Automated Windows and Linux Patching

Consistent and rapid patch management with AWS Systems Manager

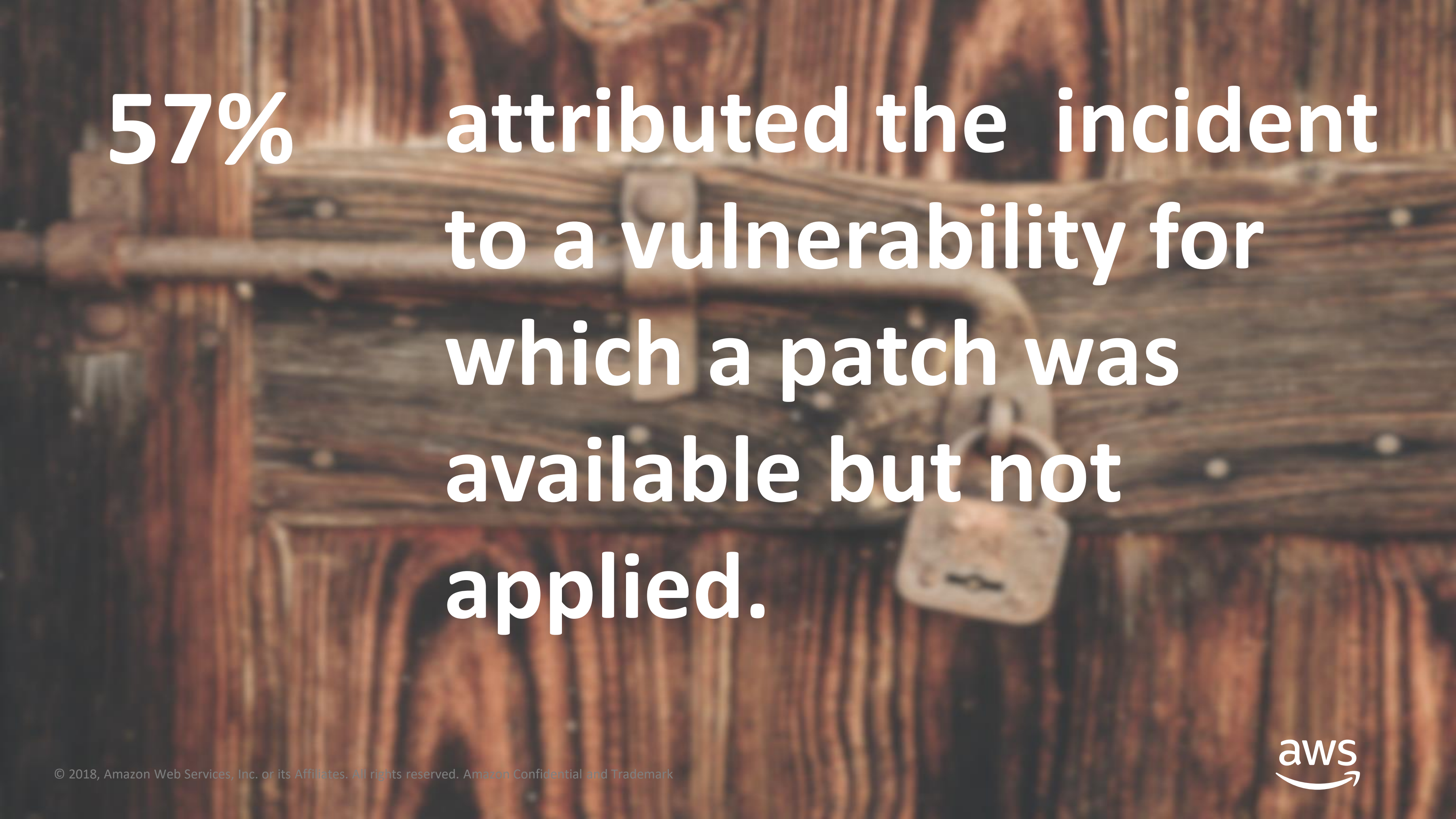
Eric Westfall, Solutions Architect
Sohaib Tahir, Solutions Architect

19 September 2018

What you will learn

- AWS Systems Manager principles, intrinsic capabilities, and Patch Manager concepts.
- How to use patch baselines to include rules for automatically approving patches within days of their release and provide a list of approved/rejected patches.
- How to leverage patch groups to organize instances into groups for patching based on environment, role, or other factors.
- How to install patches on a regular basis by scheduling patching to run as a Maintenance Window task and monitor compliance.

48% of respondents reported one or more data breaches in the last two years.



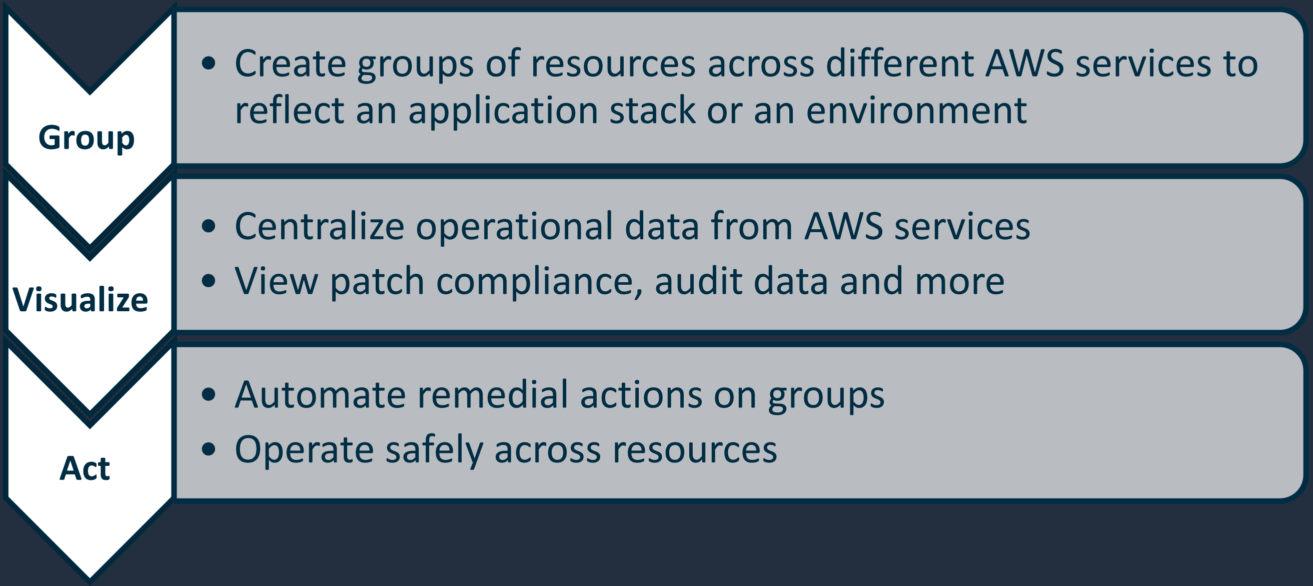
57% attributed the incident to a vulnerability for which a patch was available but not applied.

34% of breach victims knew they were vulnerable before they were breached.

AWS Systems Manager

Operational Visibility and Control Capabilities

AWS Systems Manager



Group

- Create groups of resources across different AWS services to reflect an application stack or an environment

Visualize

- Centralize operational data from AWS services
- View patch compliance, audit data and more

Act

- Automate remedial actions on groups
- Operate safely across resources

Cross-platform

Manage on AWS or on-premises

Natively works with other AWS services

AWS Systems Manager

Patch Manager Introduction

Patch Manager

- Automates the process of patching managed instances with security-related updates.
- You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type.
- Employs the intrinsic capabilities of AWS Systems Manager (Run Command, Documents, Maintenance Windows) to enable remediation of OS vulnerabilities in a safe and scalable fashion.

Patch Approval

Automate the approval of patches using patch baselines.

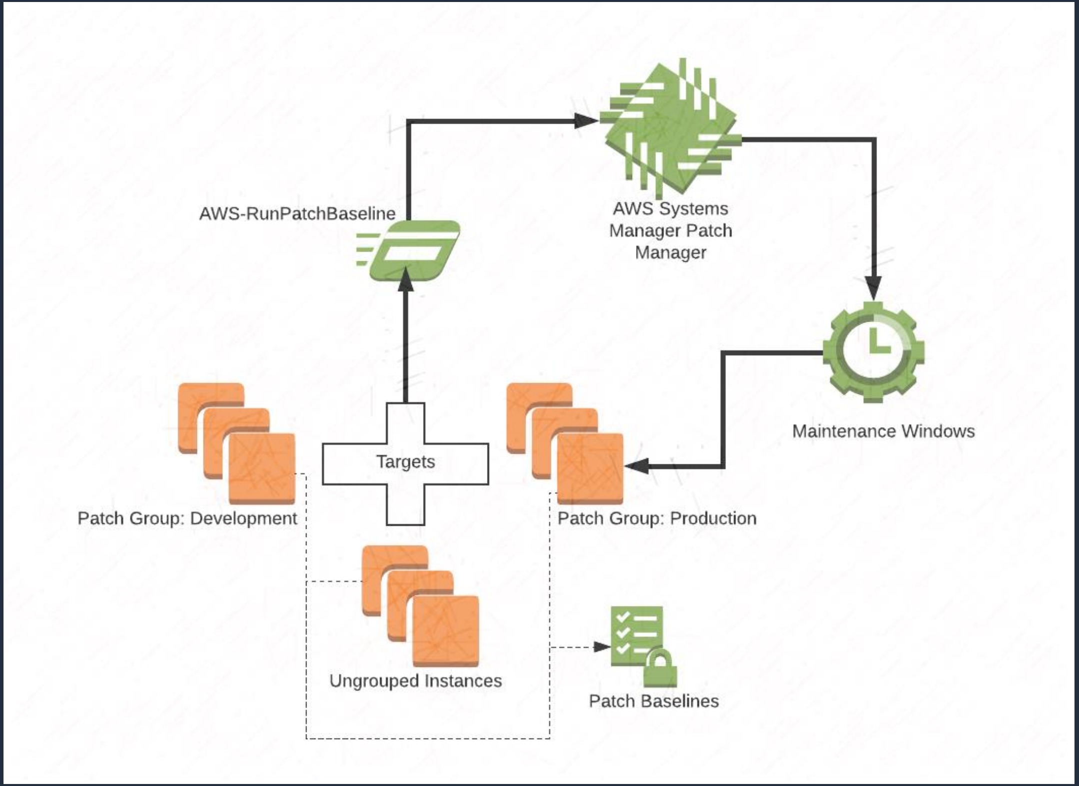
Patch Deployment

Schedule the deployment of patches using Maintenance Windows to reduce impacts on availability.

Patch Reporting

Compliance reporting for audit and remediation.

Patch Manager Workflow



AWS Systems Manager

How Patch Manager Selects Patches

Security Patch Selection

- The primary focus of Patch Manager is on installing operating system security-related updates on instances.
- By default, Patch Manager doesn’t install all available patches, but rather a smaller set of patches focused on security.
- Patch Manager uses a different process to evaluate which patches should be present on Windows managed instances versus Linux managed instances.

Security Patch Selection

Windows

- Single source repository (wsus2.cab)
- Contains only updates identified by Microsoft as being related to security
- Updates are removed as they are replaced by later updates
- Systems Manager evaluates patch baseline rules and the list of approved and rejected patches directly in the service

Linux

- Multiple pre-configured repositories on each instance
- Different package managers and source repositories treat updates differently (update notice, patch, etc.)
- Systems Manager evaluates patch baseline rules and the list of approved and rejected patches on each managed instance

✓ Alternative Patch Source Repositories

AWS Systems Manager

Understanding Patch Baselines

Patch Baseline

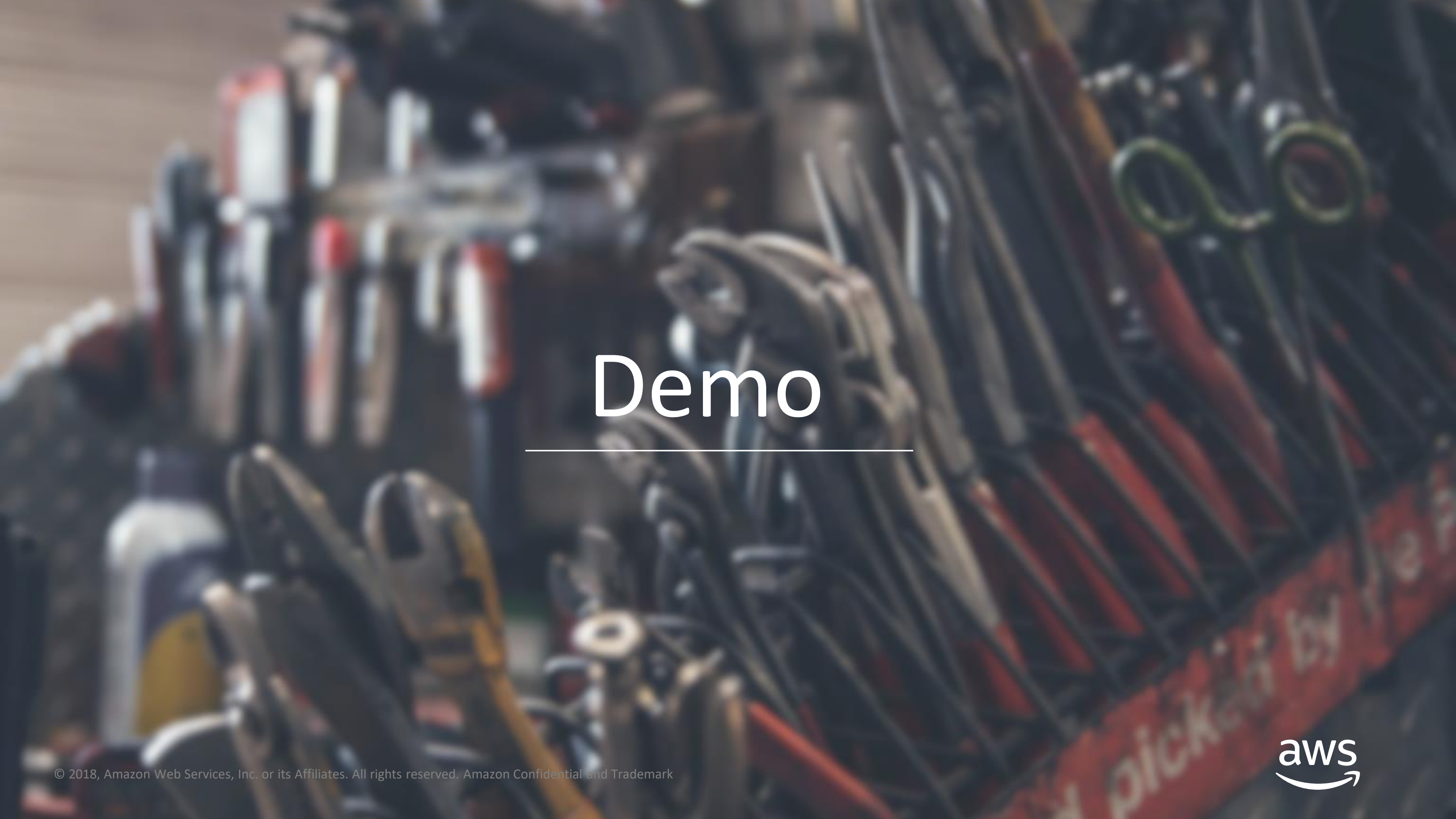
Defines which patches are approved for installation on your instances. Specify approved or rejected patches one by one or setup auto-approval rules.

Patch Baseline

A patch is installed on an instance only if it applies to software on the instance, even if the patch has otherwise been approved for the instance.

Default Baselines

Systems Manager provides pre-defined patch baselines for each of the operating systems supported by Patch Manager. Use as they are or create your own patch baselines.



Demo

AWS Systems Manager

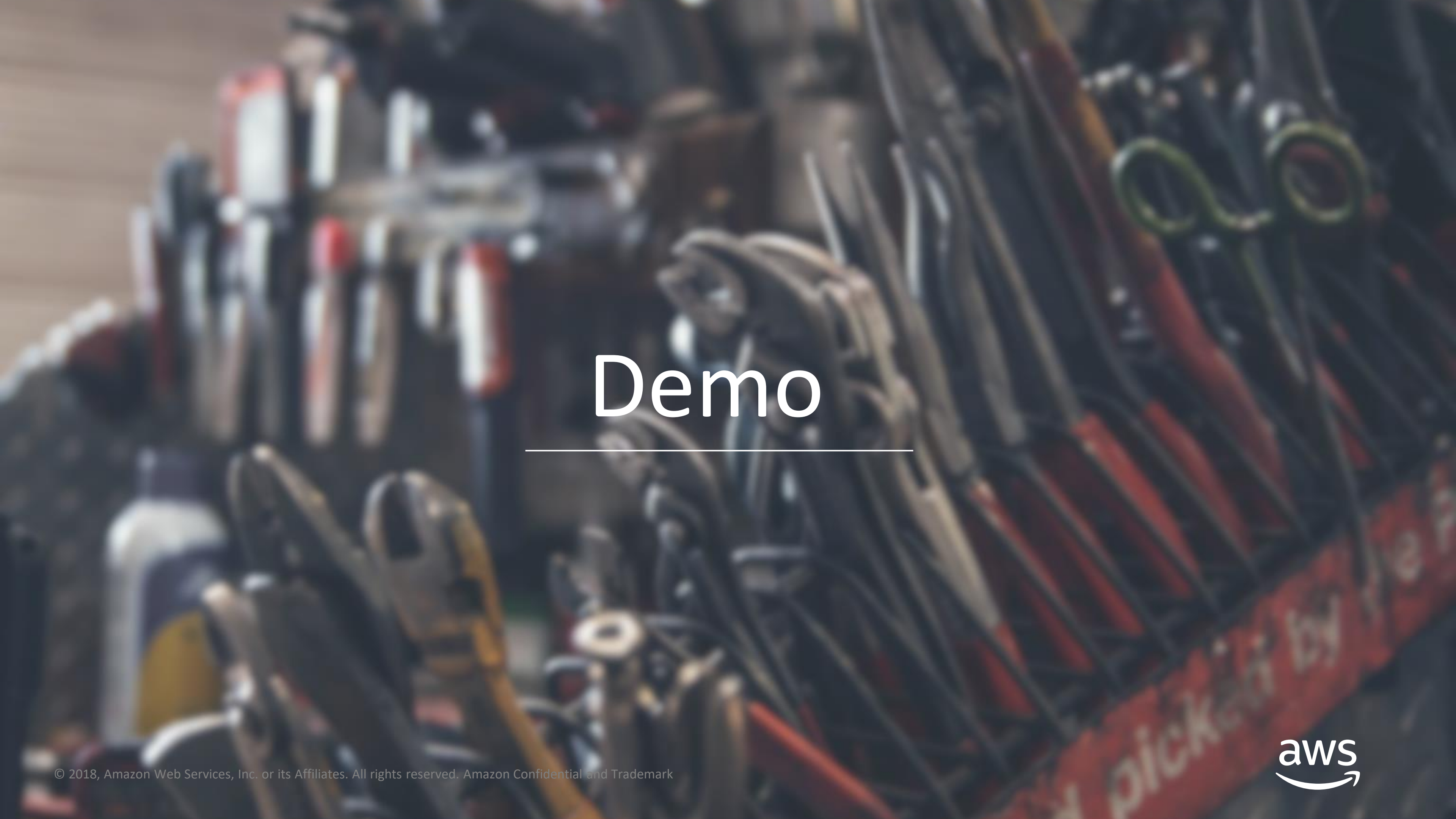
Organizing Instances into Patch Groups

Patch Groups

Provides an optional means of organizing instances into groups for patching. Patch groups can help you avoid deploying patches to the wrong set of instances and ensure adequate testing.

Patch Groups

You can register patch groups with a patch baseline. By registering the patch group with a patch baseline, you ensure that the correct patches are installed during the patching execution.



Demo

AWS Systems Manager

Schedule Patching with Maintenance Windows

Maintenance Windows

Reduce the impact on server availability by specifying a time to perform the patching process that doesn't interrupt business operations.

Maintenance Windows

Each Maintenance Window has a schedule, a duration, a set of registered targets, and a set of registered tasks.

AWS Systems Manager

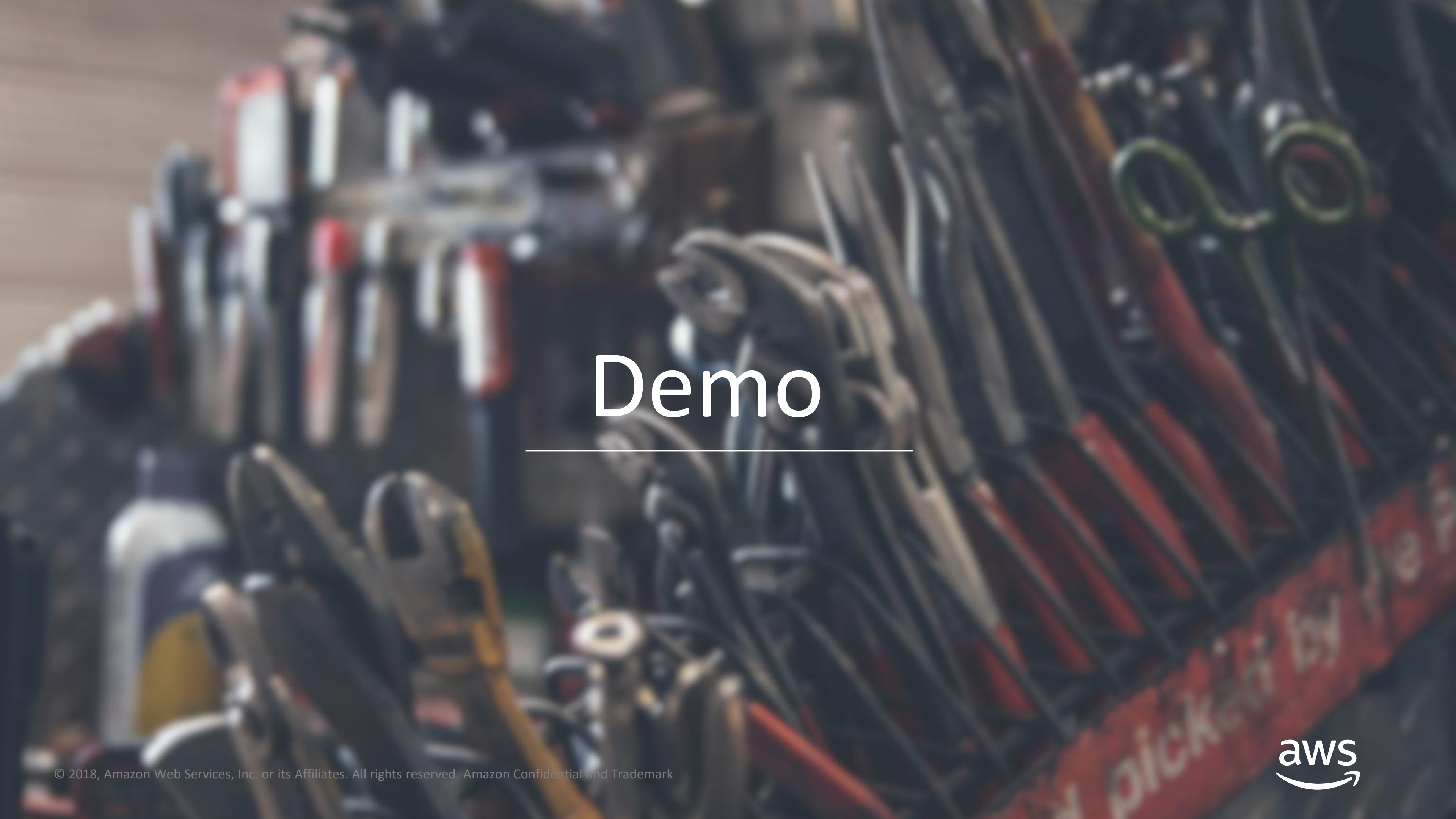
Run Command and the AWS-RunPatchBaseline Document

Run Command

Enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. Leveraged by Patch Manager for patching operations.

AWS-RunPatchBaseline

Systems Manager command document that supports executing patch operations on both Windows and Linux managed instances. The document will perform the appropriate actions for each platform.



Demo

AWS Systems Manager

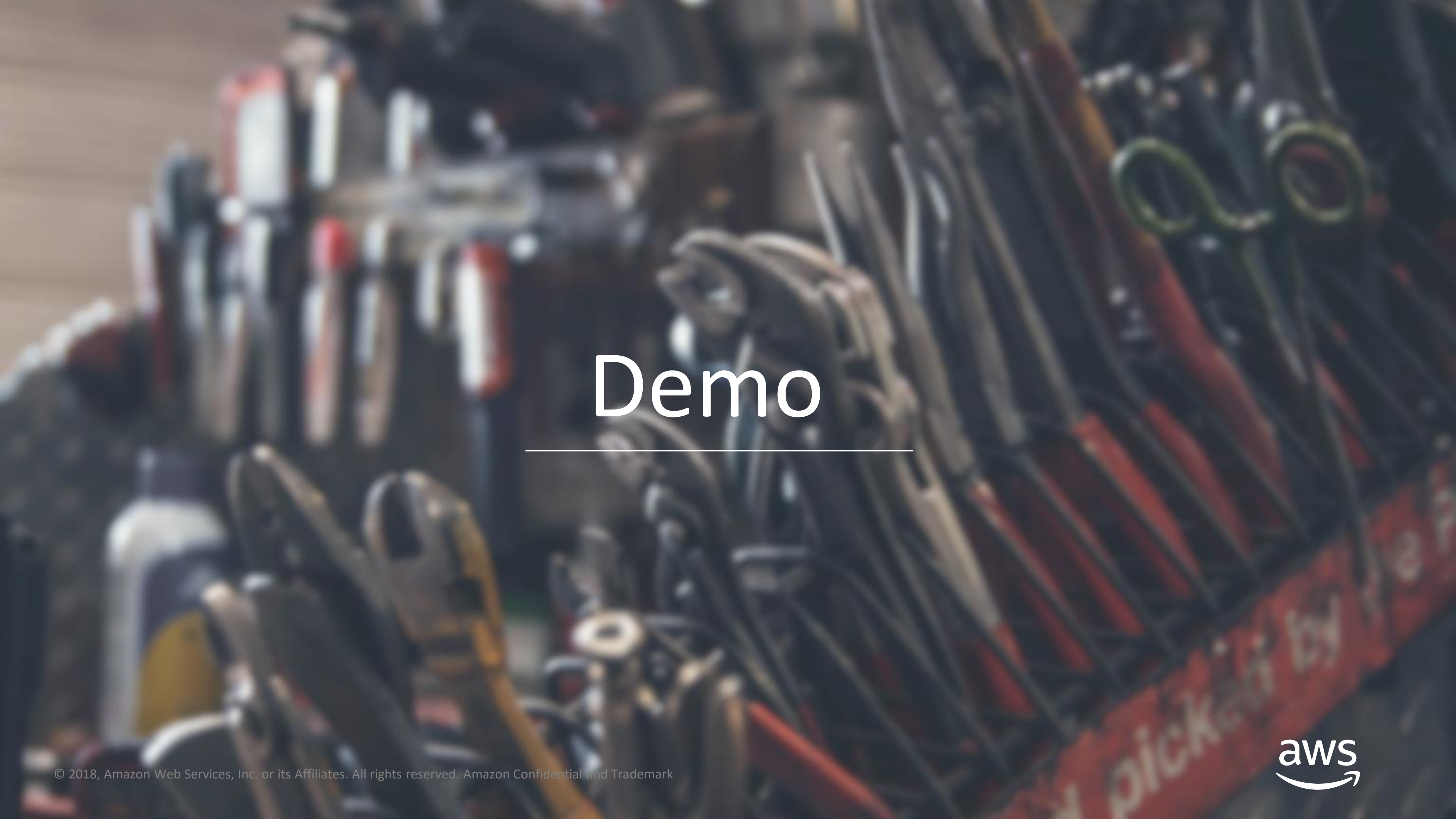
Monitoring Patch Compliance

Compliance Status

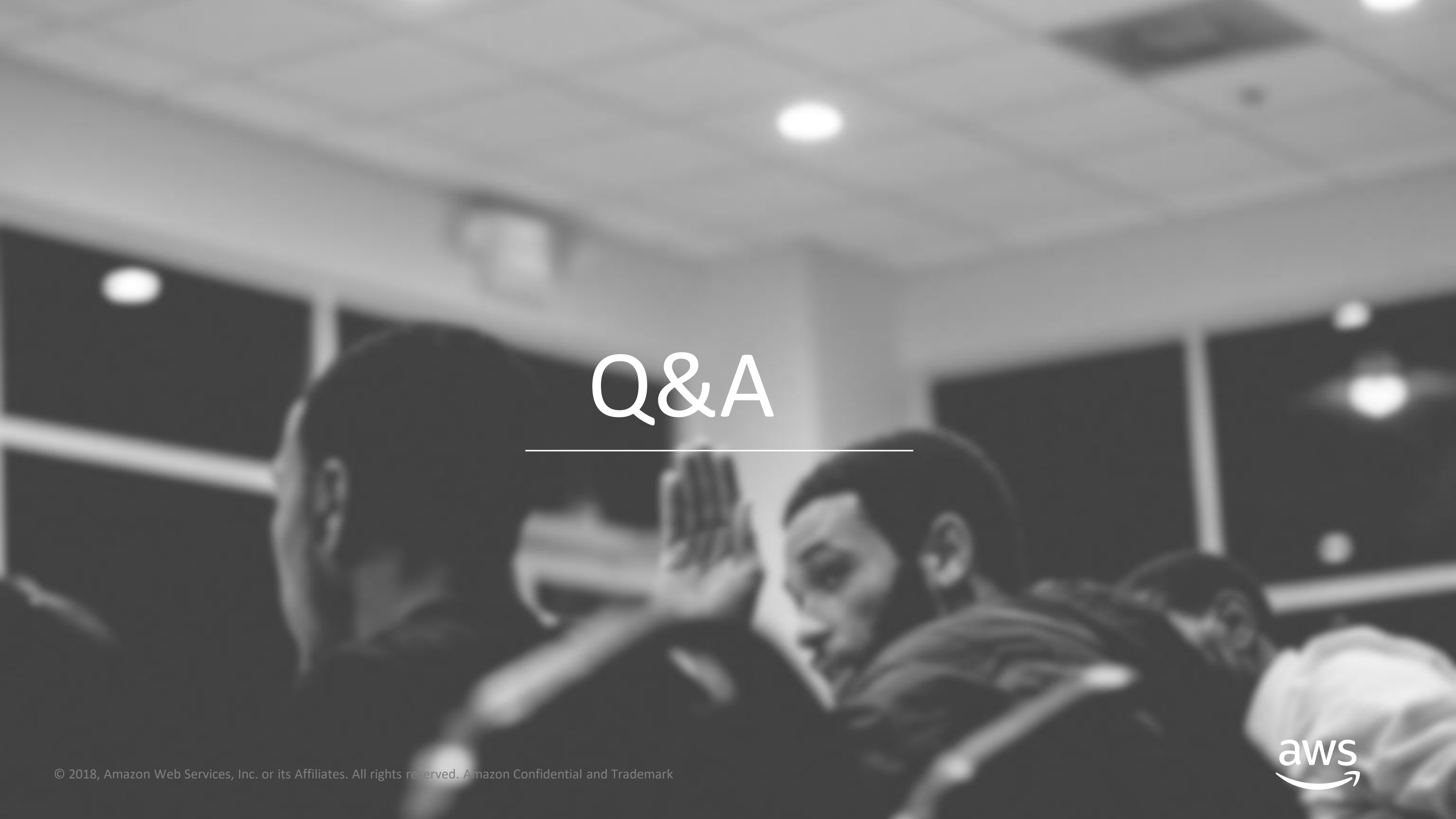
After you use Patch Manager to install patches on your instances, compliance status information is immediately available to you in the console or in the responses to a set of AWS CLI commands or corresponding Systems Manager API actions.

Compliance Status

Installed	Either the patch was already installed, or Patch Manager installed it when the document was run on the instance.
Installed_Other	The patch is not in the baseline, but it is installed on the instance. An individual might have installed it manually.
Missing	The patch is approved in the baseline, but it's not installed on the instance.
Not_Applicable	The patch is approved in the baseline, but the service or feature that uses the patch is not installed on the instance.
Failed	The patch is approved in the baseline, but it could not be installed.



Demo



Q&A

Eric Westfall
Solutions Architect
erwestfa@amazon.com

Sohaib Tahir
Solutions Architect
sohaibt@amazon.com