



ENABLING LARGE FILE TRANSFERS WITHOUT MAKING IT THE WILD WEST

Striking a balance between the users' needs to send large files and retaining management controls, data security, governance and brand integrity





ENABLING LARGE FILE TRANSFERS WITHOUT MAKING IT THE WILD WEST

STRIKING A BALANCE BETWEEN THE USERS' NEEDS TO SEND LARGE FILES AND RETAINING MANAGEMENT CONTROLS, DATA SECURITY, GOVERNANCE AND BRAND INTEGRITY

It's a situation we all recognise: users from the intern to the chief executive think they know better than IT so they bring in their own smartphones, tablets, laptops, websites, software and apps and use them to do the job "better" than was possible with the tools officially sanctioned. For them, IT is a provider of old-fashioned services that don't work as well as consumer offerings so, quite literally, they take matters into their own hands.

Bring Your Own Device mania is endemic in workplaces. Some say BYOD is great because it allows people to be more creative and effective. Others hate it because they think it means that organisations are losing control, leaving themselves open to licensing issues at least, and security and data privacy challenges at worst. It's every IT director's worst nightmare: discovering that critical data has been compromised, lost or sent to the wrong person and yet it's happened to so many big organisations from Sony to Credit Suisse, HMRC and the Ministry of Defence. And it's even worse if the IT director only finds out about it by reading about it in the news.

The issue of large file transfer (and 'Bring Your Own File Transfer') highlights the problem here. Many office workers need to send big files outside the organisation but, in order to preserve bandwidth and storage, the IT department's email usage policies preclude attachments over a certain size. So, rather than involve IT, users go their own way, deploying consumer-grade services better suited to kids swapping music than the best practices of a well-run enterprise. It's a very common scenario and understandable to some extent but everything we know about security, corporate governance, branding and management control tells us that this can't be allowed to continue.

Organisations need to provide secure services for users to send the rich media files and sensitive corporate information. The alternative is to risk an anarchic scenario closer to a Wild West saloon than a healthy, functioning corporate environment.



ENABLING LARGE FILE TRANSFERS WITHOUT MAKING IT THE WILD WEST

STRIKING A BALANCE BETWEEN THE USERS' NEEDS TO SEND LARGE FILES AND RETAINING MANAGEMENT CONTROLS, DATA SECURITY, GOVERNANCE AND BRAND INTEGRITY

Thankfully, there is a middle ground. The answer to the large file transfer conundrum is to introduce a service that is as simple to use as the consumer-grade offerings but packs all the administrative controls, security settings and branding control of a corporate tool.

Today, with regulators and legislators taking even more interest in data protection and privacy, it has become critical for companies to deploy serious large file transfer services. We have all seen the headlines about companies that have lost data or revealed the names, addresses or credit card details of their customers. The issue is one that can wreak havoc overnight, trashing reputations and leaving companies open to the worst sort of publicity, as Sony discovered when PlayStation user data was compromised. Big fines and reputational damage await those that don't take the issues of data loss and compromise seriously. There is also the risk of network congestion and voiding contractual and legal terms by having data sit outside national or regional domains.

By introducing systems that can cope with large files in a way that preserves reputation, together with the necessary security and governance controls, organisations can avoid chaos.

Organisations need to think about how they create an environment for secure data transfer:

- Create a policy with regard to secure data transfer within your organisation, explaining clearly why consumer-grade services are inappropriate and the alternative you are proposing
- Create a single, central view of all user accounts and the data they contain
- Have a policy for what happens when users join and leave the company
- Create a policy for what happens in the event of a data breach

Managing IT today is a difficult task and no environment is perfect but with a sensibly thought out and well communicated policy, business communications needn't be a Wild West.