Tenable and Amazon Web Services
Secure assets in the AWS cloud quickly and easily with Nessus Solutions

Key Challenges

Today, enterprises and government agencies are running applications in the cloud to reduce costs, scale the business, or even “go green” – and Amazon Web Services (AWS) is leading the charge. Of course, running IT systems in public and/or private clouds doesn’t mitigate everyday network security risks, and it certainly doesn’t grant IT organizations a waiver from demonstrating regulatory compliance. Actively monitoring an organization’s cloud infrastructure for vulnerabilities and security misconfigurations is just as important as doing so on premise.

Without a full-featured security and compliance management solution that leverages and protects an organization’s cloud infrastructure, AWS customers face the following challenges:

- Identifying and continually managing risk from AWS instances whose IPs can change over time
- Inability to perform scan of vulnerabilities, compliance violations, and advanced threats for AWS instances
- Annoyance of having to submit an AWS Vulnerability / Penetration Testing Request Form each time to scan AWS instances
- Complexity in deploying, managing and administering individual scanners, policies, and users in the AWS cloud

Solution Overview

Tenable provides the most flexible solutions for scanning AWS infrastructure and applications running on that infrastructure. This enables organizations to quickly identify vulnerabilities, security weaknesses, and non-compliant systems and confidently transition their infrastructure and services to the AWS cloud.

- **Nessus Enterprise for AWS**: Nessus Enterprise for AWS is pre-authorized to scan your AWS deployments. It scans AWS instances for vulnerabilities, identifies misconfigurations and audits the AWS environment for compliance, check for adherence to AWS best practices, identifies malware, and perform web application scanning in your AWS environment. Once installed as an Amazon Machine Image (AMI), the user simply configures the scan policy using AWS instance IDs (in place of IP addresses).

- **Nessus (BYOL)**: Nessus (BYOL) is installed as an Amazon Purchased on the AWS marketplace as a BYOL version, it is installed in the Amazon cloud as an AMI by the user and configured to scan systems outside of the AWS cloud by specifying the target host IP address. The scan results can be viewed directly via the Nessus scanner web interface or be transmitted back to the Tenable SecurityCenter™ management console for a complete cloud and on-premises analysis, combined with passive and log analysis.

Solution Components

- Tenable Nessus Enterprise for AWS
- Tenable Nessus (BYOL) (optional)
- Tenable Nessus vulnerability scanner (optional)
- Tenable SecurityCenter management console (optional)
- AWS console
- AWS API

Key Benefits

- Quickly roll out Nessus scanners in the AWS cloud
- Avoid the manual approval process for scanning AWS instances
- Integrated assessment of AWS instances for vulnerabilities, advanced threats, web application security, and compliance violations
- Centralize cloud and on-premises scan results for visibility and analysis across the organization
- Simplify administration of multiple Nessus scanners, users, and policies
- Maintain compliance with industry and government regulations (e.g., PCI, HIPAA, FISMA)

**UPDATE**

• **Nessus**: Nessus can audit the AWS infrastructure based on AWS Security Best Practices and AWS Identity and Access (IAM) Best Practices to provide information such as running AWS instances, network ACL’s, firewall configurations, user listings, changes based on AWS Config API, Trusted Advisor recommendations and more. The scan results can be viewed directly via the Nessus scanner web interface or be transmitted back to the Tenable SecurityCenter™ management console for a complete cloud and on-premises analysis, combined with passive and log analysis.

**How It Works**

**Nessus Enterprise for AWS:**

**Step 1.** Available on the AWS Marketplace as an AMI, Nessus Enterprise for AWS (Manager) queries AWS via special AWS APIs. Scans are configured in the management console and targets are identified by their AWS Instance ID so that scans can be performed even if the underlying IP addresses change, common in AWS environments.

**Step 2.** Nessus Enterprise for AWS (Scanner) performs the actual security and compliance scanning of the AWS instances. Unlike other solutions, Nessus Enterprise for AWS provides integrated scanning that identifies vulnerabilities, advanced threats, web application security, and compliance violations and reports the results to the Nessus Enterprise (Manager).

**Nessus (BYOL):**

**Step 1.** Nessus users can download the Nessus (BYOL) AMI from the AWS Marketplace.

**Step 2.** Once installed in the AWS cloud, users scan assets outside of the AWS cloud by configuring a scan policy and specifying IP addresses of targets outside of the AWS cloud.

**Nessus:**

**Step 1.** Purchase Nessus and install according the Installation Guide. Nessus can be purchased on the Tenable Store in a variety of form factors.

**Step 2.** Once installed in your environment, users configure a scan policy using the AWS scan wizard. As part of the configuration, you will be prompted to provide the access keys to your AWS account, which will be used to perform an audit of your AWS environment.

**Benefits of Tenable-AWS Deployment**

Tenable provide the most flexible deployment and scanning options for AWS customers. AWS users can deploy Nessus on-premises or in the AWS cloud to quickly and easily to secure their AWS environment. Tenable solutions perform auditing of the AWS environment to ensure infrastructure is hardened and correctly configured per AWS best practices and industry standards. With Nessus Enterprise for AWS, customers can scan their AWS instances to identify vulnerabilities and detect malware. Tenable’s Nessus provides peace of mind by ensuring that critical IT applications are hardened and secure whether hosted on-premise or in the AWS cloud.

**About Amazon Web Services**

Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of enterprise, government and startup customers businesses in 190 countries around the world. Amazon Web Services offer over 30 different services, including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) and Amazon Relational Database Service (Amazon RDS). AWS services are available to customers from data center locations in the U.S., Brazil, Europe, Japan, Singapore and Australia. To learn more about Amazon Web Services, please visit aws.amazon.com.

**About Tenable**

Tenable Network Security is relied upon by more than 20,000 organizations in over 100 countries, including the entire U.S. Department of Defense and many of the world’s largest companies and governments, to stay ahead of emerging vulnerabilities, threats, and compliance-related risks. Its award-winning Nessus and SecurityCenter solutions have received the highest-possible rating in Gartner’s MarketScope for Vulnerability Assessment and continue to set the standard for identifying vulnerabilities, preventing attacks, and complying with a multitude of regulatory requirements. For more information about Tenable, please visit tenable.com.

**About CDW**

CDW is a leading multi-brand technology solutions provider to business, government, education and healthcare. A FORTUNE 500 company, CDW was founded in 1984 and employs more than 7,200 coworkers. For the twelve months ending March 31, 2015, the company generated net sales of more than $12.0 billion. For more information about CDW, please visit CDW.com.