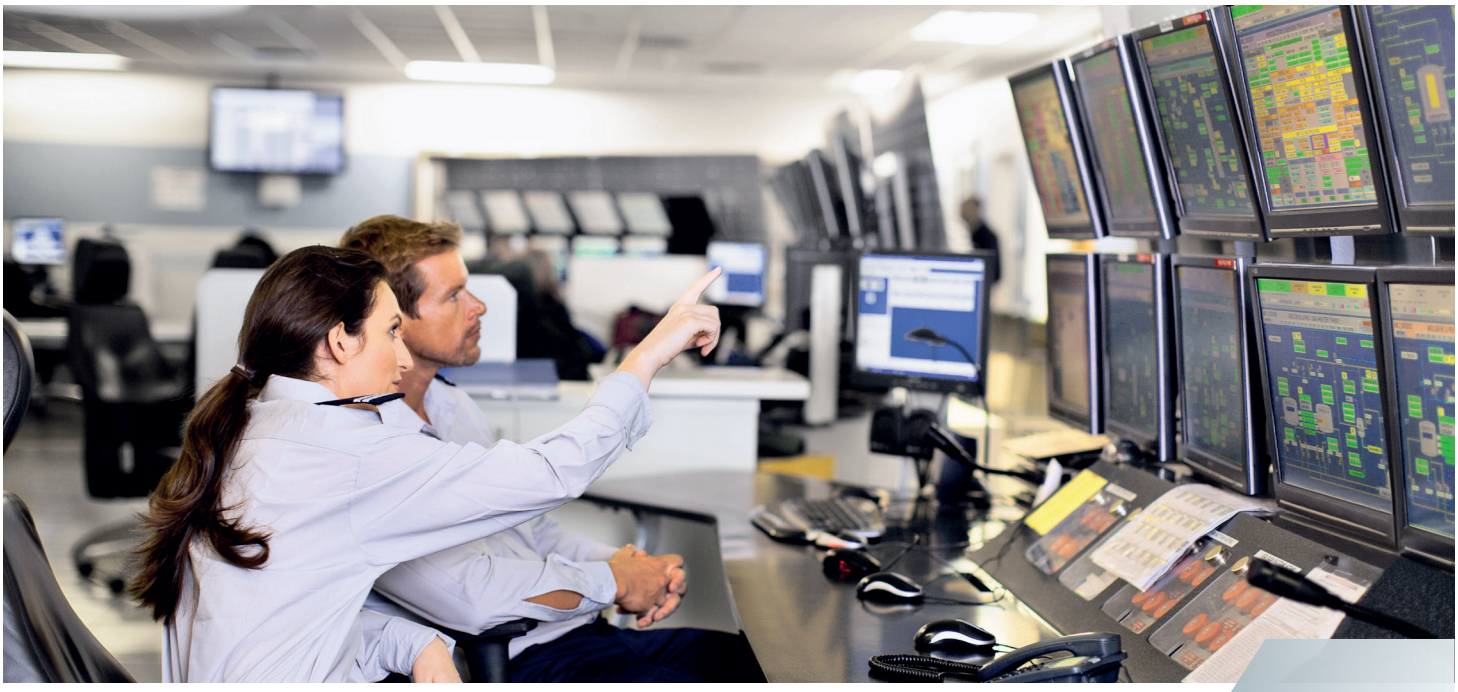
ORACLE
CLOUD PLATFORM

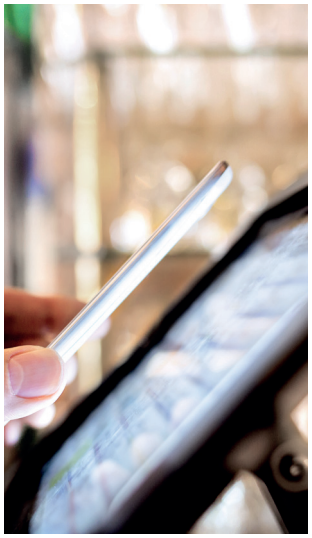


A secure path to digital transformation

How digital security can enable the journey to the cloud

ORACLE

Table of Contents



"Security is both a technical and a cultural issue within businesses, and if businesses are to transform boldly and with confidence, both must be addressed."

An urgent need to transform

The pace of business and innovation is increasing all the time. Organizations face an urgent imperative to transform and meet heightened consumer expectations. To succeed, they must implement a 'digital first' business model and improve the effectiveness of their digital channels. This includes responding to disruptive brands that are shaking up industries with new ways of engaging consumers. They must act now, because those organizations that do not respond effectively may be left behind, or consigned to history altogether.

An Oracle Cloud Agility study shows that businesses do recognise the threat of more innovative competitors and understand the importance of the rapid development of new business applications and services. But they must now put that knowledge into practice.

Much of this shift in the competitive landscape is driven by unprecedented levels of new data insight and from leaders recognising the economic significance of information their organization creates and owns.

For many, the necessary transformation remains a major challenge, particularly as many organizations, by their own admission, do not have the IT infrastructure in place at present to deliver on their ambition.

At the heart of digital transformation is a need to address two major factors – company culture and technology. Businesses have to want to change and have to commit to doing so in an effective way, bringing in new skills, adapting roles, encouraging innovation and instilling confidence in new business models, but they must also have the technology and the infrastructure to enable change to happen.

No issue sits at the intersection of culture and technology more clearly than security and in this report we look at the importance of security in helping businesses transform quickly without an increase in risk or any loss of control.

Security is both a technical and a cultural issue within businesses, and if businesses are to transform boldly and with confidence, both must be addressed.

This report shares the findings of research into the attitudes of security professionals and looks at how security, as an integral element of cloud technology, can become an enabler of transformation.

Businesses must transform and adopt new technologies to make them faster and more reactive, but they must do so in a secure, measured way.

Digital transformation is not just about smarter use of technology and opening up digital channels, such as online and mobile, to consumers. It is also about the smarter use of data which, if used to inform better decisions can have a huge value to business. However, that increasing value must be reflected by the measures in place to keep that data secure wherever and whenever it is in use, in transit or at rest.

With digital services increasingly vital in achieving the goal of establishing transformative business models and improved customer engagement, it is clear mastering digital identities is crucial. Users must be able to access information from a growing range of locations and devices.

With the right security in place, businesses can achieve the freedom and flexibility they need to thrive in a digital economy with confidence.

52% of businesses believe the opportunity to improve their data security will be a key driver for cloud adoption, while 48% believe the opportunity to better enforce security policies will increase cloud adoption.

Research Methodology

Oracle commissioned Coleman Parkes to survey more than 1,000 senior security decision makers – encompassing the job titles of head of IT security, chief information and security officer, head of compliance, chief security officer and head of information security. The businesses ranged in size from 500 employees to more than 10,000 and were drawn from manufacturing, financial services, telecommunications, media and entertainment, retail and distribution, public sector, and energy and utilities. The research covers the UK, Germany, Italy, Benelux, Poland, Russia and Turkey, providing a representative section of the European market as a whole.

Cloud and digital security: the foundations of digital transformation

The combination of cloud technology and digital security hold the key to making digital transformation a reality.

Cloud technology provides the opportunity to unify business processes and free data from silos. It offers an agile environment that will give businesses the ability to adapt quickly to the changing needs of their customers and their industry.

Cloud also supports the key requirements of the data-driven business, namely the automation of tasks for customers and employees and the use of data to discover ways to create new products, services and business models.

In short, cloud provides the platform and processes that support transformation, allowing businesses to grow and innovate freely and quickly.

But the efficiencies and flexibility gained from the journey to the cloud must be complemented by security. Indeed, digital security must be ever-present, as standard. It can no longer be an add-on or an obstacle to giving employees the freedom to work quickly and effectively.

As such, it must be woven in to the way businesses work and inevitably that will mean residing in the cloud along with the data and applications businesses are using. By taking this approach, security can, and should be, an enabler of the journey to the cloud.

And this is backed up by Oracle research, which found that 52% of businesses believe the opportunity to improve their data security will be a key driver for cloud adoption, while 48% believe the opportunity to better enforce security policies will increase cloud adoption.

Of the following, which are the most relevant security factors that could increase cloud adoption in your organisation?

When cloud and digital security are combined, they represent a strong foundation that supports digital transformation. If one is missing, the transformational edifice could come crashing down.

Finding the secure path to the cloud

The journey to the cloud must be plotted strategically, with digital security at its very centre. It cannot happen overnight. It must not be hasty – or worse, reckless.

If the enterprise approach to IT has become fragmented over time then it is highly likely there is a patchwork of security in place.

That patchwork of security, related to piecemeal or ad hoc implementations of applications and infrastructure over time, is not necessarily insecure, but it will be difficult to manage and costly to maintain and complexity certainly creates the potential for greater insecurity.

"80% of those surveyed believe digital transformation, underpinned by strong security, will help them improve customer experience and ultimately grow their business".

A well planned move to the cloud will allow businesses to create a consistent, company-wide level of digital security. The move to the cloud must not replicate the issue of silos that exist within the on-premise environments of some businesses. This may be particularly relevant to organisations who have already made standalone, tactical investments of cloud.

Many cloud solutions on the market are often narrow in scope and are too inflexibly tethered to one definition of the cloud. The reality is businesses stand to benefit a great deal from using an integrated blend of public, private and hybrid cloud.

For businesses to achieve the flexibility they need, data and applications need to be transferred with speed and ease between different cloud instances and accessed via multiple devices, whether by customers or by employees. This requires a unified environment based on flexible cloud infrastructure, a powerful standards-based platform and a comprehensive portfolio of business applications, unified by a common ease of use, subscription-based payment and security at every layer.

Anything else is unnecessary complexity, with the potential security issues that creates.

Security as an enabler

Businesses are clearly taking cloud very seriously and many of the security professionals surveyed have overcome some outdated concerns about the security of the cloud. In fact, most now see it as the most secure way to transform their business.

Research conducted by Oracle found that many companies are at different stages of their journey to the cloud and are approaching it in very different ways.

The research found around half (48%) of businesses already have a company-wide policy in place governing the use of cloud services for employees and departments, and about 36% define a list of minimum security requirements that each cloud service has to meet. However, it was also revealed that 10% leave it up to individual business units to set their own policies regarding the use of cloud applications and services, and 6% didn't set any policy.

This approach needs to be addressed, as it can lead to implementations that are disjointed and lack an all-encompassing approach to security. This patchwork of policies may leave businesses with gaps in their security.

Organisations may find it beneficial to put in place a company-wide strategy for their journey to the cloud, at the infrastructure, platform and application layer, in order to unlock the benefits of improved consistency and security.

The importance of transformation has made cloud a topic for boardroom conversation, with 93% of respondents saying the use of cloud services is now a subject for consideration around the top table. Clearly businesses, from the top down, are keen to embrace the benefits cloud can deliver.

A similar number (94%) said the security of data in the cloud is also subject to consideration at the very top of the business.

The move to the cloud will not happen overnight, but it is bound to happen eventually. 80% of those surveyed believe digital transformation, underpinned by strong security, will boost their business and improve customer experience.

In addition, security professionals understand security cannot be an obstacle to progress. It must be an enabler. Almost four-fifths (78%) say business agility and the ability to react quickly to changing business demands is just as important as being secure.

"More than three quarters (78%) agreed that cloud providers are more likely to be able to keep security measures current and up to date than they can".

Fortunately, the two are not mutually exclusive. Businesses can now have the transformational benefits of cloud in a highly secure way.

The majority of security professionals accept that cloud providers will be an important ally in securing and transforming their businesses. More than three quarters (78%) agreed that cloud providers are more likely to be able to keep security measures current and up to date than they can.

Of course not all cloud vendors are the same and each must work hard to earn and repay the trust of their customers. Cloud vendors must have the strictest measures in place and the strongest defences.

That starts and ends with their own people. Cloud vendors are taking measures to ensure access to their systems is strictly controlled and limited only to essential personnel, with thorough vetting, screening and ongoing, audited monitoring of access in place.

Cloud providers are also taking steps to ensure the most robust defences against external threats, from denial-of-service mitigation to world class anti-malware and intrusion detection and prevention.

Undoubtedly, leading cloud providers can do this more effectively than individual businesses but they must never get complacent. Indeed, 78% of respondents to Oracle's research either agreed or strongly agreed that it can be easier for large cloud service providers to implement the latest security technologies and quickly react to threats than internal staff.

Cloud security must continually evolve if it is to stay ahead of the threats which exist. But while cloud providers play a crucial role in securing businesses, the responsibility for security cannot lie solely with them. Cloud infrastructure and platform services must operate under a model of shared responsibility.

The cloud vendor is responsible for the security of the underlying cloud infrastructure, but it is down to the customer to ensure workloads and platform services are also secured.

As an example, the location of and access to encryption keys was deemed a high risk associated with moving to the cloud by 39% of survey respondents and of medium concern by 47%. Customers should therefore consider keeping encryption keys within their data centers to be handled locally, rather than putting them in the cloud. .

Of course, the configuration work customers must perform is dependent on the services they use, but it is critical they play a prominent role.

Who goes there?

Key to making the move to cloud secure and as effective as possible will be the smarter use of identity and access management to ensure services and data can be accessed readily and securely.

For example, by 2020 87% of organizations expect to be delivering a multi-channel experience and 67% will interact with customers via mobile apps supported by cloud services. When it comes to managing digital identity, organizations need to make these interactions as secure – but also as seamless – as possible and plan also to enable increased self-service.

More than half (53%) of businesses surveyed by Oracle are already managing all identity and access management on-premise on corporate owned systems. But 79% of security

"79% of security decision makers are either likely or very likely to put identity and access management in the cloud".

decision makers would be likely or very likely to put identity and access management in the cloud, providing they could maintain full control.

That 'best of both worlds' scenario is certainly achievable. With a hybrid identity solution, businesses can maintain control of a single point of management and a single view of employees, partners, and customers across their integrated on-premise and cloud environments.

Such a hybrid approach allows businesses to decide how they manage identities, whether on-premise, in the cloud, or both. This is particularly important while businesses are on their journey to the cloud from an on-premise world, particularly with developers accessing data and resources across different environments.

A fit-for-cloud identity and access management system must also ensure security without eroding any of the efficiency and ease of use businesses stand to benefit from. As such, some of the onus for keeping data secure must be taken off the users. A benefit of cloud is that it is easier to integrate technologies such as context-aware authentication which draws upon the ability to see not just what the user knows in terms of password or user ID, but also what they are doing and where they are, to determine validity and verification.

Oracle builds security into its integrated technology stack, with the Identity Cloud Service (IDCS) the latest example of this thinking. The on-demand identity service grants users single sign-on access to cloud applications for a seamless and secure experience across multiple channels.

IDCS can determine whether a user is who they say they are by examining factors received from the device, location, or network. If anything is out of the ordinary, IDCS will simply ask for additional information to verify. It enables businesses to manage identities across cloud and on-premise environments.

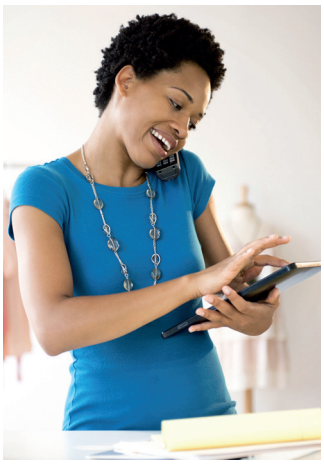
It's obviously important to recognise the perceived security threats of moving to the cloud. The top three risks cited in our research were loss or theft of critical data; confidentiality of information/data in the light of legislation, laws and regulations; and encryption of data and the strength of encryption. All of these can be addressed, however, by adopting an effective compliance and security strategy.

Just under half (45%) of respondents rated the loss or theft of critical data is a high risk with 40% classing it as a medium risk. But this can be addressed, among others, by timely examination of audit data to detect unauthorised activity before it has a financial impact.

Oracle Database Security provides the comprehensive auditing, collection and reporting needed to enable this, while Oracle Audit Vault and Database Firewall provides real-time monitoring through the consolidation of audit data from a wide range of sources.

A slightly lower proportion of businesses (43%) felt confidentiality of information/data in the light of legislation, laws and regulations is a high risk, with another 44% saying it is a medium risk.

Again, there are ways to help address this in the cloud. For example, Oracle Advanced Security – Data Redaction can provide selective, on-the-fly redaction or masking of personal data in SQL query results before returning it to applications. This ensures unauthorised users won't be able to view the data.



Encryption of data and the strength of encryption, meanwhile, was seen as a high risk by 41% and a medium risk by 45%. Oracle Database Security can help here, as it provides preventive controls that have a minimal impact on performance and IT operations, while Oracle Advanced Security - Transparent Data Encryption encrypts data directly at the source, avoiding the resource-intensive task of locating and encrypting data in backup, data dumps and log files.

Which areas do you consider to pose the highest risk

However, businesses can rest assured that the applicable security best practices they are already familiar with can be retained when moving to the cloud.

Currently, 62% of those surveyed said their companies currently encrypt data, 53% support privileged user access control, 49% apply governance and auditing, 47% implement mobile security and 44% apply two-factor authentication. All of these can be retained when moving to the cloud.

What are you waiting for?

Businesses may want to consider making the move to the cloud in order to achieve their digital transformation goals – goals that are critical in the digital economy.

As this report has established, most security professionals have overcome many of the perceived concerns about cloud security that may have been holding them back from the benefits the cloud can deliver and the freedom to innovate that it brings.

By planning the move effectively businesses can now improve their working practises and improve operational efficiency and security.

As has been the case since computing became integral to businesses operations, security is a fundamental requirement. The journey to the cloud to achieve digital transformation is no different.

To learn more please go to **oracle.com/identity** and **oracle.com/database/security**

ORACLE

Oracle Corporation, Worldwide Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

facebook.com/oraclesecurity

twitter.com/OracleSecurity

blogs.oracle.com/oracleidm

blogs.oracle.com/securityinsideout/

www.oracle.com/identity

Integrated Cloud Applications & Platform Services

Oracle is committed to developing practices and products that help protect the environment