



Security Questions and Unisys Answers

Want to move sensitive applications to the public cloud to achieve cost savings? Unisys Stealth (cloud) enables you to provide an extra layer of security to sensitive applications running in the Amazon Elastic Compute Cloud (EC2) platform, while maintaining a logical segregation of these applications.

Need to effectively address the issue of insider and external threat vectors to your applications? Stealth(cloud) can provide an additional level of protection for your EC2 instances on AWS against unauthorized access from within and outside your AWS Virtual Private Cloud (VPC) by virtue of cryptographic micro-segmentation.

Want a single mechanism for defining security policies across your infrastructure? Stealth(cloud) enables you to mirror your on-premise application infrastructure on the AWS cloud platform, with identical security policy definitions for both environments, facilitating rapid disaster recovery.

Want a cloud security solution that can provide efficiency improvements as well? Unlike competing security solutions, Stealth(cloud) access control policies are defined by roles and identity rather than IP addresses and protocols. This results in reduced complexity and cost of management, and supports your AWS deployment at scale. In addition, the use of roles rather than IP addresses significantly reduces the risk of configuration errors that can leave your applications exposed to unauthorized users.

A Comprehensive, Innovative Approach to Cloud Security

Agility, efficiency, and reductions in capital expenditure are the primary drivers for the adoption of public clouds such as the Amazon Web Services (AWS) platform. Enterprises want to do everything possible to prevent unauthorized access to their sensitive data and applications on public clouds – be it from external sources or even from malicious insiders within the enterprise itself.

Unisys Stealth(cloud) is optimized for the AWS environment, and aims to address concerns by providing additional security for your AWS EC2 instances. Stealth(cloud) uses encryption to both cloak your EC2 instances from non-authorized users and protect communication between EC2 instances in your VPC.

Stealth-enabled EC2 instances are invisible to hackers and unauthorized users – pings and probes from non-authorized users are simply ignored. Stealth(cloud) also encrypts traffic between all Stealth protected endpoints and enables you to micro-segment your AWS environment, establishing access control on a need to know basis. A Stealth-protected AWS instance can only communicate with other instances with which it shares a role. Together these Stealth capabilities bring additional security to your AWS environment and help your enterprise meet compliance standards such as PCI DSS, HIPAA and SOX.

Stealth(cloud) can be launched from the AWS Marketplace, automating the deployment of Stealth security capabilities into your AWS environment, and significantly reducing the cyber-attack surface area of application environments running within AWS.

Award Winning Portfolio:

ADVANCED PRODUCTS

LOGICAL

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

PHYSICAL

- LPSS
- Identity Management
- Image Processing
- Fraud Detection

EXPERIENCED PROFESSIONAL SERVICES

TECHNICAL

- Testing
- Incident Response
- Architecture

EFFICIENT MANAGED SERVICES

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

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?

Stealth(cloud) can also be deployed to securely extend from your data center into an AWS VPC. This deployment, known as Stealth(cloud) Extended Data Center for AWS, is designed to ensure end-to-end security of data in motion from a VM in the data center all the way to the destination instance in the AWS VPC, enabling you to dynamically extend your on-premise infrastructure to the AWS platform on demand.

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.

Stealth(cloud) for AWS Key Features

Enhances Security & Minimizes Risk by:

- Cloaking EC2 instances from detection by non-authorized users, and even from users with explicit authorization to access other instances in the same VPC.
- Encrypting traffic between EC2 instances in a VPC, and permitting communication only between EC2 instances that share a role, thus designed to prevent any attack from spreading laterally in your VPC.
- Enabling segregation of EC2 instances in your VPC by department or role, so as to achieve isolation at department or role level as per your business requirements.

Reduces Complexity and Cost by:

- Enabling definition of access control policies through roles and identities, rather than IP addresses, making them simpler to manage and reducing the risk of any unintentional configuration errors.
- Reducing the scope of regulatory compliance by strictly limiting visibility among EC2 instances in your VPC through role-based access control.
- Supporting phase-wise deployments, enabling you to prioritize the security of your most sensitive applications.

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

It's time to try a fresh approach to your cloud security, from a provider that's already solved many tough security challenges. To get more information or to schedule a discussion and demonstration, please contact your Unisys sales executive or visit: www.unisys.com/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.

STEALTH™