White paper
The new security challenges for delivering bimodal IT

The demands of employees and customers on enterprise IT have never been greater. It means IT must be faster and smarter in the face of digital disruption, rapidly evolving markets and new ways of working and doing business - while still retaining the control and oversight required to guarantee compliance and security.

Introduction

The demands of employees and customers on enterprise IT have never been greater. It means IT must be faster and smarter in the face of digital disruption, rapidly evolving markets and new ways of working and doing business - while still retaining the control and oversight required to guarantee compliance and security.

It requires a new type of IT delivery - what Gartner has coined 'bimodal IT' - that balances the stability, safety and accuracy of legacy in-house IT investments with the agility, speed and innovation of continuous delivery through cloud services and apps.

Make no mistake; bimodal IT is taking hold in the enterprise. Gartner predicts three-quarters of organisations will have implemented bimodal IT strategies by 2017 and says 39 per cent of European CIOs are already on a journey towards bimodal IT.

Getting bimodal IT delivery right can bring huge benefits to the business. In a world of constant evolution and digital disruption this two-pronged approach enables IT to support this evolution. It supports faster prototyping and rapid delivery and enables the business to better respond to changing markets and customer demands.

Underpinning bimodal IT and fundamental to getting it right, however, is security. This new and evolving model of IT delivery poses new security challenges that organisations must address if they want to protect their data, avoid reputational damage and reap the benefits of bimodal IT.

What are the new security challenges for managing bimodal IT?

The security challenges around traditional 'mode 1' legacy in-house IT will already be familiar to most organisations - infrastructure, security (across the network, data and applications) and enabling mobility. So how is 'mode 2' security different? This fast, continuous and agile IT delivery demands more focus on data and information security. The challenges here are exacerbated by pace, control and broader stakeholders. 'Mode 2' is about being able to protect and back-up that data wherever it resides and secure the data flows and communications across different environments and services.

It is fundamentally a shift from purely securing the assets and infrastructure to one that secures data across both legacy and cloud environments. Here are some of the new security challenges for bimodal IT delivery.

Continuous delivery

DevOps is a key component of 'mode 2' IT delivery. It uses agile, iterative development methods and continuous integration and delivery to reduce application release cycles. This means IT can better meet the rapidly evolving needs of business users and customers. The security question here is how do you maintain the appropriate security controls and governance in this continuous delivery and integration environment?

Cloud service integration

The potential security weak link here is the integration and communication between those 'mode 2' cloud services and your 'mode 1' in-house systems of record. Specifically the risk is in the software code and configuration. For example, if you misconfigure or change the security profile in your cloud service this can be easily missed and leave a weak entry point to internal systems given the public internet-facing nature of some of these cloud services. The question is how do you maintain the consistency and protection of your environment when developers have operational access to infrastructure and network configuration in the cloud? A key issue here is controlling both what developers have access to and what they are allowed to do to those applications and services they have authorisation to configure and update.

Shadow IT

Gartner estimates that just over a third (35 per cent) of the money spent on cloud is being spent on shadow IT. This is evident across many organisations where individual departments such as marketing and HR are acting like small start-ups within the organisation, buying in new tools and cloud services - often sidestepping the IT department altogether and potentially exposing the organisation to issues around security, compliance, visibility and cost management.

Integration of multiple cloud suppliers

Putting the cloud at the forefront of service delivery means organisations will have to integrate and manage many more suppliers than before. A key question that organisations need to be able to answer is if your service goes down, do you know where the data resides and do you have access to a back-up? Contractual terms and use cases may differ around issues such as ownership and location of data. Some of these suppliers will also have limited terms or mitigations such as physical access. The implications of these SLAs and contractual terms for data security are that they are often not

understood by shadow IT adopters who might be deploying these cloud services and apps without the necessary IT governance and oversight.

Increased risk of reputational damage

By using bimodal IT to deliver more digital services this in itself increases security risks. The very nature of digital business with mobile apps, use of social media and online services puts the organisation at risk of cyber-attack and reputational damage.

Mobile device consumption being the norm

The number of mobile devices staff use to perform their jobs on a daily basis will continue to proliferate, as will the breadth of the application ecosystem to enable them to fulfil their daily tasks. Businesses will also need to balance the strategic view on application development with the tactical approach to exploit opportunities. The challenge in bimodal IT is that for these mobile mode 2 applications to deliver their outcomes, they will need to interact with transactional systems; hence the unavoidable necessity to address the security requirements of these aspects.

Recommendations - how to secure your organisation's data in a bimodal IT world

Don't approach the two modes of bimodal IT as silos in isolation when it comes to security. The key is to understand the links between the traditional and new environments.

The first step for security in this transition to a bimodal IT model is risk assessment for each element of the IT environments based on the data that flows between them. Understand the data flows then adjust your risk model accordingly. It is ultimately about risk assessment and management across both 'mode 1' and 'mode 2' - not separately in silos.

Here are some key ways to address the security challenges of bimodal IT.

Continuous risk management

After the initial risk assessment for bimodal IT a set of control requirements can then be defined. Moving into operational mode, these control mechanisms can be flexed in line with business requirements and based on how the risk changes following any change in data flows. The continuous delivery nature of DevOps and cloud in a bimodal environment means these risk management processes are not one-off exercises. If the business is operating in a continuous delivery model then risk management also needs to be continuous.

Automation

Automation is absolutely essential to addressing bimodal IT security issues. Application and data monitoring and automation of the risk management processes ensure they can be operationalised in an easy and repeatable way. One example is the risk around continuous software integration and release cycles. This can be mitigated through principles and security processes that include technology to automate the identification and resolution of poor coding practice.

Encryption

There is a greater requirement for encryption technologies in bimodal IT delivery to remove some of the risks posed to the data as it flows across public or private clouds and in-house IT. An example is the use of tokenisation, where a piece of sensitive data is substituted with a token containing no meaningful sensitive data. This token links back to the original data through a tokenisation system that keeps it encrypted and securely stored. Also consider technologies such as data leakage prevention and monitoring tools.

Identity

Identity management is essential to enforce the appropriate levels of trust and verification for people accessing data. Manage multiple IDs and multiple personas both internally and externally and know where data is being stored and from where it is being accessed. This covers areas such as identity and access management across multiple cloud service providers and it is also about being able to distinguish when access should be granted in one context and limited or denied in another. But it's not just about the technology. Back this up with effective and workable security policies, supported by people-centric education and awareness frameworks.

Security by design

Bake security in from the start and then throughout. Trying to retrofit security to a bimodal IT environment once the data is flowing will be a nightmare and need a lot more in terms of data/application traffic discovery to get right.

Summary

Clearly bimodal IT delivery poses new questions about how to manage security for the IT department. But these challenges aren't insurmountable. The fundamental thing to remember is that it is about securing data and information - wherever it flows and is stored.

Here at Fujitsu we recommend a risk-based approach across both 'slow' and 'fast' modes of IT that is aligned with business needs. And this isn't a tick-box exercise of compliance in isolation.

It's important that security for bimodal IT isn't so risk averse or cumbersome that it doesn't support the speed of continuous change required by the business. This means 'just enough' but effective governance, engagement with business, data asset owners and security stakeholders to ensure that bimodal IT security risks are articulated and managed effectively.

This is a continuous process and needs effective buy-in to deliver against the needs to manage the risk in an environment of increasing speed to change.

Next steps

Tackling these security challenges around bimodal IT delivery will enable businesses to unlock the benefits of the cloud and Hybrid IT and innovate and respond rapidly to the speed of change in today's digital world.

For more information on Fujitsu's approach and recommendations for managing bimodal IT security in a Hybrid IT world please contact us at: askfujitsu@uk.fujitsu.com

Contact
ASK FUJITSU
Tel: +44 (0) 1235 79 7711
E-mail: askfujitsu@uk.fujitsu.com
Ref: 3595
www.uk.fujitsu.com