Microsoft Azure Security, Privacy, & Compliance
Technology trends: driving cloud adoption

### BENEFITS

<table>
<thead>
<tr>
<th>Speed</th>
<th>Scale</th>
<th>Economics</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 weeks to deliver new services vs. 6-12 months with traditional solution (Case Study: HarperCollins Publishers)</td>
<td>Scale from 30,000 to 250,000 site visitors instantly (Case Study: Autocosmos)</td>
<td>$25,000 in the cloud would cost $100,000 on premises (Microsoft Azure BI Team, STMG Proof Points Central)</td>
</tr>
</tbody>
</table>

### AZURE ADOPTION

- 430B+ Microsoft Azure AD authentications
- 280% year-over-year database growth in Microsoft Azure
- 50% of Fortune 500 use Microsoft Azure

### Cloud Trend:

- 70% of CIOs will embrace a cloud-first strategy in 2016

  (IDC CIO Agenda webinar)
60% cited concerns around data security as a barrier to adoption. 45% concerned that the cloud would result in a lack of data control.

Benefits realized:
94% experienced security benefits they didn’t previously have on-premise.

62% said privacy protection increased as a result of moving to the cloud.

Barriers to Cloud Adoption study, ComScore, September 2013

Microsoft Azure
Microsoft Azure
UNIFIED PLATFORM FOR MODERN BUSINESS

Global Physical Infrastructure
servers / network / datacenters

- Automated
- Managed Resources
- Elastic
- Usage Based

N Central US, S Central US, N Europe, W Europe, E Asia, SE Asia + 24 Edge CDN Locations
Trustworthy foundation
BUILT ON MICROSOFT EXPERIENCE AND INNOVATION

**Compliance Standards:**
Investing heavily in robust compliance processes, including ISO 27001, FedRAMP, and HIPAA
## Shared responsibility

REDUCE SECURITY COSTS + MAINTAIN FLEXIBILITY, ACCESS, & CONTROL

<table>
<thead>
<tr>
<th>On-Premises</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Runtime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O/S</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Customer** | **Microsoft**

Microsoft Azure
Transparency & independent verification
AID CUSTOMERS IN MEETING SECURITY & COMPLIANCE OBLIGATIONS

- Third-party verification
- Access to audit reports
- Compliance packages
- Best practices and guidance
- Trust Center
- Cloud Security Alliance
- Security Response Center progress report
- Security intelligence report
Microsoft approach in action

Security  Privacy  Compliance
## Design & operations

<table>
<thead>
<tr>
<th>Software Development Lifecycle (SDL)</th>
<th>Operational security controls</th>
<th>Assume breach</th>
<th>Incident response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security embedded in planning, design, development, &amp; deployment</td>
<td>Rigorous controls to prevent, detect, contain, &amp; respond to threats</td>
<td>Hardening cloud services through simulated real-world attacks</td>
<td>Global, 24x7 incident response to mitigate effects of attacks</td>
</tr>
</tbody>
</table>

Microsoft Azure
Security development lifecycle

Education
Administer and track security training

Process
Guide product teams to meet SDL requirements

Accountability
Establish release criteria & sign-off as part of FSR
Incident Response (MSRC)

Training Requirements Design Implementation Verification Release Response

Ongoing Process Improvements
Prevent Breach

- Threat model
- Code review
- Security testing

Assume Breach

- War game exercises
- Live site penetration testing
- Centralized security logging & monitoring

Assume breach identifies & addresses potential gaps

Scope ongoing live site testing of security response plans to drastically improve mean time to detection & recovery

Reduce exposure to internal attack (ensuring once inside, attackers do not have broad access)

Periodic environment post breach assessment & clean state
Incident response

- In-depth 9-step incident response process
- Focus on containment & recovery
- Makes contractual commitments regarding customer notification
## Infrastructure protection

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 hour monitored physical security</td>
</tr>
<tr>
<td>Secure multi-tenant environment</td>
</tr>
<tr>
<td>Firewalls</td>
</tr>
<tr>
<td>Patch management</td>
</tr>
<tr>
<td>System monitoring and logging</td>
</tr>
<tr>
<td>Antivirus/antimalware protection</td>
</tr>
<tr>
<td>Threat detection</td>
</tr>
<tr>
<td>Forensics</td>
</tr>
</tbody>
</table>
Service security starts with physical data center

- Cameras
- 24X7 security staff
- Barriers
- Fencing
- Alarms
- Two-factor access control: Biometric readers & card readers
- Security operations center
- Seismic bracing
- Days of backup power

**Perimeter**

**Building**

**Computer room**
Architected for secure multi-tenancy

**AZURE:**
- Centrally manages the platform and helps isolate customer environments using the Fabric Controller
- Runs a configuration-hardened version of Windows Server as the Host OS
- Uses Hyper-V, a battle tested and enterprise proven hypervisor
- Runs Windows Server and Linux on Guest VMs for platform services

**CUSTOMER:**
- Manages their environment through service management interfaces and subscriptions
- Chooses from the gallery or brings their own OS for their Virtual Machines
Firewall protection

**AZURE:**
- Restricts access from the Internet, permits traffic only to endpoints, and provides load balancing and NAT at the Cloud Access Layer
- Isolates traffic and provides intrusion defense through a distributed firewall

**CUSTOMER**
- Applies corporate firewall using site-to-site VPN
- Configures endpoints
- Defines access controls between tiers and provides additional protection via the OS firewall
Patch management

**Azure:**
- Applies regularly scheduled updates to the platform
- Releases critical patches immediately
- Rigorously reviews & tests all changes

**Customer:**
- Applies similar patch management strategies for their Virtual Machines
### AZURE:
- Performs monitoring & alerting on security events for the platform
- Enables security data collection via Monitoring Agent or Windows Event Forwarding

### CUSTOMER:
- Configures monitoring
- Exports events to SQL Database, HDInsight or a SIEM for analysis
- Monitors alerts & reports
- Responds to alerts

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Computer</th>
<th>Event Description</th>
<th>Severity</th>
<th>DateTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1150</td>
<td>Machine1</td>
<td>Example security event</td>
<td>4</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>2002</td>
<td>Machine2</td>
<td>Signature Updated Successfully</td>
<td>4</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>5007</td>
<td>Machine3</td>
<td>Configuration Applied</td>
<td>4</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>1116</td>
<td>Machine2</td>
<td>Example security event</td>
<td>1</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>1117</td>
<td>Machine2</td>
<td>Access attempted</td>
<td>1</td>
<td>04/29/2014</td>
</tr>
</tbody>
</table>
Antivirus/antimalware

AZURE:
- Performs monitoring & alerting of antimalware events for the platform
- Enables real time protection, on-demand scanning, and monitoring via Microsoft Antimalware for Cloud Services and Virtual Machines

CUSTOMER:
- Configures Microsoft Antimalware or an AV/AM solution from a partner
- Extracts events to SIEM
- Monitors alerts & reports
- Responds to alerts

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Computer</th>
<th>Event Description</th>
<th>Severity</th>
<th>DateTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1150</td>
<td>Machine1</td>
<td>Client in Healthy State</td>
<td>4</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>2002</td>
<td>Machine2</td>
<td>Signature Updated Successfully</td>
<td>4</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>5007</td>
<td>Machine3</td>
<td>Configuration Applied</td>
<td>4</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>1116</td>
<td>Machine2</td>
<td>Malware Detected</td>
<td>1</td>
<td>04/29/2014</td>
</tr>
<tr>
<td>1117</td>
<td>Machine2</td>
<td>Malware Removed</td>
<td>1</td>
<td>04/29/2014</td>
</tr>
</tbody>
</table>
**AZURE:**
- Performs big data analysis of logs for intrusion detection & prevention for the platform
- Employs denial of service attack prevention measures for the platform
- Regularly performs penetration testing

**CUSTOMER:**
- Can add extra layers of protection by deploying additional controls, including DOS, IDS, web application firewalls
- Conducts authorized penetration testing of their applications
Forensics

AZURE:
- Performs coordination, analysis of logs and VHD images in the event of platform-level incident

CUSTOMER:
- Contacts Microsoft for forensic data when needed
- Uses standard security response and forensics processes
Network protection

<table>
<thead>
<tr>
<th>Network isolation</th>
<th>Virtual Networks</th>
<th>Cloud to on-premises connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevents traffic from other customers/internet to customers’ private IP Addresses</td>
<td>Connects one or more cloud service using private IP addresses</td>
<td>Site to site, point to site, and ExpressRoute help enable secure connections to Azure</td>
</tr>
</tbody>
</table>
**Network isolation**

**Microsoft Azure**
- Does not enable general internet access by default, except for remote administration endpoints configured when Virtual Machines are created in the Portal.

**CUSTOMER:**
- Configure endpoints for required access.
- Creates connections to other cloud and on-premises resources.
Virtual networks

**AZURE:**
- Allows customers to create isolated virtual private networks

**CUSTOMER:**
- Creates Virtual Networks with Subnets and Private IP addresses
- Enables communications between their Virtual Networks
- Can brings their own DNS
- Can domain join their Virtual Machines
VPN connections

AZURE:
- Enables connection from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs

CUSTOMERS:
- Configures the VPN client in Windows
- Manages certificates, policies, and user access
ExpressRoute connections

AZURE:
- Offers private fiber connections via ExpressRoute
- Enables access to Compute, Storage, and other Azure services

CUSTOMERS:
- Can establish connections to Azure at an ExpressRoute location (Exchange Provider facility)
- Can directly connect to Azure from your existing WAN network (such as a MPLS VPN) provided by a network service provider
- Manages certificates, policies, and user access
Identity & access

Microsoft employee access management

Enterprise cloud identity – Azure AD

Monitor & protect access to cloud apps

Multi-Factor Authentication
Microsoft employee access management

• No standing access to the platform and no access to customer Virtual Machines
• Grants least privilege required to complete task
• Multi-factor authentication required for all administration
• Access requests are audited and logged

Microsoft Azure

Microsoft Corporate
Network

BLOBS
TABLES
QUEUES
DRIVES

Just in Time & Role-Based Access

Leadership grants temporary privilege

Pre-screened Admin requests access
Enterprise cloud identity – Azure AD

AZURE:
• Provides enterprise cloud identity and access management
• Enables single sign-on across cloud applications
• Offers Multi-Factor Authentication for enhanced security

CUSTOMER:
• Centrally manages users and access to Azure, O365, and hundreds of pre-integrated cloud applications
• Builds Azure AD into their web and mobile applications
• Can extend on-premises directories to Azure AD
Microsoft Azure

**AZURE:**
- Uses password hashes for synchronization
- Offers security reporting that tracks inconsistent traffic patterns, including:
  - Sign ins from unknown sources
  - Multiple failed sign ins
  - Sign ins from multiple geographies in short timeframes
  - Sign ins from suspicious IP addresses and suspicious devices

**CUSTOMER:**
- Reviews reports and mitigates potential threats
- Can enable Multi-Factor Authentication

Monitor & protect access to cloud apps
## Data protection

<table>
<thead>
<tr>
<th>Data encryption options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data segregation</td>
</tr>
<tr>
<td>Data location and redundancy</td>
</tr>
<tr>
<td>Data destruction</td>
</tr>
</tbody>
</table>
Encryption in transit

**AZURE:**
- Encrypts most communication between Azure datacenters
- Encrypts transactions through Azure Portal using HTTPS
- Supports FIPS 140-2

**CUSTOMER:**
- Can choose HTTPS for REST API (recommended)
- Configures HTTPS endpoints for application running in Azure
- Encrypts traffic between Web client and server by implementing TLS on IIS

Microsoft Azure
Encryption at rest

Virtual Machines:
- Data drives – full disk encryption using BitLocker
- Boot drives – BitLocker and partner solutions
- SQL Server – Transparent Data and Column Level Encryption
- Files & folders - EFS in Windows Server

Storage:
- Bitlocker encryption of drives using Azure Import/Export service
- StorSimple with AES-256 encryption

Applications:
- Client Side encryption through .NET Crypto API
- RMS Service and SDK for file encryption by your applications
Data segregation

Storage isolation:
• Access is through Storage account keys and Shared Access Signature (SAS) keys
• Storage blocks are hashed by the hypervisor to separate accounts

SQL isolation:
• SQL Database isolates separate databases using SQL accounts

Network isolation:
• VM switch at the host level blocks inter-tenant communication
Data location and redundancy

**AZURE:**
- Creates three copies of data in each datacenter
- Offers geo-replication in a datacenter 400+ miles away
- Does not transfer Customer Data outside of a geo (ex: from US to Europe or from Asia to US)

**CUSTOMER:**
- Chooses where data resides
- Configures data replication options

Note: Microsoft Azure data centers, Australia – Q2 FY15
Data Deletion

- Index immediately removed from primary location
- Geo-replicated copy of the data (index) removed asynchronously
- Customers can only read from disk space they have written to

Disk Handling

- Wiping is NIST 800-88 compliant
- Defective disks are destroyed at the datacenter
Privacy by design

<table>
<thead>
<tr>
<th>Privacy by Design</th>
<th>Restricted data access &amp; use</th>
<th>Contractual commitments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy controls built into Azure design and operations</td>
<td>Customer data is only used to provide the service and is never used for advertising</td>
<td>Data Processing Agreements, EU Model Clauses, HIPAA BAA</td>
</tr>
</tbody>
</table>
Azure does not share data with its advertiser-supported services

Azure does not mine Customer Data for advertising

Read the fine print of other cloud service provider’s privacy statements

Information we collect

We collect information to provide better services to all our users—from figuring out basic stuff like which language you speak, to more complex things like which ads you’ll find most useful or the people who matter most to you online.
Contractual commitments

**EU Data Privacy Approval**
- Microsoft meets high bar for protecting privacy of EU customer data
- Microsoft offers customers EU Model Clauses for transfer of personal data across international borders
- Microsoft’s approach was approved by the Article 29 committee of EU data protection authorities – the first company to obtain this

**Broad contractual scope**
- Microsoft makes strong contractual commitments to safeguard customer data covered by HIPAA BAA, Data Processing Agreement, & E.U. Model Clauses
- Enterprise cloud-service specific privacy protections benefit every industry & region
## Simplified compliance

<table>
<thead>
<tr>
<th>Information security standards</th>
<th>Effective controls</th>
<th>Government &amp; industry certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27001</td>
<td>SOC 1 Type 2 SOC 2 Type 2</td>
<td>FedRAMP/FISMA PCI DSS Level 1 UK G-Cloud HIPAA/HITECH</td>
</tr>
</tbody>
</table>
Continuous Compliance approach

- Security goals set in context of business and industry requirements
- Security analytics & best practices deployed to detect and respond to threats
- Benchmarked to a high bar of certifications and accreditations to ensure compliance
- Continual monitoring, test and audit
- Ongoing update of certifications for new services

Security Compliance Framework

Business Objectives

Industry Standards & Regulations

Test and audit

Security analytics

Risk management best practices

Security benchmark analysis

Certificates and Attestations
## Certifications & programs

<table>
<thead>
<tr>
<th>Program</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27001</td>
<td>The ISO/IEC 27001:2005 certificate validates that Azure has implemented the internationally recognized information security controls defined in this standard.</td>
</tr>
<tr>
<td>SOC 1 SSAE 16/ISAE 3402</td>
<td>Azure has also been audited against the Service Organization Control (SOC) reporting framework for SOC 1 Type 2 (formerly SAS 70), attesting to the design and operating effectiveness of its controls.</td>
</tr>
<tr>
<td>SOC 2</td>
<td>Azure has been audited for SOC 2 Type 2, which includes a further examination of Azure controls related to security, availability, and confidentiality</td>
</tr>
<tr>
<td>FedRAMP/FISMA</td>
<td>Azure has received Provisional Authorization to Operate from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB), having undergone the assessments necessary to verify that it meets FedRAMP security standards.</td>
</tr>
<tr>
<td>PCI DSS Level 1</td>
<td>Azure has been validated for PCI-DSS Level 1 compliance by an independent Qualified Security Assessor (QSA).</td>
</tr>
<tr>
<td>UK G-Cloud IL2</td>
<td>In the United Kingdom, Azure has been awarded Impact Level 2 (IL2) accreditation, further enhancing Microsoft and its partner offerings on the current G-Cloud procurement Framework and CloudStore.</td>
</tr>
<tr>
<td>HIPAA BAA</td>
<td>To help customers comply with HIPAA and HITECH Act security and privacy provisions, Microsoft offers a HIPAA Business Associate Agreement (BAA) to healthcare entities with access to Protected Health Information (PHI).</td>
</tr>
</tbody>
</table>
Microsoft commitment

Enhance Security
Protect Privacy
Simplify Compliance

Unified platform for modern business
Trusted by leading companies
Get started today!

- Talk to a Microsoft security expert
- Explore additional resources:
  - Trustworthy Computing Cloud Services: [www.microsoft.com/trustedcloud](http://www.microsoft.com/trustedcloud)
Microsoft Azure

Azure Active Directory
Azure Active Directory

**Option 1: Cloud Authentication**

Windows Server Active Directory → IdentitySync with password hash sync → Windows Azure Active Directory

User attributes are synchronized using IdentitySync including a password hash, Authentication is completed against Windows Azure Active Directory

**Option 2: Federated Authentication**

Windows Server Active Directory → IdentitySync → AD FS → Windows Azure Active Directory

User attributes are synchronized using IdentitySync, Authentication is passed back through federation and completed against Windows Server Active Directory
Microsoft Azure

Multi-Factor Authentication
Multi-Factor Authentication

Mobile apps

Phone calls

Text messages
1. Users sign in from any device using their existing username/password.

2. Users must also authenticate using their phone or mobile device before access is granted.
Microsoft Azure

Express Route
Customers want Microsoft Azure on their network

**IPsec VPN over Internet**
- Greater networking costs and latency since data is hair pinned through a customer data center
- Data travels over the open Internet to connect to cloud
- Bandwidth is limited

**Cloud on your WAN**
- Avoids risks from exposure to Internet
- Avoids complexity and added costs
- Provides lower latency, higher bandwidth and greater availability
IPSec VPN and ExpressRoute

**Scenario 1: IPSec VPN over internet**
- **Customer DC** to **Azure**
- Connect via an encrypted link over public internet

**Scenario 2: Exchange Provider**
- **Customer site** to **ExpressRoute partner location**
- Peer at an ExpressRoute location, an Exchange Provider facility

**Scenario 3: Network Service Provider**
- **Customer site 1** to **Customer site 2** to **Customer site 3** to **Microsoft Azure**
- Connection from a WAN provided by Network Service Provider (e.g. telco). Azure becomes another site on the customer's WAN network.

**Virtual Network - Compute only.**
- Microsoft Azure

**ExpressRoute - Provides customer choice and include access to compute, storage, and other Azure services.**
<table>
<thead>
<tr>
<th>Services</th>
<th>ISO/IEC 27001:2005</th>
<th>SOC 1 and SOC 2 SSAE 16/ISAE 3402</th>
<th>FedRAMP</th>
<th>PCI DSS</th>
<th>UK G-Cloud</th>
<th>HIPAA BAA</th>
<th>EU Model Clauses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Cloud Services</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Websites</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Mobile Services</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Data Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>SQL Database</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>HDInsight</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Cache</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site Recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Service Bus</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Media Services</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Notification Hubs</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Multi-Factor Authentication</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>BizTalk Services</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Scheduler</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rights Management Service</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Network Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Network</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Traffic Manager</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>ExpressRoute</td>
<td></td>
<td></td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>