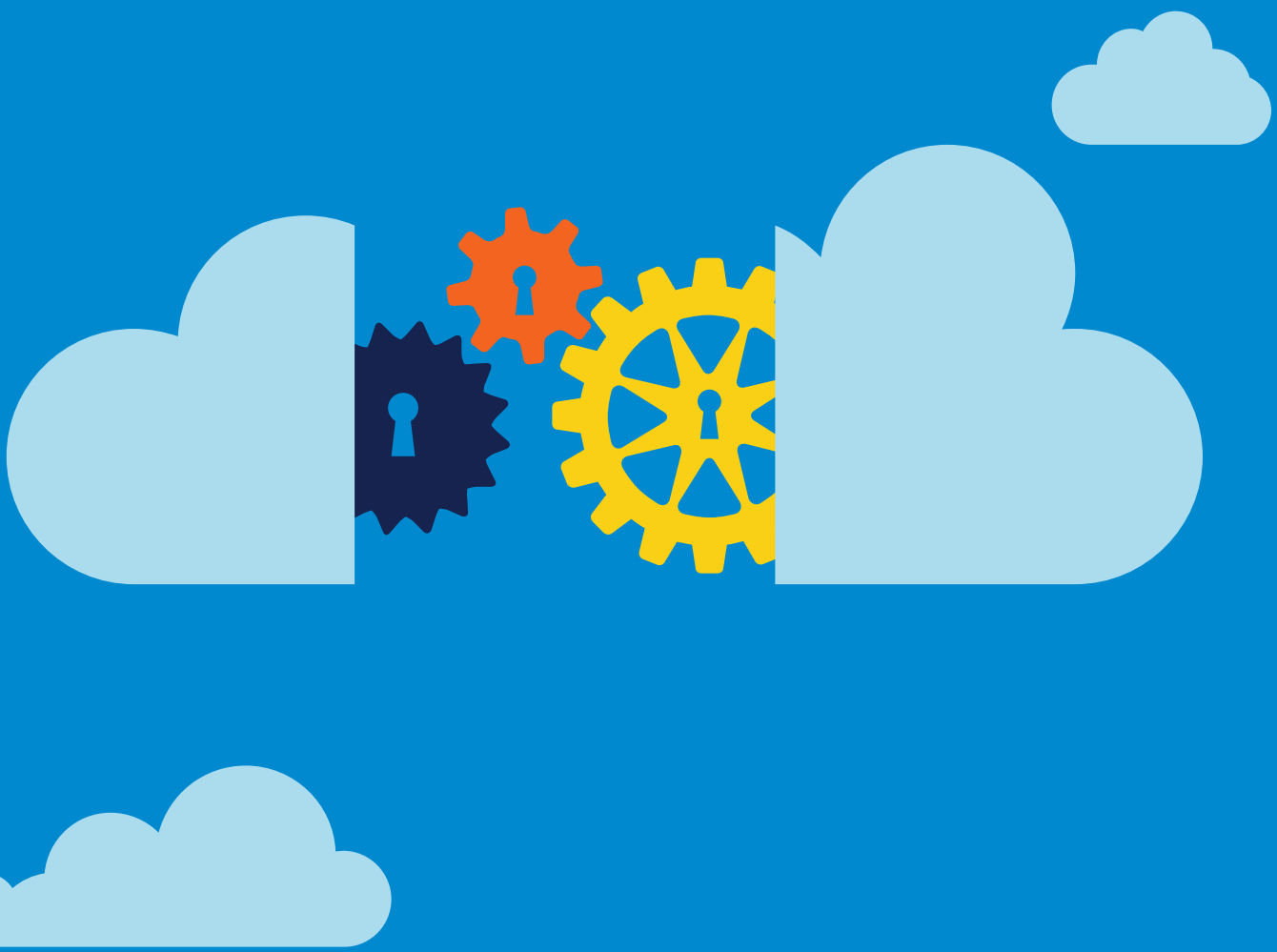
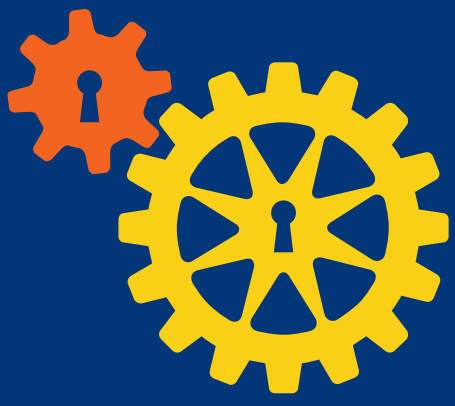
Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance

April 2015



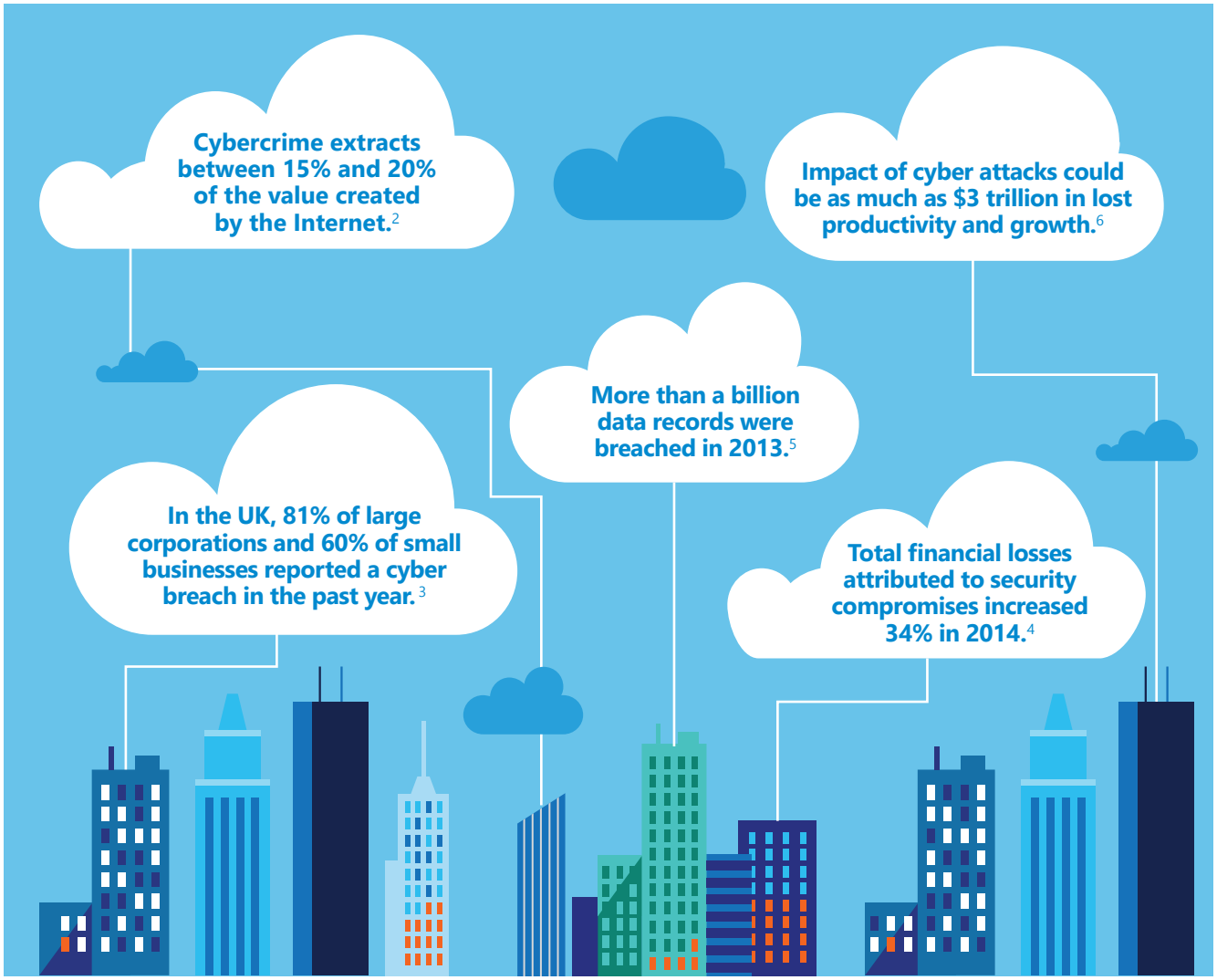
Microsoft

Contents



Introduction

With the emergence of cloud computing, today's IT organizations are playing an increasingly important role in driving business strategy. While cost reduction is still a top priority, scalability and business agility have stepped to the forefront for IT decision makers. As a result, spending on cloud solutions is expected to grow 30 percent from 2013 to 2018, compared with 5 percent overall growth for enterprise IT. And cloud services are keeping pace[1]. Analysts expect to see a ten-fold increase in the number of cloud-based solutions on the market in the next four to five years.



Sources:

1 Forbes, "Roundup of Cloud Computing Forecasts and Market Estimates, 2015," 1/24/2015. http://aka.ms/forbes-cloud-2015

2 Intel/McAfee, "Net Losses: Estimating the Global Cost of Cybercrime," June 2014. http://aka.ms/mcafee-cybercrime-report

3 UK Dept. for Business, Innovation and Skills, "2014 Information Security Breaches Survey." http://aka.ms/uk-gov_breach-survey

4 PWC, "Global State of Information Security Survey: 2015." http://aka.ms/pwc-cybercrime

5 Gemalto, 2014 Breach Level Index Report

6 McKinsey & Company, report for World Economic Forum, Jan. 2014

Still, many CIOs hesitate to fully embrace a cloud-first approach. Their hesitation stems in part from anxiety over a wide range of privacy and security related issues. Large-scale data breaches dominated headlines in 2014 and continue in the news today, raising a critical question for IT leaders everywhere: How can organizations build scalable cloud solutions and increase business agility while taking the necessary steps to secure our data and ensure privacy and compliance across the enterprise?

Without a clear answer, security concerns threaten to stall innovation and stifle business growth. IT and business leaders need a trusted partner to bridge the gap between innovation and security. With the right technologies and processes, even the most complex enterprise can move to the cloud with confidence.

"71% of strategic buyers cite scalability, cost and business agility as the most important drivers for using cloud services."

Gigaom Research

What customers want from cloud providers

Every business has different needs and every business will reap distinct benefits from cloud solutions. Still, customers of all kinds have the same basic concerns about moving to the cloud. They want to retain control of their data, and they want that data to be kept secure and private, all while maintaining transparency and compliance.

Secure our data. The scale and scope of intrusions are growing. In 2014, cyber criminals compromised more than a billion data records in more than 1500 breaches.[7] In a 2014 report for the World Economic Forum[8] , McKinsey & Company estimated the risk of cyberattacks "could materially slow the pace of technology and business innovation with as much as $3 trillion in aggregate impact." In any security attack, target organizations are only as safe as their weakest link. If any component is not secured, then the entire system is at risk. While acknowledging that the cloud can provide increased data security and administrative control, IT leaders are still concerned that migrating to the cloud will leave them more vulnerable to hackers than their current in-house solutions.

Keep our data private. Cloud services raise unique privacy challenges for businesses. As companies look to the cloud to save on infrastructure costs and improve their flexibility, they also worry about losing control of where their data is stored, who is accessing it, and how it gets used. Since the revelations of widespread surveillance by the US government in 2013, privacy concerns have become more accentuated, and the cloud has come under greater scrutiny as a result.

Give us control. Even as they take advantage of the cloud to deploy more innovative solutions, companies are very concerned about losing control of their data. The recent disclosures of government agencies accessing customer data, through both legal and extralegal means, make some CIOs wary of storing their data in the cloud. Many companies are therefore looking to choose where their data resides in the cloud and to control what entities have visibility into that data.

Promote transparency. While security, privacy, and control are important to business decision makers, they also want the ability to independently verify how their data is being stored, accessed, and secured. Businesses understand that they cannot control what they cannot see. To create this sort of visibility for customers, cloud providers must offer transparency of their security, privacy and compliance practices and actions to give customers the information they need to make their own decisions.

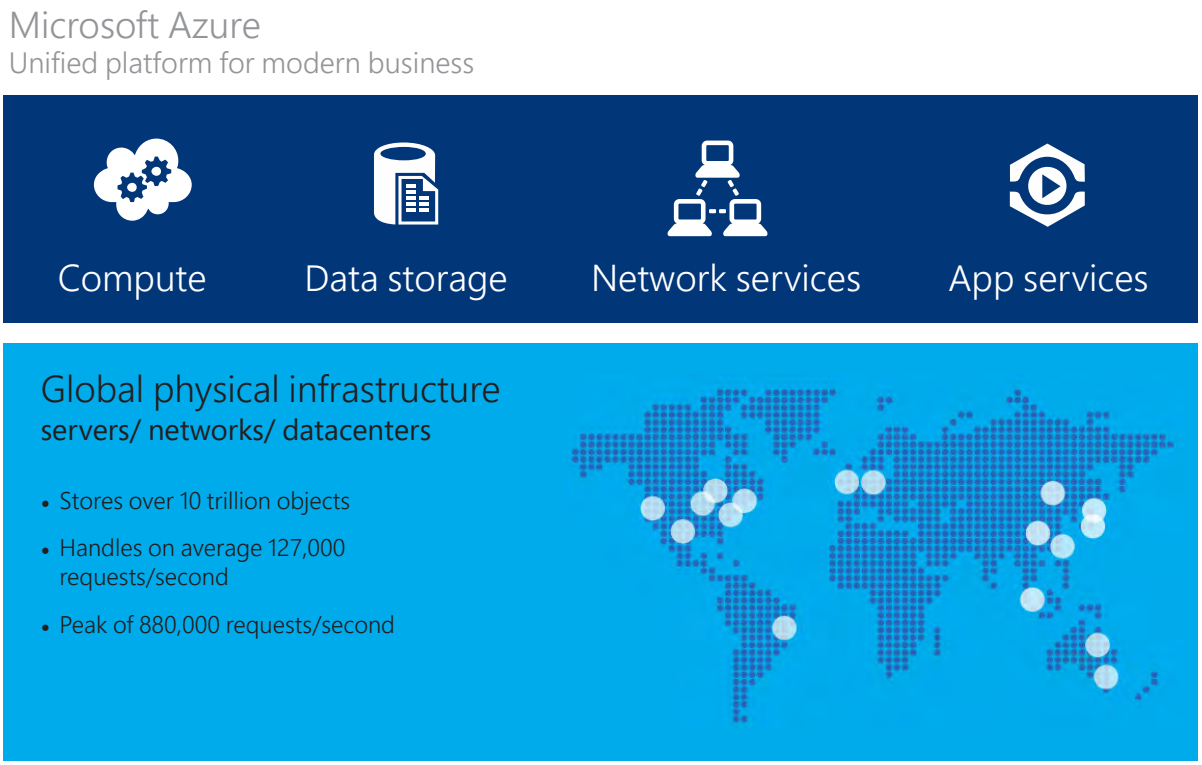
7 Gemalto, 2014 Breach Level Index Report

8 McKinsey & Company, for World Economic Forum, Jan. 2014

Maintain compliance. As companies and government agencies expand their use of cloud technologies, the complexity and scope of standards and regulations continues to evolve. Companies need to know that their compliance standards will be met, and that compliance will evolve as regulations change over time.

Microsoft Azure: Built for trust

Microsoft Azure provides cloud services for a wide range of enterprise and government customers. The core of Microsoft Azure provides four primary functions on which customers build and manage virtual environments, applications, and associated configurations.



Microsoft, with its unique experience and scale, delivers these services to many of the world's leading enterprises and government agencies. Today, the Microsoft cloud infrastructure supports over 1 billion customers across our enterprise and consumer services in 140 countries and supports 10 languages and 24 currencies. Drawing on this history and scale, Microsoft has implemented software development with enhanced security, operational management, and threat mitigation practices, helping it to deliver services that achieve higher levels of security, privacy, and compliance than most customers could achieve on their own.

Microsoft shares best practices with government and commercial organizations and engages in broad security efforts through the creation of centers of excellence, including the Microsoft Digital Crimes Unit, Microsoft Security Response Center, and Microsoft Malware Protection Center.

Security: Working to keep customer data safe

Azure can help reduce the cost, complexity, and risk associated with security and compliance in the cloud. A survey funded by Microsoft and performed by ComScore[9] found that while many organizations have initial concerns about moving to the cloud, a majority of cloud adopters reported that they achieved significant security benefits. These security benefits are reported because few individual organizations can replicate the technology and operational processes that Microsoft uses to help safeguard its enterprise cloud services and comply with a wide range of international standards. When companies use Azure, they benefit from Microsoft's unmatched scale and experience running compliant online services around the globe. Microsoft's expertise becomes the customer's expertise.

Initial concern

60% cited concerns around data security as a barrier to adoption

45% concerned that the cloud would result in a lack of data control

Realized benefit

94% experienced security benefits they didn't previously have on-premise

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

Microsoft Cloud Experience:

- 200+ cloud services
- 1+ million servers
- $15B+ infrastructure investment
- 1 billion customers
- 20 million businesses
- 140 countries worldwide

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, from code development to incident response.

Design for security from the ground up. Azure code development adheres to Microsoft's Security Development Lifecycle (SDL). The SDL is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. The SDL became central to Microsoft's development practices 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.

9 http://aka.ms/twc-cloud-trust-study

Enhancing 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/or administrative activity:

- Tight access controls on sensitive data, including a requirement for two-factor smartcard-based authentication to perform sensitive operations.
- Combinations of controls that enhance independent detection of malicious activity.
- Multiple levels of monitoring, logging, and reporting.

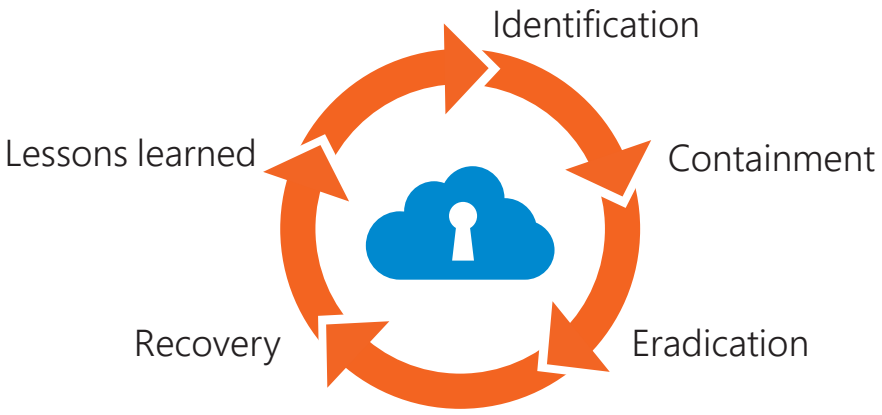
Additionally, Microsoft conducts background verification checks of certain operations personnel and limits access to applications, systems, and network infrastructure in proportion to the level of background verification.

Assume breach. One key operational best practice that Microsoft uses to harden its cloud services is known as the "assume breach" strategy. A dedicated "red team" of software security experts simulates real-world attacks at the network, platform, and application layers, testing Azure's ability to detect, protect against, and recover from breaches. By constantly challenging the security capabilities of the service, Microsoft can stay ahead of emerging threats.

"We don't have the resources to respond to security threats all day, 365 days a year, the way that Microsoft does."

Bo Wandschneider,
CIO and Associate Vice Principal
Queen's University (Canada)

Incident management and response. Microsoft has a global, 24x7 incident response service that works to mitigate the effects of attacks and malicious activity. The incident response team follows established procedures for incident management, communication, and recovery, and uses discoverable and predictable interfaces with internal and external partners alike. In the event of a security incident, the security team follows these five phases:



- **Identification**: If an event indicates a security issue, the incident is assigned a severity classification and appropriately escalated within Microsoft.
- **Containment**: The immediate priority of the escalation team is to ensure the incident is contained and data is safe.
- **Eradication**: After the situation is contained, the escalation team moves toward eradicating any damage caused by the security incident and identifies the root cause of the security issue.
- **Recovery**: Software or configuration updates are applied to the system and services are returned to full working capacity.
- **Lessons Learned**: Each security incident is analyzed to ensure the appropriate mitigations are applied to protect against future recurrence.

Infrastructure Protection

Azure infrastructure includes hardware, software, networks, administrative and operations staff, and the physical data centers that house it all. Azure addresses security risks across its infrastructure.

Physical security. Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

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 provide visibility to customers.

Perimeter	Buildings	Computer room
• Security staff around the clock • Facility setback requirements • Barriers • Fencing	• Alarms • Security operations center • Seismic bracing • Security cameras	• Two-factor access control: biometric and card readers • Cameras • Days of backup power

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 OS, web application, and database scans of the Azure environment.

Antivirus and antimalware. Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan. In addition, Microsoft provides native antimalware on all Azure VMs. Microsoft recommends that customers run some form of antimalware or antivirus on all virtual machines (VMs). Customers can install Microsoft Antimalware for Cloud Services and Virtual Machines or another antivirus solution on VMs, and VMs can be routinely reimaged to clean out intrusions that may have gone undetected.

Penetration testing. Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of our customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their own—and only their own—applications hosted in Azure.

DDoS Protection. Azure has a defense system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques. Azure's DDoS defense system is designed to withstand attacks generated from outside and inside the platform.

Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Because Azure's shared infrastructure hosts hundreds of millions of active VMs, protecting the security and confidentiality of network traffic is critical.

In the traditional datacenter model, a company's IT organization controls 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. Customers do not have physical access, but they implement the logical equivalent within their cloud environment through tools such as Guest operating system (OS) firewalls, Virtual Network Gateway configuration, and Virtual Private Networks.

Network isolation. Azure is a multitenant service, meaning that multiple customers' deployments and VMs are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Virtual networks. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.

VPN and Express Route. Microsoft enables connections from customer sites and remote workers to Azure Virtual Networks using Site-to-Site and Point-to-Site VPNs. For even better performance, customers can use an optional ExpressRoute, a private fiber link into Azure data centers that keeps their traffic off the Internet.

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

"If you're resisting the cloud because of security concerns, you're running out of excuses."

FORRESTER

Data Protection

Azure allows customers to encrypt data and manage keys, and safeguards customer data for applications, platform, system and storage using three specific methods: encryption, segregation, and destruction.

Data isolation. Azure is a multitenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware.

Protecting data at rest. Azure offers a wide range of encryption capabilities, giving customers the flexibility to choose the solution that best meets their needs. Azure Key Vault helps customers easily and cost effectively streamline key management and maintain control of keys used by cloud applications and services to encrypt data.

Protecting data in transit. For data in transit, customers can enable encryption for traffic between their own VMs and end users. Azure protects data in transit, such as between two virtual networks. Azure uses industry standard transport protocols such as TLS between devices and Microsoft datacenters, and within datacenters themselves.

Encryption. Customers can encrypt data in storage and in transit to align with best practices for protecting confidentiality and data integrity. For data in transit, Azure uses industry-standard transport protocols between devices and Microsoft datacenters and within datacenters themselves. You can enable encryption for traffic between your own virtual machines and end users.

Data redundancy. Customers 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.

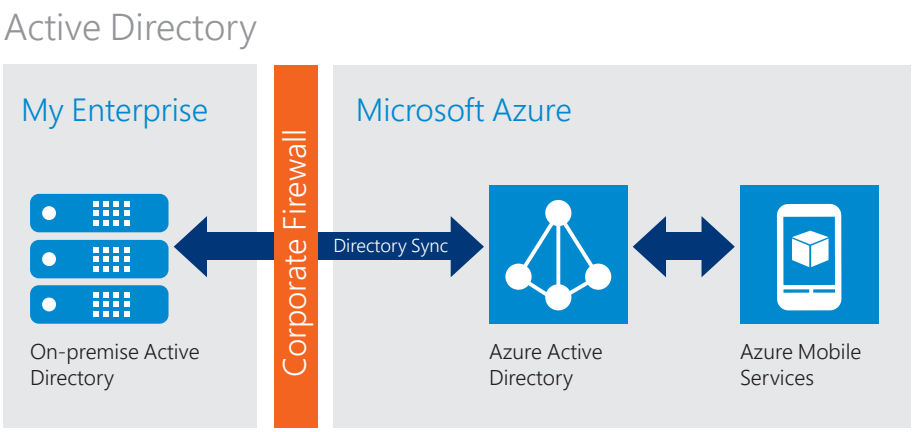
Data destruction. When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse. As part of our agreements for cloud services such as Azure Storage, Azure VMs, and Azure Active Directory, we contractually commit to specific processes for the deletion of data.

> **"From a security point of view, I think Azure is a demonstrably more secure environment than most banks' datacenters."**
>
> John Schlesinger,
> *Chief Enterprise Architect, Temenos (Switzerland)*

Identity and Access

Microsoft has strict controls that restrict access to Azure by Microsoft employees. Azure also enables customers to control access to their environments, data and applications.

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 Active Directory makes it easy for developers to build policy-based identity management into their applications. Azure Active Directory Premium includes additional features to meet the advanced identity and access needs of enterprise organizations. Azure Active Directory enables a single identity management capability across on-premises, cloud, and mobile solutions.



Multi-Factor Authentication. Microsoft Azure provides Multi-Factor Authentication (MFA). This helps safeguard access to data and applications and enables regulatory compliance while meeting user demand for a simple sign-in process for both on-premises and cloud applications. It delivers strong authentication via a range of easy verification options—phone call, text message, or mobile app notification—allowing users to choose the method they prefer.

Access monitoring and logging. Security reports are used to monitor 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. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.

Privacy: Customers own and control their data

Customers will only use cloud providers in which they have great trust. They must trust that the privacy of their information will be protected, and that their data will be used in a way that is consistent with their expectations.

We build privacy protections into Azure through Privacy by Design, a program which describes how we build and operate products and services to protect privacy. Standards and processes that support Privacy by Design principles include the Microsoft Online Services Privacy Statement (which details Microsoft's core privacy requirements and practices) and the Microsoft Secure Development Lifecycle (which includes addressing privacy requirements).

"The question is no longer: 'How do I move to the cloud?' Instead, it's 'Now that I'm in the cloud, how do I make sure I've optimized my investment and risk exposure?'"

We then back those protections with strong contractual commitments to safeguard customer data, including offering EU Model Clauses (which provides terms covering the processing of personal information), and complying with international standards.

Microsoft uses customer data stored in Azure only to provide the service, including purposes compatible with providing the service. Azure does not use customer data for advertising or similar commercial purposes.

Contractual commitments. Microsoft was the first major cloud service provider to make contractual privacy commitments that help assure the privacy protections built into in-scope Azure services are strong. Among the many commitments that Microsoft supports are:

- EU Model Clauses. EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). Microsoft offers customers the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services. Europe's privacy regulators have determined that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Microsoft is the first cloud provider to receive this recognition.
- US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Program. Microsoft abides by these frameworks set forth by the US Department of Commerce regarding the collection, use, and retention of data from the EEA and Switzerland.
- ISO/IEC 27018. Microsoft is the first major cloud provider to adopt the first international code of practice for cloud privacy. ISO/IEC 27018 was developed to establish a uniform, international approach to protecting the privacy of personal data stored in the cloud. The British Standards Institution independently verified that Microsoft Azure is aligned with the guideline's code of practice. ISO 27018 controls include a prohibition on the use of customer data for advertising and marketing purposes without the customer's express consent

Restricted access by Microsoft personnel. Access to customer data by Microsoft personnel is restricted. Customer data is only accessed when necessary to support the customer's use of Azure. This may include troubleshooting aimed at preventing, detecting, or repairing problems affecting the operation of Azure and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam). When granted, access is controlled and logged. Strong authentication, including the use of multi-factor authentication, helps limit access to authorized personnel only. Access is revoked as soon as it is no longer needed.

Notification of lawful requests for information. Microsoft believes that customers should control their data whether stored on their premises or in a cloud service. We will not disclose Azure customer data to law enforcement except as a customer directs or where required by law. When governments make a lawful demand for Azure customer data from Microsoft, we strive to be principled, limited in what we disclose, and committed to transparency.

- Microsoft does not provide any third party with direct or unfettered access to customer data. Microsoft only releases specific data mandated by the relevant legal demand.
- If a government wants customer data—including for national security purposes—it needs to follow the applicable legal process, meaning it must serve us with a warrant or court order for content or subpoena for account information. If compelled to disclose customer data, we will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.

- Microsoft will only respond to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. Every request is explicitly reviewed by Microsoft's legal team, who ensures that the requests are valid, rejects those that are not, and makes sure we only provide the data specified in the order.

In its commitment to transparency, Microsoft regularly publishes a Law Enforcement Requests Report that discloses the scope and number of requests we receive.

Greater transparency and simplicity of data use policies.
Microsoft keeps customers informed about the processes to protect data privacy and security, including practices and policies. Microsoft also provides the summaries of independent audits of services, which helps customers pursue their own compliance.

Customers are in control of their data

For many organizations, the benefits of moving to the cloud are clear. Still, fear of losing control causes their decision makers to hesitate. Where will data be stored? Who owns the organization's data? Who will be accessing the data? And what happens if the organization wants to switch providers? These are all valid questions—questions Microsoft has in mind when making a clear commitment to provide customers with control over their data. This commitment is unique among major cloud service providers.

Customers own their data. This belief is fundamental to the Microsoft approach. When a customer utilizes Azure, they retain exclusive ownership of their data. Microsoft takes steps to protect many types of data.

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, Customer through use of the Online Service." For example, this includes data that you upload for storage or processing and applications that you run in Azure.

Customers can access their own customer data at any at any time and for any reason without assistance from Microsoft. Microsoft will not use customer data or derive information from it for advertising. We will use customer data only to provide the service or for purposes compatible with providing the service.

"Just as computer users back up their laptops in case they break or are lost, Estonia is working out how to back up the country, in case it is attacked by Russia."

The Economist,
reporting on Estonia's Azure cloud backup

- **Customer data** is all data, including all text, sound, video or image files, and software that are provided to Microsoft by or on behalf of the customer through use of Azure. For example, it includes data uploaded for storage or processing and applications uploaded by the customer for hosting on Azure.
- **Administrator data** is the information about administrators (including account contact and subscription administrators) supplied during signup, purchase, or administration of Azure, such as name, phone number, and email address.
- **Metadata** includes configuration and technical settings and information. For example, it includes the disk configuration settings for an Azure virtual machine or the database design for an SQL Database. Metadata does not include information from which customer data could be derived.
- **Access control data** is data that is used to manage access to other types of data or functions within Azure. It includes passwords, security certificates, and other authentication-related data.

Control over data location. When customers entrust their data to Microsoft, they are not giving up control. For many customers, knowing and controlling the location of their data can be an important element of data privacy, compliance, and governance. Microsoft Azure offers an ever-expanding network of data centers across the globe. Most Azure services permit customers to specify the particular geography where their customer data will be stored. Data may be replicated within a selected geographic area for redundancy, but will not be replicated outside it for redundancy.

Encryption key management. To ensure control over encrypted data, customers have the option to generate and manage their own encryption keys, and determine who is authorized to use them. They also have the option to revoke Microsoft's copy of their encryption key, although this may limit Microsoft's ability to troubleshoot or repair problems and security threats.

Role based access control. Microsoft provides an approach allowing customers to restrict system access to authorized users based on role assignment, role authorization, and permission authorization. Tools in multiple Microsoft cloud services support authorization based on a user's role, simplifying access control across defined groups of users.

Control over data destruction. When customers delete data or leave a Microsoft cloud service, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware, including contractual commitments to specific processes for the deletion of data and the destruction of storage hardware.

"Our brand rests on the continuity of our IT systems, which are now more available running in Azure."

Andrew Goodin,
Global Manager of Information Systems
Zespri International (New Zealand)

Transparency

For customers to effectively exercise their right to control their data, they must have access and visibility to that data. They must know where it is stored. They must also know, through clearly stated and readily available policies and procedures, how the cloud provider helps secure customer data, who can access it, and under what circumstances.

Where and how data is stored and used. Microsoft gives Azure customers visibility to where their customer data is stored in an ever-expanding network of datacenters around the globe. Customers can balance the need to store backups at multiple locations in case of a disaster with the need to keep their data out of certain geographies. Microsoft provides clear data maps and geographic boundary information for all datacenters.

How data is secured. Customers have access to up-to-date information regarding security policies and procedures. Microsoft promotes transparency by publishing and adhering to the Security Development Lifecycle.

Who requests access to customer data. Microsoft will never disclose Azure customer data to a government or law enforcement agency except as directed by the customer or where required by law. In response to lawful demands for Azure customer data, Microsoft strives to be principled, limited in disclosure, and committed to transparency. Microsoft regularly publishes a Law Enforcement Requests Report that discloses the scope and number of government requests received.

Breach notification. In the event that customer data is compromised, Microsoft will notify its customers. Azure has comprehensive, transparent policies that govern incident response from identification all the way through to lessons learned.

Audit standards certifications. Rigorous third-party audits, such as those conducted by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate. As part of Microsoft's commitment to transparency, customers can verify Azure's implementation of many security controls by requesting audit results from the certifying third parties.

Customer guidance. Microsoft publishes a Security Response Center Progress Report and a Security Intelligence Report to provide customers with insights into the threat landscape, and provide prescriptive guidance for managing risk to protect their assets.

Transparency Centers. Microsoft operates Transparency Centers that provide government customers with the ability to review source code, reassure themselves of its integrity, and confirm there are no back doors.

"By 2020 clouds will stop being referred to as 'public' and 'private'. It will simply be the way business is done and IT is provisioned."

Compliance: Azure conforms to global standards

Microsoft invests heavily in the development of robust and innovative compliance processes. The Microsoft compliance framework for online services maps controls to multiple regulatory standards. This enables Microsoft to design and build services using a common set of controls, streamlining compliance across a range of regulations today and as they evolve in the future.

Microsoft compliance processes also make it easier for customers to achieve compliance across multiple services and meet their changing needs efficiently. Together, security-enhanced technology and effective compliance processes enable Microsoft to maintain and expand a rich set of third-party certifications. These help customers demonstrate compliance readiness to their customers, auditors, and regulators. As part of its commitment to transparency, Microsoft shares third-party verification results with its customers.

Certifications and attestations. Azure meets a broad set of international as well as regional and industry-specific compliance standards, such as ISO 27001, FedRAMP, SOC 1 and SOC 2. Azure's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Azure services work with and meet world-class industry standards, certifications, attestations, and authorizations.

Comprehensive, independently verified compliance. Azure is designed with a compliance strategy that helps customers address business objectives and industry standards and regulations. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analysis to achieve certificates and attestations. Microsoft Azure offers the following certifications for all in-scope services.

CDSA. The Content Delivery and Security Association (CDSA) provides a Content Protection and Security (CPS) standard for compliance with anti-piracy procedures governing digital media. Azure passed the CDSA audit, enabling secure workflows for content development and distribution.

CJIS. Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy, which commits Microsoft to adhere to the same requirements that law enforcement and public safety entities must meet.

CSA CCM. The Cloud Security Alliance (CSA) is a nonprofit, member-driven organization with a mission to promote the use of best practices for providing security assurance within the cloud. The CSA Cloud Controls Matrix (CCM) provides detailed information about how Azure fulfills the security, privacy, compliance, and risk management requirements defined in the CCM version 1.2, and is published in the CSA's Security Trust and Assurance Registry (STAR).

EU Model Clauses. Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU. Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. This ensures that Azure customers can use Microsoft services to move data freely through our cloud from Europe to the rest of the world.

FDA 21 CFR Part 11. The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 lists requirements for the security of electronic records of companies that sell food and drugs manufactured or consumed in the United States. The compliance reports produced by Azure's independent third party SSAE and ISO auditors identify the procedural and technical controls established at Microsoft and can be used to satisfy the requirements of CFR Title 21 Part 11. Microsoft is able to show how relevant controls within these reports have an impact on compliance with the FDA 21 CFR 11 regulations.

FedRAMP. Azure has been granted a Provisional Authority to Operate (P-ATO) from the Federal Risk and Authorization Management Program (FedRAMP) Joint Authorization Board (JAB) at a Moderate impact level based upon the FIPS 199 classification. FedRAMP is a US government program that provides a standard approach to security assessment, authorization, and monitoring for cloud services used by federal agencies and thereby saves the taxpayer and individual organizations the time and cost of conducting their own independent reviews.

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 use and disclosure restrictions imposed by FERPA.

FIPS 140-2. Azure complies with the Federal Information Processing Standard (FIPS) Publication 140-2, a US government standard that defines a minimum set of security requirements for products and systems that implement cryptography.

HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI). Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

IRAP. Azure has been assessed against the Australian Government Information Security Registered Assessors Program (IRAP), which provides assurance for public sector customers that Microsoft has appropriate and effective security controls.

ISO/IEC 27018. Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

ISO/IEC 27001/27002:2013. Azure complies with this standard, which defines the security controls required of an information security management system.

MLPS. Multi-Level Protection Scheme (MLPS) is based on the Chinese state standard issued by the Ministry of Public Security. Azure operated by 21Vianet adheres to this standard, which provides assurance for both the management and technical security of cloud systems.

MTCS. Azure has achieved Level-1 certification with the Multi-Tier Cloud Security Standard for Singapore (MTCS SS), a cloud security standard covering areas such as data security, confidentiality, business impact, and operational transparency, developed under the Singapore Information Technology Standards Committee.

PCI DSS. Azure is Level 1 compliant with Payment Card Industry (PCI) Data Security Standards (DSS) version 3.0, the global certification standard for organizations that accept most payments cards, as well store, process, or transmit cardholder data.

SOC 1 and SOC 2. Azure has been audited against the Service Organization Control (SOC) reporting framework for both SOC 1 Type 2 and SOC 2 Type 2. Both reports are available to customers to meet a wide range of US and international auditing requirements.

The SOC 1 Type 2 audit report attests to the design and operating effectiveness of Azure controls. The SOC 2 Type 2 audit included a further examination of Azure controls related to security, availability, and confidentiality. Azure is audited annually to ensure that security controls are maintained.

TCS CCCPPF. Azure operated by 21Vianet is among the first cloud providers in China to pass the Trusted Cloud Service certification developed by the China Cloud Computing Promotion and Policy Forum (CCCPPF).

UK G-Cloud. The UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received OFFICIAL accreditation from the UK Government Pan Government Accreditor.

Additional resources

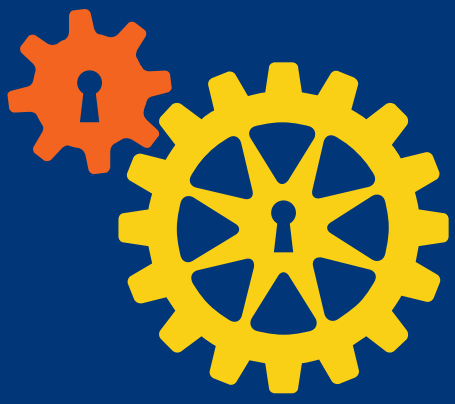
Azure Trust Center
http://azure.microsoft.com/trustcenter

Cloud Security Alliance Cloud Controls Matrix
https://cloudsecurityalliance.org/research/ccm/

Microsoft Cloud Security Readiness Tool
http://www.microsoft.com/trustedcloud

Microsoft Online Services Privacy Statement
http://aka.ms/onlineservices-privacy

Microsoft Privacy Practices
http://aka.ms/privacy-practices



NOTE: Certain recommendations contained herein may result in increased data, network, or compute resource usage, and increase your license or subscription costs.