ENTERPRISE MOBILITY & CLOUD

Security Risks & Solutions

NETCONNECT

Powered By
NorthbridgeSecure

The IT world is changing faster than ever. The rapid evolution and consumerisation of smart devices has resulted in users demanding compatibility across a range of solutions to perform their work activities. Further complicating this evolving device landscape are users' requirements to access their work wherever and whenever they need, all posing significant threats to the business environment.

What's more, consumer-grade cloud solutions, and freely available mobile apps, that multiply daily, project the illusion that enterprise mobility can be achieved simply. This approach overlooks the fundamental risks involved in any company-wide change and often leads users to take unnecessary risks, jeopardizing company data for the sake of working from anywhere.

Successful business owners, however, know that protecting their data is essential. Whether financial data, customer data, business plans or intellectual property, data is a core asset, and its integrity and security is at the core of business success. Data leakages can destroy a business overnight & if the right data falls into the wrong hands like competitors, or at worst hackers, it can potentially destroy lives.

Figure 1 - Data Leakage Incidents

What enterprise needs is a solution that empowers businesses to enable mobility, cloud-based or not, without taking unwarranted risks.

Businesses today are facing unique challenges when it comes to the management of IT. On the one hand, they understand the need to protect their data & on the other, their users have devices in their pockets more powerful & prolific in day-to-day use than ever. The boundaries between work and private life have blurred, and users demand the ability to work from anywhere, just as much as they demand the right to use their personal devices at work. This makes the separation of business and private data difficult to manage.

Enterprise responds to these demands in different ways. The most common reactions vary from enforcing stronger security policies, making urgent or unplanned migrations to the cloud, or relying on an archaic VPN solution. Yet, these answers carry a significant level of risk for the organization.

[1]Help Net Security
<https://www.helpnetsecurity.com/2015/09/30/file-insecurity-the-final-data-leakage-frontier/>

Let's discuss why;

Businesses that decide to protect their data, locking down all access, face the largest risk. Users are getting smarter, and will find a way to do what they want, regardless of what they are allowed to do. There is no point fighting against the tide. The market is experiencing enormous growth of what is now called BYOC - Bring Your Own Cloud. In laymen's, this is when users, restricted in their access to work by IT policies, sign up for free consumer-grade cloud based storage solutions, copy their data to the cloud in order to enable out-of-office access and working capabilities.

This is of course in complete breach of most IT policies, yet users will rationalise & justify the migration claiming the need to access data anywhere to remain productive in their role.

"If IT is too stupid to understand that I need access to data outside the office, I'll do it myself. Surely my boss would agree with me that this is in the best interest of the company."

The direct impact is that data falls outside the control of the company. Poor passwords, unlocked devices, apps permanently connected, means that device loss or theft is a major potential catastrophe for the company.

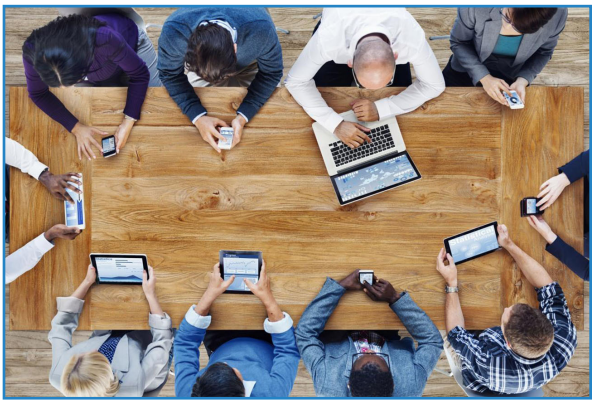
Even if the device is not lost, the availability of data in an external platform without the business knowledge or control is a huge risk. Large cloud solution providers are often the target of hacker attacks, and may eventually fail. Very few cloud providers actually mention the security measures they put in place. The largest are audited yearly and publish a report, however this report does not provide any information, and, not surprisingly, only shows a formal approval from the auditors, without mentioning what was audited.

This casts a logical doubt on the actual level of security in place. Even Dropbox is thought to have been hacked, and thousands of passwords have been made public. Controlling the management of this data when employees leave becomes impossible. What's more, free consumer-grade cloud based solutions are inherently risky.

Consider this: 'If you are not paying for a product, you are the product.'

Or in this case, your data is. What this means is that most "free" cloud solution providers, who could not be considered charity organisations, welcome your data because they can find a way to monetise it. Whether by analysing your data to send targeted advertising, or by actually claiming ownership of your data, there is always a catch. Of course, one can freely decide to accept this on a personal level, but should not accept it on behalf of their company without prior consultation.

There is no denying that enabling remote access to data and work environments is a necessity for most businesses today - don't do it, and your users will find their own way, putting your data at risk without your knowledge, and certainly outside your control.



On the other hand, finding the right solution to allow mobile working practices can be complex. Business-grade cloud solutions, while very attractive in their pricing models, contain inherent levels of risk:

- Controlling access to your data is difficult. By relying on a third party provider, you relinquish security to someone you may not know. Some providers provide a very high level of security, yet lack direct control of the environment, subjecting you to a significant level of risk.

- Using a cloud solution invariably requires migrating your data and changing your ways of working. Data is not in the same place & your users' habits must change. This can cause disruption for users throughout the company. A cloud migration often results in the need to re-train users to understand how to use the new system, even those who have no requirement for mobile access to the office. Technically challenged users historically react quite strongly, and usually negatively to this type of change.

- The hidden costs of cloud solutions can be extensive & exorbitant. Migrating a large file storage to a cloud solution often results in a significant upgrade to Internet connectivity, or face very disgruntled users when the performance is poor. Often, the cost savings of a cloud solution are far outweighed by the additional cost of Internet connection. Yet the delays & frustrations caused by not scoping these additional requirements leaves users feeling disconnected & unproductive with the new solution, resulting in resistance to adopting the new platform.

- Of course, migrating to a cloud environment is a gamble, and often a one-way trip. Removing data from the cloud should the solution not fit your requirements will mean a new migration, potential re-training. What this means is that there is no real way of trialling a cloud solution – it's all in or nothing in this case.

- Very few cloud solutions allow password synchronization with existing systems. This then requires users to remember additional passwords. Typically, when 2 or 3 or more passwords are required, the level of security for an average user drops significantly. Ultimately, this means IT needs to manage an additional level of access to data, often leading to vulnerabilities when employees leave an organization.

- Cloud solutions generally standardized their feature set, and are rarely a perfect fit for small business, who rely on multiple solutions internally to perform daily activities. The result is generally a half migration, only providing a fraction of the expected benefits, with the same

As a result, cloud solutions, while attractive in their model, inherently carry a high level of risk, while not necessarily providing the right solution. In particular, when mobility is only required for a small number of users such as sales people, management and technicians, the migration is unlikely to be cost-effective.

On the other hand, companies who elect to maintain all data on site generally use a customary VPN solution. This traditional scenario affords internal IT departments greater control of the data, whilst enabling the work environment to be accessed by mobile users.

This approach is far less intuitive for users, who experience the increasing evolution of mobile device capabilities on essentially a daily basis, to be restricted in functionality by their VPN solution. VPN solutions offer a 'one-size fits all' approach to mobility, which in an age of device reliance & individuality is far from a suitable solution. Additionally, VPN solutions are fraught with deployment complications and a minimum level of IT understanding from the user, while often carrying a high level of risk:

- Usually, VPN solutions will integrate the entire device on the company network. This usually requires some configuration on the source device to provide a familiar experience to the end user. IT dpeartments typically control this by only allowing company-managed devices to connect to the VPN. As mentioned earlier, this goes against what users really want, and leads them to work around the limitations in place.

- Alternatively, most standard or uncontrolled VPN solutions allow remote devices to connect to the company's network and allow access to all resources - files, financial data & customer information are all then at risk. With minimal control performed on the device connecting to the network, this device becomes a perfect opportunity for viruses and hackers to enter the network. Once they are in, data is as good as lost.

- Most entry-level VPN solutions require proprietary clients to be deployed to remote devices. This results in a complex (and costly) deployment for IT, who need to have access to all devices that may need to connect to the VPN. It also means that any changes to the VPN requires a re-deployment. Even with a standard solution that does not require any specific client, the configuration of the VPN requires IT knowledge, and is different from device to device.

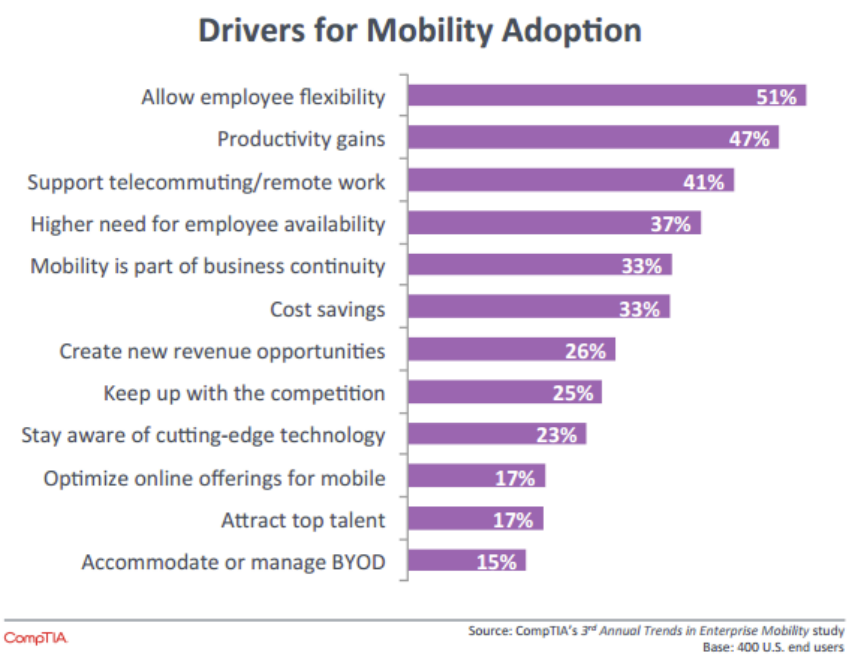
- Finally, mobile devices can only perform limited actions, even when successfully connected via VPN. Connecting to servers may require separate apps, with additional configuration for each one, adding to management complications for any IT department.

The result is that most organizations are faced with a difficult challenge, stuck between the need to make data available to their users outside the office, the need to control where the data is going, and the need to control costs.

From an employee's perspective, they want to use their device of choice, to fulfill their role & have this device integrate seamlessly in their work environment. This is a standard expectation of user's in the modern IT landscape.

Very large corporate institutions, with large IT departments, big budgets, and access to first-grade solutions, struggle with this problem. Businesses with no IT support often feel helpless.

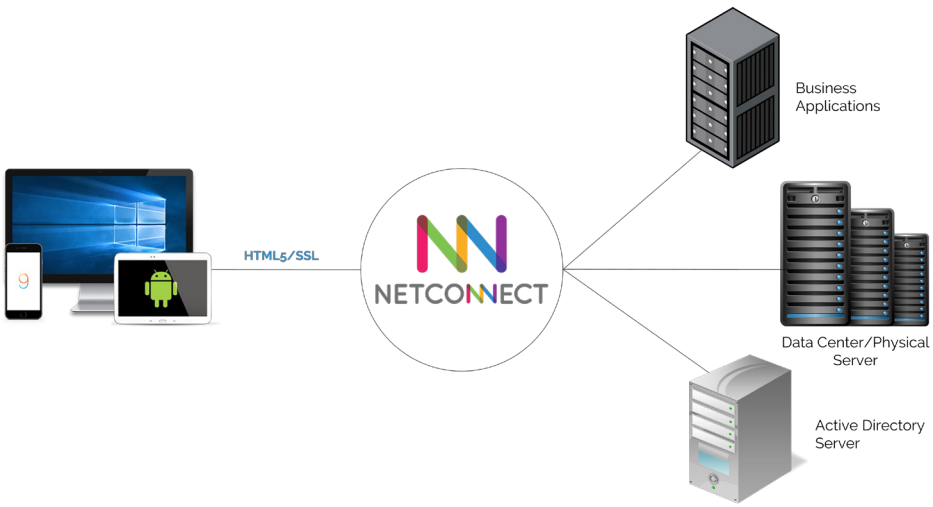
Figure 2 - Mobility Adoption Drivers



[2]Macquarie Telecom Group
<https://macquarietelecomgroup.com/news/byod-top-6-trends/>

So where does that leave us? Damned if you do, damned if you don't? Not really… NetConnect, a solution designed and developed by NorthbridgeSecure Systems, provides an elegant response to all these seemingly conflicting requirements.

At NorthbridgeSecure, security is our top priority and we focus on ensuring you can enable mobility for your employees with complete peace of mind. NetConnect has been designed from the outset as a security product. With extensive security safeguards in all layers of the solution, even the mobility layer, NetConnect is in a better position than most mobility solutions when it comes to protecting your data.



Some of the major security features of NetConnect include:

- **Retaining full control of your data:** Unlike most cloud solutions that require a complex data migration, NetConnect does not require you to relinquish control over your data. Data remains on your servers, made available outside the organization with complete security. Yet, NetConnect is also fully-flexible allowing you to migrate data to your cloud solution of choice, and still use NetConnect to make this data available on mobile devices. You retain full control of who can access data, and carry no risk of trusting a third-party cloud provider to host your data.

- **You manage your infrastructure:** NetConnect resides within your environment, and is managed by you. You do not need to trust a third-party organisation to secure your data.

- **Active Directory integration:** NetConnect integrates with Active Directory to ensure your internal policies apply to any access you enable from external sources. This ensures you only need to control one username and password across your organisation.

- **No direct network connectivity:** Unlike most VPN solutions who connect remote devices to the company network, allowing any virus on a remote device to infiltrate the network, our NetConnect HTML5 Gateway only provides a mirror of your applications and data to your mobile users, and the remote device is never actually connected to the network. This way, even if a device is compromized, data remains safely within the boundaries of your organization.

- **No global central password database:** Most large cloud providers have reportedly been hacked, with password leaks occurring on a regular basis (Dropbox, Facebook, TeamViewer). NetConnect does not have a global central database, so hackers do not have the ability to penetrate your network if they do not know your passwords.

- **Full data encryption:** NetConnect uses the latest SSL protocol to ensure all data transiting over the internet is fully encrypted and cannot be eavesdropped by anyone over the line.

- **Server Certificates:** The use of certificates reduces the risk of "man in the middle" attack to ensure that your device connects correctly to your server and looks at your data, even if someone manages to redirect the communication from your device.

- **Selective access for each user:** Unlike traditional VPN solutions, NetConnect gives you the ability to enable access for individual users to those applications, for which they are authorised. This way, you can let your support team connect to a ticketing system and your accountant to an accounting package, with no crossover between these levels of access.

- **No data stored on device:** NetConnect only provides a window to your work environment and data, with no data ever stored on the device. This ensures that in the case of device theft or loss, your data is never compromised, and anyone using the device afterward is unable to access any of your data.

- **Secure appliance:** NetConnect is the gatekeeper between your network and the Internet. In order to ensure this is fully secure, NetConnect has been designed to sit as a separate server in your environment. Based on a Linux Kernel, modified to be as secure as possible, NetConnect is locked down to provide a greatly limited surface of potential attack.

- **Regular security updates:** We are constantly improving the security of the product & maintain a regular patch cycle to ensure we cover any new threat identified on the Internet, on any protocol we use.

- **Constant audit:** We consistently check the security of NetConnect and never stop challenging our own thinking. In fact, one of our employees is tasked with attempting to break the system indefinitely! This helps us identify whether there are any potential weaknesses in the system & immediately fix them.

- **Monitoring:** NetConnect has a full reporting module, allowing you to check who has been accessing your network, at what time, from what place. This is extremely useful to confirm what is happening with your data.

- **Integration:** NetConnect integrates natively with multiple 2-factor authentication solutions. This allows you to take secure access even further and ensure that only users with the right token can access the system.

To trial NetConnect, please contact the Enforce Technology NetConnect team at 08444 935 935 or email sales@enforcetechnology.com.