UNISYS

Stealth(cloud) for AWS

Overview

Unisys Stealth(cloud)™ for AWS offers an innovative approach to manage security in the AWS cloud and address both external and internal threat agents. Stealth(cloud) for AWS is part of the Unisys Stealth software-defined security portfolio that delivers a consistent security methodology across a range of deployment environments.

Stealth(cloud) delivers award-winning technology that provides an additional layer of security for your AWS EC2 instances. As a leading micro-segmentation solution, Stealth(cloud) defends against east-west attacks within your AWS Virtual Private Cloud (VPC) and isolates your EC2 instances from other users in the cloud. Stealth(cloud) also protects against internal and external threats by cloaking EC2 instances and encrypting communication between EC2 instances in your VPC. Stealth protected EC2 instances are invisible to hackers and unauthorized users – pings and probes from non-authorized users are simply ignored. A Stealth-protected AWS instance can only communicate with other instances with which it shares a role. So with Stealth(cloud), you can micro-segment your AWS environment, establishing access control on a need to know basis.

Stealth(cloud) for AWS is now available on the AWS Marketplace.

Components of Stealth(cloud) for AWS

The primary components of a Stealth(cloud) environment in AWS include the Management Server instance and Endpoint instances. These components can be launched from the AWS Marketplace. In addition, one EC2 instance in the VPC must be configured as an Administration and Diagnostics system.

Management Server

This is an AWS EC2 Windows Server instance that runs the Stealth(cloud) Enterprise Manager software, which is used to authorize Stealth endpoint instances in AWS. The Enterprise Manager also provides the user interface for managing the Stealth environment. Only one instance of the Management Server can be deployed in a VPC.

Stealth Management Server	
Operating System	Windows Server 2012 R2
Delivery Method	64-bit Amazon Machine Image (AMI) launched through an AWS Cloud Formation Template

The Management Server instance must be sized appropriately so that it can manage all of the Stealth-protected endpoint instances in your VPC. Resizing of the Management Server post-deployment is supported.

Management Server size	EC2 Instance type	No. of endpoints supported
Small	m4.large	25
Medium	m4.large	50
Large	m4.xlarge	250
Extra Large	m4.2xlarge	500

Stealth Endpoint EC2 Instances

These are AWS EC2 Windows or Linux instances that run the Stealth endpoint software. Stealth-protected EC2 instances need to be deployed in the same VPC as the Management Server. A Stealth role needs to be assigned to an EC2 endpoint instance at the time of deployment. Only EC2

instances that share a Stealth role can communicate with each other. These instances can however communicate with all available Amazon Services (for instance, Amazon S3 for storage and Route53 service for DNS).

The Stealth role associated with the EC2 instance can be modified post-deployment.

The Management Server must be deployed prior to deploying any Stealth-protected EC2 endpoint instances.

Stealth(cloud) for AWS does not currently support Stealth-enabling existing workloads in your VPC. This functionality will be made available in a future release. You must deploy new EC2 instances enabled with Stealth, and then install any desired software (for instance, web server, application server or database) on the respective Stealth endpoint instances.

Stealth Endpoint EC2 Instances	
Delivery Method	64-bit Amazon Machine Image (AMI) launched through an AWS Cloud Formation Template
Operating systems supported	Windows Server 2012 R2, Windows Server 2008 R2, Red Hat Enterprise Linux 6.6 and 7.1, SUSE Linux Enterprise Server 11, Ubuntu Linux 14.04
EC2 Instance types supported	HVM (Hardware Virtual Machine) instance types on AWS

Administration and Diagnostics System

In addition to the Management Server and endpoint instances, a single EC2 Windows instance in the VPC is used to provide administrative access to the Management Server and the endpoints. This instance, known as the Administration and Diagnostics System should be configured to access the Management Server and Windows endpoint instances over RDP, and the Linux endpoint instances over SSH.

Micro-Segmenting your AWS VPC Using Stealth(cloud) for AWS

The Stealth Enterprise Manager displays a Stealth network dashboard, which provides an overview of your configuration.

When a Stealth endpoint instance is launched, a certificate is added to the EC2 instance based on the role associated with that instance. These certificates are used to authorize endpoint instances so that they can communicate with one another.

Communication among EC2 instances that share a role is encrypted using OS-native Internet Protocol security (IPsec) with 256-bit encryption. The IPsec Internet Key Exchange (IKE) protocol is preceded by the Unisys-developed Secure Community of Interest Protocol (SCIP), which controls the IKE and IPsec parameters used to setup, rekey, and transport data through encrypted tunnels. SCIP/IPsec is completely transparent to applications running on the Stealth-enabled EC2 instance.

The use of SCIP/IPsec ensures that a Stealth-protected endpoint does not respond - even to pings or probes - from endpoints with which it does not share a role, effectively cloaking it from any communication from non-authorized endpoints. The use of roles rather than IP addresses to define access policies significantly lowers complexity and cost of managing access control among the workloads in the VPC.

These capabilities enable role-based micro-segmentation of the AWS VPC, which can be used to isolate workloads belonging to different business units on the same VPC. Stealth(cloud) can also help your enterprise meet compliance standards such as PCI DSS, HIPAA and SOX, in addition to reducing the cyber-attack surface area of application environments running within your VPC.

Stealth Security for your Datacenter

Unisys also offers Stealth(core) for cryptographic micro-segmentation of your datacenter. Your Stealth(core) deployment in the datacenter can be extended to the AWS cloud using Stealth(cloud) *Extended Datacenter (XDC)*. This enables Stealth-protected EC2 instances in your VPC and endpoints in your datacenter to share roles and communicate with each other, while remaining cloaked from other EC2 instances or systems in the datacenter with which they do not share a role. For more details, please refer to https://unisyssecurity.com/aws/

For more information visit www.unisys.com