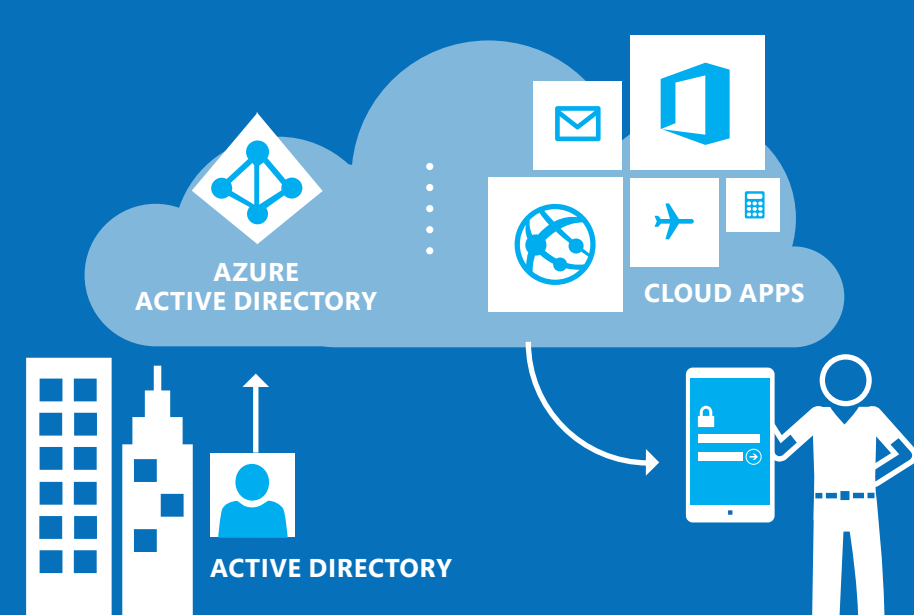


# cloud security

Windows Azure

## Join forces with Windows Azure

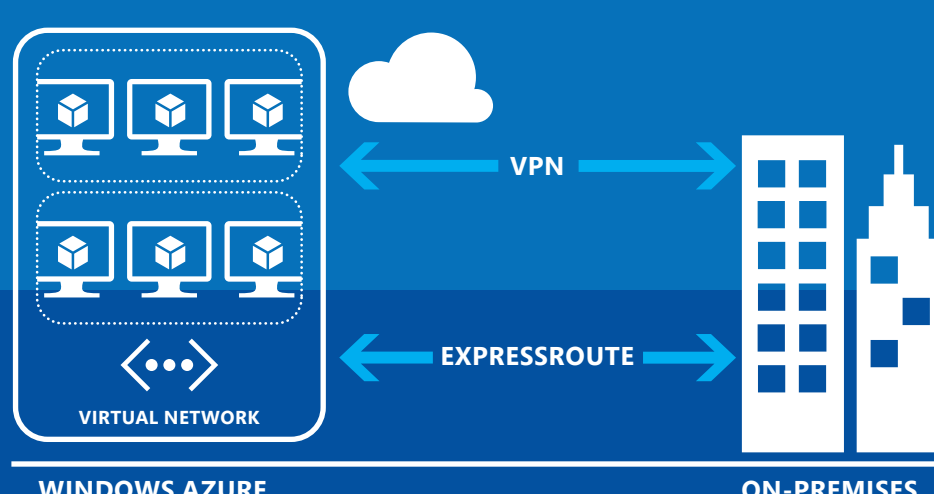
Benefit from Microsoft's unmatched scale and experience running trusted enterprise cloud services around the globe. Leverage our deep investments in technology, operational processes, and expertise to provide a trusted platform for your cloud initiatives. With Microsoft as your ally, you can take advantage of the cloud more quickly while reducing security and compliance costs and minimizing risk to your organization.



### IDENTITY AND ACCESS

Windows Azure offers enterprise-level cloud identity governance that enables you to manage access for your users:

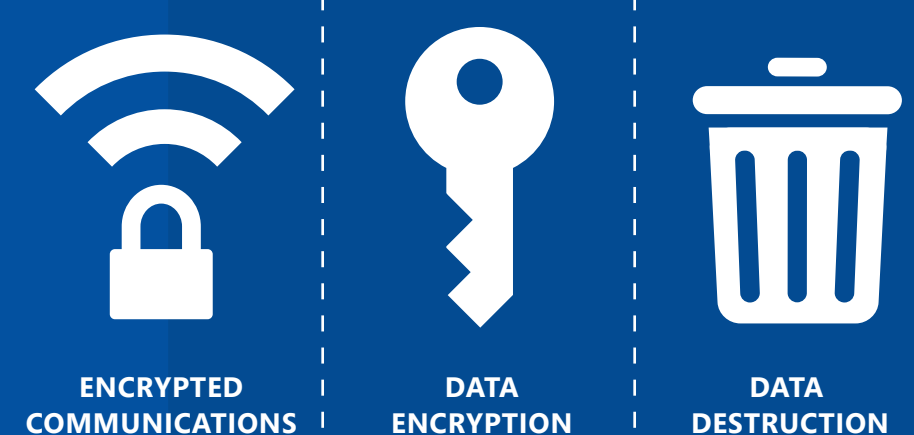
- Sync existing identities and enable single sign-on to Windows Azure, Office 365, and a world of other cloud applications
- Monitor access patterns to identify and mitigate potential threats
- Help prevent unauthorized access with Windows Azure Multi-Factor Authentication
- Empower end users with self-service identity management capabilities



### NETWORK SECURITY

Your Windows Azure virtual machines and data are isolated from undesirable traffic and users. However, you can access them through encrypted or private connections:

- Benefit from firewalled and partitioned networks to help protect against unwanted traffic from the Internet
- Securely connect to your on-premises datacenter or a single computer using Windows Azure Virtual Network
- Manage your virtual machines with encrypted remote desktop and Windows PowerShell sessions
- Keep your traffic off the Internet by using Windows Azure ExpressRoute, a private fiber link between you and Windows Azure



### DATA PROTECTION

Microsoft makes data protection a priority. Technology safeguards, such as encryption, and operational processes about data destruction keep your data yours only:

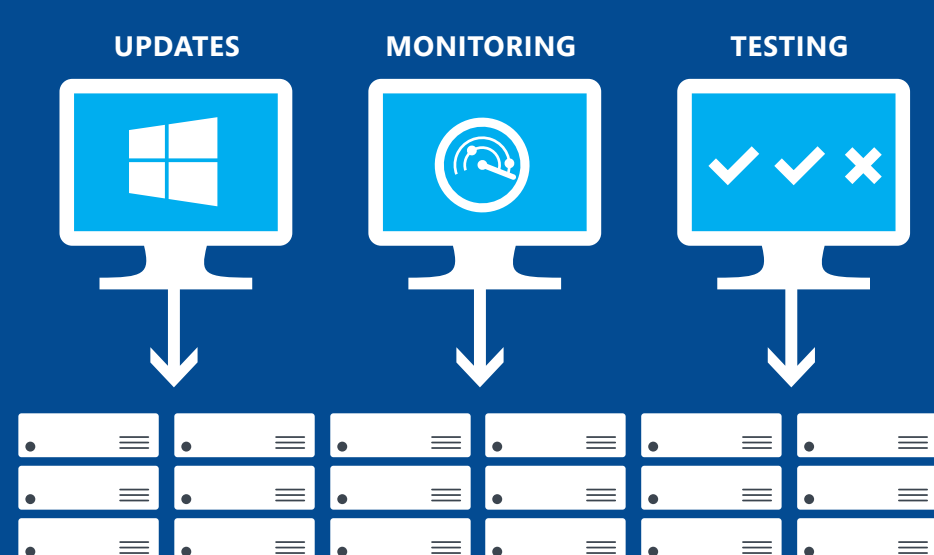
- Encryption is used to help secure data in transit between datacenters and you, as well as between and at Microsoft datacenters
- Customers can choose to implement additional encryption using a range of approaches—you control the encryption method and keys
- If you delete data or leave Windows Azure, we follow strict industry standards that call for overwriting storage resources before reuse, as well as physically disposing of decommissioned hardware



### DATA PRIVACY

Microsoft is committed to safeguarding the privacy of your data. You control where your data resides and who can access it:

- Specify the geographic areas where your data is stored—and data can be replicated within a geographic area for redundancy
- Get additional contractual commitments about the transfer of personal data to address the E.U. Data Protection Directive
- Limit Microsoft access and use of your data. We strictly control and permit access only as necessary to provide or troubleshoot the service, and we never use your customer data for advertising purposes



### THREAT DEFENSE

Protection from known and emerging threats requires constant vigilance, and an array of defenses is in place:

- Integrated deployment systems manage security updates for Microsoft software, and you can apply update management processes to your virtual machines
- Continuous monitoring and analysis of traffic reveal anomalies and threats. Forensic tools dissect attacks, and you can implement logging to aid analysis
- You can conduct penetration testing of applications you run in Windows Azure. We take care of penetration testing for Windows Azure services



### COMPLIANCE PROGRAMS AND CERTIFICATIONS

Cloud compliance is easier with Windows Azure. By providing compliant, independently verified services, we help you streamline compliance for the infrastructure and applications you run in Windows Azure. We share detailed information—including audit reports and compliance packages—to provide insight into how specific regulatory standards are met.

SECURITY + PRIVACY + COMPLIANCE

MICROSOFT



Like it? Get it.