STEALTH™

Unisys Stealth(cloud) Extended Data Center for Multiple Public Clouds

Security Questions and Unisys Answers

Want to securely leverage the agility and efficiency of public clouds?

Unisys Stealth® employs cryptographic micro-segmentation to protect your workloads in the data center and the cloud against unauthorized access. With Stealth, you can seamlessly use the same security policies across both on-premise and multiple cloud infrastructures.

Want to reduce the attack surface while extending on-premise applications and DevOps environments to the public cloud?

Stealth cloaks endpoints – both on-premise and in the cloud – from unauthorized users and systems. A Stealth-enabled workload can communicate only with other workloads with which it shares pre-authorized Communities of Interest (COIs). This means you can securely scale your applications to the cloud with the same role-based access control policies used on-premise. Lateral movement is restricted to within the COI only, resulting in a reduced surface area for attacks.

Want to deploy a uniform security posture across your on-premise and cloud workloads without increasing complexity?

Stealth offers centralized management with access control policies based on identity rather than IP addresses and protocols. Stealth COI membership is defined using your existing identity management system (Active Directory or LDAP), ensuring that security is provisioned identically irrespective of whether a workload is deployed in the data center or in a public cloud. This reduces complexity of management while ensuring scalability. Stealth(cloud) XDCm delivers a unified experience while securing your workloads across on-premise, AWS cloud and Azure cloud environments.

Security Without Limits - Extending Enterprise Grade Security from your Data Center to the Cloud

Adoption of the public cloud can lower your costs, increase the elasticity of your IT infrastructure and enable you to address fluctuations in demand. However, the multi-tenant nature of public clouds can also introduce new threat vectors.

Unisys Stealth(cloud) Extended Data Center for multiple public clouds (XDCm) enables you to securely extend workloads from your on-premise environment to both AWS and Azure public clouds. It adds an additional layer of security to your AWS and Azure resources and delivers a consistent security approach – across on-premise, AWS cloud, and Azure cloud deployments– with your users having the same privileges no matter where the environment they are accessing is located.

Stealth is an award-winning micro-segmentation technology that uses encryption to cloak endpoints (servers, virtual machines or PCs) from non-authorized users and to secure communication between Stealth-enabled endpoints. A Stealth-enabled endpoint can communicate only with pre-authorized groups of users, endpoints and devices called Communities of Interest (COIs). Pings and probes from other endpoints are simply ignored. This enables micro-segmentation of the infrastructure, with access control defined on a need-to-know basis.

Stealth(cloud) XDCm enables you to securely scale capacity to meet peak demand for computing resources without increasing your physical data center capacity. With Stealth(cloud) XDCm, your on-premise endpoints can share COIs with endpoints in both the AWS and Azure clouds. Stealth encrypts data in motion end-to-end, between on-premise and cloud endpoints as well as between Stealth-protected endpoints in the cloud itself.

With Stealth(cloud) XDCm, your enterprise gains the flexibility to leverage multiple public cloud resources, with a consistent security approach across your on-premise, AWS cloud and Azure cloud deployments.

Award Winning Portfolio:

ADVANCED PRODUCTS

LOGICAL

- Stealth(core)
- Stealth(cloud)
- Stealth(mobile)
- Stealth(identity)
- Stealth(aware)
- Stealth(analytics)

PHYSICAL

- LPSS
- Identity Management
- Image Processing
- Fraud Detection

EFFICIENT MANAGED SERVICES

- SIEM
- Endpoints
- Firewalls
- Applications
- Assurance
- GRC
- Threat Analysis
- Data Loss Prevention
- Video/Image Management

EXPERIENCED PROFESSIONAL SERVICES

TECHNICAL

- Testing
- Incident Response
- Architecture

STRATEGIC

- CISO Advisory
- Security Assessments
- Security Planning
- Systems Integration

"Unlike other solutions that are based on topologies, the groundbreaking innovation of Unisys Stealth is designed on the principles of authentication and authorization, ultimately concealing the networks from prying eyes."

"Stealth effectively provides solutions for control networks, mobile devices and cloud environments by isolating, encrypting and cloaking procedures."

Frost & Sullivan 2015

Why Unisys?

The Unisys Stealth family of products is just one component of our portfolio of solutions that is trusted by government and commercial clients around the world to deliver advanced security to counter 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

Stealth(cloud) XDCm Key Features

Business Benefits

- **Address peak demand for infrastructure securely and cost-effectively:** Securely extend your applications to AWS and Azure public cloud without disrupting your existing IT infrastructure or introducing new threat vectors.
- **Build a cost effective HA/DR capability:** Replicate your on-premise infrastructure inexpensively in the public cloud and ensure that changes are synced across both environments, so that you can seamlessly failover to the cloud for disaster recovery.
- **Reduce risk of attacks:** Secure data from insider attacks by restricting lateral movement to within the COI, ensuring that attacks originating in the data center or the cloud have a minimal surface area.

Deployment Benefits:

- **Non-disruptive:** Incorporates immediately into your existing eco-system with no changes required to the underlying hardware.
- **No loss of control:** Ensures cryptographic keys remain in your control and are never transmitted in the clear.

"To ensure data security, it is encrypted while moving between networks, making the connection invisible as well as the cloud virtual machines that are Stealth - enabled.... While a majority of end users rely on channel partners and cloud service providers to protect their systems, Unisys strengthens existing security in the cloud and also provides its end users with the opportunity to be in control of their security systems."

Frost & Sullivan 2015

Unisys Award Winning Solutions for:

- Cloud Security
- Enterprise Security
- Endpoint Protection
- IoT Security
- ICS/SCADA Security
- Data Center Consolidation
- Regulatory Compliance
- Micro Segmentation
- Access Control
- Identity Management
- Video/Image Security

STEALTH™

© 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.

Printed in the United States of America 12/16 16-0563