Microsoft

Trusted Cloud:

Microsoft Azure Security, Privacy, Compliance, Reliability/Resiliency, and Intellectual Property

Author

Debra Shinder

Contents

Introduction

Cloud computing plays an increasingly important role in the operations of organizations of all sizes and in all industries around the world. While cost reduction is still a top priority, scalability, mobility, connectivity, and business agility have stepped to the forefront for decision makers. The cloud offers all this and more. A digital transformation is taking place in the business world. Anticipated growth of artificial intelligence (AI) applications and the Internet of Things (IoT) means the demands on computing resources are increasing at a pace that makes it hard for enterprises to keep up. Projections indicate that the number of IoT devices will increase to over 55 billion by 2025. The global AI market is expected to grow approximately 150% during the period from 2017 to 2025.

The cloud enables these exciting technologies, and trust is the foundation on which cloud computing is built. Customers will not use technologies or technology providers they don't trust. Trust in cloud computing requires the ability to rely on services and data being available when you need them. You must be able to recover quickly from problems or outages. Reliability and resiliency are critical elements in the trust relationship between cloud provider and customer. Trust is a major consideration in cloud adoption and decision making. You want assurance that your data will be accessible to those who need it to do their jobs, and secured against unauthorized access, tampering, or loss. Thus data protection is a major concern.

Threats to cloud security and data privacy are on the rise. In the healthcare sector alone, as of August 2019 the number of patient records that had been breached was more than double that of the entire previous year. A report by Risk Based Security indicated that 4.1 billion records were exposed in the first half of 2019.

Organizations are more security conscious than ever, but trust is about more than just security features. It's also about protecting personal privacy while at the same time promoting the free flow of data. It's about reliability and resiliency. It's about preventing cybercrime and reducing technology-related fraud and online exploitation. It's about providing affordable and accessible connectivity everywhere, for everyone. This requires a consistently trusted, responsible, and inclusive cloud policy.

Trust begins with keeping customer data safe. Data breaches are costly and can cause irreparable damage to your customers and to your company's reputation. New data protection laws, regulations, and industry standards have increased compliance requirements. Organizations must navigate increased data protection requirements and address dynamic threats to privacy and security, while embracing digital transformation. Today, many organizations find that the best way to achieve these goals is through the cloud—but not just any cloud. Choosing a trustworthy cloud services provider is vital. IT and business leaders need a trusted partner with the right technologies and processes to help build scalable, reliable, inclusive cloud solutions and increase business agility while taking the necessary steps to secure data and help ensure privacy and compliance across the enterprise.

At Microsoft, we take these principles seriously, and we have invested heavily in building trust. Microsoft Azure provides a collection of integrated cloud services for the enterprise and government that you can use to help protect your business assets while reducing security costs and complexity. Building on the principles of security, privacy, compliance, resiliency, and intellectual property protection, Microsoft strives to earn and keep your trust.

Microsoft Azure: Built on a foundation of trust

Azure is a rapidly growing cloud computing platform that features an ever-expanding suite of cloud services. These include analytics, computing, database, mobile, networking, storage, and web. Azure integrates tools, templates, and managed services. These work together to make it easier to build and manage enterprise, mobile, web, and Internet of Things (IoT) apps faster, using the tools, applications, and frameworks you choose.

As a public cloud service, Azure delivers these services to organizations of all sizes, including many of the world's leading enterprises.

Additionally, Microsoft Cloud for US Government delivers Azure services, such as Azure Government, and supports mission-critical government workloads. This includes a unique cloud instance, exclusively for government customers and their solution providers, and hardened US datacenters operated by screened personnel.

The Azure approach to trust is based on the following foundational principles: security, privacy, compliance, resiliency, and intellectual property (IP) protection.

Security: Azure helps you keep customer data secure

The Security Development Lifecycle (SDL) introduces and emphasizes security and privacy early and throughout all phases of the development process.

- Azure is built on leading security technologies to help organizations manage and control user identity and access, which are central elements in securing your environment.
- Azure delivers network and infrastructure security technologies and tools to help protect your applications and data.
- Azure uses encryption to protect communications and operational processes including your data in transit. Azure also offers encryption for your data at rest.
- Azure offers advanced tools to detect and defend against threats.

Privacy: You own and control your data

The Azure approach to privacy and data protection is grounded in a commitment to give organizations ownership of and control over the collection, use, and distribution of customer data.

- You own all your data in Azure, and Microsoft will use it only to provide the services agreed upon. Microsoft will not mine your data for marketing or advertising purposes.
- You have control over where your data is located, who can access it, and on what terms.
- You can access your own customer data at any time and for any reason.
- Microsoft imposes carefully defined requirements for government and law enforcement requests for customer data.
- If you discontinue the service, Microsoft follows strict standards for removing your data.

The Azure approach to trust is based on the following foundational principles: security, privacy, compliance, resiliency, and protection of intellectual property.

Compliance: Azure conforms to global standards

Compliance plays a critical role in providing assurance for customers and is an important element in the trust relationship. Through rigorous and widely recognized formal standards that are certified by independent third parties, Microsoft helps organizations comply with constantly shifting requirements and regulations governing the collection and use of individuals' data.

With Azure, you can take advantage of more than 90 current compliance certifications, including over 50 region- and country-specific offerings for the United States, the United Kingdom, the European Union, Germany, Japan, India, China, and more. You can also benefit from over 35 compliance offerings specific to the needs of such key industries as healthcare, government, finance, education, manufacturing, and media.

New legislation and regulations are constantly emerging, but Microsoft engages globally with both governmental and non-governmental regulators and standards bodies to keep your current and future compliance needs covered.

Azure offers a broad set of key global and industry-specific standards and supporting materials for key regulations, including, for example, ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1, 2, and 3 Reports. Azure also meets regional and national standards that include the EU Model Clauses, EU-U.S. Privacy Shield, Singapore MTCS, and the CS Mark in Japan.

Reliability and Resiliency: Azure keeps your applications up and running and your data available

Azure helps you to avoid potential disasters and quickly recover if your organization does get hit by disaster. Azure offers resiliency for your cloud-based applications and data by providing for business continuity in the following ways:

- High availability
- Disaster recovery
- Backup

Azure was the first cloud platform to provide a built-in backup and disaster recovery solution. Alternatively, you may have your own solution, and that works on Azure too. Azure is cost effective, simple, and scalable, and offers an industry-leading certification portfolio.

Managing IP risks: Azure helps protect your IP

Trust in the cloud encompasses not only the assurance of security, privacy, compliance, and resiliency, but also clarity and confidence that your intellectual property will be protected against frivolous infringement claims, including when you develop innovative solutions working with a cloud provider. Azure IP Advantage and the Shared Innovation Initiative can offer that assurance.

These principles are supported by the Microsoft commitment to transparency, by which you get broad visibility into Azure processes and practices. This white paper explains in plain, clear language what Microsoft does with your customer data, how it protects and secures that data, and why you can rely on Azure to keep your data available to you when you need it and recover your data if a disaster occurs.

Learn more: Visit the Microsoft Trust Center for the most comprehensive and up-to-date information about the policies, processes, and practices that help you exercise your right to control your data and comply with government and industry regulations.

Learn more: Find out how Azure resiliency can help you build comprehensive business continuity solutions, keep your applications up and running, and create a resilient environment faster.

Security:

Azure helps you keep customer data secure

Microsoft is committed to providing you with a trusted set of cloud services. We have leveraged our decades-long industry experience building enterprise software and running some of the world's largest online services to create a robust set of Azure security technologies and practices. These work to help reduce the cost, complexity, and risk associated with security in the cloud.

Our mission is to deliver the highest levels of security, privacy, compliance, and availability to private and public sector organizations and help you protect your business assets while reducing security costs. Toward that end, Microsoft invests over $1 billion annually in cybersecurity, including the Azure platform, and employs over 3500 dedicated cybersecurity professionals.

Azure helps you strengthen your security posture, streamline your compliance efforts, and enable digital transformation. Thousands of companies and governments all over the world have chosen Azure as their trusted cloud and benefit from its industry-leading infrastructure and operational security foundation.

Microsoft takes a defense-in-depth approach to security in Azure. We work together with customers, combining built-in security controls and partner solutions to help you get protected faster across identity, network, and data, as well as providing tools to help you with security management and threat protection.

Defense in Depth

Identity & Access	Apps & Data Security	Network Security	Threat Protection	Security Management
Role-based access	Encryption	DDOS Protection	Antimalware	Log Management
Multifactor Authentication	Confidential Computing	NG Firewall	AI-Based Detection and Response	Security Posture Assessment
Central Identity Management	Key Management	Web App Firewall	Cloud Workload Protection	Policy and Governance
Identity Protection	Certificate Management	Private Connections	SQL Threat Protection	Regulatory Compliance
Privileged Identity Management	Information Protection	Network Segmentation	IoT Security	SIEM

Microsoft invests over $1 billion annually in cybersecurity, including the Azure platform, and employs over 3500 dedicated cybersecurity professionals.

Automated Azure processes in the cloud can reduce or eliminate human error that is responsible for many security breaches. State-of-the-art physical security protecting Microsoft datacenters is designed, built, and operated to internationally recognized standards. Microsoft is invested in making the Azure infrastructure resilient to attack, safeguarding user access to the Azure environment, and helping keep customer data secure.

- **Physical security.** Microsoft datacenters have extensive layers of protection to reduce the risk of unauthorized physical access to datacenter resources.
- **Security design and operations.** Microsoft makes Azure security a priority at every step, including code development that follows the Security Development Lifecycle (SDL), a company-wide, mandatory process based on a rigorous set of security controls that govern operations, as well as robust incident response strategies. Operational Security Assurance (OSA) makes Microsoft business cloud services more resilient to attack by decreasing the amount of time needed to prevent, detect, and respond to real and potential internet-based security threats.
- **Infrastructure protection.** The guiding principle of our security strategy is to "assume breach." The Microsoft global incident response team works around the clock to mitigate the effects of any attack against our cloud services.
- **Network protection.** Azure provides the infrastructure to securely connect virtual machines (VMs) to one another and to connect on-premises datacenters with Azure VMs. The Azure infrastructure ensures that all infrastructure communications (for which Microsoft is responsible) that carry customer information are encrypted over the wire. Distributed denial-of-service (DDoS) protection at every Azure datacenter helps protect against even the largest of DDoS attacks seen on the internet today.
- **Data protection.** Azure safeguards customer data for applications, platform, system, and storage using four specific methods: segregation, encryption, redundancy, and destruction. Azure offers protection for customer data both in transit and at rest, and supports encryption for data, files, applications, services, communications, and drives.
- **Identity and user access management and control.** Azure manages and controls identity and user access to enterprise environments, data, and applications by federating user identities to Azure Active Directory and enabling multifactor authentication for more secure sign-in. Microsoft uses stringent identity management and access controls to limit data and systems access to those with a genuine business need (least-privileged).

This paper discusses each of these in greater detail below.

Physical security

Microsoft designs, builds, and operates datacenters in a way that strictly controls physical access to the areas where your data is stored. Microsoft has hundreds of Azure datacenters in 54 regions (as of 2019), and each of these has extensive multilayered protections to ensure unauthorized users cannot gain physical access to your customer data. Layered physical security measures at Microsoft datacenters include access approval:

- At the facility's perimeter.
- At the building's perimeter.
- Inside the building.
- On the datacenter floor.

Physical security reviews of the facilities are conducted periodically to ensure the datacenters properly address Azure security requirements.

Security design and operations

Secure cloud solutions are the result of comprehensive planning, innovative design, and efficient operations. Microsoft makes security a priority at every step, and operational security best practices are integrated into every aspect of Azure. This includes implementing controls that restrict unauthorized access from Microsoft personnel and contractors.

Microsoft provides multilayered security across physical datacenters, infrastructure, and operations. We help our developers build more secure software and meet security compliance requirements, and Azure operations and security professionals work to protect your data from unauthorized access.

Microsoft provides multilayered security across physical datacenters, infrastructure, and operations.

Security embedded in software development

Azure code development adheres to the Microsoft Security Development Lifecycle (SDL). The SDL is a software development process that helps developers build more secure software and address security and compliance requirements while reducing development cost. The SDL became central to Microsoft development practices over a decade ago and is shared freely with the industry and customers. It embeds security requirements into systems and software through the planning, design, development, and deployment phases.

The SDL process has evolved to encompass not only traditional desktop applications but also cloud-based applications and the agile development methodology.

Learn more: Agile Development Using Microsoft Security Development Lifecycle

Enhanced operational security

Azure adheres to a rigorous set of security controls that govern operations and support. Microsoft deploys combinations of preventive, defensive, and reactive controls including the following mechanisms to help protect against unauthorized developer and administrative activity:

- Tight access controls on sensitive data, including a requirement for multifactor authentication to perform sensitive operations
- Combinations of controls that enhance independent detection of malicious activity
- Multiple levels of monitoring, logging, and reporting
- Just-in-time access, to minimize the number of people who have administrative privileges on a permanent or ongoing basis

Microsoft also conducts background verification checks of operations personnel and limits access to applications, systems, and network infrastructure in proportion to the level of background verification.

To support a comprehensive, cross-company approach to security, every year Microsoft invests more than a billion dollars in security research and development. These investments include:

- The Cyber Defense Operations Center, a state-of-the-art facility that brings together cybersecurity specialists and data scientists from across the company to combat cyber adversaries, and protect against, detect, and respond to threats in real time.
- The Cybersecurity Solutions Group, a dedicated group of security experts worldwide that delivers security solutions, expertise, and services to help organizations modernize IT platforms, securely move to the cloud, and help keep data safe from modern security risks.

Assume breach

One key operational principle that Microsoft follows in hardening its cloud services is to "assume breach." Traditionally, a large proportion of resources in the application development lifecycle were dedicated to preventive measures, such as application security, network segmentation, and host hardening. The current mindset recognizes that prevention alone, while very important, is only the beginning of an effective security strategy.

"Assume breach" assumes that attackers will be able to get in. If an attack is successful, you must be prepared to mitigate the impact through effective detection and response capabilities. This assumption necessitates greater emphasis on and investment in early detection and rapid response efforts.

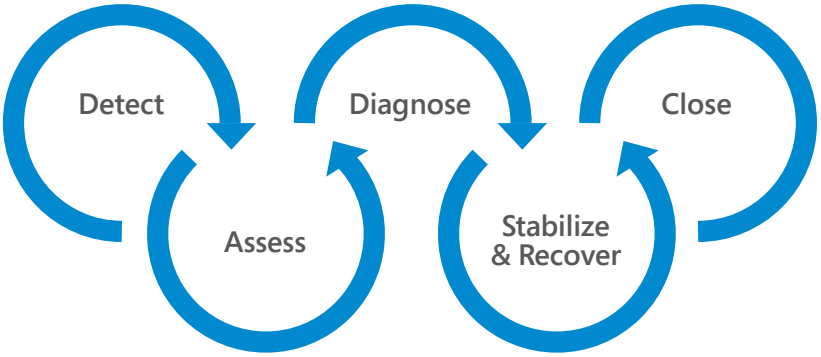
"Red teaming" was developed by the military to improve effectiveness by assuming an adversarial role. At Microsoft, a dedicated red team of software security experts simulates real-world attacks at the network, platform, and application layers, testing the ability of Azure to detect, protect against, and recover from breaches. By constantly challenging the security capabilities of the service, Microsoft works continuously to stay ahead of emerging threats.

Learn more: Microsoft Enterprise Cloud Red Teaming

Incident response and management

The Microsoft global incident response service works every day to mitigate the effects of attacks and malicious activity.

The goal of security incident management is to identify and remediate threats quickly, investigate thoroughly, and notify affected parties. The incident response team follows an established set of procedures for incident management, communication, and recovery.



Microsoft takes five steps to respond to and manage incidents:

1. **Detect**. This is the first indication that a security event has occurred and initiates an investigation.
2. **Assess.** An incident response team member assesses the impact and severity of the event. Based on the evidence gathered, the assessment may or may not result in further escalation to the security response team.
3. **Diagnose.** Security response experts conduct a technical or forensic investigation to identify containment, mitigation, and workaround strategies. If the security team believes that customer data may have been exposed to an unauthorized individual or that an unlawful act has occurred, the customer incident notification process begins in parallel.
4. **Stabilize and recover.** The incident response team creates a recovery plan to mitigate the issue. Crisis containment steps such as quarantining impacted systems may occur immediately and in parallel with diagnosis. Longer term mitigations may be planned to occur after the immediate risk has passed.
5. **Close.** The incident response team creates a post-mortem record that outlines the details of the incident, with the intention to revise policies, procedures, and processes to prevent a reoccurrence.

Microsoft recognizes that shared responsibility means you need tools to conduct your own incident response.

Azure Security Center can play a key role in your incident response strategy. It provides you with insight into the source of the attack, identifying impacted resources and making policy-based recommendations to help you remediate detected issues and resolve them quickly, as well as suggestions for preventing future attacks.

Azure Security Center provides a centralized, real-time monitoring view into the security state of your hybrid cloud resources. Azure Security Center's Investigation Path helps in identifying all the entities involved an attack, such as SQL injection, and quickly remediate against the attack.

In addition, Azure Sentinel can be used in the incident response process by providing a powerful, cloud-based Security Information and Event Manager (SIEM). Security analysts can investigate threats with AI and hunt suspicious activities at scale by tapping into decades of cybersecurity work at Microsoft.

Learn more: Azure Security Response in the Cloud discusses the Microsoft response process in detail and examines how Microsoft investigates, manages, and responds to security incidents within Azure.

Learn more: What is Azure Sentinel provides an overview of what Sentinel can do to support your SIEM requirements.

Learn more about Azure Security Center detection and investigation capabilities.

Azure Security Center provides a centralized, real-time monitoring view into the security state of your hybrid cloud resources.

Infrastructure protection

Infrastructure security is a key component of the secure foundation on which Microsoft cloud services are built. Azure addresses security risks across its infrastructure, which includes hardware, software, networks, administrative and operations staff, and the physical datacenters that house it all.

Physical security

Azure runs in geographically distributed and highly secured Microsoft facilities around the world, sharing space and utilities with other Microsoft Online Services. Physical access is strictly controlled on a "need to" basis and limited in both area and time.

Each facility is designed to run 24 hours a day, 365 days a year, and employs multiple layers of security measures to help protect operations from power failure, physical intrusion, and network outages.

- **Perimeter:** Security staff around the clock, facility setback requirements, fencing and other barriers, and continuous surveillance camera monitoring
- **Buildings:** Alarms, seismic bracing, and security cameras, routine patrol of the datacenter by well-vetted and highly trained security personnel
- **Server facilities:** Multifactor-authentication-based access controls that use biometrics and card readers, cameras, and backup power supplies
- **Datacenter floor:** Full body metal detection screening and additional security scan, video monitoring, and restriction on allowed devices

Microsoft datacenters comply with industry standards (such as ISO/IEC 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel. Microsoft conducts periodic physical security reviews of the facilities to ensure the datacenters properly address Azure security requirements.

Learn more about how Microsoft datacenters are physically secured.

Monitoring and logging

Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities further enhance visibility.

Azure reviews and updates configuration settings and baseline configurations of hardware, software, and network devices annually. Changes are developed, tested, and approved prior to entering the production environment from a development and/or test environment. The baseline configurations that are required for Azure-based services are reviewed by the Azure security and compliance team and by service teams.

Learn more about Azure infrastructure monitoring.

In keeping with the shared responsibility model, Azure provides you with a wide array of configurable security auditing and logging options for insight into your security state and security-related events. These include Azure Active Directory reporting, Azure Key Vault logs, Azure Storage Analytics, and more. Logs from your Azure resources can be integrated with your on-premises security information and event management (SIEM) system.

Azure Monitor helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on. It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. Azure Monitor also includes several features and tools that provide valuable insights into your applications and other resources that they depend on.

Azure Security Center gives you a centralized view of the security state of your hybrid resources and the configurations of the security controls that are in place to protect them. This enables you to detect threats more quickly and respond more effectively. REST APIs support integration with existing change management and security operations systems.

Learn more about Azure Security Center monitoring and logging.

Azure Sentinel is a SIEM reinvented for the public cloud that helps you see and stop threats before they cause harm. Sentinel puts the cloud and large-scale intelligence from decades of Microsoft security experience to work and makes your threat detection and response smarter and faster with artificial intelligence (AI). It helps eliminate security infrastructure setup and maintenance, and elastically scales to meet your security needs while reducing IT cost.

Update management

Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run operating system, web application, and database scans of the Azure environment.

Security teams perform vulnerability scans on a regular basis. Microsoft contracts with independent assessors to perform penetration testing of the Azure boundary. Red team exercises are also routinely conducted, and the results are used to make security improvements, including those in operational security.

Under the shared responsibility model, you are responsible for managing updates and patches for your virtual machines running on Azure. You can enable and use the Update Management solution to quickly assess the status of available updates, schedule installation of required updates, review deployment results, and create an alert to verify that updates apply successfully.

Learn more about how to manage Windows updates by using Azure Automation.

Antivirus and antimalware

Malicious code is one of today's top security threats, so Microsoft implements a multiplicity of measures to address it.

- Azure software components must go through a virus scan before deployment. Each virus scan creates a log within the associated build directory, detailing what was scanned and the results of the scan. The virus scan is part of the build source code for every component within Azure. Code is not moved to production without a clean and successful virus scan.

- Microsoft provides native antimalware on all Azure virtual machines (VMs) that run and manage the fabric, to guard against subsequent infestation. When using Azure App Service, the underlying service that hosts the web app has Microsoft Antimalware enabled on it.

The Microsoft Antimalware Client and Service is not installed by default in the Virtual Machines platform. It is available as an optional feature through the Azure portal and Visual Studio Virtual Machine configuration under Security Extensions. Under the shared responsibility model, you are responsible for virus protection within your virtual machines. Microsoft recommends that organizations install and run some form of antimalware or antivirus, such as Microsoft Antimalware for Azure Cloud Services and Virtual Machines, on all VMs.

Microsoft Antimalware is a single-agent solution for applications and tenant environments designed to run in the background without human intervention. You can deploy protection based on the needs of your application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring. You can also deploy Microsoft Antimalware through Azure Security Center.

In addition, VMs can be routinely reimaged to clean out intrusions that may have gone undetected.

Azure Advanced Threat Protection (ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Azure ATP enables SecOp analysts and security professionals to detect advanced attacks in hybrid environments in the following ways:

- Monitors users, entity behavior, and activities with learning-based analytics.
- Protects user identities and credentials stored in Active Directory.
- Identifies and investigates suspicious user activities and advanced attacks throughout all phases of a cyberattack.
- Provides clear incident information on a simple timeline for fast triage.

Penetration testing

Microsoft conducts regular penetration testing to improve Azure security controls and processes, as described above.

Microsoft understands that in a shared responsibility model, security assessment is also an important part of your application development and deployment. Thus, Microsoft has established a policy that allows for organizations to carry out authorized penetration testing on their own—and only their own—applications hosted in Azure.

As of June 15, 2017, Microsoft no longer requires pre-approval to conduct penetration tests against Azure resources. Customers who wish to formally document upcoming penetration testing engagements against Azure are encouraged to fill out the Azure Service Penetration Testing Notification form.

If, during your penetration testing, you believe you have discovered a potential security flaw related to the Microsoft Cloud or any other Microsoft service, please report it to Microsoft within 24 hours by following the instructions on the Report a Computer Security Vulnerability page. Once submitted, you agree that you will not disclose this vulnerability information publicly or to any third party until you hear back from Microsoft that the vulnerability has been fixed. All vulnerabilities reported must follow the Coordinated Vulnerability Disclosure principle.

Learn more: Microsoft Cloud Penetration Testing Rules of Engagement. This document describes the unified rules for customers wishing to perform penetration tests against their Microsoft Cloud components.

Distributed denial-of-service (DDoS) protection

Azure has a defense system to help protect against DDoS attacks on Azure platform services. Using standard detection and mitigation techniques, it is designed to withstand attacks generated from both outside and inside the platform. The Basic DDoS protection is automatically enabled as part of the Azure platform. Azure DDoS Protection Basic tier provides always-on traffic monitoring with near real-time detection of a DDoS attack, with no intervention required. DDoS Protection automatically mitigates the attack as soon as it's detected. The DDoS service understands your resources and resource configuration and uses intelligent traffic profiling to learn application traffic patterns over time.

Azure DDoS Protection Standard tier is an optional service that provides additional mitigation capabilities over the Basic service tier, and is tuned specifically to Azure Virtual Network resources. These include real-time attack metrics and diagnostic logs, post-attack mitigation reports, near real-time log stream for Security Information and Event Management (SIEM) integration, and access to DDoS experts during an active attack.

Learn more about Azure DDoS Protection.

Identity and user-access management and control

Identity is a crucial boundary layer for security. Many consider it to be the primary perimeter for security. This is a shift from the traditional focus on network security, as network perimeters keep getting more porous.

Microsoft has strict controls that restrict access to Azure by Microsoft personnel. Microsoft personnel do not have default access to cloud customer data. Instead, they are granted access, under management oversight, only when necessary.

Azure enables you to restrict access to your environments, data, and applications to authorized users based on role assignment, role authorization, and permission authorization.

Azure enables you to restrict access to your environments, data, and applications to authorized users based on role assignment, role authorization, and permission authorization.

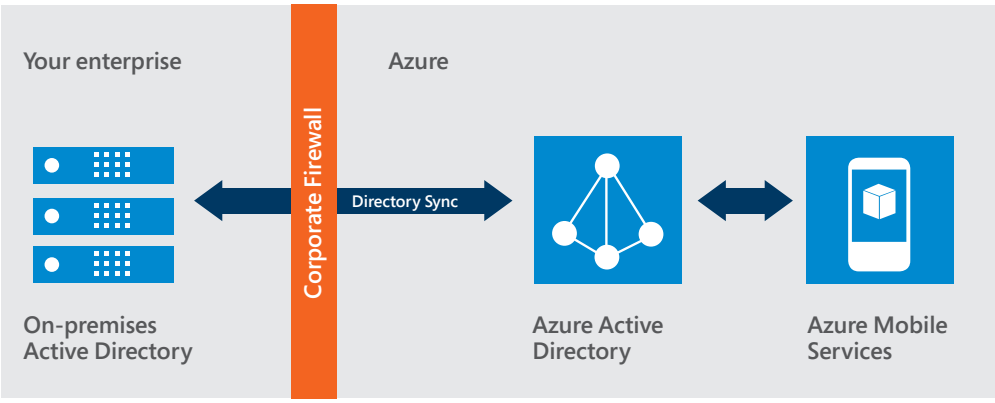
Enterprise cloud directory

Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure AD makes it easy for your developers to build policy-based identity management into your organization's applications.

Azure AD Premium editions include additional features to meet the advanced identity and access needs of enterprise organizations, such as:

- The ability for someone to sign in to thousands of applications, including on-premises business applications as well as cloud-based and consumer apps.
- Multifactor authentication.
- Conditional access based on group and location, or device state.
- Azure IoT device-level authentication.
- Access monitoring and logging.
- Cloud App Discovery.
- Self-Service Password Reset (SSPR).

Azure AD enables a single identity management capability across on-premises, cloud, and mobile solutions.



The Azure AD Premium P2 edition offers three important features:

- Azure AD Identity Protection leverages the anomaly detection of Azure AD to detect anomalies in real time. It uses adaptive machine-learning algorithms and heuristics to detect indications that an identity has been compromised. With Azure AD Identity Protection, you can detect potential vulnerabilities affecting your organization's identities, configure automated responses to detected suspicious actions that are related to your organization's identities, investigate suspicious incidents, and take appropriate action to resolve them.
- Azure AD Privileged Identity Management helps you manage, control, and monitor access within your organization, by identifying Azure AD administrators, enabling just-in-time administrative access to online services, and providing reports and alerts about administrative access.
- Access reviews provide governance of identities to ensure users and administrators have the correct access to apps and resources over time. Access reviews enable IT organizations to review access to groups or resources and confirm they still need access to perform their tasks.

Learn more For a comprehensive list of the features included in each of the Active Directory editions, see Azure Active Directory Pricing Details.

Multifactor authentication

The use of multiple authentication factors reduces the risk of unauthorized user access, such as through phishing attacks, and Azure MFA works for both on-premises and cloud applications and across both in a hybrid configuration, helping to safeguard access to data and applications. It delivers strong authentication through a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer for both on-premises and cloud applications.

Learn more about Azure MFA and how it works.

Conditional access. Users can access your organization's resources by using a variety of devices and apps from anywhere, so just focusing on who can access a resource is not sufficient anymore. You need to make sure that these devices meet your standards for security and compliance. With Azure AD conditional access, you can make automated access-control decisions for accessing your cloud apps that are based on conditions such as device state, location, client application, and sign-in risk.

Learn more about conditional access in Azure AD.

Azure IoT device-level authentication. Authentication applies to devices as well as users, especially in today's Internet of Things (IoT). Azure IoT supports X.509 certificates for enhanced authentication at the device level. Device identity can be transmitted safely and securely from the edge to the cloud. You can use the IoT Hub device identity registry to configure per-device security credentials and access control using tokens. Azure IoT Hub grants access to endpoints by verifying a token against the shared access policies and identity registry security credentials. Security credentials, such as symmetric keys, are never sent over the wire.

Learn more about identity registry in your IoT hub.

There are two types of risks related to user accounts that are flagged by Azure AD.

Risky sign-in is real time, based on the location, device and sign-in behavior, and indicates that someone other than the legitimate account owner might be attempting to sign in.

Risky users are flagged for indications of the possibility of a compromised account, based on data collected on the user. For example, if a user's credentials are suspected to have been leaked, that is a risky user.

Azure AD creates a risk event record whenever it detects either type of suspicious action.

Learn more about users flagged for risk security report.

Access monitoring and logging. Security reports are used to detect access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. You can turn on additional access monitoring in Azure and use third-party tools to detect additional threats. You can also request reports from Microsoft that provide information about user access to your environment.

Learn more about Azure identity management.

Cloud App Discovery provides a comprehensive view into your cloud app usage, enabling you to address Shadow IT. You can measure app usage by number of users, volume of data, and web requests, and identify which users are using an application. You can also export data for additional analytics and manage applications with Azure Active Directory to enable single sign-on (SSO) and user management.

Learn more about Azure AD Cloud App Discovery.

Self-Service Password Reset (SSPR). Azure AD SSPR provides both a web-based and Windows-integrated experience that enables users to reset their own passwords. This provides a better, faster, and more efficient password reset experience for users.

Learn more about how Azure AD Self-Service Password Reset works.

Network protection

Azure networking provides the infrastructure to securely connect virtual machines (VMs) to one another and to connect on-premises datacenters with Azure VMs and PaaS services. The Azure shared infrastructure hosts hundreds of millions of active VMs, so protecting the security and confidentiality of network traffic is critical.

In the traditional datacenter model, your corporate IT organization controls your networked systems, including physical access to networking equipment. In the cloud service model, the responsibilities for network protection and management are shared between the cloud provider and the customer. You don't have physical access to switches, routers, and other network devices, but you implement the logical equivalent within your cloud environment using tools such as guest operating system firewalls, virtual network gateway configuration, and virtual private networks.

Azure provides features and tools to help you secure your virtual networks.

Virtual networks. You can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other through private IP addresses. All resources in a virtual network can communicate outbound to the Internet by default. You can communicate inbound to a resource by assigning a public IP address or a public load balancer.

Azure resources communicate securely with each other through a virtual network or through a virtual network service endpoint.

Learn more about virtual network service endpoints.

Network isolation. Azure is a multitenant service, meaning that your data, deployments, and VMs may be stored on the same physical hardware as that of other customers. Azure uses logical isolation to segregate virtual networks and processing for each customer to help ensure that your customer data is not combined with anyone else's over your virtual networks in Azure. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Azure Virtual Networks enable you to use network isolation yourself by creating separate virtual networks (VNets) for different purposes (development, testing, production). Each VNet is isolated from other VNets. You can also segment a VNet into multiple subnets.

Learn more about network isolation with Azure best practices for network security.

Virtual machine encryption. You can encrypt Azure VMs using Azure Disk Encryption to protect the contents of both Windows and Linux VMs. This uses BitLocker for Windows and DM-Crypt for Linux to encrypt both the operating system volume and the data disks. Encryption keys are managed via Azure Key Vault. You can use Azure Storage Service Encryption (SSE) to encrypt VHD files stored in Azure blobs.

Learn more about Azure Disk Encryption for Windows and Linux IaaS VMs VPN.

Microsoft enables connections from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs. A Site-to-Site (S2S) VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE VPN tunnel. A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer.

Learn more about creating a site-to-site VPN and a point-to-site VPN in Azure.

For even better performance, you have the option to use ExpressRoute, a private fiber link into Azure datacenters that keeps your traffic off the Internet. ExpressRoute connections offer more reliability, faster speeds, and lower latencies than typical internet connections.

Learn more about Azure ExpressRoute.

Encrypting communications. Built-in cryptographic technology enables you to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises datacenters.

Azure offers many mechanisms for keeping data private as it moves from one location to another, including Transport Layer Security (TLS) and Perfect Forward Secrecy (PFS). When you interact with Azure Storage through the Azure portal, all transactions take place over HTTPS.

Learn more about Azure Encryption.

Threat detection. Azure Security Center uses new behavioral analytics to detect insider threats and attempts to persist within a compromised system. Detection algorithms are continuously developed and refined to create insights that you can use to remediate attacks more quickly.

Azure Advanced Threat Protection (ATP) is a cloud-based security solution that helps you detect and investigate security incidents across your enterprise by monitoring user, device, and resource behaviors and identifying anomalies right away.

Advanced Threat Protection for Azure SQL Database is a unified package for advanced SQL security capabilities. It includes functionality for discovering and classifying sensitive data, surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database.

Learn more about Azure Advanced Threat Protection and Advanced Threat Protection for Azure SQL Database

Azure Sentinel enables you to see and stop threats before they harm your network with this next generation Security Information and Event Management (SIEM) solution. It provides you with a bird's-eye view across your enterprise and uses artificial intelligence and integrated automation and orchestration to detect, investigate, and respond to incidents rapidly. Azure Firewall is a managed, cloud-based network security service that helps protect your Azure Virtual Network resources. It is a fully stateful firewall as a service that features:

- Built-in high availability with unrestricted cloud scalability.
- Ability to centrally create, enforce, and log application and network connectivity policies.
- Source and destination Network Address Translation (SNAT and DNAT) support.
- Full integration with Azure Monitor for logging and analytics.
- Support for hybrid connectivity through deployment behind VPN and ExpressRoute Gateways.

Learn more about Azure Firewall.

Data protection

Your data is your most valuable digital asset. Azure enables you to encrypt data and manage keys. It safeguards your customer data for applications, platform, system, and storage using four specific methods: segregation, encryption, redundancy, and destruction.

Data segregation. As a multitenant service, Azure uses logical isolation to segregate storage and processing for each customer to help ensure that your customer data is not combined with anyone else's.

Data encryption. You can encrypt data in storage and in transit to align with best practices for protecting the confidentiality and integrity of your data. Azure supports various encryption models, including both client-side and server-side encryption.

For data at rest, Azure offers a wide range of encryption capabilities, giving you the flexibility to choose the solution that best meets your needs.

Azure Disk Encryption leverages the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks. Transparent data encryption (TDE) helps protect Azure SQL Database.

Learn more about Azure Disk Encryption for IaaS VMs and TDE for SQL Database and Data Warehouse.

Azure Key Vault helps you easily and cost-effectively streamline key management and maintain control of keys used by cloud applications and services to encrypt data. Encryption at rest with Azure Site Recovery supports Storage Service Encryption (SSE).

Learn more about Azure Storage Service Encryption for Data at Rest.

For data in transit, Azure uses industry-standard transport protocols such as TLS 1.2+ between devices and Microsoft datacenters and within datacenters themselves. You can enable encryption for traffic between your own virtual machines and end users.

SMB 3.0 can be used in VMs that are running Windows Server 2012 or later to make data transfers secure by encrypting data in transit over Azure Virtual Networks. Administrators can enable SMB encryption for the entire server or just specific shares.

Secure Shell (SSH) can be used to connect to Linux VMs running in Azure. SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections.

Azure VPN encryption creates a secure, encrypted tunnel to protect the privacy of data sent across the network. Site-to-Site VPNs use IPsec for transport encryption. You can configure Azure VPN gateways to use a custom IPsec/IKE policy with specific cryptographic algorithms and key strengths. Point-to-Site VPNs use Secure Socket Tunneling Protocol (SSTP) to create the VPN tunnel that allows individual client computers access to an Azure virtual network.

Learn more about Azure encryption of data in transit.

Data redundancy. You may opt for in-country storage for compliance or latency considerations or out-of-country storage for security or disaster recovery purposes. Data may be replicated within a selected geographic area for redundancy.

Data in your Azure storage account is always replicated to ensure durability and high availability. You can choose from the following replication options:

- Locally redundant storage
- Zone-redundant storage
- Geo-redundant storage
- Read-access geo-redundant storage

Learn more about replication options in Azure Storage.

Azure is based on a shared responsibility model, in which part of the responsibility for security lies with the cloud services provider and part belongs to the customer.

Advanced Threat Protection for Azure Storage provides an additional layer of security intelligence that detects unusual and potentially harmful attempts to access or exploit storage accounts. This layer of protection allows you to address threats without the need to be a security expert or manage security monitoring systems.

Security alerts are triggered when anomalies in activity occur. These security alerts are integrated with Azure Security Center, and are also sent via email to subscription administrators, with details of suspicious activity and recommendations on how to investigate and remediate threats.

Advanced Threat Protection for SQL Database is part of the Advanced Data Security (ADS) offering, which is a unified package for advanced SQL security capabilities. It detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases. This provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities.

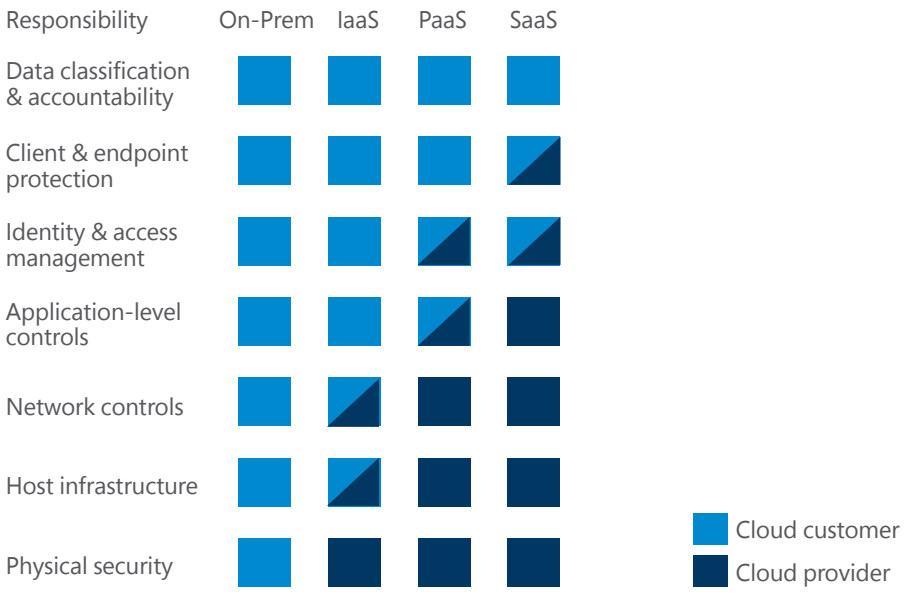
Data destruction. When you delete data or leave the Azure service, Microsoft follows industry-standard processes for overwriting storage resources before reuse, including following the National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines for media sanitization.

Learn more about NIST SP 800-88 R1.

Shared responsibility for security

Azure is based on a shared responsibility model, in which part of the responsibility for security lies with the cloud services provider and part belongs to the customer. This is in contrast to the traditional on-premises datacenter model, in which the organization that owns the data is solely responsible for securing it from end to end.

The division of responsibilities between cloud customers and cloud providers depends on the cloud service model in use (infrastructure, platform, or software as a service), as illustrated by the figure below.



In the Azure cloud, Microsoft is responsible for the security of the physical machines and the infrastructure within the Microsoft datacenter that hosts a customer's virtual machines (VMs). Microsoft endeavors to make its services secure by default, but it is the customer's responsibility to use those services in a secure way.

For example, the security within the confines of the VMs, such as data classification, access management, and application-level controls, is the responsibility of the customer. Likewise, the security of client and endpoint devices is the customer's responsibility. However, Microsoft provides tools that customers can use to protect cloud data and applications, and monitor and respond to security incidents that fall under your area of responsibility, such as:

- Encryption options. Many network encryption options are available to users to secure the network data for which they're responsible. These include Azure Disk Encryption, Azure Storage Service Encryption, and other encryption options as discussed in the preceding section.
- Azure Active Directory is the Microsoft multitenant, cloud-based directory, and identity management service that is built to work for apps in the cloud, on mobile, or on-premises.
- Azure Key Vault helps you increase security by safeguarding the cryptographic keys and other secrets (such as passwords) used by cloud apps and services.
- Azure Information Protection (AIP) (Rights Management Services) helps you classify your data based on sensitivity, define who can access data and what they can do with it, and track activities on shared data.
- Azure Security Center provides you with a unified view of security across all of your on-premises and cloud workloads, so you can find and fix vulnerabilities before they can be exploited.
- Antimalware protection. Azure offers Microsoft Antimalware for Azure to protect cloud services and virtual machines, and also employs intrusion detection, distributed denial-of-service (DDoS) attack prevention, and regular penetration testing.

Learn more: Shared Responsibilities for Cloud Computing explains the relationship between cloud service providers and their customers, and delineates their roles and responsibilities.

Privacy:

Azure gives customers ownership and control of their data

Microsoft understands that when you use Azure, you are entrusting us with your most valuable asset—your data. You trust that its privacy will be protected and that it will be used only in a way that is consistent with your expectations.

For many organizations, keeping your data private is no longer merely desirable—it's mandatory. Government and industry regulations require that you protect the privacy of certain types of data. Breaches that expose personal information can have serious consequences.

The Microsoft approach to privacy is grounded in its commitment to give you control over the collection, use, and distribution of your customer data. Knowledge is the key to controlling your data, and with Azure:

- You know how Microsoft manages your data. Microsoft uses your customer data only to provide the services agreed upon and does not mine it for marketing or advertising. If you leave the service, Microsoft takes the necessary steps to ensure the continued ownership of your data.
- You know where your data is located. Customers who want to maintain their data in a specific geographic location can rely on the expanding network of Azure datacenters around the world. Microsoft also complies with international data protection laws regarding transfers of customer data across borders.
- You know who can access your data and on what terms. Microsoft takes strong measures to protect your data from inappropriate access, including restrictions that limit access for Microsoft personnel and subcontractors. However, you can access your own customer data at any time and for any reason.
- You know how Microsoft responds to government and law enforcement requests to access your customer data. Microsoft will not disclose customer data hosted in the Microsoft Cloud to a government or law enforcement except as you direct or where required by law.

How Microsoft manages your data

With Azure, you are the owner of your customer data and you retain all right, title and interest in the data. You can access your own customer data at any time and for any reason without assistance from Microsoft.

Microsoft does not share customer data for advertising. Your data is your business. Microsoft does not share business customer data with Microsoft advertiser-supported services, or mine it for marketing or advertising. Microsoft uses your Azure customer data only to provide the service and for purposes compatible with providing the service, including day-to-day operations and troubleshooting.

When Microsoft deletes your data

If you end your Azure subscription, Microsoft will retain your customer data for a period of time as specified in the Microsoft Online Services Terms so you can extract the data. After the specified retention period ends, Microsoft will delete the customer data and personal data unless Microsoft is permitted or required by applicable law to retain such data or is authorized to do so in the agreement.

If you leave the Azure service or your subscription expires, Microsoft is governed by strict standards and follows specific processes that adhere to the contractual agreement for:

- Removing customer data from cloud systems under its control within specified time frames.
- Overwriting storage resources before reuse.
- Physical destruction of decommissioned hardware.

Learn more about how Microsoft handles data upon service termination. Download Data Protection in Azure and see "Data Deletion" on page 21.

Where your data is located

As a customer of Azure services, you know where your data is stored. Azure offers an ever-expanding network of datacenters across the globe.

- Most Azure services permit you to specify the region where your customer data will be stored.
- Microsoft does not control or limit the locations from which you or your users may access, copy, or move customer data. Customers and their end users may move, copy, or access their customer data from any location globally.
- Microsoft may replicate customer data to other regions for data resiliency, but will not replicate or move customer data outside the geographic region.
- Microsoft complies with international data protection laws for transfers of customer data across borders.
- Microsoft will not transfer to any third party (not even for storage purposes) data that you provide to Microsoft through the use of Azure services that are covered under the Microsoft Online Services Terms.

Find Azure datacenter locations and get information about data storage for both regional and global services.

Learn more: Where your data is located

Microsoft defines customer data as "all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, the customer using the online service." For example, this includes data that you upload for storage or processing and applications that you run in Azure.

Who can access your data and on what terms

Microsoft takes strong measures to help protect your customer data from inappropriate access or use by unauthorized persons. In addition to the physical and technological protections discussed in the Security section of this paper. These include restricting access by Microsoft personnel and subcontractors, and carefully defining requirements for responding to government requests for customer data.

You can access your customer data at all times. You can retrieve a copy of Azure customer data at any time and for any reason without the need to notify Microsoft or ask for assistance. At all times during the term of your Azure subscription, you can access, extract, and delete your customer data stored in Azure. You can also take your customer data with you if you end your subscription.

How Microsoft limits access to customer data. The operational processes that govern access to customer data in Microsoft business cloud services are protected by technical and organizational measures that include strong authentication and access controls, both physical and logical.

- Access to physical datacenter facilities is guarded by outer and inner perimeters with increasing security at each level.

  Learn more about how Azure secures its datacenters.

- Virtual access to customer data is restricted based on business need by role-based access control, multifactor authentication, minimizing standing access to production data, and other controls.

  Learn more about how Azure controls access to your data.

- To ensure control over encrypted data, you have the option to generate and manage your own encryption keys, determine who is authorized to use them, and revoke Microsoft copies of your encryption keys.

  Learn more about how Azure protects your data.

Azure is a multitenant service. This means your data, deployments, and virtual machines may be stored on the same physical hardware as that of other customers. Microsoft uses logical isolation to segregate storage and processing for each customer to help ensure that your customer data is not combined with anyone else's.

Microsoft limits access to your customer data by its personnel. Microsoft has automated most of its service operations so that only a small set requires human interaction.

- Microsoft engineers do not have default access to cloud customer data. Instead, they are granted access under management oversight and only when necessary.
- Microsoft personnel will use customer data only for purposes compatible with providing the contracted services. These may include troubleshooting aimed at preventing, detecting, or repairing problems affecting the operation of Azure, and the improvement of features such as protecting against threats, like malware.

Microsoft limits access to your customer data by subcontractors whom it hires to provide limited services on its behalf.

- Subcontractors can access and use customer data only to deliver the services they were hired to provide.
- The Microsoft Online Services Subcontractor List discloses the names of subcontractors who have access to customer data and provides advance notice of new subcontractors.

Learn more: Who can access your data and on what terms

Microsoft notifies you in case of a security breach. If Microsoft becomes aware of a breach of security that results in unauthorized access or disclosure of your customer data, Microsoft will:

- Promptly notify you of the security incident.
- Investigate the security incident and provide you with detailed information about it.
- Take reasonable steps to mitigate the effects and to minimize any resulting damage.

The Microsoft approach to privacy is grounded in its commitment to give you control over the collection, use, and distribution of your customer data.

How Microsoft responds to government requests for customer data

Microsoft imposes carefully defined requirements on government and law enforcement requests for customer data. Such requests for customer data must comply with applicable laws. When governments or law enforcement agencies make a lawful request for customer data, Microsoft is committed to transparency and limits what it discloses.

- Microsoft will not disclose customer data hosted in Azure to a government or law enforcement except as you direct or where required by law. Microsoft does not give any third party, including law enforcement and government entities, direct or unfettered access to customer data.
- Microsoft always attempts to redirect third-party requests to you.

If Microsoft is compelled by law to disclose customer data, you will be promptly notified and provided with a copy of the request, unless Microsoft is legally prohibited from doing so. Microsoft takes care to provide only the data specified in the legal order.

- Microsoft has taken steps to ensure that there are no "back doors" for use in government surveillance, and Microsoft does not provide any government with encryption keys or the ability to break the encryption that protects customer data.

Microsoft demonstrates its commitment to transparency by publishing semi-annual reports regarding requests for customer data made by law enforcement agencies. The Law Enforcement Requests Report site provides you with information about such requests made for customer data.

Learn more: Get detailed Microsoft data privacy standards.

Privacy is built into the Azure infrastructure, and is governed by Microsoft privacy policies and the Microsoft Privacy Standard, the cornerstone of the Microsoft privacy program.

Microsoft sets and adheres to stringent privacy standards

Microsoft is transparent about the specific policies, operational practices, and technologies that help ensure the privacy of your data in Microsoft business cloud services.

Microsoft builds privacy protections into Azure

Privacy is built into the Azure infrastructure, governed by Microsoft privacy policies and the Microsoft Privacy Standard, the cornerstone of the Microsoft privacy program. This authoritative document delineates the general privacy requirements for developing and deploying all Microsoft products and services, including Azure.

Standards and processes that support these principles include the Microsoft Online Services Privacy Statement (which details Microsoft core data protection policies and practices) and the Microsoft Security Development Lifecycle (which integrates privacy requirements in the software development process).

Microsoft contractual commitments back its privacy best practices

Microsoft backs these privacy protections with strong contractual commitments to safeguard customer data, including:

ISO/IEC 27018. Microsoft was the first major cloud provider to adopt the first international code of practice for cloud privacy. An independent audit has verified that Azure is aligned with the ISO/IEC 27018 code of practice.

EU Model Clauses. EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). Microsoft EU Standard Contractual Clauses provide specific contractual guarantees around transfers of personal data for covered services, which Europe's privacy regulators have determined meet EU standards for international transfers of data.

EU-U.S. Privacy Shield. Microsoft is certified to the EU-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the EU to the United States. Microsoft also abides by Swiss data protection law regarding the processing of personal data from the EEA and Switzerland.

FERPA. The Family Educational Rights and Privacy Act (FERPA) is a US federal law that protects the privacy of student educational records. Microsoft agrees to the use and disclosure restrictions imposed by FERPA on Azure.

HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure and Azure Government offer customers a HIPAA Business Associate Agreement (BAA).

HITRUST. The Health Information Trust (HITRUST) Alliance created and maintains the Common Security Framework (CSF) to help healthcare organizations and cloud providers demonstrate their security and compliance.

LOPD (Spain). Microsoft was the first hyperscale cloud service provider to receive an authorization from the Spanish Data Protection Agency for its compliance with the high standards governing international data transfer under Spanish Organic Law 15/1999 (Ley Orgánica 15/1999 de Protección de Datos, or LOPD). Microsoft is also the first hyperscale cloud service provider to obtain a third-party audit certification for its online services' compliance with the security measures set forth in Title VIII of Royal Decree 1720/2007.

My Number Act (Japan). The "My Number" system created by Japan's legislature establishes a personal identification number assigned to every resident, foreign and domestic. Microsoft does not have standing access to My Number data stored in Azure; however, Microsoft contractually commits that Azure has implemented technical and organizational security safeguards to help customers protect individuals' privacy.

PDPA (Argentina). In a data transfer agreement, Microsoft makes a contractual commitment that Azure in-scope services have implemented the applicable technical and organizational security measures stated in Regulation 11/2006 of the Argentine Data Protection Act. It also makes important commitments regarding notifications, auditing of our facilities, and use of subcontractors.

PIPEDA, PIPA, and BC FIPPA (Canada). The Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta Personal Information Protection Act (PIPA), and British Columbia Freedom of Information and Protection of Privacy Act (BC FIPPA) are Canadian privacy laws that require organizations to take reasonable steps to safeguard information in their custody or control. Microsoft contractually commits that Azure and Intune in-scope services have implemented security safeguards to help protect the privacy of individuals, based on established industry standards.

EU General Data Protection Regulation (GDPR). The European Union's GDPR became enforceable on May 25, 2018. The GDPR sets a new bar globally for privacy rights, security, and compliance. It imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU, or that collect and analyze the personal data of everyone residing in the EU, whether or not they are citizens. The GDPR applies to such organizations no matter where they are located.

Microsoft has developed the following materials to help you prepare for compliance with the GDPR:

- Overview of the GDPR serves as an introduction to GDPR and its key concepts
- How Azure Can Help Organizations Become Compliant with the EU GDPR
  This white paper, written for decision makers, privacy officers, and security and compliance personnel, helps organizations identify and catalog personal data in Azure systems, build more secure environments, and simplify management of GDPR compliance.

  Learn more: visit the Microsoft GDPR home page

Microsoft tools simplify your privacy burden

Microsoft simplifies your privacy burden with tools to help you automate privacy. Built-in controls, configuration management tools, and data subject request tools accelerate your compliance and save you money.

Azure Information Protection. You can add classification and protection information for persistent protection that stays with your data regardless of where it's stored or with whom it's shared. Azure Information Protection lets you configure policies to classify, label, and protect data based on its sensitivity. Classification is fully automatic, driven by users, or based on recommendation.

You can choose how your encryption keys are managed, and you can track activities on shared data and revoke access if necessary. Data classification and protection controls are integrated into Microsoft Office and common applications.

Azure Policy. You can define and enforce policies that help your cloud environment become compliant with internal policies as well as external regulations using Azure Policy. You can build custom policies with flexibility or apply built-in policies from Microsoft to govern your Azure resources.

Azure Data Subject Request (DSR) Portal. The GDPR gives data subjects specific rights to their personal data; these rights include obtaining copies of personal data, requesting corrections to it, restricting the processing of it, deleting it, or receiving it in an electronic format so it can be moved to another controller. A formal request by a data subject to a controller to take an action on their personal data is called a Data Subject Request or DSR.

The Azure Data Subject Request (DSR) portal enables you to fulfill GDPR requests and shows you how to use Microsoft products, services, and administrative tools to find and act on personal data that resides in the Microsoft cloud to respond to DSRs.

Learn more about: Azure Information Protection

Compliance:

Azure conforms to global standards

Compliance plays a critical role in providing assurance for customers, and is an important element in the trust relationship. Through rigorous and widely recognized formal standards that are certified by independent third parties, Microsoft helps organizations comply with constantly shifting requirements and regulations governing the security, collection, and use of individuals' data.

Azure offers a broad set of key global and industry-specific standards and supporting materials for key regulations, including ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1, 2, and 3Reports. Azure also meets regional and national standards that include the EU Model Clauses, EU-U.S. Privacy Shield, Singapore MTCS, and the CS Mark in Japan. You'll find a complete list of Azure compliance offerings below.

Rigorous audits (many of which require annual review of Azure facilities and capabilities) are conducted by independent accredited third parties such as BSI and Deloitte, which validate Azure's adherence to these standards.

Through its long-standing relationship with the legal and compliance community, Microsoft has developed a wealth of resources for professionals who need relevant information on the key regulatory and compliance considerations associated with cloud computing. This includes both privacy law requirements that apply across all industries, and sector-specific guidelines and regulations.

While it is up to you to determine whether Azure services comply with the specific laws and regulations that are applicable to your business, we help you make these assessments, by providing the specifics of our compliance programs, including audit reports and compliance packages. Your auditors can compare Azure results with your own legal and regulatory requirements, and you can verify the Azure implementation of controls by requesting detailed audit results and reports, many of which are free to Azure customers and trial customers through the Service Trust Platform.

Learn more: For the most current information about Azure compliance, visit the Microsoft Trust Center compliance offerings and choose Azure from the Product or Service list.

Azure compliance offerings

Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider to help you comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data.

These include compliance offerings that are: globally applicable, US government regulations, other region- or country-specific regulations, and industry-specific requirements. Below is a list of our compliance offerings as of October 2019.

Globally applicable offerings

Compliance offerings covered in this section have global applicability across regulated industries and markets. They can often be relied upon by customers when addressing specific industry and regional compliance obligations.

- **CIS Benchmark.** The Center for Internet Security Microsoft Azure Foundations Benchmark.
- **CSA STAR Attestation.** The Cloud Security Alliance audit of a cloud provider's security posture.
- **CSA STAR Certification.** The Cloud Security Alliance certification that involves an independent third-party assessment of a cloud provider's security posture.
- **CSA STAR Self Assessment.** The Cloud Security Alliance level 1 offering that is free and open to all cloud services providers.
- **ISO/IEC 20000-1:2011.** International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) certification in Information Technology Service Management.
- **ISO 22301.** International Organization for Standardization (ISO) Business Continuity Management Standard.
- **ISO/IEC 27001.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Information Security Management Standards.
- **ISO/IEC 27017.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Code of Practice for Information Security Controls.
- **ISO/IEC 27018.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Code of Practice for Protecting Personal Data in the Cloud.
- **ISO 9001.** International Organization for Standardization Quality Management Systems Standards.
- **SOC 1, 2, and 3.** Service Organization Controls standards for operational security.
- **WCAG 2.0.** Web Content Accessibility Guidelines 2.0.

US government

The following compliance offerings are focused primarily on addressing the needs of US Government. Azure, Azure Government, and Azure Government for DoD have the same comprehensive security controls in place, as well as the same Microsoft commitment on the safeguarding of customer data.

- **CJIS**. Criminal Justice Information Services Security Policy.
- **DFARS.** Defense Federal Acquisition Regulation Supplement for defense contractors.
- **DoD DISA L2, L4, L5.** US Department of Defense Provisional Authorization.
- **DoE 10 CFR Part 810.** Department of Energy Code of Federal Regulations.
- **EAR.** US Export Administration Regulations.
- **FDA CFR Title 21 Part 11.** Food and Drug Administration Code of Federal Regulations.

Microsoft offers the most comprehensive set of compliance offerings of any cloud service provider—the deepest and broadest coverage in the industry.

- **FedRAMP.** Federal Risk and Authorization Management Program.
- **FERPA.** Family Educational Rights and Privacy Act.
- **FIPS 140-2.** Federal Information Processing Standard.
- **IRS 1075.** US Internal Revenue Service Publication.
- **ITAR.** International Traffic in Arms Regulations.
- **NIST 800-171.** National Institute of Standards and Technology Special Publication on Protecting Unclassified Information in Nonfederal Information Systems and Organizations.
- **NIST Cybersecurity Framework (CSF).** National Institute of Standards and Technology Cybersecurity Framework.

Other region- and country-specific regulations

The following compliance offerings are specific to various regional and national laws and regulations. Some of these offerings are based on independent third-party certifications and attestations; others provide contract amendments and guidance documentation to help customers meet their own compliance obligations.

- **Argentina PDPA.** Personal Data Protection Act 25,326.
- **Australia IRAP Unclassified.** Information Security Registered Assessors Program.
- **Australia IRAP PROTECTED.** Information Security Registered Assessors Program highly sensitive data security level.
- **Canada Privacy Laws.** Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta Personal Information Protection Act (PIPA), and British Columbia Freedom of Information and Protection of Privacy Act (BC FIPPA).
- **China GB 18030:2005.** Chinese Coded Character Set standard set by the China Electronics Standardization Institute (CESI).
- **China DJCP (MLPS) Level 3.** Information Security Technology—Basic Requirements for Classified Protection of Information System Security (multilevel protection scheme).
- **China TRUCS / CCCPPF.** Trusted Cloud Service Certification.
- **EU EN 301 549.** European Union Accessibility Requirements Suitable for Public Procurement of ICT Products and Services.
- **EU ENISA IAF.** The European Union Agency for Network and Information Security Information Assurance Framework.
- **EU GDPR.** European Union General Data Protection Regulation.
- **EU Model Clauses.** European Union data protection law Standard Contractual Clauses.
- **EU-US Privacy Shield.** Designed by the U.S. Department of Commerce, and the European Commission.
- **Germany C5.** Cloud Computing Compliance Controls Catalog.
- **Germany IT-Grundschutz workbook.** IT-Grundschutz workbook for Internet and cloud usage.
- **India MeitY.** Ministry of Electronics and Information Technology accreditation for public cloud, government virtual private cloud, and government community cloud.
- **Japan CS Mark Gold.** Cloud Security Gold Mark for IaaS and PaaS.
- **Japan My Number Act.** Social Benefits and Tax Number resident identification number system.
- **Netherlands BIR 2012.** Baseline Informatiebeveiliging Rijksdienst standard.
- **New Zealand Gov CC Framework.** New Zealand Government Cloud Computing Security and Privacy Considerations.

- **Singapore MTCS Level 3.** Multi-Tier Cloud Security Standard for Singapore certification for IaaS, PaaS, and SaaS.
- **Spain ENS High.** Spain Esquema Nacional de Seguridad (ENS) High Level Security Measures.
- **Spain DPA.** Spanish Data Protection Agency guidelines.
- **TISAX (Germany).** Trusted Information Security Assessment Exchange.
- **UK Cyber Essentials Plus.** Cyber Essentials PLUS requirements outlined in the Cyber Essentials Scheme Assurance Framework.
- **UK G-Cloud.** United Kingdom Government-Cloud services classification v6.
- **UK PASF.** United Kingdom Police Assured Secure Facility standards.

Industry-specific

The following compliance offerings are intended to address the needs of customers subject to various industry regulations such as those in financial services, healthcare and life sciences, media and entertainment, and education. Azure is not subject directly to oversight by these regulators; however, Azure can help customers meet their own compliance requirements.

- **23 NYCRR Part 500.** New York State cybersecurity requirements for licensed financial institutions.
- **AFM and DNB (Netherlands).** Dutch Authority for the Financial Markets (Autoriteit Financiële Markten, AFM) and the Dutch Central Bank (De Nederlandsche Bank, DNB) financial services regulations.
- **AMF and ACPR (France).** The French Financial Authority (Autorité des Marchés Financiers, AMF) and the French Prudential Authority (Autorité de Contrôle Prudentiel et de Résolution, ACPR) financial services and insurance industry regulations.
- **APRA (Australia).** The Australian Prudential Regulation Authority (APRA) regulations for banks, credit unions, insurance companies, and other financial services institutions.
- **CDSA.** The Content Delivery & Security Association (CDSA) Content Protection & Security (CPS) Standard.
- **CFTC 1.31.** The United States Commodity Futures Trading Commission (CFTC) Rule 1.31 recordkeeping requirements.
- **DPP (UK).** The Digital Production Partnership (DPP) and North American Broadcasters Association (NABA) broadcasters cybersecurity requirements.
- **EBA (EU).** European Banking Authority.
- **FACT (UK).** Federation Against Copyright Theft.
- **FCA and PRA (UK).** Financial Conduct Authority and Prudential Regulation Authority.
- **FFIEC.** The US Federal Financial Institutions Examination Council.
- **FINMA (Switzerland).** The Swiss Financial Market Supervisory Authority.
- **FINRA 4511.** The Financial Industry Regulatory Authority Rule 4511.
- **FISC (Japan).** The Center for Financial Industry Information Systems.
- **FSA (Denmark).** The Danish Financial Supervisory Authority.
- **GLBA.** The Gramm-Leach-Bliley Act regulating the US financial services industry.
- **GxP.** Good Clinical, Laboratory, and Manufacturing Practices (GxP), and regulations enforced by the US Food and Drug Administration (FDA) under CFR Title 21 Part 11.
- **HDS (France).** Health Data Hosting (Hébergeurs de Données de Santé, HDS) certification.
- **HIPAA/HITECH.** Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health.

- **HITRUST.** Health Information Trust Alliance.
- **KNF (Poland).** The Polish Financial Supervision Authority (Komisja Nadzoru Finansowego).
- **MARS-E.** The Center for Medicare and Medicaid Services Minimum Acceptable Risk Standards for Exchanges.
- **MAS + ABS (Singapore).** Monetary Authority of Singapore (MAS) and the Association of Banks in Singapore.
- **MPAA.** Motion Picture Association of America.
- **NBB and FSMA (Belgium).** National Bank of Belgium (NBB) and the Financial Services and Markets Authority.
- **NEN-7510 (Netherlands).** Dutch Standardisation Institute healthcare standard.
- **NERC.** North American Electric Reliability Corporation.
- **NHS IG Toolkit (UK).** National Health Service Information Governance toolkit.
- **OSFI (Canada).** Office of the Superintendent of Financial Institutions.
- **PCI DSS.** Payment Card Industry Data Security Standards.
- **RBI and IRDAI (India).** The Reserve Bank of India and Insurance Regulatory and Development Authority of India.
- **SEC 17a-4.** United States Securities and Exchange Commission.
- **Shared Assessments.** Shared Assessment Program formerly known as BITS Shared Assessments, used in the banking industry.
- **SOX.** Sarbanes-Oxley Act of 2002, administered by the Securities and Exchange Commission.
- **TISAX (Germany).** Trusted Information Security Assessment Exchange for the automotive industry.

Compliance tools and guidance

Frequent updates to the laws and rules from the many regulatory bodies around the world create a challenge for organizations. Compliance personnel need assistance to help meet evolving requirements. Microsoft helps customers meet compliance obligations by providing an extensive repository of resources that include tools, documentation, and guidance.

Microsoft Trust Center

The Microsoft Trust Center is your resource for learning how we implement and support security, privacy, compliance, and transparency in all our cloud products and services. The Trust Center features a comprehensive set of all current certifications, attestations, and other compliance offerings.

Service Trust Center

The Service Trust Portal contains additional guidance and tools to help meet your security, compliance, and privacy needs when using Azure and other Microsoft Cloud services. These audit reports, Azure Security and Compliance Blueprints, and trust documents to help you understand cloud features, and to verify technical compliance and control requirements.

Azure Blueprints

The Azure Blueprint service helps customers build Azure applications that are secure and comply with many regulations, including the GDPR and HIPAA, both internally and externally. They also help simplify large scale Azure deployments by packaging key environment artifacts, such as Azure Resource Manager templates, resource groups, role-based access controls, and policies, in a single blueprint definition.

Microsoft helps customers meet compliance obligations by providing an extensive repository of resources that include tools, documentation, and guidance.

This free service provides you with templates to create, deploy, and update fully governed cloud environments to consistent standards and comply with regulatory requirements. It differs from Azure Resource Manager (ARM) and Azure Policy in that Blueprints is a package that contains different types of artifacts—including Resource Manager templates, resource groups, policy assignments, and role assignments—all in one container, so you can quickly and easily deploy all these components in a repeatable configuration.

You can use the built-in blueprints or create your own custom blueprints. Blueprints can be created in the Azure portal or using the REST API with tools such as PowerShell. If the latter method is used, you can define blueprint parameters to prevent conflicts when reusing certain blueprints.

Implementation guidance

Organizations face many challenges in achieving their compliance goals. Microsoft provides guidance to help Azure customers reach those goals and comply with industry and government regulations in the cloud:

- Overview of Microsoft Azure Compliance
- How Microsoft Azure Can Help Organizations Become Compliant with the EU GDPR
- A Practical Guide to Designing Secure Health Solutions using Microsoft Azure
- Microsoft Azure HIPAA/HITECH Act Implementation Guide

Resiliency/Reliability:

Azure keeps your applications up and running and your data available

Resiliency is not about avoiding failures but responding to failures. The objective is to respond to failure in a way that avoids downtime and data loss. Business continuity and data protection are critical issues for today's organizations, and business continuity is built on the foundation of resilient systems, applications, and data.

Reliability and resiliency are closely related. Reliability is defined as dependability and performing consistently well. Resiliency is defined as the capacity to recover quickly. Together, these two qualities are key to a trustworthy cloud service.

Despite your best efforts, disasters happen; they are inevitable but mostly unpredictable, and vary in type and magnitude. There is almost never a single root cause of a major issue. Instead, there are several contributing factors, which is the reason an issue is able to circumvent various layers of mitigations/defenses.

There is no way to always prevent bad things from happening. All we can do is add layers and minimize gaps.

Making systems reliable

Making systems reliable in the public cloud is not the same as in your own datacenter. The cloud is an ever-changing, constantly evolving platform, unlike the usual on-premises IT model where you can achieve greater availability by avoiding change. In the public cloud, change is both inevitable and beneficial, but you must plan for it.

Complex systems can fail in complex ways, and you need resilience to deliver reliability. Reliability is the goal, whereas resilience is the method by which you achieve that goal.

Achieving resilience

Resilience begins with availability. Reducing the amount of downtime and the number of disruptions to service is important to the continued operation of your core business functions. Organizations today are dependent on their online presence for communications with vendors, sales to customers, financial transactions, and more. Downtime means lost revenue and can damage your business reputation.

High availability is about providing undisrupted continuity of operations whereas disaster recovery is about recovering from a natural or human-induced outage and providing continuity of operations. Disaster recovery usually involves some amount of downtime.

The direct and indirect monetary cost of down time for your organization depends on several factors, including your field of business, how you do business (percentage of sales made online), total revenues, time of day or day of week, and so forth. According to the

Azure was the first cloud platform to provide a built-in backup and disaster recovery solution.

Ponemon Institute, the average cost of a datacenter outage can be $9000 per minute.

An effective disaster recovery strategy has two parts: preparedness and recovery. The two are closely related but are not the same. Preparedness is the theoretical plan for the procedures you will follow in response to a catastrophic event, whether it's physical destruction of systems due to a natural disaster or a devastating cyberattack. Recovery is the actual implementation of the processes that make up that plan.

Your data is a valuable asset. According to multiple studies, the leading cause of data loss is human error, attributable to both users and IT professionals. Better training and tighter access controls can help reduce the incidence, but data loss can still occur. To implement a full recovery, you need a good backup system so that if your data is lost or corrupted, you can restore it.

Azure helps you to avoid many potential disasters and quickly recover if your organization does get hit by disaster. Azure offers resiliency for your cloud-based applications and data by providing for business continuity in the following ways:

- High availability
- Disaster recovery
- Backup
- Resilient app design best practices

Availability is often expressed as percentage of uptime, using a "table of nines." For example, if the level of availability over a year is 99.99%, it is said to be "four nines." This translates to average downtime of 1.01 minutes per week, 4.32 minutes per month, or a total of 52.56 minutes per year.

Shared responsibility

Just as security is a responsibility that's shared between cloud provider and customer, building systems that will survive failure is also a shared responsibility. Microsoft builds and operates the resilient foundation, then you choose to enable relevant services to help with your resiliency needs. Your apps and workloads sit on top of both.

Azure resilient foundation

Everything is built on top of the resilient foundation, which is a requirement for any application to achieve resiliency. To achieve resilience—the application on top has to take advantage of the resilient services built on the foundation.

The three pillars of the Azure resilient foundation are:

- Design: How Microsoft designs its global fiber network, evolving datacenters, and storage protections built into the Azure platform.
- Operate: How Microsoft rolls out releases into the environment, performs maintenance (planned and unplanned), and uses machine learning to predict failures and protect customer workloads.
- Observe: How customers can observe what's happening in their environment(s), inform people and systems to make informed decisions before/during issues, and determine their own availability requirements.

IT systems are subject to failure. If all your systems and data are located on your premises, a fire, flood, tornado, or other natural disaster can bring your operations to a halt for weeks or months. When your applications and data are hosted on a cloud service, you have redundant, distributed implementations of your IT resources across physical locations.

Even in the cloud, however, hardware can fail, the network can have transient failures, and rarely, an entire service or region may experience a disruption. Thus, your cloud service provider's dedication to business continuity is vital. Azure provides a comprehensive set of native business continuity solutions that protect you against failures within datacenters and even the failure of entire datacenters.

Business continuity is based on the ability to perform essential business functions during and after adverse conditions, such as a natural disaster or a downed service. Azure is the first hyperscale cloud provider to be certified under ISO-22301, the first international standard to demonstrate the ability to prevent, mitigate, respond to, and recover from disruptive incidents.

The reliability and performance of cloud services are determined in part by the network and (in addition to having more datacenter regions than any of our competitors) the Microsoft network is also one of the largest in the world. Unlike with many other public cloud providers, data that traverses between Azure datacenters and regions doesn't go through the public internet—it stays in the Microsoft network.

High availability

A key aspect of a resilient foundation is availability. High availability is all about maintaining acceptable continuous performance despite temporary failures in services, hardware, or datacenters, or fluctuations in load. Highly available systems are consistently operational over long periods of time.

Azure uptime, expressed as a rolling 12 month average to June 2019, was 99.996%, or approximately 26 minutes of downtime per year. Availability can never be 100% because hardware and software failures happen, and human error occurs. But the Service Level Agreement (SLA) describes our commitment for uptime and connectivity. Microsoft provides SLAs that define the guaranteed availability levels for each Azure service. Microsoft also provides support for high availability at the virtual machine, datacenter, and regional levels, through a number of features and functions across the categories of compute, storage, and networking.

Traffic Manager and Load Balancer can be used individually, or you can use them together or in combination with Azure Application Gateway to create a deployment that is geographically redundant.

Azure Availability Zones. This provides redundancy at the regional level. It is a high-availability offering that protects your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region. The physical separation of Availability Zones within a region protects applications and data from datacenter failures. With Availability Zones, Azure offers industry best 99.99% virtual machine uptime SLA.

Learn more about Azure Availability Zones.

Availability Sets. This provides redundancy at the datacenter level. An Availability Set is a logical grouping capability that you can use in Azure to ensure that the VM resources you place within it are isolated from each other when they are deployed within an Azure datacenter. If a hardware or Azure software failure occurs, only a subset of your VMs are impacted, and your overall application stays up and continues to be available to your customers.

Learn more about deploying highly available VMs by creating an Availability Set.

Data residency boundary. This provides redundancy across two regions that share the same regulatory requirements for data replication and storage. Your data is protected from loss of an entire region with geo-redundant storage and Azure Site Recovery.

Learn more about Azure Regions.

Azure Load Balancer. Load Balancer can scale your applications and create high availability for your services. Load Balancer automatically scales with increasing application traffic, and you can use the internal load balancer for traffic between virtual machines inside your private network.

Learn more about Azure Load Balancer.

Azure Traffic Manager. This is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.

Learn more about choosing the correct Azure load balancing solution.

Azure compute resiliency solutions. You can apply autoscaling to virtual machines for high availability and easily spread your workloads across the virtual machines in your virtual machine scale set.

Network support for high availability. You can deploy VPN and ExpressRoute gateways in Azure Availability Zones. This brings resiliency, scalability, and higher availability to virtual network gateways. Deploying gateways in Azure Availability Zones physically and

logically separates gateways within a region, while protecting your on-premises network connectivity to Azure from zone-level failures.

Highly available storage options. The data in your Azure storage account is always replicated to ensure durability and high availability. Azure Storage replication copies your data so that it is protected from planned and unplanned events ranging from transient hardware failures, to network or power outages, to massive natural disasters, and so on. You can choose to replicate your data within the same datacenter, across zonal datacenters within the same region, and even across regions.

When you create a storage account, you can select one of the following replication options:

- Locally redundant storage (LRS) replicates your data within a storage scale unit that is hosted in a datacenter in the region in which you created your storage account.
- Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region, where each storage cluster is physically separated from the others and resides in its own availability zone.
- Geo-redundant storage (GRS) replicates your data to a secondary region that is hundreds of miles away from the primary region.
- Read-access geo-redundant storage (RA-GRS) provides read-only access to the data in the secondary location, in addition to geo-replication across two regions.

Learn more about these Azure storage replication options.

Disaster recovery

Your disaster recovery strategy is key to business continuity. Site recovery and data backup are elements of a disaster recovery plan. Organizations using the cloud tend to take the reliability of the public cloud for granted, not recognizing that they may be responsible for choosing and implementing backup and recovery mechanisms.

As a cloud customer, you will confront more opportunities to spend extra time and money on optional backup than you can ever take advantage of, so you need to make explicit and careful choices as to what you will and will not do.

Your disaster recovery plan should:

1. **Identify** and classify the threats and risks that may lead to disasters.
2. **Define** the resources and processes that ensure business continuity during the disaster.
3. **Define** the reconstitution mechanism to get the business back to normal from the disaster recovery state, after the effects of the disaster are mitigated.

An effective disaster recovery plan plays its role in all stages of operations and it is continuously improved by disaster recovery mock drills and feedback capture processes.

Disaster recovery happens in the following sequential phases:

1. **Activation Phase:** In this phase, the disaster effects are assessed and announced.
2. **Execution Phase:** In this phase, the actual procedures to recover each of the disaster-affected Azure services are executed. Business operations are restored into the Azure paired region.
3. **Reconstitution Phase:** In this phase the original Azure region hosted system/service is restored, and execution phase procedures are stopped.

Microsoft provides tools and services to help you implement and test your disaster recovery plan.

Azure Site Recovery is the Azure built-in disaster recovery as a service (DRaaS) solution that can help keep your applications up and running during an IT outage. You can ensure compliance by testing your disaster recovery plan without impacting production workloads

or end users and keep applications available during outages with automated recovery from on-premises to Azure or Azure to another Azure region.

Azure helps you to reduce the cost of deploying, monitoring, patching, and maintaining on-premises disaster recovery infrastructure by eliminating the need for building or maintaining a costly secondary datacenter. You pay only for the compute resources you need to support your applications in Azure.

Several different types of disaster scenarios can affect a customer's current Azure infrastructure topology. Region-wide service disruptions are not the only cause of application-wide failures. Poor design and administrative errors can also lead to outages. It's important to consider the possible causes of a failure during both the design and testing phases of your disaster recovery plan. A good plan takes advantage of Azure features and augments them with application-specific strategies.

Learn more about Azure Site Recovery.

Backup

Azure Backup helps you reduce data restoration time and reliability challenges. It's built into the Azure platform, with seamless support for virtual machines running in Azure and on-premises. It's cost effective because it doesn't require any additional infrastructure. Multiple authentication layers help to keep your data safe and guard against loss from ransomware.

Data backup is a critical part of disaster recovery. If the stateless components of an application fail, you can always redeploy them. If data is lost, the system can't return to a stable state. Data must be backed up, ideally in a different region in case of a region-wide disaster.

Azure provides resiliency for your databases. Azure Backup automatically discovers if a selected virtual machine is running SQL and backs up your SQL database natively with support for fifteen-minute recovery time objective (RTO). Azure also provides data resiliency. You can back up important files natively in Azure, with item-level restore. Azure Backup supports full, differential, and incremental backup.

Backup is distinct from data replication. Data replication involves copying data in near real time, so that the system can fail over quickly to a replica. Data replication can reduce the length of time it takes to recover from an outage by ensuring that a replica of the data is always standing by. However, data replication won't protect against human error. If data is corrupted because of human error, the corrupted data just gets copied to the replicas.

Thus, you still need to include long-term backup in your disaster recovery strategy.

Learn more about Azure Backup.

Resilient app design best practices

Your mission-critical applications and data should be built for resiliency. One of the primary ways to make an application resilient is through redundancy. You need to plan for this redundancy when you design the application. The level of redundancy that you need depends on your business requirements; in general, there is a tradeoff between greater redundancy and reliability versus higher cost and complexity.

Azure has a number of features to make an application redundant at every level of failure, from an individual VM to an entire region. These include Availability Sets and Availability Zones as well as Azure Site Recovery and Azure Backup.

The Azure Architecture Center provides detailed information to get started quickly and build apps correctly the first time. This includes guidance on building for security, scalability, performance, cost, and manageability—including tested deployment scripts and verified recommendations for your production workloads.

Managing IP risks:

Azure helps protect your IP

Learn more about designing resilient applications for Azure.

In today's business world, companies produce not only tangible goods but also intellectual property (IP), including concepts, ideas, inventions, original artistic works, software code, logo designs, and identifying names.

Copyright, patent, trademark, and other intellectual property protections are designed to safeguard the IP owner's rights to derive the value from such creations of the human mind. This encourages creativity and innovation and allows creators and investors to benefit from their efforts and receive a return on their investment of time, mental energy, and/or money.

Business method and software patents provide a lucrative opportunity for non-practicing entities (NPEs), who stockpile large numbers of patents with no intention of developing products, but for the purpose of suing companies and individuals for infringement. This type of cloud-based patent litigation is increasing, and lawsuits and countersuits can cost your organization money and time and damage your reputation. The aggressive tactics of NPEs discourage innovation.

Trust in the cloud encompasses not only the assurance of security, privacy, compliance, and resiliency, but also clarity and confidence that your innovations will be protected against frivolous infringement claims, including when you co-develop innovative solutions working together with a cloud provider. Microsoft Azure IP Advantage and the Shared Innovation Initiative can help offer that assurance.

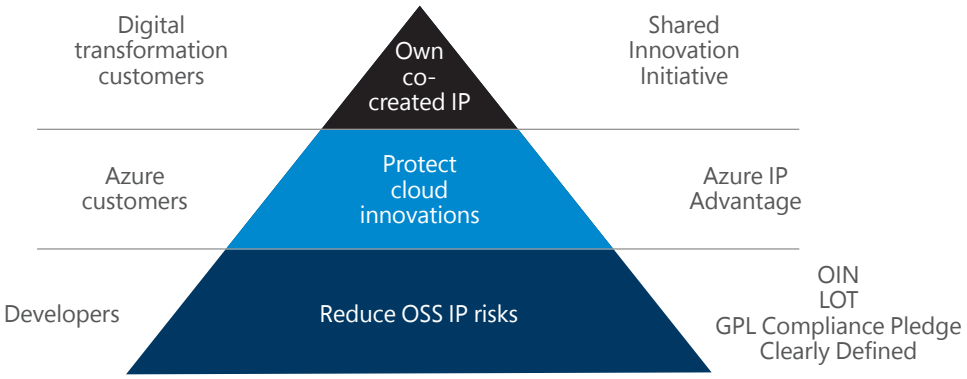
The following steps will get you started on the road to protecting your innovations and developing with confidence:

- Assess your cloud IP protection and business risks.
- Identify a plan to protect your innovation in the cloud.
- Continue your digital transformation with Microsoft Cloud as a trusted partner.

IP in the cloud

As computing shifts to the cloud, new risks to innovation emerge. These include risks to developers, to Azure customer organizations working in the cloud, and to customers who co-create intellectual property with Microsoft as part of their digital transformation.

Microsoft trust and IP initiatives build on one another to provide protections to all three of these categories.



Azure IP Advantage

Intellectual property is increasingly being created, stored, and shared in digital form. Digital transformation has brought a paradigm shift to the business environment as companies embrace new approaches to creating, communicating, and interacting with customers, partners, and the public.

NPEs see this as an opportunity; they collect and hoard patents and then assert patent infringement against innovators. This is a growing concern for cloud services customers, and the fear of a patent suit discourages innovation in the cloud. Cloud providers can help their customers reduce the risk to be able to innovate with confidence, and Microsoft Azure offers best-in-industry protection against IP risks. Azure IP Advantage includes:

- **Uncapped indemnification.** This covers claims for IP infringement and extends to open source software (OSS) incorporated by Microsoft in Azure services (for example, Apache Hadoop used for Azure HDInsight). It is provided by default for all Microsoft cloud customers.
- **Patent Pick.** Microsoft provides a portfolio of 10,000 patents that customers can pick from and use to deter and defend against patent lawsuits. It is available to consuming Azure customers with an Azure usage of $1k/m over the last three months who have not filed a patent infringement lawsuit against another Azure customer for their Azure workloads in the last two years. This helps to discourage excessive litigation.
- **Springing license.** This provides peace of mind with future patent protection; if Microsoft sells any of its patents to an NPE in the future, its customers will receive a license, so the NPE won't have an infringement suit against the customer. This is available to all consuming Azure customers with an Azure usage of $1k/m over the last three months. Unlike other cloud providers, Microsoft does not require a reciprocal commitment from the customer for its patents. In addition, Microsoft is a member of the LOT Network, a non-profit community of companies that was formed to preserve the traditional uses of patents while providing immunization against the patent troll problem.

These protections help free companies to concentrate more on building their businesses, leveraging open source software, and serving their customers, and less on dealing with patent litigation.

Shared Innovation Initiative

Every company today is becoming in part a software company. Companies are increasingly collaborating with their cloud providers to co-create intellectual property to transform their business operations. There is growing concern that without an approach

that ensures customers own key patents to these new solutions, tech companies will use the knowledge to enter their customers' market and compete against them—perhaps even using the IP that customers helped create.

Microsoft developed its Shared Innovation Initiative in response to these concerns when customers collaborate with Microsoft to develop new products and services that run on the Azure platform. We've created contract terms that lay out these principles for engagements where the parties are co-creating new IP. Shared Innovation builds on our approach outlined in the AIPA, and is based on seven guiding principles:

1. **Respect for ownership of existing technology.** We each own the existing technology and IP that we bring to the table when we partner together. As we work with customers, we'll ensure that we similarly will each own the improvements made to our respective technologies that result from our collaboration.

   The co-creation of new technology in the world today seldom starts from scratch. At Microsoft we bring our existing products, IP, and expertise, and our customers do the same thing, often reflecting their world-leading expertise in their particular field. Our ability to co-create relies on both companies respecting each other's IP.

2. **Assuring customer ownership of new patents and design rights.** As we work together to create new technology, our customers, rather than Microsoft, will own any patents that result from our shared innovation work.

   Among other things, this means that Microsoft will cooperate in the filing of any patent applications resulting from the new invention work. This also means that Microsoft will assign to the customer all of the rights, titles, and interest in the patents we create together.

3. **Support for open source.** If our shared innovation results in the creation of source code and our customers so choose, Microsoft will work with them to contribute to an open source project any code the customer is licensed to use.

4. **Licensing back to Microsoft.** Microsoft will receive a license back to any patents and design rights in the new technology that results from the shared innovation, but the license will be limited to improving our platform technologies.

   For this purpose, our own platforms include existing and future versions of Azure, Azure Services (e.g., Cognitive Services), Office 365, Windows, Dynamics, Enterprise Mobility Solution, Cortana, Bing, Xbox, Xbox Live, HoloLens, System of Intelligence, and code and tools developed by or on behalf of Microsoft that are intended to provide technical assistance to customers in their respective businesses.

5. **Portability.** We won't impose contractual restrictions that prevent customers from porting to other platforms the new, shared innovations they own.

   In the world today, customers want to retain the contractual freedom to move the work they co-create to an alternative platform in the future if they so choose. We respect their right to do so. We're committed to retaining our customers' business by offering better performance and value than anyone else, not by locking customers in to something they no longer want to use.

6. **Transparency and clarity.** We will work with customers to ensure transparency and clarity on all IP issues as the shared innovation project moves forward.

   IP issues can get complicated, and shared innovation works well only if there is transparency and clarity for customers throughout the process. We're committed to well-organized and defined processes that ensure that our customers always

have clear and complete information. We'll also each appoint executive sponsors to help address quickly any questions or issues that may arise during shared innovation work.

7. **Learning and improvement.** We'll continue to learn from this work and use this learning to improve further our shared innovation work.

   We look forward to listening to and learning with our customers as we do more of this important work. We look forward to using what we learn to make future improvements to these principles.

Shared innovation projects represent the next frontier in developing cutting-edge technology, and the ability to co-create relies on both companies respecting each other's IP. These principles offer a path that will ensure that the co-creation of digital technologies creates new economic value to companies throughout the economy and around the world, and strikes a balance that enables Microsoft and its customers to focus on what each does best and work together with trust and confidence to help each other become more successful.