Microsoft Azure: Infrastructure as a Service (IaaS)

Conditions and Terms of Use

Microsoft Confidential

This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other Internet Web site references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

© 2013 Microsoft Corporation. All rights reserved.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see Use of Microsoft Copyrighted Content at

http://www.microsoft.com/about/legal/permissions/

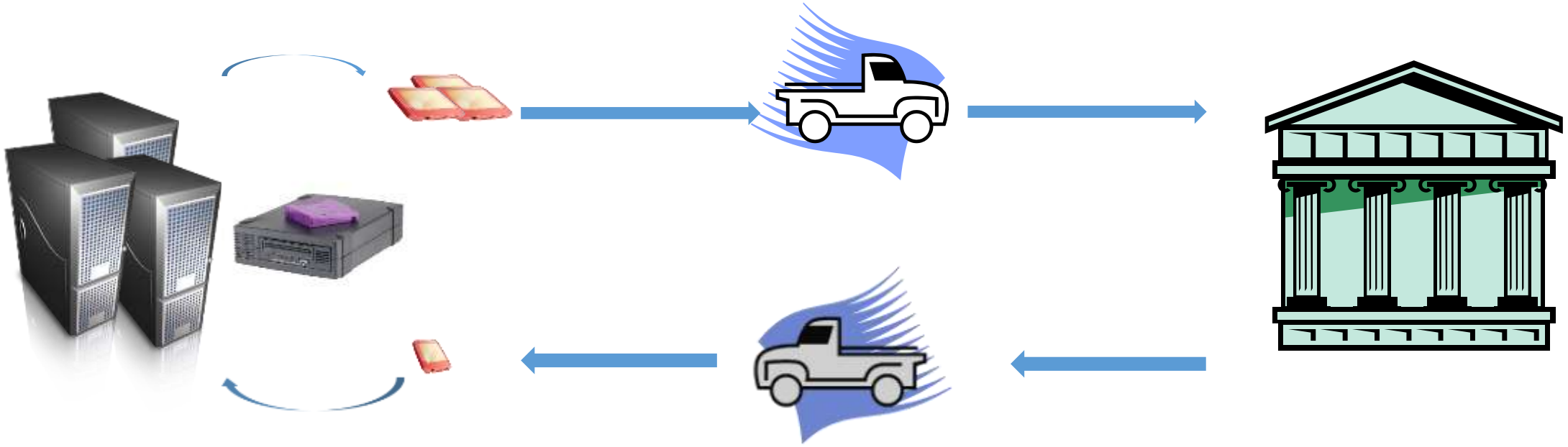
Active Directory, BitLocker, BizTalk, DirectX, Hyper-V, Internet Explorer, Microsoft, Outlook, Server logo, SharePoint, SkyDrive, SQL Server, Windows, Microsoft Azure, Windows Intune, Windows PowerShell, Windows Server, Windows Vista, Xbox 360 and Zune are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Module 7: Backup

Backup Introduction

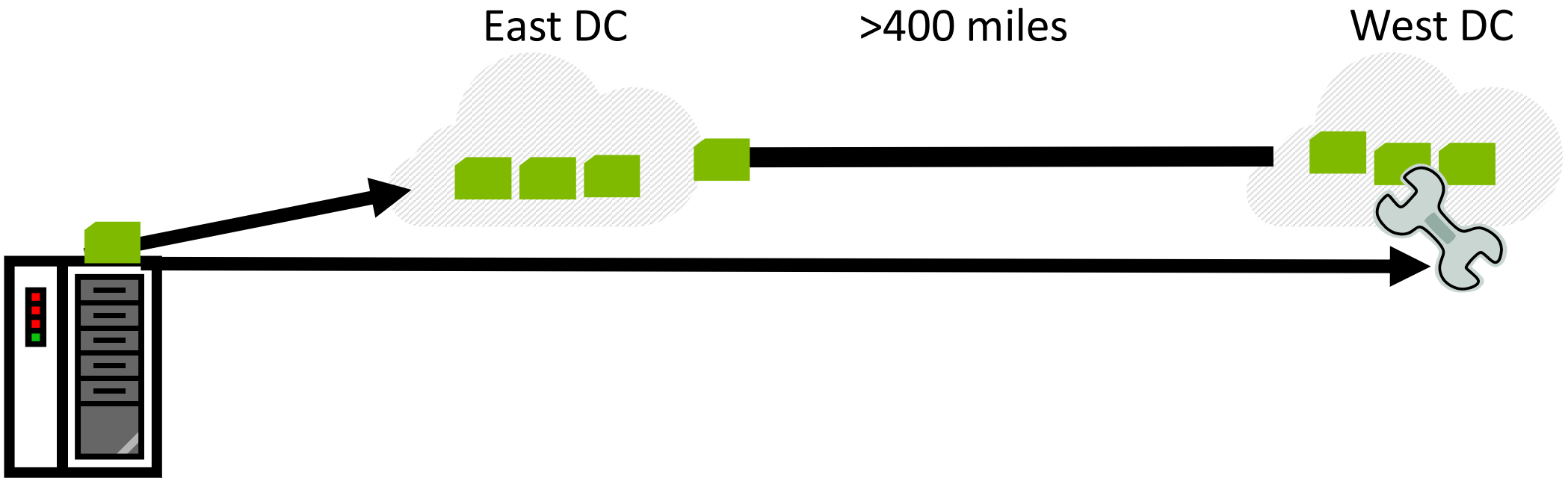
Traditional Offsite Backup

- Time consuming
- Manual data movement
- Difficult to store, index, find recall physical tapes or media

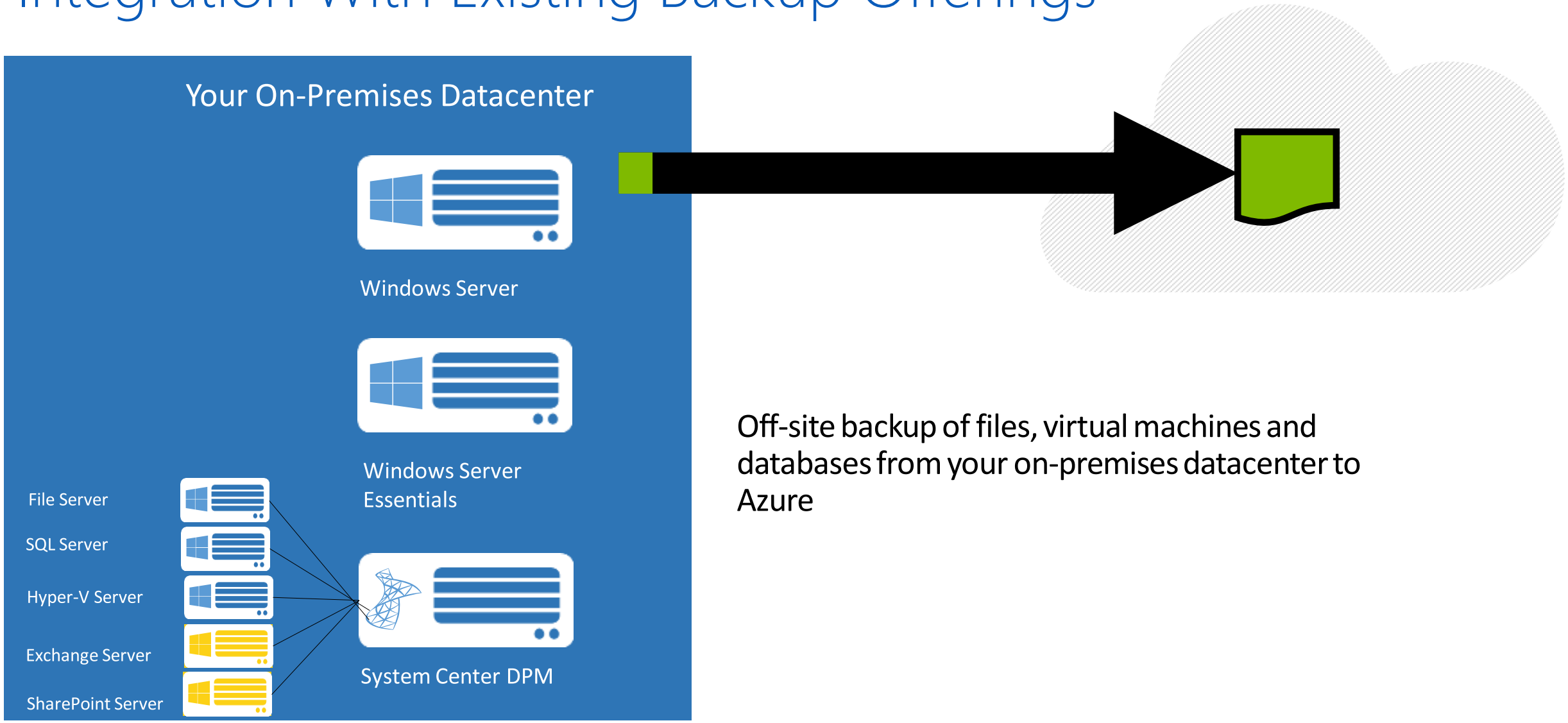


Azure Backup

- Secure: Encryption is done at the source using customer's encryption keys
- Reliable: 99.9% availability SLA, 3 copies of the data within the Azure datacenter, 3 more copies geo-replicated to a second Azure datacenter
- Efficient: Only changed data is sent, bandwidth usage controlled with throttling
- Simple: User interface integrated with Windows Server Backup, System Center Data Protection Manager, and Server Essentials Dashboard



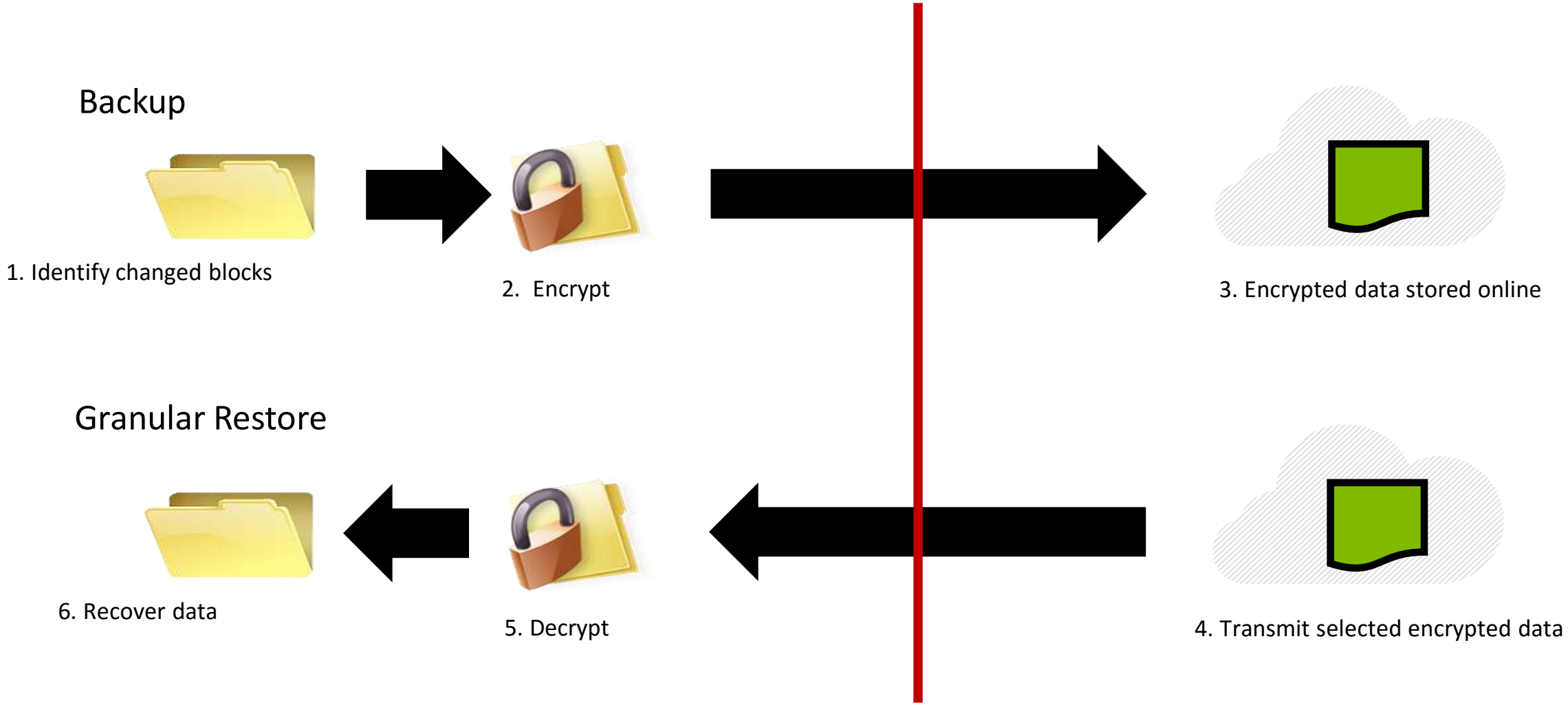
Integration With Existing Backup Offerings



Off-site backup of files, virtual machines and databases from your on-premises datacenter to Azure

Microsoft Confidential

How Azure Backup Works



Microsoft Confidential

Demo: Backup and Restore Scenario

Backup of Azure VMs

- Application-consistent backup of virtual machines
  - Backup with no impact to production workloads
  - No shut down of VM required
  - Application level consistency for Windows OSes
  - File system level consistency for Linux OSes
- Fabric level backup
  - Unlimited scalability, with no customer resources required for backup
  - Agentless backup of multiple VMs at the same time
  - Single, central management interface through the Azure portal
  - Detailed Jobs view for tracking progress and success/failure
- Policy-driven backup and retention
  - Configuration of scheduled backup
  - On-demand backup
  - Automatic management of recovery points within Azure Backup vault
  - Retain backup data in Azure Backup vault even if the original VM is deleted

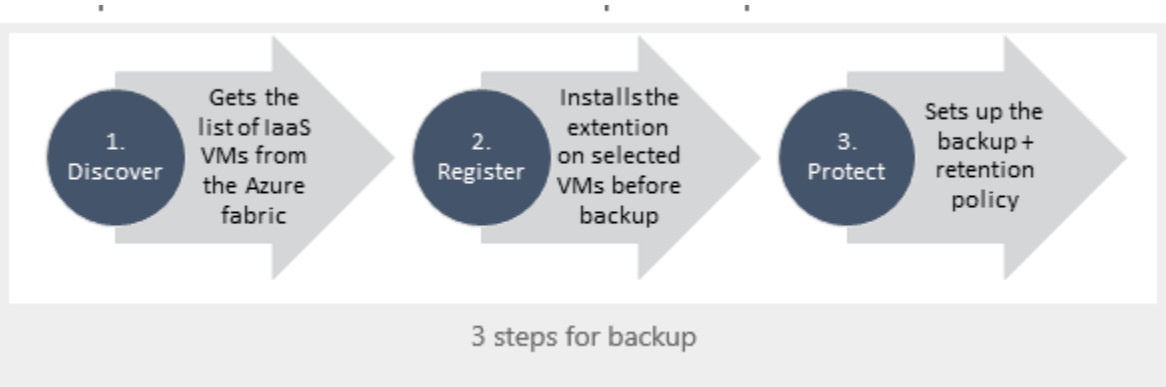
Microsoft Confidential

Azure VM Backup Design Principles

- Independent isolated backup copy – accidental destruction of original data prevented
- Application-consistent backup
- Predictable IO and Backup time – optimized blob copy
- Efficient storage consumption – only changes backed up
- Zero infrastructure deployment and maintenance – no need to deploy anything

Microsoft Confidential

Azure VM Backup Steps



- **Discover -** This step gets a list of all IaaS VMs in the same region that have not already been protected.
- **Register -** This one-time step installs the backup extension into the selected VMs in preparation for backup.
- **Protect -** This step involves setting the backup and retention policy for the VM. As per the backup policy, the initial replication of the VM's data will automatically be done, and will be followed by incremental backup at the predefined schedule

Microsoft Confidential

Backup File security

First level of Security

- You cannot decipher the data unless you have the key
- Without the passphrase, even the Azure team can’t access the data

Second level of Security

- All the machines are registered to backup vault using vault credentials
- Only the machines registered to same vault will be able to recover the data from the backup vault
- Additionally, the Vault credential itself is secured by your need to have access to Azure subscription (which is protected by Two Factor Authentication)
- You can use a single passphrase for all machines registered in the same vault

Microsoft Confidential

What is Azure Site Recovery (ASR)?

- Azure Backup and ASR are part of Azure Recovery Services
- ASR is represented as a way to back up on-premises VMs into Azure storage
- ASR Scenarios
  - On-premises Hyper-V to Azure protection with Hyper-V replication
  - On-premises VMM site to on-premises VMM site protection with Hyper-V replication
  - On-premises VMM site to on-premises VMM site protection with SAN replication
  - On-premises VMM site to Azure protection
  - On-premises VMWare site to on-premises VMWare site with InMage
- ASR requires the creation of a vault, similar to Azure Backup

Microsoft Confidential

Module 7: Automation

Automation Introduction

Microsoft Confidential

Automation Overview

- Automate time-consuming, error prone, operational tasks
- Increase reliability of your business processes
- Boost the efficiency of your platform
- Lower your operational costs
- Integrate with and extend existing systems

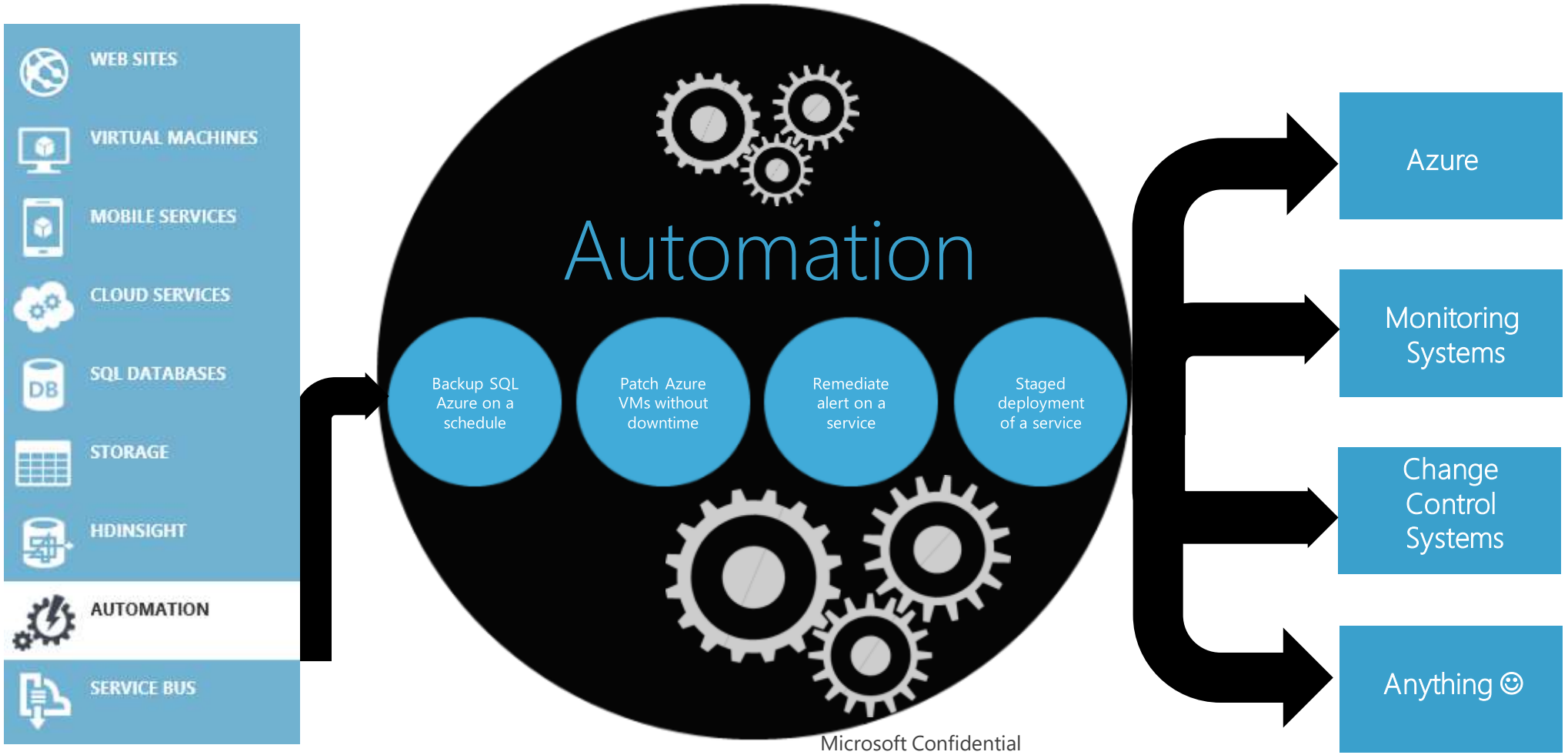
Microsoft Confidential

Azure Automation Primary Features

Runbook Authoring in Azure:
Create runbooks to automate all aspects of cloud operations, from deployment, monitoring, and optimizations

Highly Available Engine:
Support requirements for scale and H/A.
Built on PowerShell Workflow. Isolation for runbook jobs

Integration into other systems:
Import PS modules and create additional modules and runbooks for Azure services or to connect into 3rd party systems



Microsoft Confidential

Pricing

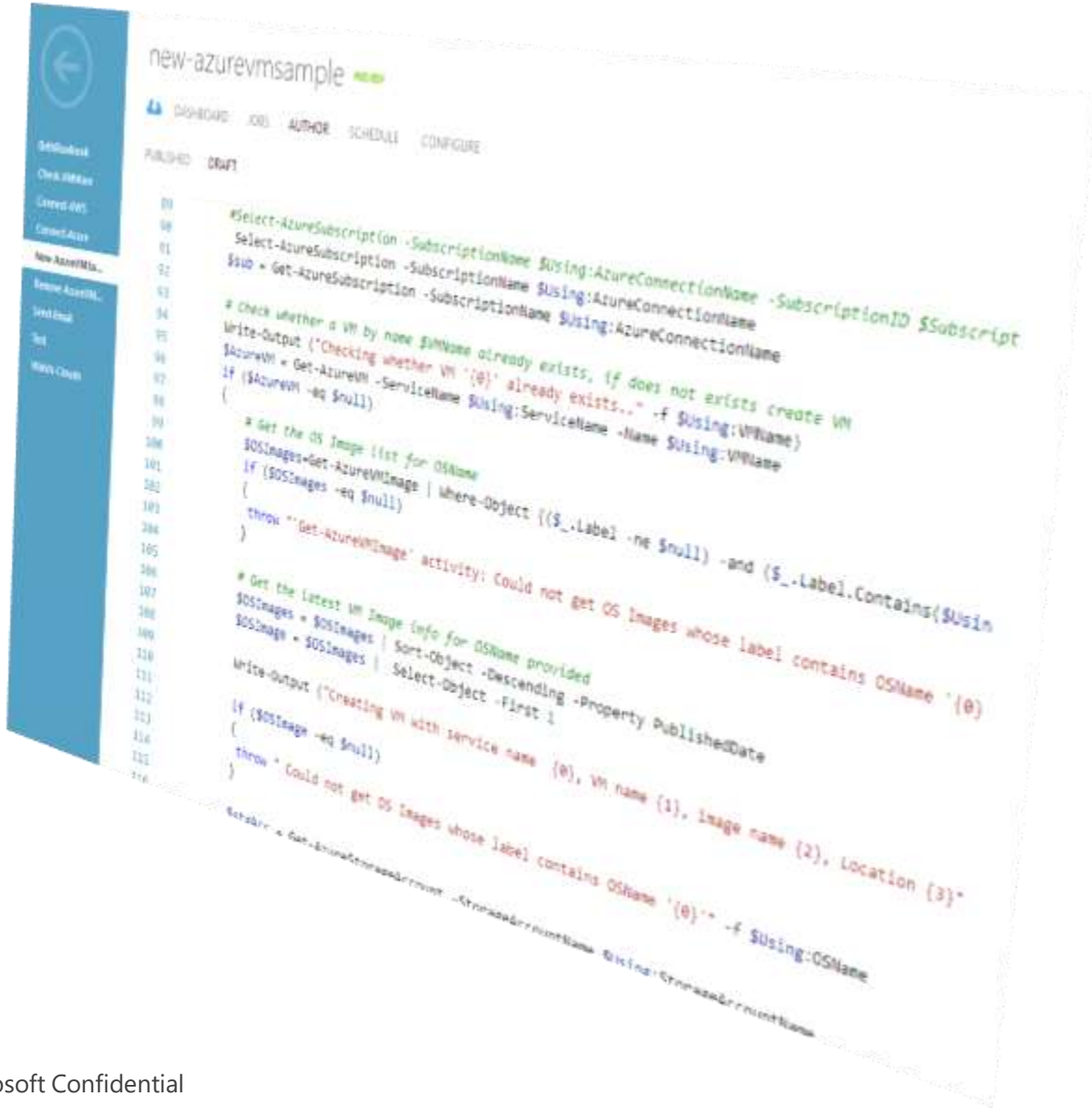
- Current pricing posted here: http://azure.microsoft.com/en-us/pricing/details/automation/
- Billed by the minute according to actual run time of your jobs
- Free tier gives you 500 minutes of job run time
- Standard tier costs $20 per 10,000 min, SLA 99.9% jobs start within 30 min of requested time

Automation Account

- The first thing you must create to use Azure Automation
- Security and resource boundary for Azure Automation
- Contains Runbooks
- Contains assets that support Runbook execution
- Ties infrastructure and assets needed to execute Runbooks to an Azure region
- Specifies the Azure subscription to be billed for Automation usage
- Limited to 25 accounts per subscription

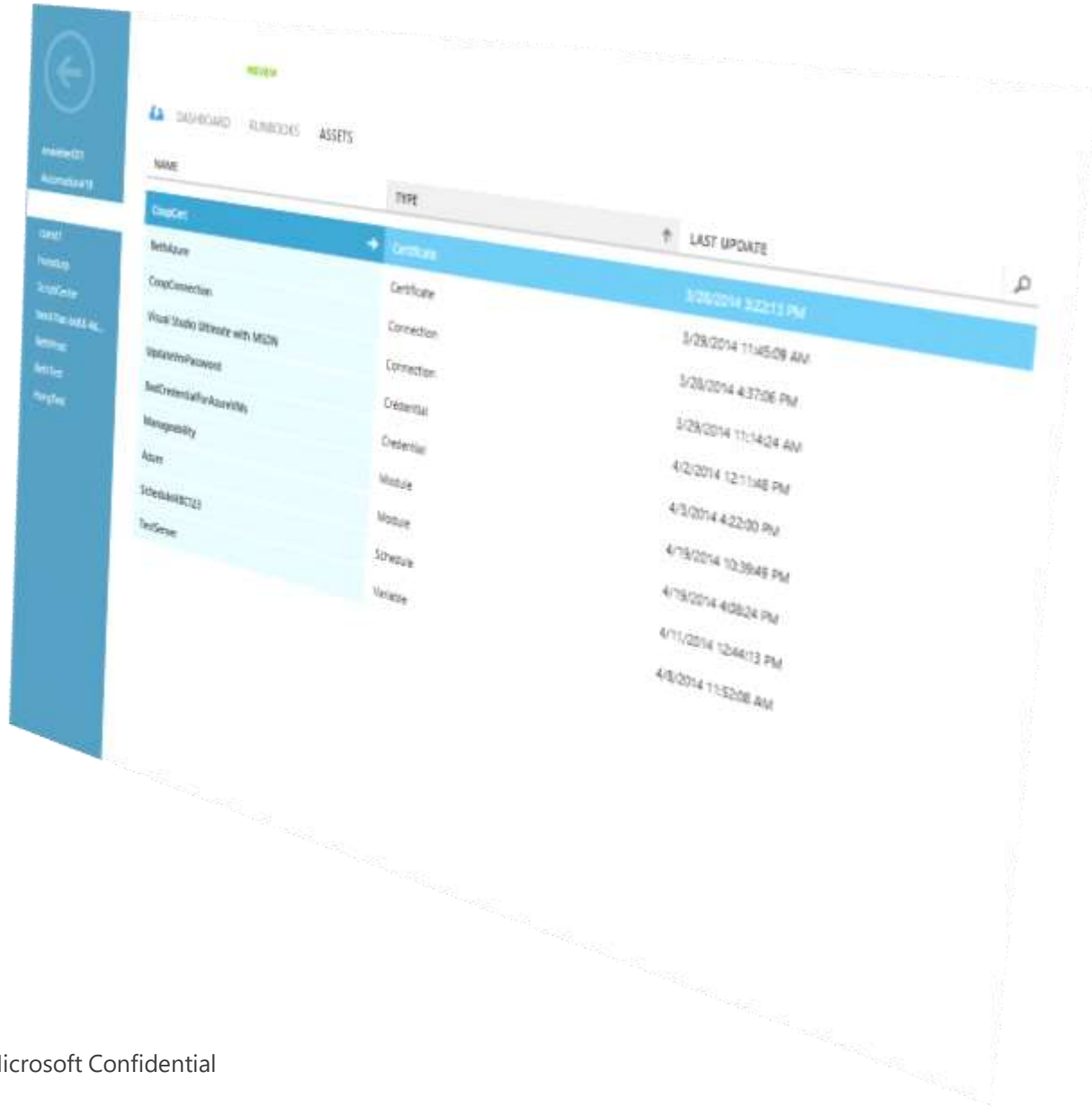
Automation Runbooks

- **Runbooks** – central concept for Automation. They contain a set of instructions in the form of PowerShell Workflows to execute your maintenance tasks
- Monitor Runbook execution status, history and usage through the portal
- Author Runbooks through the portal or on your laptop and import them
- Test Runbooks and publish them through the portal
- Runbooks execute in jobs running on Azure Automation Worker roles



Automation Assets

- Certificates
- Credentials
- PowerShell modules
- Connections
- Schedules
- Variables



Demo: Tour of the Azure Automation Portal

Demo: Importing, Testing, and Running a Gallery Runbook

Automation Summary

- Author runbooks to automate all forms of Azure operations
- Highly available execution engine
- Built on Windows PowerShell Workflows

Microsoft Confidential

Microsoft