UNISYS

# Stealth(cloud) Extended Data Center for AWS

## Security Questions and Unisys Answers

**Want to securely leverage the agility and efficiency of the public cloud?** Unisys Stealth(cloud)™ Extended Data Center (XDC) for AWS enables secure provisioning of cloud resources, so you can scale your infrastructure quickly without incurring capital expenditure. Stealth(cloud) leverages cryptography to seamlessly protect datacenter workloads and AWS EC2 instances against unauthorized access from within and outside your datacenter and AWS Virtual Private Cloud (VPC).

**Want to extend on-premise applications to the AWS cloud?** A Stealth-enabled instance can communicate only with a pre-authorized Community of Interest. Stealth cloaks endpoints – both on-premise and in the cloud – from users and systems without explicit business requirement for access. Lateral movement is restricted to within the COI only, resulting in a reduced surface area for attacks. So you can securely scale your applications to the cloud with the same role-based access control policies used on-premise.

**Want a uniform security solution to protect your workloads across the enterprise and public cloud environment?** Stealth(cloud) XDC 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 datacenter or in AWS. This reduces complexity of management while ensuring scalability.

## Security With No Limits - Extending Enterprise Grade Security From Your Data Center to the Cloud

Adoption of the public cloud can result in significant cost savings as well as increased efficiency. Leveraging public cloud resources can 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 (XDC) for AWS enables you to create EC2 instances as needed in the AWS cloud and add an additional layer of security to these instances by provisioning them with Stealth. 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 and devices called Communities of Interest (COIs). Pings and probes from other users are simply ignored. This enables micro-segmentation of the infrastructure, with access control defined on a need-to-know basis.

Stealth(cloud) XDC for AWS enables you to expand your on-premise Stealth deployment to the AWS cloud, so that you can meet peak demand for computing resources without expanding your private data center. With Stealth(cloud) XDC, your on-premise endpoints can share COIs with AWS EC2 instances. This results in a consistent security approach – both on-premise and in the cloud. Data-in-motion is encrypted end-to-end, all the way from the on-premise endpoint to the destination EC2 instance in your AWS VPC, as well as between EC2 instances in the VPC.

With Stealth(cloud) XDC, your enterprise gains the ability to seamlessly expand to leverage AWS resources securely, without incurring additional complexity. The result is an agile environment delivering the flexibility and security your enterprise requires.

**Award Winning Portfolio:**

### ADVANCED PRODUCTS

*LOGICAL*

- Stealth(core)
- Stealth(cloud)
- Stealth(mobile)

*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) XDC for AWS Key Features

### Business Benefits:

- **Address peak demand for infrastructure securely and cost-effectively:** Flexibly extend your applications to the AWS cloud when required 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 AWS 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 that originate in the data center or the cloud have a minimal surface area.

### Deployment benefits:

- **Non-disruptive:** Incorporates immediately into your existing ecosystem with no code changes required to your applications.
- **No loss of control:** Ensures cryptographic keys are never transmitted in the clear and are never exposed to the cloud service provider, facilitating regulatory compliance.

"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

UNISYS

© 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 03/16 16-0140