Tenable and Amazon Web Services

Comprehensive Vulnerability Management for the Cloud

The Challenge

Moving your datacenter assets to AWS represents a big change from your traditional on-premises IT environment. With AWS, you provision and pay for servers, storage, databases and application services exactly when you need them, instead of going through the time- and resource-consuming process of ordering, installing, and then maintaining assets on-premises. But it also saves you from the headaches of finding space, managing backup power and cooling systems, and countless other tasks needed with traditional on-premises IT . As a result, enterprises are rapidly using AWS and other cloud infrastructure-as-a-service (IaaS) providers to give them more flexibility to better support complex business needs.

What doesn't change – whether you're on-premises or in AWS – is security. The servers, applications, databases and services running in AWS need to be as secure as IT assets that are on-premises. AWS uses a Shared Responsibility Model; AWS is responsible for the physical security of the cloud; and, you are responsible for security of your applications and data in the cloud. Being able to scan instances, audit configurations, and continually monitor logs for vulnerabilities and threats is as critical in AWS as in other IT environments.

Gaining visibility into vulnerabilities and threats in AWS can be challenging. First, there are organizational challenges like simply finding security professionals with expertise in cloud security. Or, you might hesitate to take on the additional cost and complexity of licensing, deploying, and learning new tools for the cloud. There are technical differences as well. For example, servers can come and go in AWS at any time, meaning different techniques are needed to identify vulnerabilities and threats. And since those servers can be started by practically anyone, IT is no longer centrally managed, meaning new ways to get visibility into assets in AWS are needed.

The Solution

Tenable works with AWS in a variety of ways to help you ensure the security of what you deploy in AWS. Tenable solutions help you secure your applications and workloads by:

- Scanning AWS instances to detect vulnerabilities, malware, and compliance issues
- Auditing AWS infrastructure for adherence to AWS and security best practices
- Connecting directly to AWS for CloudTrail event monitoring

Tenable solutions provide complete visibility across your IT environments. That means you can get visibility into vulnerabilities and threats in physical, virtual and cloud environments without having to install, deploy, learn and maintain different solutions in different places.

Tenable Solutions for AWS

Nessus Professional

Nessus Professional, the world's most widely-deployed vulnerability, configuration, and compliance assessment product, can be installed in AWS to both scan AWS EC2 instances, as well as provide hardening guidance for key AWS services using the CIS Amazon Foundations Benchmark. To use Nessus Professional in AWS, purchase a license either from Tenable's e-Commerce store at store.tenable.com or an authorized reseller and use the activation code provided when provisioning Nessus from an AWS account.

Benefits

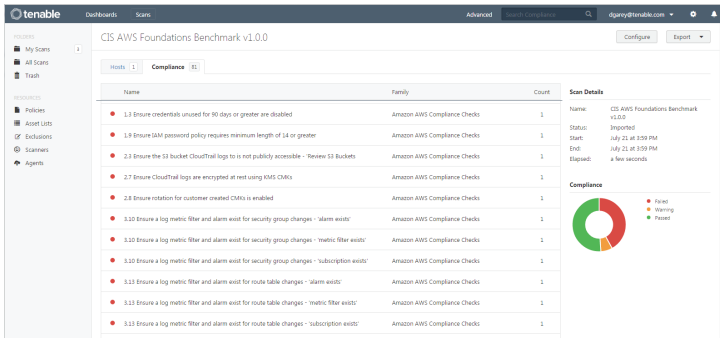
- **Centralizes** cloud and on-premises scan results for security and compliance assessment across the organization
- **Hardens** AWS configurations based on AWS and industry best practice guidance
- **Provides** flexible options for running scans in AWS, including agents that can be scripted to deploy automatically when new servers are spun up in AWS
- **Connects** to AWS to monitor CloudTrail events which offers additional visibility into user activity and monitors for outside attacks
- **Reduces** CapEx and OpEx costs by eliminating the need to buy new licenses or learn new tools

Products

- Nessus® Professional
- Nessus® Cloud with scanner and agent-based scan options
- SecurityCenter Continuous View™ (CV)

Feature / Capability	Nessus Professional	Nessus Cloud	SecurityCenter CV
Scan AWS instances to detect vulnerabilities, malware and compliance issues	x*	x*	x*
Audit AWS infrastructure for adherence to AWS and security best practices	x	x	
Use agents to scan AWS instances and audit AWS infrastructure for adherence to AWS and security best practices		x	
Connect directly to AWS for CloudTrail event monitoring			x

*Scanned by IP only



Tenable is the first security vendor to be certified by Center for Internet Security (CIS) for the Amazon AWS Foundations Benchmark, a set of industry guidelines for hardening an AWS environment.

Nessus Cloud

Nessus Cloud, the AWS cloud-hosted version of Nessus, offers all the capabilities of Nessus Professional, as well as multi-scanner and user support, pre-built integration with popular patch, mobile device and credential management systems, and the ability to perform vulnerability and configuration audit scans with a scanner or using agents. Agents support popular AWS operating systems like Ubuntu and Amazon Linux and can run a variety of scans in the AWS cloud computing platform. In addition, agents can be scripted to deploy automatically when new servers are spun up in AWS. For example, agents can be included in Chef recipes to automatically spin up agents on new AWS assets.

SecurityCenter Continuous View (SecurityCenter CV)

The SecurityCenter CV solution builds on the scan and configuration auditing data collected by Nessus, adding data from additional sensors to provide a continuous view of IT security. One data source available to SecurityCenter CV is AWS CloudTrail, the web service that records AWS API calls for an AWS account. These API calls record activity for the account, for example, which users are active, when, from where, and what actions they've taken. SecurityCenter CV connects directly to AWS to monitor CloudTrail events. SC CV customers can use this event information to identify internal users of AWS, as well as to monitor for attacks against AWS infrastructure from outside.

About Tenable

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

About Amazon Web Services

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 70 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 35 Availability Zones (AZs) across 13 geographic regions in the U.S., Australia, Brazil, China, Germany, Ireland, Japan, Korea, Singapore, and India. AWS services are trusted by more than a million active customers around the world – including the fastest growing startups, largest enterprises, and leading government agencies – to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

For More Information: Please visit tenable.com
Contact Us: Please email us at subscriptionsales@tenable.com or visit tenable.com/contact