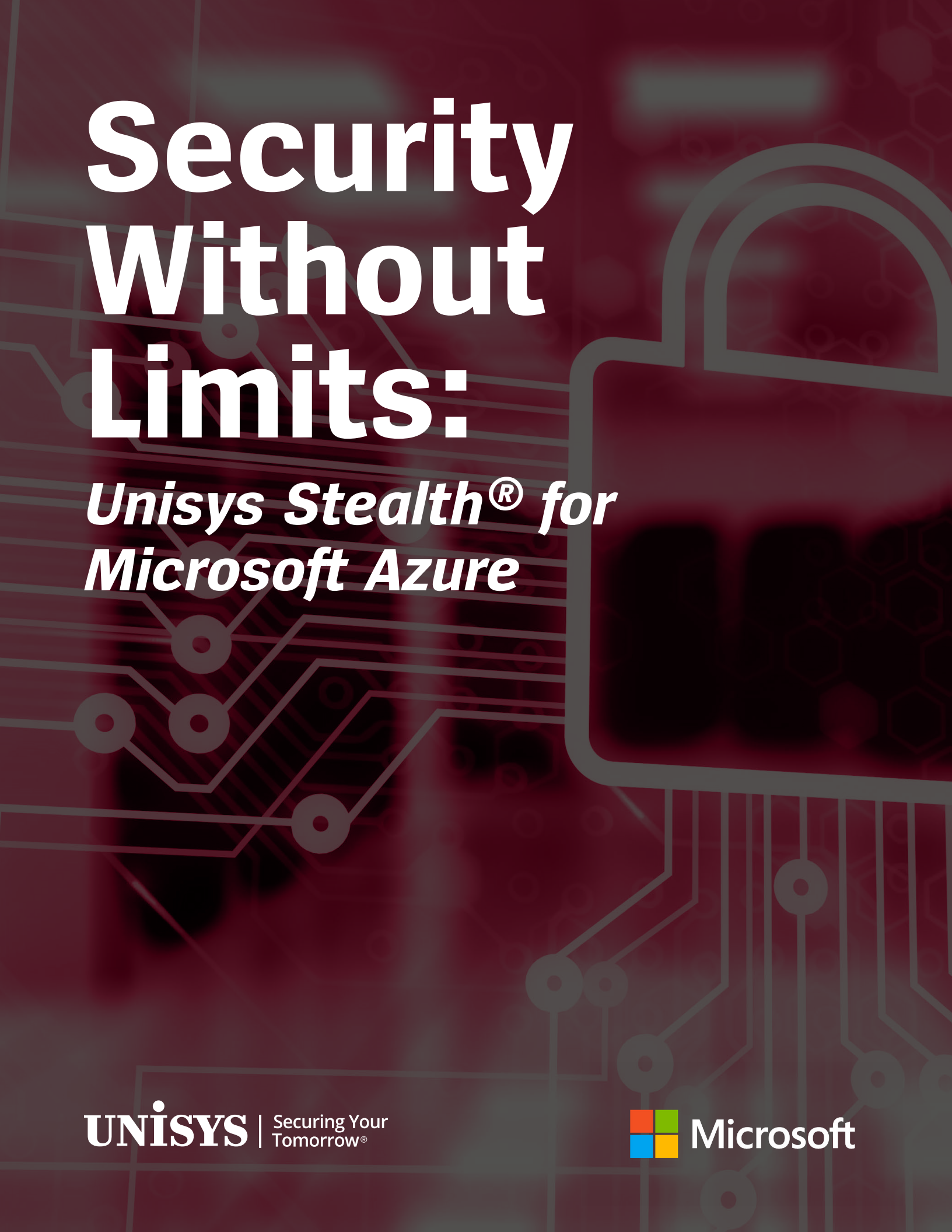
Security Without Limits:

Unisys Stealth® for Microsoft Azure



UNISYS | Securing Your Tomorrow®

Microsoft

Introduction

As federal agencies scale their digital capabilities with cloud, mobile and Internet of Things (IoT) to improve customer experiences and operational efficiencies, security perimeters become more difficult to define and defend. Traditional security controls are insufficient to protect from cyberattacks in the digital age, compelling the government to work to adopt what's called a zero trust network. The principles are simple: Trust no user, workload or device inside or outside the private network and grant as little access as possible upon reliable authentication.

As agencies shift from data centers to the cloud, efficiency, security and compliance are the keys to success.

Unisys Stealth® is a Zero Trust software suite that uses identity-based micro-segmentation to transform your existing network — both on-premises and in the cloud — into a zero trust network. Stealth overlay technology requires no changes to your existing software and can even simplify your design, as it eliminates the need for multiple subnets.

The suite is trusted by both government and commercial organizations. Stealth's achievements include the National Security Agency's (NSA) National Information Assurance Partner (NIAP) certification. It is also approved for use by the Department of Defense (DoD) Information Security Risk Management Committee (ISRMC), the Defense Security/Cybersecurity Authorization Working Group (DSAWG), Cross Domain Technical Advisory Board (CDTAB) and the NSA as the approved Cross-Domain Separation Solution for Cross Domain Access.

Now, Unisys has integrated Unisys Stealth with Microsoft Azure, giving agencies unparalleled security, greater controls and lower costs with increased operational efficiency when working with Azure.

Expanding on Microsoft's security built into Azure, Stealth layers on additional protection to data and applications on the Azure cloud platform using encryption and identity-driven micro-segmentation techniques. This provides a new approach to security that allows enterprises to quickly and easily divide physical networks into thousands of logical micro-segments without needing to fragment the network (subnet) or Re-IP address systems. Even if adversaries infiltrate into one micro-segment, they would not be able to move to other parts of the enterprise environment. They would simply not "see" any other workloads.

In addition, enterprises that want to dynamically extend their on-premises infrastructure to Azure can easily use the extended data center capability of Stealth, which automates the shifting of secure workloads from their data centers directly into Azure, saving time and money.

Stealth allows agencies to seamlessly expand protection from their data centers to the Azure cloud platform on demand, providing end-to-end data encryption from a workstation, server or virtual machine in the data center to a virtual machine in Azure.

By providing these security features for Azure, Stealth removes roadblocks for agencies looking to cloud as a way of remaining mission-driven, secure and efficient in today's digital environment.

Stealth Approved With NSA NIAP Certification

Unisys Stealth has achieved a Authority to Operate (ATO) from Defense Information Systems Agency (DISA) and U.S. Air Force to secure Secret and above workloads for Coalition Partner Information Sharing. Unisys Stealth was concurrently certified by the National Information Assurance Partnership (NIAP) for use by governments in more than 20 countries to protect their most sensitive systems and information. NIAP certification, established by the NSA and the U.S. National Institute of Standards and Technology, is recognized by governments in countries such as Australia, Canada, Germany, India, Malaysia, New Zealand and the United Kingdom.

Unisys' Stealth Platform Delivers Award-Winning Micro-Segmentation Security on Microsoft Azure

Unisys has collaborated with Microsoft in integrating Stealth into Azure cloud and Azure Stack to provide high security across Microsoft public, private and hybrid clouds based on Unisys' industry-leading micro-segmentation and dynamic isolation technology.

Stealth for Azure is part of the Unisys Stealth software-defined security portfolio that delivers a consistent security methodology across a range of deployment environments.

Unisys Stealth for Azure eliminates risks of cyberattacks, enables extremely rapid dynamic isolation of cloud workloads at signs of suspicious activities and mitigates the risks associated with hosting legacy workloads in the cloud.

As a leading Zero Trust micro-segmentation solution, the platform defends against east-west attacks within Azure. It also protects against internal and external threats by cloaking instances and encrypting communication between instances in your virtual private cloud. Stealth-protected instances are invisible to hackers and unauthorized users – it simply ignores pings and probes from non-authorized users. A Stealth-protected instance can only communicate with other instances with which it shares a role. With Stealth, you can micro-segment your Azure environment, establishing access control on a need-to-know basis.

Stealth for Azure Features

Simplified Network Architecture: Stealth's software-defined boundary removes the need for multiple subnets, routers, switches and firewalls, therefore reducing network architecture complexity. With Stealth, you can quickly define communities of interest with users and systems through identity-driven group policies.

Unified Security Architecture: Unisys Stealth for Azure enables you to confidently extend your data center grade security to Azure. It secures applications that span public cloud and on-premises environments. Stealth begins with a deployment in your data center and extends that secure environment into an Azure Virtual Network. This allows you to launch Azure Virtual Machines on demand in Azure, and provision them with Stealth protection – all from your data center.

Protecting Legacy Devices: Stealth allows users to integrate on-premises resources into the rest of the hybrid infrastructure in a secure manner, effectively creating this protective bubble around legacy devices.

Dynamic Isolation: Stealth empowers clients to swiftly respond to threats. It provides clients with the ability to quickly and proactively isolate users and devices, by working in tandem with LogRhythm SIEM systems to automate breach detection and response, which shortens response time.

Cyber Recovery: Stealth protects your organization from sophisticated attacks focused on destroying data or holding it hostage. Stealth adds an additional level of protection, increases deployment flexibility and lowers your risk profile.

Outcomes

ATO Acceleration: Stealth overlays a zero trust security boundary on existing infrastructure, accelerating lengthy and cumbersome authority to operate (ATO) process.

Enhances Security Posture: Stealth provides enhanced security protection of any cloud workloads for agencies.

Rapid Threat Response: Stealth enables faster responses and more effective security event handling. Stealth rapidly isolates suspicious workloads and provides effective protection to any security threats.

Stay Flexible and Efficient

You can deploy Stealth incrementally and scale it efficiently using rich application programming interface (APIs) and advanced automation. Stealth provides API and robust scripting support for unattended automated installation. It is also easy to use and manage, reducing the complexity, expense and operations associated with firewall, VLAN and VPN static security controls.

Stealth Software Suite Offerings:

Stealth(aware)™ enables total network visibility through live discovery, simplified network maps, intelligent classification, intuitive security policy creation and on-the-fly policy updates.

Stealth(core)™ reduces the attack surface with identity-based micro-segmentation, encryption of data in motion and cloaking to protect network assets without network or application changes.

Stealth(cloud)™ extends Stealth security to private, public and hybrid cloud environments.

Stealth(mobile)™ protects data center assets from threats introduced by mobile devices while providing mobile users appropriate access to Stealth-secured data center.

Stealth(identity)™ prevents fraud with biometric enrollment, identity verification and risk-based, multifactor authentication.

Stealth Services™ help you get the most out of your Stealth deployment, from proof of concept to expert security management, with a full range of installation, integration and managed services.

Why Unisys Stealth?

The Unisys Stealth family of products is just one component of our portfolio of solutions that is trusted by government clients around the world to deliver advanced security countering advanced threats. We have extensive subject knowledge and global delivery experience in providing fast, well-managed and cost-effective services for Stealth to our clients.

It's time to try a fresh approach to your cloud security, from a provider that's already solved many of the problems you face today. To get more information or to schedule a discussion and demonstration, please contact your Unisys sales executive or visit www.unisys.com/stealth.

UNISYS | Securing Your Tomorrow®