SOLUTION OVERVIEW

# Tenable for Amazon Web Services (AWS)

## Business Challenge

AWS enables businesses to quickly build and scale new infrastructure and rapidly react to customer demands. This speed and scalability can be a double-edged sword without the right capabilities in place to detect and manage vulnerabilities and misconfigurations in an ever-changing environment. Traditional vulnerability management can't keep pace with this new paradigm, and point solutions lead to information silos without a unified view of all vulnerabilities. Security teams need to be able to find all vulnerabilities across their attack surface, but focus first on the most critical security issues that matter most – vulnerabilities that are the most likely to be exploited.

## Solution

The Tenable Cyber Exposure platform gives security teams the ability to detect cloud instances and even Docker hosts and web applications in production, giving you total visibility into your AWS environment. This platform is powered by Nessus, an AWS pre-authorized vulnerability scanner, that's trusted by over 27,000 organizations worldwide and backed by the world-class Tenable Research organization. Tenable is #1 in vulnerability coverage, #1 in accuracy, and #1 in adoption to help you confidently take advantage of everything AWS has to offer.

Tenable Lumin and Tenable.io are built inside AWS and work seamlessly to secure your AWS assets. The solution provides the most accurate visibility and insight into assets and vulnerabilities in highly dynamic environments like AWS. Tenable helps you to centrally manage and measure your cyber risk across cloud and on-prem assets to make better decisions and prioritize remediation efforts. With the Tenable Cyber Exposure platform, you can:

- Continuously detect new AWS instances as they're spun up using the AWS Cloud Connector and automatically assess them for vulnerabilities and misconfigurations.
- Deploy a combination of passive, active and agent-based scanners gain a complete picture of where you are exposed.
- Move beyond static CVSS-based vulnerability ratings with Predictive Prioritization to focus on the 3% of vulnerabilities that are most critical to your organization right now.
- Transform vulnerability data into meaningful insights to understand the cyber exposure of your AWS environment and focus remediation efforts.

## Technology Components

- Tenable Lumin
- Tenable.io
- Nessus Scanners (Pre-Authorized)
- Nessus Scanners (Bring Your Own License)

## Key Benefits

- Pay for only what you use with consumption- based pricing and flexible licenses
- Provide a unified view of all assets and vulnerabilities across cloud, on-prem, and OT environments
- Gain live visibility into cloud assets as new instances are spun up and turned off
- Focus first on the most critical vulnerabilities mostly likely to be exploited
- Tenable.io licensing counts against AWS Enterprise Discount Program annual spend commitments

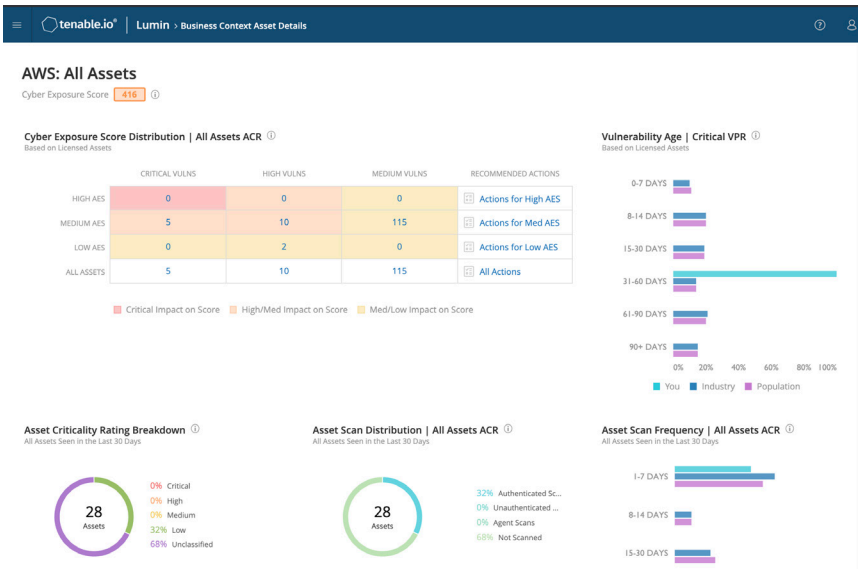
## ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at **www.tenable.com**.

## ABOUT AWS

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 165 fully featured services from data centers globally. Millions of customers —including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs.

Learn more at **https://aws.amazon.com/**




*Visualize and explore your AWS cyber exposure, track risk reduction over time, and benchmark against your peers with Tenable Lumin*

# Features

The Tenable platform provides the following industry-leading capabilities:

- Predictive prioritization to focus first on the vulnerabilities that matter most
- Robust reporting and fully customizable dashboards
- Cloud connectors to automatically detect new AWS assets without the need for key-based authentication
- Nessus agents support popular AWS operating systems, such as Ubuntu and Amazon Linux, and deploy automatically as part of your Chef recipes and other deployment scripts
- Support for AWS and CIS Benchmark configuration audits
- Active, passive, and agent based sensors with 130,000+ detection plugins for flexibility and complete scan coverage
- Integration with AWS Security Hub for a comprehensive view of security alerts
- Integration with AWS Elastic Container Registry (ECR) to assess container images for vulnerabilities and malware

# More Information

You can get the latest app here: **www.tenable.com/downloads/integrations**

Compatibility, Installation and configuration documentation:
**https://docs.tenable.com/integrations/AWS/Content/TenableioAWS/Welcome.htm**

For support please contact: **support@tenable.com**