UNISYS | Securing Your Tomorrow®

Microsoft

Unisys Stealth® and Security in Microsoft Azure Cloud

KEY FEATURES AND BENEFITS

- ***Simplified Network Architecture***
  Stealth's software-defined approach removes the need for multiple subnets, routers, switches and firewalls, reducing network complexity.
- ***Unified Security Architecture***
  Stealth secures applications with one set of security polices that spans both public cloud and on-premises environments.
- ***Dynamic Isolation***
  Stealth dynamically isolates suspicious users and endpoints, restricting their access in the network and limiting the proliferation of threats in your environment.

Make the Move to Unisys Stealth for Azure

Unisys Stealth is a Zero Trust software suite that uses identity-based microsegmentation to transform your existing network into a Zero Trust network—whether on-premises or in the cloud. Unisys has integrated Unisys Stealth for Azure, giving enterprises unparalleled security, greater controls and lower costs with increased operating efficiency when working in Azure.

Unisys Stealth expands on the security that Microsoft built into Azure, adding protection to data and applications on the Azure cloud platform. This is accomplished using encryption and identity-driven microsegmentation to divide physical networks into small logical microsegments. This assures that, even if one microsegment becomes accessible to a hacker or other adversary, they are not able to move to other parts of the enterprise environment.

Stealth(cloud)™ Extended Datacenter (XDC) for Azure secures your hybrid applications that straddle Azure and on-premises environments. Stealth COI membership in the is defined using your existing identity management system (Active Directory or LDAP) providing a secure environment that is consistent irrespective of where a workload is deployed—in the data center or in the Azure cloud.

With Stealth(cloud) XDC, enterprises can "expand on demand" to extend their Stealth protection from their data centers to Azure cloud. End-to-end data encryption can be provided from a workstation, server or virtual machine in the data center to a virtual machine in Azure.

Stealth helps enterprises remain mission-driven by making sure they are operating securely and efficiently in today's digital world.

Eliminate the Risks of Cyberattacks in Azure

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.

Stealth for Azure helps enterprises act fast to contain threats by enabling extremely rapid dynamic isolation of users or devices at any sign of suspicious activities.

As a leading Zero Trust microsegmentation solution, Stealth defends against east–west attacks within Azure as well as internal and external threats by cloaking instances and encrypting communication between instances in your virtual private cloud. Stealth-protected instances can only communicate with other instances with which they share a role. They ignore pings and probes from hackers and other unauthorized users. With Stealth, you can microsegment your Azure environment and establish access control on a need-to-know basis.

By collaborating with Microsoft, Unisys integrates Stealth into Azure cloud and Azure Stack to provide high security across Microsoft public, private and hybrid clouds based on Unisys' industry-leading microsegmentation and dynamic isolation technology.

Stealth Leverages Microsoft Azure Service Tag Discovery API

Unisys Stealth security software suite leverages the Azure Service Tag Discovery application program interface (API) to provide additional security for clients accessing cloud-based Azure services. Stealth integrates with the API to automatically update security configuration rules and enable uninterrupted access to Azure services.

The Service Tag Discovery API provides a critical capability for enterprises that require secure uninterrupted access to Azure services. It lets clients accelerate the migration of sensitive workloads into Azure, protecting the most sensitive and critical government and commercial data via hypersecure tunnels, while enabling client adoption of Zero Trust architecture models.

How Stealth(cloud) XDC Works

Stealth(cloud) XDC for Azure starts with a Stealth deployment in your data center. Stealth uses encryption to cloak both servers and virtual machines from unauthorized users and protect communication between Stealth-enabled endpoints.

A Stealth-protected endpoint communicates only with pre-authorized groups of users and devices from pre-defined Communities of Interest (COIs). Stealth COI members share encryption keys, enabling them to communicate among each other, while remaining inaccessible to non-COI members. COI membership is based on user identity, and COIs are defined by mapping groups in the enterprise identity system (Active Directory or LDAP).

Stealth(cloud) XDC for Azure expands that Stealth deployment in the data center to the Azure cloud, which can help your enterprise meet compliance standards such as PCI DSS, HIPAA and SOX, in addition to reducing the cyberattack surface area of application environments running within your data center and virtual network.

Visit us at www.unisys.com/offerings/security-solutions/unisys-stealth-products-and-services

Printed in the United States of America