

REMOTE & MOBILE SECURITY

Today many companies are enjoying the cost savings inherent in allowing employees to work from remotely thanks to the proliferation of cheap mobile storage devices. However, with this flexibility comes the extra need to manage and mitigate the new inherent risks to the company network and the business critical data.

The topics of remote and mobile access, typically revolves around 3 key questions:-

- (1) [How do I protect my Mobile Device and/or the secure the Data held on the Device?](#)
- (2) [How do I Authenticate my users to prevent Unauthorised Access?](#)
- (3) [How Can I Safely and Reliably enable Remote Access for my Staff?](#)



1. PROTECTING COMPANY DATA AND MOBILE DEVICES

Data is one of the most valuable assets that companies own today. These assets are increasingly vulnerable as mobile computing has become ever more widespread: sensitive information is often stored on notebooks and removable media – without any firewall protection.

Mobile devices and media, along with the sensitive and valuable information that is stored on them, are especially at risk of loss or theft. A company's management team is responsible for taking all the appropriate steps to protect the organization's data. Laptop encryption ensures that no unauthorized user may access the device and read data or use the device as a tool to enter the company network.

If a device falls into unauthorised hands, the data is securely protected even if the hard disk is removed. Complete encryption of the entire hard disk and a user authentication procedure that runs before the operating system boots provide secure protection.

Securing the data is one aspect of mobile device safety, another is controlling the device that can transport data; examples are USB memory keys, I-pods, DVD, CDR, Palms, PSP, PDA's, XDA's, mobile phones etc. The risk is that such device acts a medium to transport a malicious threat into the network or is used to export sensitive or confidential information out of the network. The solution is to lockdown what devices are authorised and to prevent inadvertent use.

Solution – Device control

- [Secure Wave device control](#)

Solution's – Data, laptop (pre-boot encryption)

- [Safeguard Easy from Utimaco](#)
- [DISK Protect from Becrypt](#)

2. OVERVIEW OF SECURE AUTHENTICATION

The decision as to whether to grant each user access to your networked systems is entirely based upon the individual's digital identity and the rigour with which you can verify or authenticate that identity. When logging into your network, web portal, VPN or other system each user is challenged to present their 'Digital ID' which comprises their Username plus their Authentication Credentials. This Digital ID is then verified against an Authentication Server to ensure that the credentials match the identity, and that the individual has the appropriate level of authority to be allowed access.

Given that the user may be connecting from any web-connected computer anywhere, we are now entirely reliant on this Digital Identity to differentiate our trusted users from the rest of humanity on the Internet. Unfortunately, many organizations today still rely on static, reusable passwords, thereby exposing enterprise information to access by unauthorized users. Therefore replacing static passwords with strong two-factor authentication is an essential step for securing corporate networks, applications, and information assets.

Solution's – Strong Authentication

- [ActivCard from ActivIdentity](#)
- [Signify Strong Authentication \(Managed Service\)](#)

3. SECURING & ENABLING ACCESS TO YOUR NETWORK

Traditionally, providing remote workers and business partners with access to back-end servers and resources has meant deploying an IPSec VPN. For site-to-site communication, IPSec remains the market preference, but for client-to-enterprise links, it is falling out of favour precipitously. The administrative overhead associated with deploying IPSec client software has become overwhelming given the ever increasing number of clients to support. There is also the potential that IPSec tunnelling will allow an un-trusted device to punch a hole through the firewall -- and directly into the heart of the network

These kinds of basic problems with IPSec are why SSL VPNs are showing up on more and more IT radar screens. With an SSL VPN, there is no client software to install, let alone maintain. Not only does this cut down on IT labour, but it also means remote users aren't limited to specified locations. Public Internet kiosks, partner sites, a borrowed laptop -- they all work. More importantly, with an SSL VPN there is no open tunnel to the enterprise. SSL VPNs enforce security policies on each connection, allowing access only to specific resources based on user, location, and/or device. As with any good security control, everything is off-limits unless expressly allowed by the administrator.

Solution – Enabling Remote Access

- [Juniper SSL VPN \(Clientless VPN \)](#)