Microsoft

White Paper

Trusting the Cloud

According to a recent Forrester Research study, spending on public cloud services is expected to reach $106 billion in 2016, a 21% increase over projected 2015 spending levels. The ComputerWorld Forecast Study 2015 found that cloud computing initiatives are the most important project for the majority of IT departments today. Movement to the cloud is happening for many good reasons: a pay-as-you-go cost model, global access from any location or device, the ability to scale up or down as business needs change, built-in disaster recovery, and providing IT with greater agility to meet overall development and management needs at scale. As these promises are fulfilled, companies are realizing how to take their cloud operations to the next level and incorporate a cloud approach into their overall business strategy.

At the same time, however, many CIOs still have cloud adoption concerns resulting from questions about security, privacy, and compliance. Cybersecurity has been elevated to CEO and board-level attention because of its proven potential to negatively impact a company's brand, market share and revenues. Cloud providers that adopt a holistic approach and are transparent with customers and regulators can offer more risk protection than many enterprises can achieve on their own.

The Transformational Cloud

Organizations today are moving beyond the early promise of the cloud and using its speed, scale, and economic benefits to transform their business – reshaping how they engage with customers, enabling employees to do more productive work, and driving new and more rapid sources of innovation. The scale and reach of the cloud, for example, is helping companies leverage massive amounts of data to provide better business insights. Marketers are using those insights to forge better alignment with their customers. Mobile employees are sharing data and applications to improve collaboration, productivity and overall work effectiveness. Executives are developing new business models and inventing new service-based revenue streams. As reported recently by IDC[1]. the cloud services market is now entering "an innovation stage that will produce an explosion of new solutions and value creation on top of the cloud." Examples like these, all made possible by the scale and reach of the cloud, are transforming businesses and government entities in ways that are redefining our global economy.

"Companies that take a purely cost-saving approach to cloud are missing additional opportunities."

Tom Lamoureux,
Risk Consulting Leader for Technology, Media and Telecom at KPMG

[1] IDC Forecasts Public IT Cloud Services Spending, Nov. 2014

Risks and Vulnerabilities

These expanded opportunities have also introduced new risks and complex challenges. The threat landscape is evolving and cyber criminals are finding new ways to disrupt commercial and government activities. Privacy issues are top of mind, especially in light of revelations about government surveillance. Companies adopting the cloud to modernize their business are demanding more control and involvement in how their data is managed and used. In a global survey of over 2600 IT decision makers, Microsoft recently found that security, privacy, and data control top the list of most pressing business considerations for using the public cloud.

Security remains a concern

News of security breaches continues to dominate headlines, and the scale and scope of intrusions are growing. In 2014 alone, data breaches were up by 49% over the previous year, and cyber criminals compromised more than a billion data records in more than 1500 breaches.[2] In a 2014 report for the World Economic Forum[3], 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.

[2] Gemalto, 2014 Breach Level Index Report
[3] McKinsey & Company, for World Economic Forum, Jan. 2014

Types and attack methods of threat agents[4]

Threat agent	Purpose & motivation
Corporations	Collect business intelligence for competitive advantage
Nation states	Target state secrets, military intelligence, critical infrastructures
Hacktivists	Ideologically motivated or seeking media attention
Cyber terrorists	Seek to harm national security and society
Cyber criminals	Seek to gain profit from illegal activities in cyberspace
Cyber fighters	Nationally-motivated citizens, driven by political, national or religious values.
Online social hackers	Use social media to exploit psychology of social targets
Employees	Dissatisfied or frustrated internal actors
Script Kiddies	Young, tech-savvy individuals looking to prove their skills

Privacy challenges

Cloud services raise new privacy challenges for businesses given the scale at which public cloud operates in multi-tenant environments. As companies look to the cloud to save on infrastructure costs and improve their flexibility and agility, they also worry about losing control of where their data is stored, who has access to it, and how it gets used.

Many privacy concerns are directed at the government. Since the revelations of widespread snooping by the US government in 2013, privacy concerns have become more acute, and the cloud has come under greater scrutiny as a result. Cloud providers have stepped up their legal challenges to government orders seeking disclosure of customer data, and are advocating for reforms in government surveillance practices.

Even as they enthusiastically exploit the cloud to deploy more innovative solutions, companies are concerned about losing control of their data, retaining ownership of their data, and being responsible for things they cannot control. Many companies are therefore looking to choose where their data resides in the cloud, and to control what entities have visibility into that data. In a recent Microsoft survey, 75% of IT respondents said their primary obligation is to protect the privacy of their customers over national security interests.

[4] European Union Agency for Network and Information Security; ENISA Threat Landscape 2014, *Overview of current and emerging cyber-threats*

Introducing the Microsoft Trusted Cloud

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. With this unique experience and scale, Microsoft cloud services can achieve higher levels of security, privacy, and compliance than many customers could achieve on their own.

200+ cloud services
1+ million servers
$15B+ infrastructure investment

1 billion customers
90 markets worldwide
80% of Fortune 500 companies

Microsoft believes that customers need and deserve a strong advocate to defend their right to secure and private data and to set standards for security, compliance and data privacy that customers can count on. We believe such an advocate needs to work, not only for technology improvements that secure and protect, but also for updated regulatory requirements and standards, for transparency of process and approach, for proper auditing, and, where necessary, for challenges to outdated laws that have not kept pace with the innovation and transformation of cloud computing. We believe that Microsoft's experience, scale, government outreach, technology and industry leadership make us uniquely qualified to play this role.

Microsoft Trusted Cloud principles

At Microsoft, we have a set of foundational beliefs that guide the way we do business in the cloud. With respect to data, for example, we take seriously our commitments to help safeguard our customers' data, to protect customers' right to control and make decisions about that data, to help customers meet their data compliance requirements, and to be transparent about our enterprise cloud services. The following four Trusted Cloud principles articulate our vision of what enterprise organizations are entitled to expect from their cloud provider.

Security	Privacy & Control	Compliance	Transparency
We will implement strong security measures to safeguard your data.	We will provide you with control over your data to help keep it private.	We will help you meet your specific compliance needs.	We will explain what we do with your data in clear, plain language.

Move to the Cloud with Confidence

Few individual customer 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 organizations use Microsoft cloud services, they benefit from Microsoft's scale and experience running highly secure and compliant online services around the globe. Microsoft's expertise becomes the customer's expertise.

Investing in your security

Microsoft Cyber Defense Operations Center (CDOC) is a 24x7x365 state-of-the-art cybersecurity and defense facility. The CDOC is part of the company's initiative to continuously advance its efforts on cybersecurity, risk management, and data protection. The CDOC is the physical hub for the company's real-time security-focused experts, leveraging technology and analytics that protect, detect, and respond to threats to Microsoft's cloud infrastructure and customer-facing resources and the services hosted within them, our products, devices, and the company's internal resources. The teams that come together in the CDOC manage intelligence collection and correlation from our global threat landscape, real-time analysis and incident response, and provide ground zero security crisis management when needed.

Microsoft's Cyber Defense Operations Center

While Microsoft has been defending against threats and providing security protections for our online services since 1994, the CDOC represents a major investment in our continuing commitment to delivering trusted cloud services and protecting our customers.

Secure design and operations. Microsoft creates, implements, and continuously improves security in our software development, operational, and threat mitigation practices. We have adhered to the Security Development Lifecycle (SDL) for over a decade, which embeds security requirements into our software and services through the planning, design, development, and deployment phases. Our Operational Security Assurance (OSA) group works across cloud services to identify and share information about known risks.

Continuously testing and evolving security. Threat modeling, static code analysis, and security testing are useful in enumerating, reducing, and managing attack surfaces—but they do not eliminate all security risks. To uncover unforeseen vulnerabilities and refine our detection and response capabilities, we employ an ongoing exercise of breach.

The dedicated teams that closely monitor and secure Microsoft's cloud infrastructure, cloud services, products, devices, and internal resources continually simulate real-world breaches at every level—testing penetration and improving our ability to protect, detect, and recover from cyberthreats. This penetration testing strategy is executed by two core groups—the Red Team (attackers) and the Blue Team (defenders). The approach is to test our infrastructure, services, operations, and remediation capabilities using the same Tactics, Techniques, and Procedures—or TTPs—as real adversaries would, against our cloud production infrastructure. This further tests our security capabilities by a centrally-located federated team and helps identify any vulnerabilities and security issues in a controlled manner.

75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.

CyberEdge Group, 2014 Cyberthreat Defense Report, No. America & Europe

Threat detection, mitigation, and response. As the number, variety, and severity of cyberthreats have increased, so has our diligence in threat detection and response. Centralized monitoring systems provide continuous visibility and timely alerts to the teams that manage our cloud services, and additional monitoring, logging, and reporting capabilities provide visibility to customers. Frequent application of security patches and updates helps protect systems from known vulnerabilities. Intrusion and malware detection systems are designed to detect and mitigate risks from outside attacks. In the event of malicious activity, our

24x7 incident response teams follow established procedures for incident management, communication, and recovery. The team uses industry best practices to alert both internal teams and customers. Finally, security reports monitor access patterns to help proactively identify and mitigate potential threats.

Data protection. Data is the currency of the digital economy, and we take the responsibility of protecting customer data very seriously. Both technological safeguards, such as encrypted communications, and operational processes help keep customer data secured. In the cloud, data from multiple customers may be stored on the same physical hardware. Microsoft uses logical isolation to segregate each customer's data from that of others. To protect data at rest, we use a complementary set of industry-standard encryption methods that includes Microsoft Bitlocker and application encryption. For data in transit, Microsoft uses encryption protocols to protect customer data as it travels from user devices to data centers, from your data center to ours, or between servers within the Microsoft cloud. To enhance customer control over encrypted data, we are committed to providing customers with the control of encryption keys used with cloud services, giving customers the flexibility to choose the solution that best meets their needs. Customers will then have the option to revoke Microsoft's copy of their encryption key, although this may limit a customer's full use of a cloud service if there are problems or security threats and Microsoft is unable to troubleshoot or repair the problem.

Network protection. The increasing sophistication of cyber threats makes it incumbent upon us to provide secure connections, both within our cloud infrastructure, and between your data centers and ours. We start by isolating networks across our multiple deployment models, which allows us to prevent unwanted communications across tenants on the same hardware. Microsoft blocks unauthorized traffic to and within Microsoft data centers using a variety of technologies such as firewalls, NATs, partitioned Local Area Networks, and physical separation of back-end servers from public-facing interfaces. We provide virtual networking, enabling customers to assign multiple deployments within a subscription and allow those deployments to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks. Built-in cryptographic technology enables customers to encrypt communications between data center regions, and from our cloud to your on-premises data centers. Customers can also use an optional Express Route private fiber link into Microsoft data centers to keep their traffic off the Internet.

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

Forrester Research

Identity & access. Managing who has access, what level of access, to what information, from what locations and devices, are all critical elements of your security policy. We make it easy to define and manage identity and access control for one or multiple Microsoft cloud services. Microsoft Active Directory provides a comprehensive identity and access management solution for the cloud, making it easy for developers to build policy-based identity management into their applications, for use across multiple devices. Multi-factor authentication, which can be used for both on-premise and cloud applications, reduces organizational risk and helps enable regulatory compliance by providing an extra layer of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. Tools in multiple Microsoft cloud services also support authorization based on a user's role, simplifying access control across defined groups of users. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can request reports from Microsoft that provide information about user access to their environments.

Visibility and control. Protecting your data and systems is a shared responsibility, and we recognize that visibility into your security posture across a distributed infrastructure is essential to your business stability. Microsoft provides a unified view of your security status through its Operations Management Suite (OMS), by collecting security-related events and alerts, providing comprehensive assessments of missing system updates across company data centers and cloud, and performing forensic, audit and breach analyses. In addition, Azure Security Center provides a centralized view of the security state of your Azure resources, giving you more control over security policies and providing visibility that allows you to stay ahead of threats.

Protecting your data privacy

Clear guidelines and choice for data location. For many customers, knowing and controlling the location of their data can be an important element of data privacy compliance and governance. We share with customers high-level information concerning the geographic location of Microsoft data storage facilities where their data is stored. Customers will have choice, transparency and flexibility in where their data is stored, with options that include in-country storage for compliance or latency considerations, or out-of-country storage for security or disaster recovery purposes. Data

"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 cloud backup on Microsoft Azure

may be replicated within a selected geographic area for redundancy, but will not be transmitted outside it.

Restricted access by Microsoft. Access to customer data by Microsoft personnel is restricted. Lock box controls require permissions by you for Microsoft personnel and its subcontractors to obtain access to your data. To limit the amount of customer data that we manage on a customer's behalf, we apply data minimization techniques by tiering which internal team has access to the data. Customer data is only accessed when necessary to support the customer's use of our cloud service. This may include troubleshooting aimed at preventing, detecting or repairing problems affecting the operation of the service, or improvement of features that protect and detect against security threats (such as malware or spam). When granted, access is carefully controlled and logged and such reports are audited. We make available such log reports to customers to provide transparency about who has access to their data and when. 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. We don't capture, maintain, scan, index, or mine enterprise customer data for any advertising or similar commercial purposes, and there is no mingling between customer data and Microsoft consumer services.

Notification of lawful requests for information. Microsoft responds to valid legal requests for customer data and has challenged requests we believe are not valid. When contacted by law enforcement with a demand for enterprise customer data, Microsoft will make all attempts to redirect the law enforcement agency to request that data directly from the customer. If compelled to disclose enterprise customer data to law enforcement, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so. When appropriate, Microsoft is prepared to litigate to protect customer data from overbroad or invalid government demands.[5]

We do receive legal demands for customer data from law enforcement agencies around the world. We publish information about these requests every six months in the Law Enforcement Requests Report, as we believe our customers need and deserve to understand our policies, and the extent to which law enforcement requests impact them. We also believe this kind of increased transparency may help advocates and policymakers consider improvements to both privacy and security.

[5] Microsoft has filed litigation challenging a search warrant for private email communications located in our Dublin, Ireland data center. Read more about it on the Digital Constitution website.

Contractual commitments. Microsoft has led the industry in providing cloud-service-specific privacy commitments and making strong contractual promises to safeguard customer data and protect privacy. Microsoft makes the standard contractual clauses created by the European Union (known as the "EU Model Clauses") available to enterprise customers for our primary enterprise services to provide additional contractual guarantees concerning transfers of personal data. While the U.S.-EU Safe Harbor framework has been recently invalidated by the Court of Justice for the European Union, the more stringent EU Model Clauses can still be used to transfer data from the EU to the United States. The Article 29 Working Party, which is comprised of the national DPAs of each of the EU member states, and the European Commission have both confirmed the EU Model Clauses can still be used to transfer data from the EU to the United States. It has also previously validated Microsoft's implementation of the EU Model Clauses.

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 as physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request or after 180 days following service termination or expiration. Customers are entitled to take their data with them when they leave. Data portability and transferability is a key attribute in our services to avoid concerns of vendor lock-in.

Service-specific control options. Our Office 365 and Dynamics CRM Online services provide additional controls that allow customers to manage security and privacy options, including email settings for anti-virus, anti-spam and anti-malware protection, online meeting controls, legal holds to optionally preserve electronically stored information, and e-Discovery, which permits customers to find and retrieve content from across Office 365 services for the purpose of legal discovery.

Enabling your organization's compliance

Microsoft is committed to ongoing verification by third party audit firms, and shares audit report findings and compliance packages with customers to help them fulfill their own compliance obligations.

Certifications and attestations. The Microsoft Cloud 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. Microsoft's adherence to the strict security controls contained in these standards is verified by rigorous third-party audits that demonstrate Microsoft services work with and meet world-class

industry standards, certifications, attestations, and authorizations. Detailed information about compliance for our cloud services is available in our online Trust Center.

Compliance framework. 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. The security compliance framework includes test and audit phases, security analytics, risk management best practices, and security benchmark analyses to achieve certificates and attestations.

Maintaining transparency

The Microsoft Cloud is built on a firm belief in the need for transparency with customers. When we hold your data, we will explain what we do with it in clear, plain language. We give you visibility into our operations so you can monitor the state of your service, track issues, and have a historical view of availability and any changes to the service. We provide a clear, plain-language explanation of how Microsoft uses, manages, and protects your organization's data. We provide disclosures to help stakeholders evaluate our law enforcement requests, National Security Orders, and content removal requests via our Transparency Hub.

"Cloud computing technology vendors need to be more transparent about their security practices if they want to become a trusted partner to enterprises in this environment."

CIO Magazine

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

Law enforcement requests. Microsoft will never disclose 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 customer data, Microsoft strives to defend our customers' rights and privacy, and to ensure due process is followed. 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. We have comprehensive, transparent policies that govern incident response from identification all the way through to lessons learned.

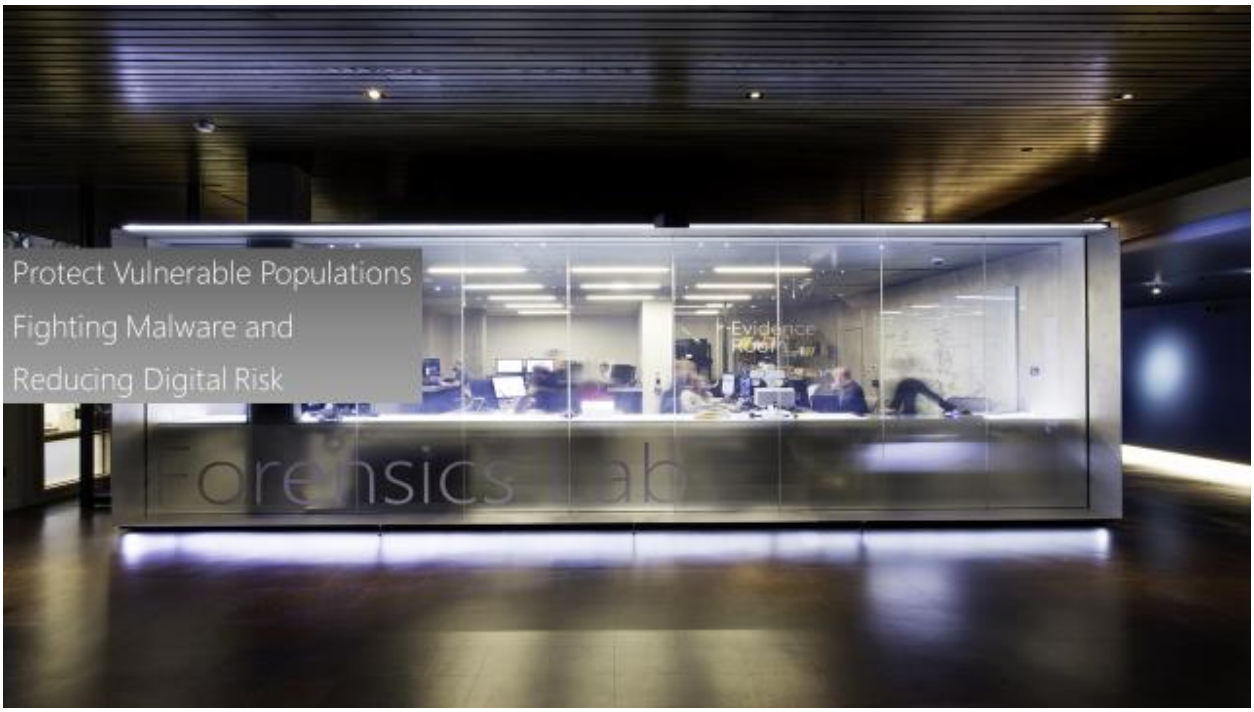
Customer guidance. Microsoft publishes a Security Response Center Progress Report and a Security Intelligence Report to provide customers with insights into the threat landscape, and provide prescriptive guidance for managing risk to protect their assets. Microsoft operates Transparency Centers that provide government customers with the ability to review source code, reassure themselves of its integrity, and confirm there are no back doors.

Industry/government partnership

Establishing security and privacy in the digital economy is more than just a technology challenge. Microsoft works collaboratively with governments, regulators, multilateral organizations, industry, and non-profit groups around the world to enhance cybersecurity across the IT ecosystem.

The Microsoft Government Security Program (GSP) fosters partnership between the government and Microsoft and is fortified through ongoing interaction, collaboration, and information exchange. Through the GSP, participating governments can access Microsoft Windows and Microsoft Office source code to verify that it meets their strict security requirements.

The Microsoft Digital Crimes Unit (DCU) is an international team of lawyers, investigators, data scientists, analysts, engineers, and business professionals fighting cybercrime globally through legal strategies and innovative technologies. This team is on proactive digital defense leveraging big data analytics, cutting-edge forensics, the cloud, and public/private partnerships providing a safer digital experience for every person and organization on the planet.



Microsoft's Digital Crimes Unit

Summary

At Microsoft, we never take customers' trust for granted. We understand that when it comes to the cloud, trust is paramount, and we take very seriously our commitment to protect our customers in today's mobile-first, cloud-first world. These beliefs are fundamental to how we provide cloud services and technologies. Our Trusted Cloud principles will continue to guide the way we do business in the cloud, enabling our customers to move to the cloud with confidence.

There are a number of opportunities for customers to learn first-hand about Microsoft's commitments and investments in security and privacy technology, practices and policies - from an executive security briefing to a data center tour to a security and cloud strategy discussion. For more information, reach out to your Microsoft account manager with questions or to arrange for an engagement that is right for your business.

Additional Resources

Trusted Cloud Website. For additional information about the Microsoft Trusted Cloud, visit our website at http://www.microsoft.com/trustedcloud.

Microsoft Trust Center. A single compliance resource that lists adherence to certifications and attestations, privacy and data protection policies and procedures, and information about data transfer and location policies. http://www.microsoft.com/trustcenter

Microsoft Transparency Hub. Customer source for disclosures to help stakeholders evaluate our law enforcement requests, U.S. National Security orders, and content removal requests. http://www.microsoft.com/transparencyhub

Cybertrust Blog. The Microsoft Cyber Trust blog provides in-depth discussions on topics of security, privacy, compliance and transparency. It includes timely news, trends, analysis, practical guidance and tools. Microsoft experts regularly share insights, report on research, and discuss our collaborative work internally and externally with industry and governments around the world. http://blogs.microsoft.com/cybertrust

Microsoft On-the-Issues Blog. The official Microsoft Blog, covering issues of online safety, cybercrime, citizenship, education and jobs, and other important issues related to technology, culture, and governments. http://blogs.microsoft.com/on-the-issues

Azure Security Blog. The Microsoft Azure Security blog includes regular updates on new security and compliance features in Azure services, important customer experiences with Azure security, and other updates contributed by the Azure security team. http://azure.microsoft.com/en-us/blog/topics/security/

Digital Constitution. Microsoft's Digital Constitution site includes news highlights, important milestones and documents, as well as video clips and blog commentary from Microsoft's legal and policy experts on key legal and privacy issues surrounding the cloud. http://digitalconstitution.com/

Microsoft Cybersecurity Services. Microsoft offers comprehensive consulting services to help customers protect their enterprise organization in today's mobile-first, cloud-first world. Read about how we can help your organization protect, detect, and respond to security threats. http://www.aka.ms/cyber-services