White paper
7 top data security risks for Hybrid IT - and how to tackle them

Traditional IT and network boundaries are blurring in the world of Hybrid IT, which blends cloud - both public and private - and internal IT to give organisations the flexibility to grow and innovate rapidly.

Introduction

Traditional IT and network boundaries are blurring in the world of Hybrid IT, which blends cloud - both public and private - and internal IT to give organisations the flexibility to grow and innovate rapidly.

Hybrid IT ultimately offers businesses the potential to use the information they have in new ways and to survive and thrive in today's digital environment. But it also has implications for data security compared to traditional IT. The question for organisations is how can they address these new risks and protect critical information assets and, in doing so, make security the enabler that supports this move to cloud and Hybrid IT environments?

In this whitepaper we will show how IT security can remove the barriers and risks associated with Hybrid IT. Done right, security can enable faster, cheaper and more flexible IT and in turn drive innovation and deliver real value to the business.

What are the security challenges for Hybrid IT?

1. Data aggregation

The aggregation of data across in-house IT systems and cloud services poses a security risk. Big Data applications might bring together items previously stored separately in different systems. Those analytics tools and applications often also require little technical expertise to deploy and use, meaning employees might not be aware of the aggregation and security implications of using them.

Public sources of data could also be pulled in as part of this aggregation. For example, an app might be consuming the location data on the user's smartphone. Aggregated, that information could change the risk profile of data, potentially making it more valuable than it is in isolation and turning it into something that could be damaging to company reputation or harm competitive advantage if it was lost or stolen.

Recommendation: Start to take control and address these challenges by defining policies on how data is monitored, how that data is secured and educating users on the potential risk. Assess your organisation, profile data and classify it. Understand what data is the most sensitive, what data is being gathered, where and how is it being stored. Which applications (and application ecosystems) are able to access this data? Who is using those applications, over which access channels? From this assessment establish the potential threats – be that system, internal and external as well as any heightened risks presented from data aggregation.

2. Application Programming Interfaces (APIs)

The use of cloud services within hybrid IT means businesses use public, or open, APIs from cloud service and application providers and open up their legacy applications to serve up data through the APIs. These APIs enable organisations to manage and integrate those cloud services with their own networks and infrastructure and to customise and add richness to the user experience.

But these APIs also bring security risks and, due to a lack of internal skills, many organisations probably don't even know what their full exposure to this risk is. Managing these API risks requires knowledge of new programming interfaces and complex network configuration, which pushes the current limits of skills and knowledge within the IT department. That skills gap potentially leaves company data exposed to security flaws embedded in a cloud service's API code, such as code that allows anonymous access or unencrypted clear-text transmission of sensitive data.

Recommendation: Ensure you have the right level of skills and tools to properly review API code and potential exploits. That might mean bringing in an external partner with the expertise to help manage that risk and bring control and insight. Addressing this risk enables the business to take full advantage of the benefits of using APIs and related cloud services and applications but with the reassurance of appropriate governance and security of the data.

3. DevOps

DevOps brings together development, operations and testing into very rapid cycles to speed up the rate of change in applications and so help businesses compete in the digital world. Indeed, analyst Gartner predicts DevOps will evolve from a niche strategy to a mainstream strategy used by a quarter of Global 2000 organisations by 2016.[1]

In a Hybrid IT environment DevOps cuts application release cycles from weeks or months to days and even hours. While that's great for getting applications out to users more rapidly and supporting the wider business needs it also means a shorter window to assess those application changes and any potential risks. Security professionals are also usually the last to be consulted in this process, which can slow things down and reduce the benefits of DevOps.

Recommendation: Involve security early in a principle-led design approach so that a governance forum and control test process exists. DevOps automation can provide the opportunity to be proactive in building security compliance into the continuous integration processes. New tools make it easier for organisations to monitor releases for security risks, particularly around public APIs, and flag up alerts that need addressing. This is more important than ever given the speed and scale of exploitation of vulnerabilities in web applications today. By balancing the audit and security needs with business goals it helps standardise secure configuration settings and enables faster deployments within a solid governance framework.

4. Resilience and redundancy

Many cloud service providers have better levels of availability and redundancy than in-house IT organisations. The latest annual study by the Uptime Institute found nearly half (47 per cent) of enterprises have suffered one or more business-impacting outages at their in-house production data centre in the past 12 months, while only 25 per cent of co-location providers reported the same.[2]

However, the rules change for Hybrid IT when integrating data across cloud service providers and internal IT systems. As applications move around that environment, where does that data reside, where is it backed up and can it be accessed if a service goes down? It might come as a surprise, for example, that many cloud service providers are under no contractual obligation to protect or recover data in the event of a loss.

Recommendation: Design resilience and redundancy into both the applications and the network, and don't assume anything about the contractual obligations of a cloud provider to secure and back up your data. Ask what security and availability guarantees your cloud provider offers and what happens if the service fails or the provider goes out of business. What is the back-up plan for maintaining access to that data and the security of it? External partners can provide this insight and due diligence to those contracts and service level agreements. Have policies to ensure information is backed up to a separate data store controlled by the organisation, whether that is another cloud service or an on-premise data vault, depending on the sensitivity and importance of the data.

5. Compliance

One of the specific issues for Hybrid IT is having the controls and oversight to ensure the integration and communication between the different computing environments is compliant with relevant regulations and legislation.

That compliance burden will vary from business to business but the barriers to moving data and applications to the cloud and a Hybrid IT setup are being lowered, even in highly regulated industries. The UK's Financial Conduct Authority, for example, issued new guidance in November 2015 giving the green light for banks and other financial services companies to use cloud services, including public cloud, so long as appropriate safeguards are in place.

But there is still a lot of data protection, privacy and industry sector-specific legislation and regulations that organisations need to stay on top of, particularly the ever changing rules governing the movement and protection of data around Europe and between Europe and other regions of the world.

Recommendation: Ensure - and be able to demonstrate - that not only your different clouds and traditional IT systems are compliant but also that processes and tools are in place to ensure the way the applications and data integrate and communicate between those environments is compliant. For sensitive data this might mean encryption such as tokenisation, for example. Also consider technologies such as data leakage prevention and monitoring tools.

6. Security integration across clouds

One of the features of Hybrid IT is that applications and data will be moving from one service provider to another at a greater rate than has been the case in the past. An organisation might, for example, want to do a market test and go from one cloud provider to another. So-called cloud bursting is another scenario when a company might want to cope with spikes in demand such as peak online shopping periods like Black Friday by bursting an application out to the cloud.

Recommendation: Have clear policies and processes to integrate and synchronise security controls over different clouds and legacy applications. Shift IT security from its traditional focus of the network perimeter and devices to the applications and data for defence in depth. Build security into applications and workloads so that it moves with them around this Hybrid IT environment, protecting the data regardless of who is accessing it and from any location.

7. Skills

Many organisations will not have the internal skills and knowledge within their own IT teams to integrate and co-ordinate security across a Hybrid IT environment so that data is protected in a robust and consistent way. Moreover they are unlikely to have the skills to satisfy themselves of the efficacy of measures that others propose to them.

Recommendation: Accurately assess your organisation's skills requirements and define a strategy to close, and keep closed, the skills gap. That could be by boosting internal skills, bringing in an external partner with that expertise or a combination of both.

Summary

You only have to read the news to see the financial and brand reputation damage done to businesses by high profile data security breaches and the threats will only continue to increase in volume and sophistication.

Hybrid IT introduces new complexities and its openness means traditional security tools and techniques are too reactive and outdated in an environment with so many moving parts. Get it wrong and there are huge risks to data security, from accidental leakage to an attacker exploiting a vulnerability in a public API to gain access to your data. But an overly restrictive approach where IT security becomes a blocker to people doing their jobs can lead to people developing less secure workarounds, through shadow IT, which comes with no oversight or control for the IT department and poses its own risks.

Get it right, however, and security allows the IT organisation to satisfy existing regulatory requirements and company security policies while exploiting the latest technologies to support innovative new services designed to improve productivity, collaboration and customer satisfaction.

By being on the front foot in addressing the challenges and risks, IT security has the opportunity to add value and become the enabler that underpins the business in the Hybrid IT world.

More on Hybrid IT

For more on this subject, check out the Hybrid Hive blog from Fujitsu partner Brocade.

Next steps

Understanding and tackling the security challenges will enable businesses to unlock the benefits of the cloud and Hybrid IT. It allows organisations to make best use of the resources they have invested in to 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 security in a Hybrid IT world please contact us at: askfujitsu@uk.fujitsu.com

Contact
Fujitsu Asia Pte Ltd
Nexus @ one north
1 Fusionopolis Link, #04-01, Singapore 138542
Email: info@sg.fujitsu.com
Web: sg.fujitsu.com