Microsoft

Security:
Azure helps you to keep customer data secure

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

Author
Debra Shinder

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.

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

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

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.

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

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

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.

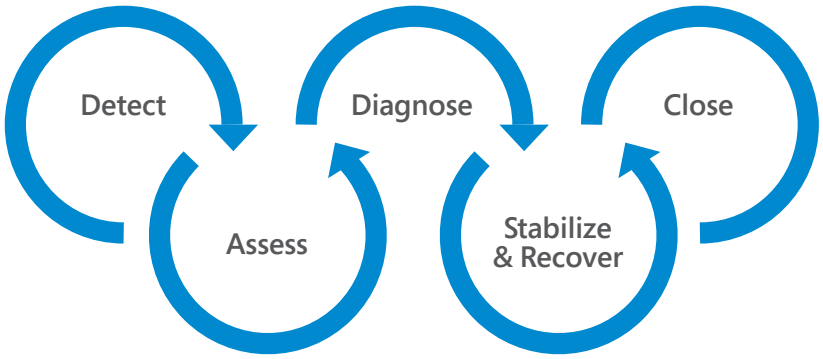
"Red teaming" was developed by the military to improve effectiveness by assuming an adversarial role. At Microsoft, a dedicated red team of software security experts simulates real-world attacks at the network, platform, and application layers, testing the ability of Azure to detect, protect against, 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.

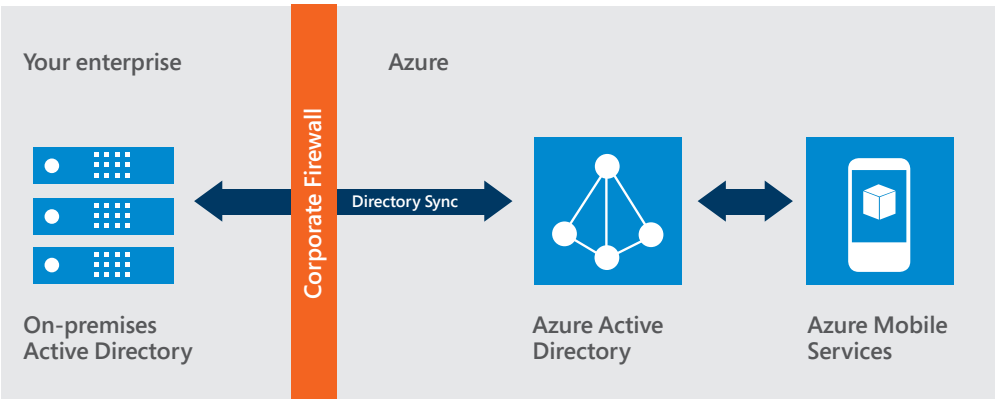
Enterprise cloud directory

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.



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

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.

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.

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.

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.

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.

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.

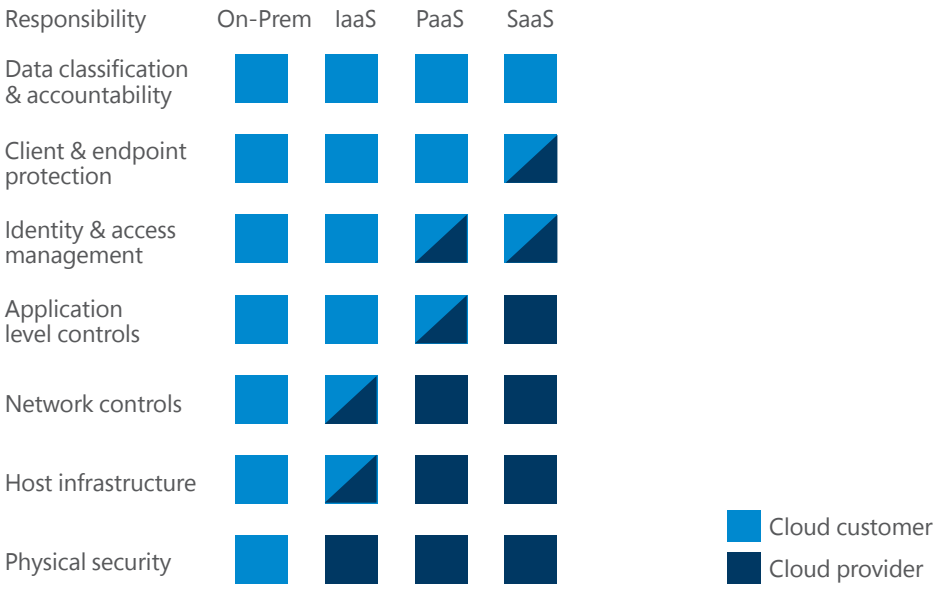
Data destruction. When you delete data or leave the Azure service, Microsoft follows industry-standard processes for overwriting storage resources before reuse, including following the National Institute of Standards and Technology (NIST) Special Publication 800-88 guidelines for media sanitization.

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.


Microsoft