ADEPT 4

IT AS A SERVICE

Security on the move

Contents

Security on the move

Protecting your data on any device, wherever you are

We're not all tied to our desks at the office any more. We're used to being able to access online tools, apps and content at any time, from any device. Staff increasingly use their own phones and tablets to keep on top of work-related activity. It means that productivity is increased and business is boosted.

It also means that information is more often than not being transmitted across devices that the organisation doesn't control, and which sit outside the corporate network.

Just look at these stats from Microsoft:

- >80% of employees use unapproved Cloud-based apps. This presents unknown security risks and potential compliance violations
- C. 17 Cloud apps are used by each employee invisibly to the company. Do they meet security, privacy and compliance requirements?
- While 13% of an organisation's files are shared externally, 25% of these are then shared publically. Unsecure file sharing such as this increases the potential for data loss and data leaks, again risking violating compliance standards
- 70%of companies permit cloud admin activity on unsecured networks creating new unprotected points of entry for external threats
- 75% of privileged cloud accounts aren't used. Not only does this mean wasted licenses but also needless potential points of entry for cyber attacks
- In 91% of organisations, employees allow their personal accounts to access a company's cloud storage, increasing the risk of identity breaches and further jeopardising data privacy.

Let's investigate the key areas of concern: identity, device and data.

1. Identity

The challenge

No-one wants to have to remember a different login for every tool or app they use and to save time and frustration, many companies have introduced Single Sign On (SSO) whereby one login process allows access to all the services an individual needs.

That's fine for on premise tools held in your own datacentre but inadequate in face of the rise of Cloud-based apps. It would be nigh on impossible to manage identities if every SaaS (Software as a Service) app had to connect to every company's on premise identity management technology.

The answer

Use Cloud to manage Cloud. With the right solution, you can still use an on premise directory but it goes through a secure gateway which performs the functionality of connecting directly to each SaaS app. It means that users' identities come from your own directory, under your control but one login provides access to both on premise and Cloud-based services.

2. Device

The challenge

Just about every one of us has at least one mobile device, and, it appears that one in ten enterprises have at least one compromised mobile device on their network[1] leaving them vulnerable to data loss, hacks and worse.

Sources of compromised devices:

- A growing number of anti-detection tools which conceal the fact that a device has been compromised so the company doesn't know it needs to take action.
- More than half of companies have at least one device that doesn't fulfil compliance requirements such as those with PIN protection that has been disabled or which haven't updated their security policies.
- <10% companies enforce data patching
- >95% don't protect against mobile malware

The answer

Mobile Device Management (MDM) and Mobile Application Management (MAM) has been the accepted route to overcome these problems. It allows IT administrators to remotely configure, manage and secure devices so that accounts can be set up on a number of devices without individuals having to come physically into the office especially for that purpose.

In addition, IT admins retain full control over the company's email. They can remotely delete emails and data should an employee leave or lose their device. Of course, it also means that security policies are followed: password, login and auto-lock policies are upheld, policies can be pushed out quickly and easily across every device on the network.

[1] Mobile Security Risk Review, MobileIron

However, traditional MDM and MAM solutions have been run on premise. That's fine as long as the remote apps being accessed from the device is run on premise too. As we've already discussed, that's not always the case, and is increasingly becoming rarer. It reduces both performance and the ability to scale. The beauty of using Cloud based MDM and MAM –in addition to the benefits of traditional methods -is that once devices receive policies via the Cloud, apps can communicate directly with both on premise and SaaS apps.

The right solution can also run and manage your servers and software for device management and update device management software automatically. This can be a particular blessing given the frequent patches and updates issued for iOS, Android and Windows – some of which affect how devices are managed so creating a knock-on effect for the device management software.

3. Data

The challenge

While we've always valued the ability to control who has access to what data - what they can do with it and how it can be protected throughout its life - now that collaboration is becoming easier with the advent of the Cloud, it is at the heart of the way we work today and becoming more and more important.

If for example, you need to share some information with another company – a customer or supplier for example – and you need to make sure only a certain set of individuals can access it, any attempt to open it has to be verified by an information protection service. Previously, that would mean establishing a point-to-point link between the two organisations' identity management systems.

Understandably, this was impractical and people were reluctant to go to the time and effort to take this route.

The answer

Collaboration between companies is a lot simpler now. By linking to specific Cloud-based services, each organisation can set up direct connections to which they only have to connect once. Identities are verified and managed, policies can be defined and upheld for sharing protected data and the information can be encrypted and /or tracked to monitor successful and unsuccessful access attempts so you can keep an eye on how the data is being used.

To make it even more simple, Rights Management can make the secure sharing of documents and information seamless both across your own organisation and outside of it. It means that rules and conditions can be placed on documents so you can define who can view them and whether they can (eg) edit, print or forward. Rights Management also lets you track the actions performed on these documents and remove rights if necessary.

4. Summary

Identity, device and content protection has traditionally been delivered by software running in-house. Identities, devices and content are no longer kept in-house. Employees are used to accessing what they need when they need it and from where they are –from on premise to software-as-a-service (SaaS) to custom cloud apps.

ADEPT 4

T: 01925 398255
E: servicedesk@adept4.co.uk
W: www.adept4.co.uk
7750 Daresbury Business Park, Daresbury Office Village
Warrington, Cheshire, WA4 4BS