# Microsoft Azure Government

The cloud platform designed to meet U.S. government demands

Azure Government delivers cloud speed, scale, and economics while addressing the security and compliance needs of U.S. federal agencies including the Department of Defense, plus state and local governments and their solution providers. Azure Government offers physical and network isolation from non-U.S. government deployments and requires specialized personnel screening. Azure Government will address government regulatory and compliance requirements such as FedRAMP, CJIS, and HIPAA.

AZURE ACTIVE DIRECTORY

CLOUD APPS

ACTIVE DIRECTORY
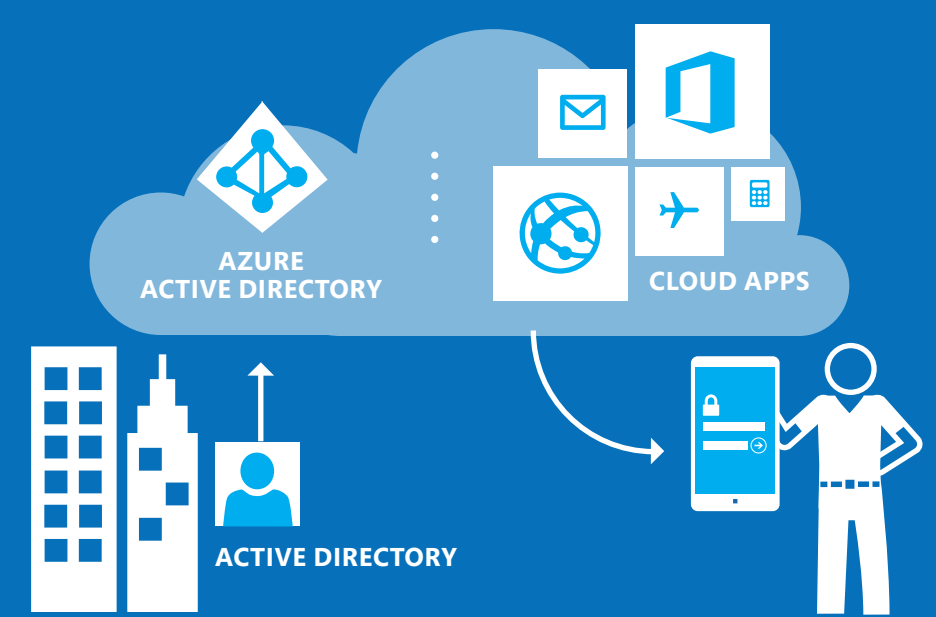
IDENTITY AND ACCESS

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

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

VPN

VIRTUAL NETWORK

AZURE

ON-PREMISES
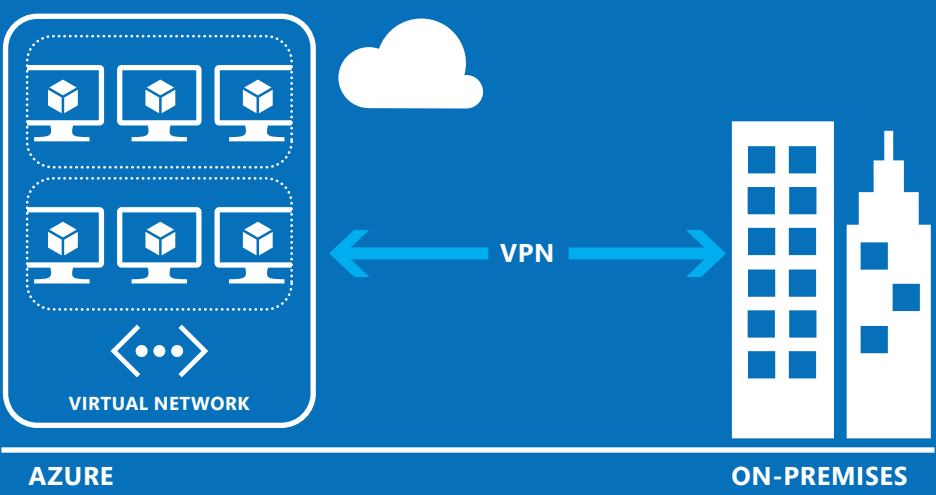
NETWORK SECURITY

Your Azure virtual machines and data are isolated from undesirable traffic. You can also access them through encrypted or private connections:

- Physical network separation from other Microsoft cloud properties
- Benefit from firewalls and partitioned networks to help protect against unwanted traffic from the Internet
- Securely connect to your on-premises datacenter or a single computer using Azure Virtual Network
- Manage your virtual machines with encrypted remote desktop and Windows PowerShell sessions
- Microsoft employs a series of defense in depth technologies to assist with Intrusion Detection and to identify Denial of Service attacks

ENCRYPTED COMMUNICATIONS

DATA ENCRYPTION
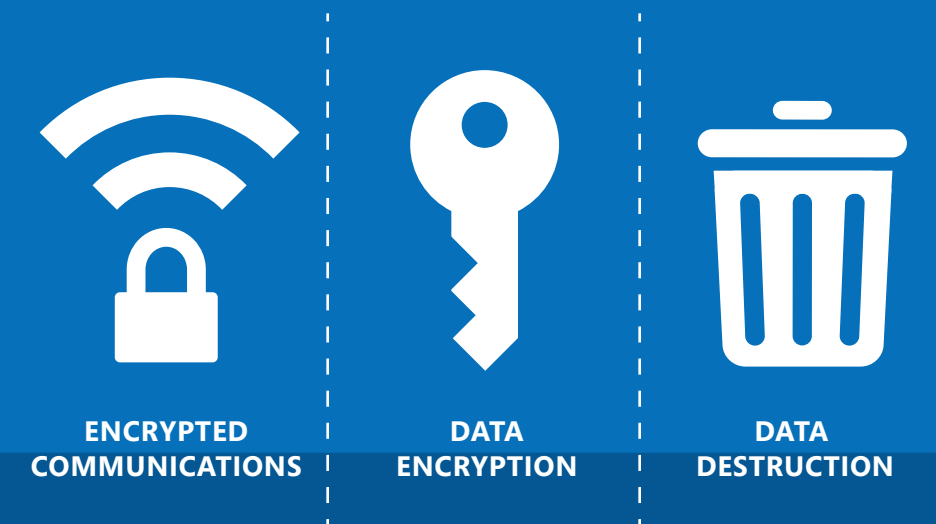
DATA DESTRUCTION

DATA PROTECTION

Microsoft makes data protection a priority. Technology safeguards, such as encryption, and operational processes about data destruction help keep your data safe and within your control:

- Encryption is used to help secure data in transit between datacenters and you, as well as between Microsoft datacenters
- You can choose to implement additional encryption using a range of approaches—you control the encryption method and keys
- Within Azure Government data can be replicated within a geographic area for redundancy, specifically Azure Government Virginia or Azure Government Iowa regions
- Screened U.S. citizens and policies to help protect customer data and applications

DATA PRIVACY

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

- Screened U.S. personnel and policies allow Azure Government to be used to build solutions capable of handling data regulated under FedRAMP, HIPAA and CJIS
- We never use your customer data for advertising purposes
- If you delete data in Azure Government, we follow strict industry standards that call for overwriting storage resources, as well as physically disposing of decommissioned hardware

UPDATES

MONITORING

TESTING
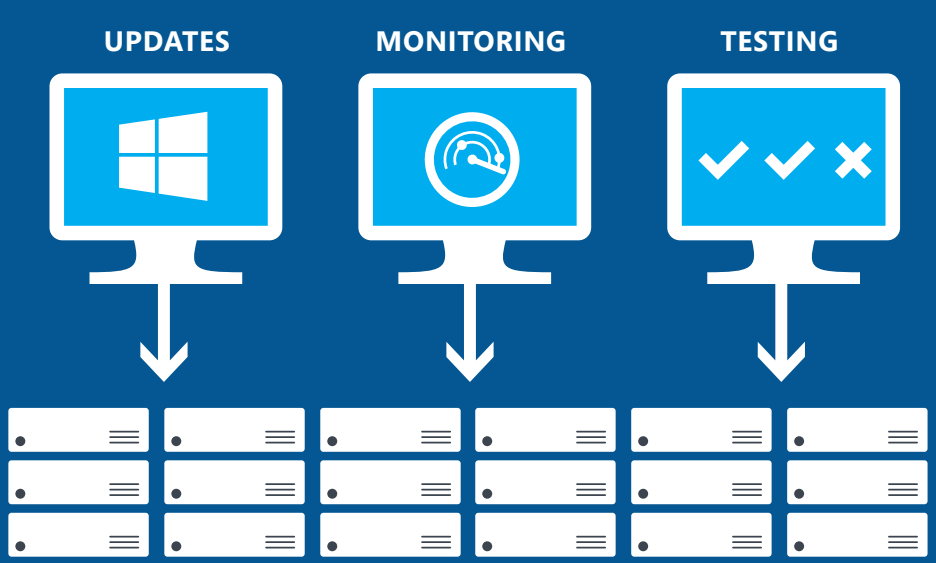
THREAT DEFENSE

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

- Integrated deployment systems manage the distribution and installation of security patches—customers can apply similar patch management processes for virtual machines deployed in Azure
- 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 Azure Government

FedRAMP
CJIS
HIPAA
DISA ECSB

COMMITMENT TO COMPLIANCE

Cloud compliance is easier with Azure. We are committed to providing a compliant, independently verified service, and to managing the service in a manner to enable our customer's compliance with various regulations. We help you streamline compliance for the infrastructure and applications you run in Azure. We share detailed information—including audit reports and compliance packages—to provide insight into how specific regulatory standards are met and what our commitments are.

Learn more at Azure.com/gov

Microsoft