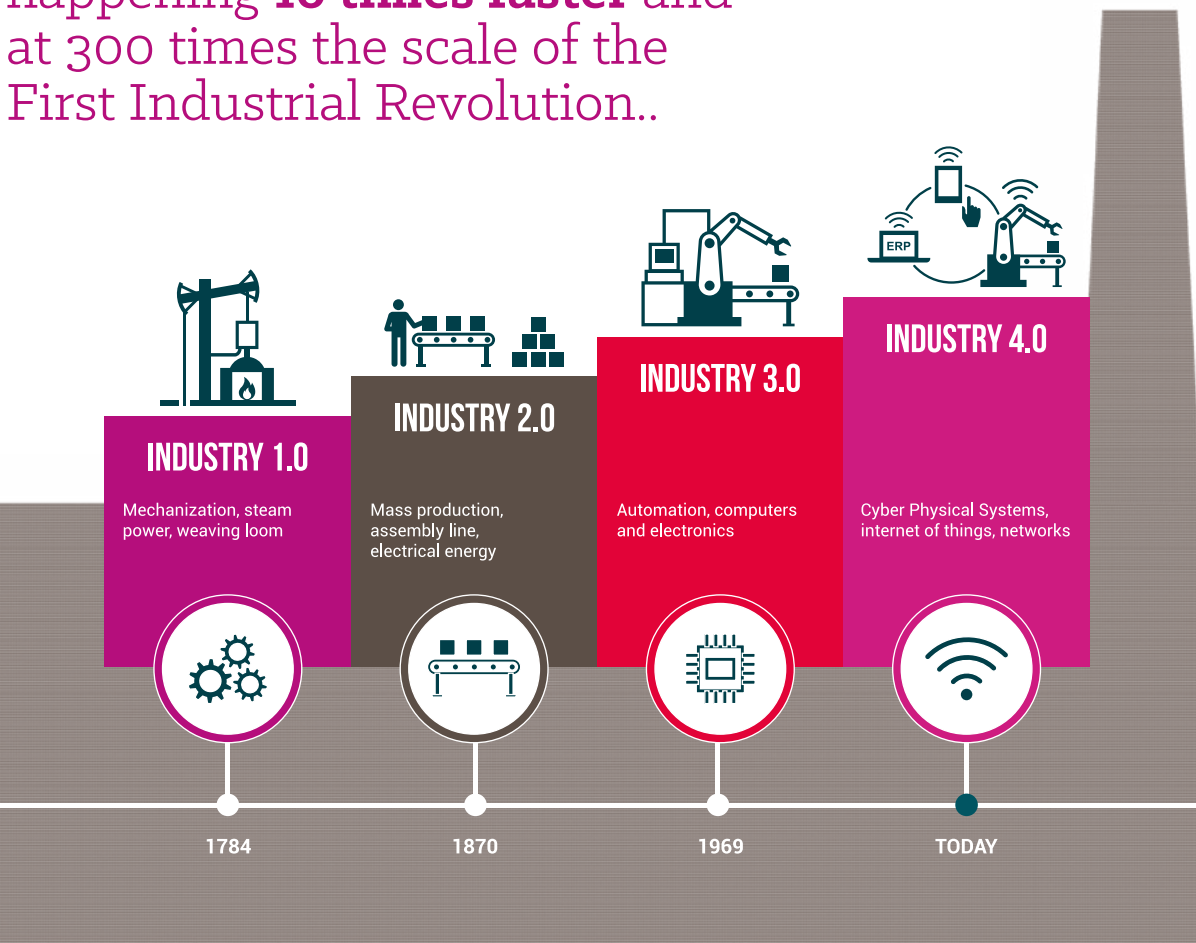# Confidence in a Trusted Cloud

We are on the cusp of a new technology age that promises to transform how we live, communicate, and learn.

The anticipated pace and scale of this transformation is so significant that it has already been termed **'The Fourth Industrial Revolution'.**

This paper will help you understand how to embrace the 'Fourth Industrial Revolution' and the ever increasing pace of change, using a secure and transparent Cloud platform. Learn how to meet the demands of increasing legislation and security requirements, putting you in control.

Insight

Rate of change today is happening **10 times faster** and at 300 times the scale of the First Industrial Revolution..

INDUSTRY 1.0

Mechanization, steam power, weaving loom

INDUSTRY 2.0

Mass production, assembly line, electrical energy

INDUSTRY 3.0

Automation, computers and electronics

INDUSTRY 4.0

Cyber Physical Systems, internet of things, networks

1784   1870   1969   TODAY

The Fourth Industrial Revolution

Richard Dobbs, James Manyika, and Jonathan Woetzel of McKinsey & Company estimate that the rate of change today is happening **10 times faster** and at **300 times** the scale of the First Industrial Revolution. These truly are unprecedented times.

There are countless technologies contributing to this Fourth Industrial Revolution, but cloud computing is perhaps the most significant catalyst.

A recent survey by Frost & Sullivan found that **80%** of companies are planning to increase their use of cloud managed services.

Despite the pervasive use of cloud services and the central role they play in this new age of information technology, there is still widespread concern surrounding security.

While these concerns are not statistically warranted, they are understandable. Cloud computing – by definition – requires the relinquishment of control. It's easy to understand

why senior decision makers and IT leaders might feel a sense of unease by surrendering their data and business critical applications to a third party.

Adding to their sense of unease is the persistent threat of cyber-attacks. These threats have evolved from the random and largely benign to sophisticated, well-funded and targeted attacks, posing very real threats to organisations of every size.

Finally, changes to legislation are forcing decision makers to take a long hard look at how cloud service providers manage their data.

The EU General Data Protection Regulation (GDPR), scheduled to come into full effect in May 2018, supersedes all existing regulations and is the most significant and far-reaching piece of data protection legislation in history. Organisations found to be in breach of GDPR could see penalties of up to 5 percent of a global turnover.

Without Trust, There is No Cloud

Security, privacy and transparency have been built into the foundations of the Azure platform.

Given the legislative and security climate, it's more important now than ever before that organisations looking to leverage cloud trust their service provider.

Given the legislative and security climate, it's more important now than ever before that organisations looking to leverage cloud, trust their service provider. Microsoft understands that without trust, there is no cloud.

Security, privacy and transparency have been built into the foundations of the Azure platform.

This begins with the Security Development Lifecycle (SDL), which addresses security at each and every phase of development.

However, building secure software is only one component of the Azure security strategy. Attacks can take advantage of infrastructure vulnerabilities such as system misconfiguration or abuse of privileges.

Operational Security Assurance (OSA) is Microsoft's framework, designed to address operational security needs by taking knowledge gathered from SDL and combining it with data gathered from hundreds of thousands of servers delivering more than 200 online services to more than 1 billion customers in 88 countries.

Physical security from the ground up

Azure is deployed in Microsoft's regional data centres. These locations are protected by layers of defence-in-depth security measures, which include closed-circuit television, security personnel, secure access management, perimeter fencing and real-time communication networks. This security model is used throughout every facility, right down to the physical server unit.

Data Security

All data is encrypted using 256-bit AES encryption,
one of the strongest block ciphers in existence.

Access to private data by Microsoft support personnel requires explicit permission from the customer, is granted on a 'just in time' basis and is revoked immediately after completion of a task.

Azure uses numerous encryption mechanisms, such as SSL/TLS, IPsec, and AES, to ensure customer data is protected, both in transit and at rest.

Data in transit between an application and Azure can be secured using Client-Side Encryption, HTTPs or SMB 3.0.

Azure Storage Service Encryption (SSE) provides encryption at rest. All data is encrypted using 256-bit AES encryption, one of the strongest block ciphers in existence. The key management, encryption and decryption processes are fully transparent and made available to the customer.

Virtual Hard Disks (VHDs) that contain sensitive information can be fully secured using BitLocker Drive Encryption.

Access to private data by Microsoft support personnel requires explicit permission from the customer, is granted on a 'just in time' basis and is revoked immediately after completion of a task. All access by support personnel is logged and made available to the customer.

Putting users in control

While Azure services have been built from the ground up to guarantee security and compliance, Microsoft also ensures that customers have the tools and flexibility needed to comply with organisational requirements and local regulations.

Azure Security Center gives organisations granular control over the security of their cloud assets.

Administrators can define policies for their subscriptions, deploy third-party security solutions and have a centralised view of the security state of all Azure resources. This makes Azure the only public cloud platform to offer continuous security-health monitoring.

Identity Management

Microsoft monitors all of its servers, networks and applications to identify and proactively prevent potential threats.

With the number of cloud-based enterprise applications increasing, identity management is becoming a challenge for many organisations. Azure Active Directory provides a powerful set of cloud-based identity and access management solutions, including Single Sign On (SSO), identity protection and Privileged Identity Management.
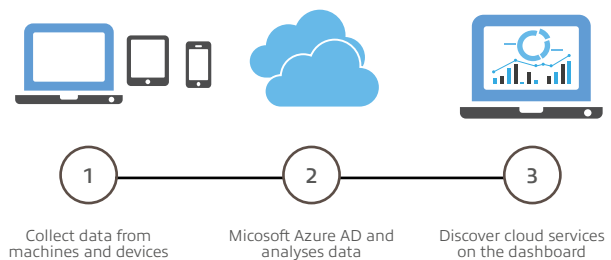
Azure AD supports thousands of enterprise-grade SaaS applications through pre-integrated templates meaning that organisations can now extend SSO into the cloud.

Controlling Shadow IT

According to Netskope's most recent Cloud Report, a typical enterprise uses more than 1,000 cloud services, 90 percent of which are not enterprise ready. The reality is, in a multi-cloud world, it is nearly impossible to eliminate shadow IT; however, Azure AD provides visibility across the IT ecosystem and discourages the use of unauthorised applications.

Azure AD Cloud App Discovery enables administrators to discover cloud applications used within the organisation. The tool detects and tracks application usage over time and identifies users.

Cloud App Discovery can track the number of users using a particular application in order to identify trends. Rather than taking a zero-tolerance approach, this data can be used by decision makers to ensure employees are given the right tools to perform effectively and educate end users as to the dangers of shadow IT.

1	2	3
Collect data from machines and devices	Micosoft Azure AD and analyses data	Discover cloud services on the dashboard

By analysing the data, it is possible to prioritise applications, bringing them under the control of IT by using single sign-on and conditional access policies.

Threat protection

Microsoft monitors all of its servers, networks and applications to identify and proactively prevent potential threats. This multifaceted threat management approach includes intrusion detection, distributed denial-of-service (DDoS) attack prevention, penetration testing, behavioural analytics, anomaly detection and machine learning capabilities.

Microsoft Antimalware for Azure not only protects Azure cloud services and virtual machines, but supports the deployment of third-party security solutions such as web application firewalls, network firewalls and intrusion detection

GDPR Compliance

Microsoft is the first global cloud services provider to publicly offer its customers a series of GDPR contractual assurances.

"So that you can trust the Microsoft products and services you use, we take a principled approach with strong commitments to privacy, security, compliance and transparency. This approach includes helping you on your journey to meet the requirements of the European Union's General Data Protection Regulation (GDPR)"

Rich Sauer – Microsoft Corporate Vice President & Deputy General Coun

Every organisation that collects, hosts or analyses the personal data of EU residents is subject to GDPR. While the financial levies for non-compliance have been well touted, many organisations have yet to realise that the new legislation affects the burden of compliance.

Under the current EU Data Protection Directive, it is the data controller (the customer) rather than processor (the cloud provider) that carries the burden of legal compliance. Processes are not directly subject to this existing legislation.

GDPR recognises the role that processors play in the protection of personal data and, as a result, cloud service providers must be able to guarantee that their services meet the technical and legal requirements set out by the legislation.

That said, controllers share the burden of responsibility and have a legal obligation to ensure that they only use processors capable of providing 'sufficient guarantees to implement appropriate technical and organisational measures' defined in GDPR.

This shared burden of responsibility results in an entirely new dynamic between the cloud service provider and the customer.

Microsoft is the first global cloud services provider to publicly offer its customers a series of GDPR contractual assurances. Microsoft has contractually committed to:

1. Respond to requests to correct, amend or delete personal data.

2. Detect and report personal data breaches.

3. Demonstrate your compliance with the GDPR.

Conclusion

> "We strongly believe that the momentum we're seeing has been possible because of what Azure offers and stands for – a comprehensive and secure Cloud platform across IaaS and PaaS, unparalleled integration with Office 365, unique hybrid experience with Azure Stack, first-class support for Linux and open-source tooling, and a robust partner ecosystem."
>
> Gartner

Microsoft is committed to delivering trustworthy cloud services and has invested significant resources into the creation and delivery of secure, private, and reliable cloud computing experiences.

Azure provides a wide range of resources and tools designed to help customers comply with complex regulations and is the only global cloud services provider to publicly offer GDPR-related contractual commitments.

We are witnessing a pivotal moment in human history. Technology has reshaped the very fabric of society. Cloud services like Azure are facilitating this revolution by enabling the collection, storage, and analysis of data at an unprecedented scale.

At a technical level, public clouds exist thanks to Moore's Law, the evolution of virtualisation technology and the development of high-speed bandwidths.

Of course, these technologies are of critical importance when it comes to attracting and retaining customers; but when it comes to signing on the dotted line, it's never about technical capabilities – it's about trust.

MKT2826-3

About Insight

From business and government organisations to healthcare and educational institutions, Insight empowers clients with Intelligent Technology Solutions™ to realise their goals. As a Fortune 500-ranked global provider of hardware, software, cloud and service solutions, our 6,400 teammates provide clients the guidance and expertise needed to select, implement and manage complex technology solutions to drive business outcomes. Through our world-class people, partnerships, services and delivery solutions, we help businesses run smarter.

For more information, please visit:

be.insight.com

Insight

Contact our Cloud team on:
+32 (0)2 263 60 20