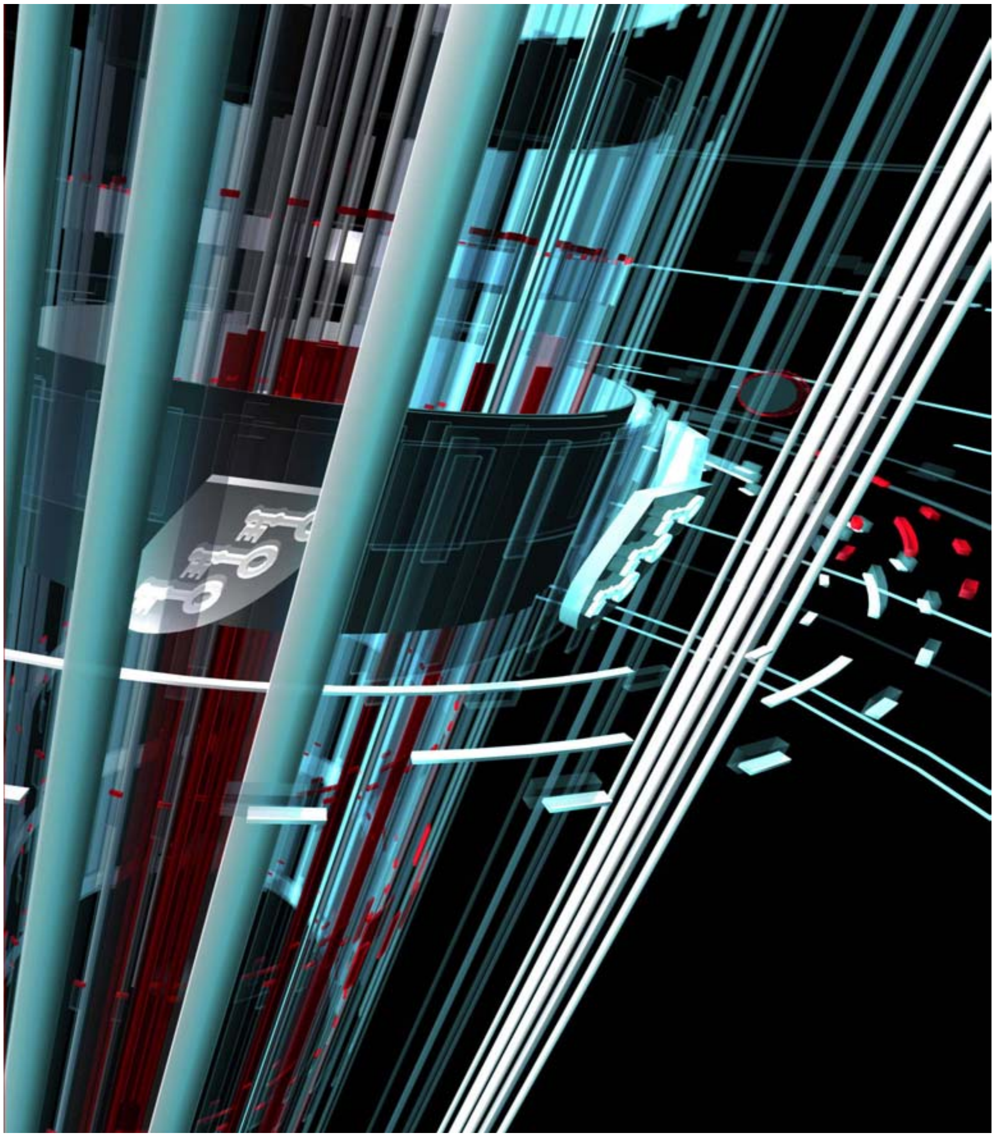


IT security –
a breath of fresh air

INTRODUCTION

Where's the timber?

Anyone who has visited InfoSec Europe, the annual IT security bun fight, will have seen for themselves how elevated 'security' has become on the corporate agenda. The glass-roofed Grand Hall was packed to the gunnels with senior managers seeking a solution to a very real problem.

Gartner sums up the demand for tighter security a bit more prosaically. In a recent report they forecast that 2003 will be the first year in which both the corporate and governmental sectors will be investing 5% of their IT budgets on security – a compound growth rate of 28% over 3 years.

Despite the spend and despite the proliferation of security tools and solutions, more than 90% of companies are still being hacked

Yet, despite the spend and despite the proliferation of security tools and solutions, more than 90% of companies are still being hacked. The problem, of course, *is* the proliferation of tools and solutions.

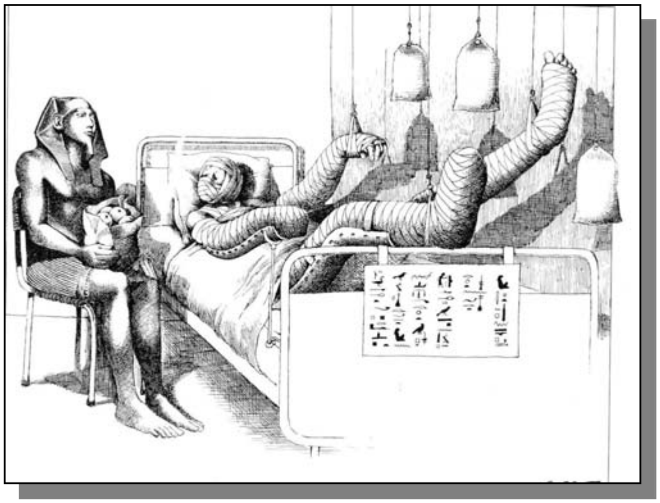
In this brief White Paper, we aim to isolate the real issues in layman's terms. We will demonstrate the inadequacies of almost all current thinking around the security question. Then we will spell out a delightfully simple concept that really does address all the concerns. Seeing the timber for the trees.

I hope you find it useful.

Steve Bale, CEO ArmourSoft

Problems, what problems?

According to IDC, corporate spend on IT security and business continuity this year will be more than $100 million, and yet corporate data is less secure than ever. Clearly, something is wrong. In this section, we look at the underlying issues.



The Elastoplast and Bandage syndrome

In response, the industry has reacted with a proliferation of ‘solutions’ – so now we are suffering from advanced stages of ‘sticking plaster and bandage syndrome’.

There are, for example, innumerable ways of authenticating users – anything from passwords to smart cards to fingerprint and iris recognition. There are even more software plasters to monitor usage of (and access to) the web. Add to that; virus checkers, e-mail monitors, SPAM filters, encryption algorithms and you begin to get the picture. Meanwhile, our friends at Microsoft keep issuing ‘patches’ on what seems like an hourly basis. IT security is beginning to resemble an extra from the film The Mummy. Not a healthy image for something that should be a non-negotiable business imperative.

IT security is beginning to resemble an extra from the film The Mummy. Not a healthy image for something that should be a non-negotiable business imperative.

Meanwhile, our friends at Microsoft keep issuing ‘patches’ on what seems like an hourly basis

Enterprise security involves more than sticking together sets of ‘point’ solutions with inevitable gaps in between - gaps that can only be bridged properly through an intimate grasp of the configuration issues. It doesn’t take much imagination to picture the problems that can arise when changing one application’s settings – the unforeseen side effects as the changes interact with other security applications.

Size matters - *scalability*

The disparate tools and partial security solutions generally available were originally designed for the workstation user, rather than for the enterprise network. This is an important distinction. They are not inherently scalable; so problems increase exponentially as the number of users, and the number of different ways in which they make use of their systems, increase.

Solutions generally available were designed for the workstation user, rather than for the enterprise network. They are not inherently scalable

Typically, workstation security products have had to be individually installed and configured for each workstation and end user. This has usually meant that large scale deployment of security applications has had to be restricted to users in a ‘high risk’ category.

Let’s give the keys to our secrets to the office junior

Kevin learns the latest corporate takeover plans

Perhaps the weakest single link of all associated with traditional solutions is their inability to separate ‘access to corporate information’ from ‘routine maintenance’. Typically, data backup and basic network maintenance tasks are performed by someone who’s just got their GCSEs. Current IT systems allow IT administration staff unlimited access to all the organisation’s information. It’s like giving the keys to your corporate secrets to the office junior – empowering them more than many members of the board.

And in an outsourced environment, this analogy equates to giving the keys to someone else’s office junior!

All change!

In a distributed environment, the cost of change is becoming a significant inhibitor in adopting new computing solutions

In a distributed environment, the cost of change is becoming a significant inhibitor in adopting new computing solutions. For the enterprise-sized organisation, rolling out applications to possibly thousands of users, often in remote places or even mobile users, entails investment in large central administrative, training and support facilities.

Sadly, the same is even truer of traditional security applications. The whole point of security products is to stop people from doing things they are not authorised to do. Roll out a new version of Office or Word and if anyone is overlooked, they can still function perfectly with the old version. Roll out new versions of security products to thousands of users and anyone overlooked instantly fail on authentication, they have no access to encryption keys and so on - effectively, they have become castrated!.

The whole point of security products is to stop people from doing things they are not authorised to do. Roll out new versions of security products to thousands of users and the odd person overlooked effectively becomes castrated

To achieve a small increase in security has meant a disproportionate increase in complexity, heavier demands on users and significantly increased overheads.

To achieve even a small increase in security has meant a disproportionate increase in complexity, heavier demands on users and significantly increased overheads.

In summary

- Suppliers have developed disparate, fragmented and often incompatible security tools and solutions
- Solutions have not been designed for the enterprise – they are not scalable
- They entrust the keys of the system to junior staff
- They inhibit the movement to outsourcing
- They carry considerable management overheads in terms of training and on-going support

In short, the whole thing is a mess.

Perhaps those nice people at Microsoft have an answer

Security flies out of the Windows

It has become fashionable over recent years to take pot-shots at Microsoft – the unavoidable fate of any individual or any organisation that is successful. And Microsoft is phenomenally successful. For years, the mighty IBM was stringing along a geek called Gates, while it developed what was planned to be the definitive, world-beating operating system, OS2…….. Rest in Peace, *OS2!*

For all its faults, Microsoft has transformed the face of computing and has succeeded because the benefits it has brought to the table have far outweighed the downsides.

Security has been seen as a workstation issue rather than a network-wide issue. That's why managing security across enterprise networks has become a nightmare

One downside, though, is pretty formidable. The legacy of where Microsoft comes from – personal computing – means that Security has been seen as a workstation issue rather than a network-wide issue. That's why managing security across enterprise networks has become a nightmare. Where they do have enterprise security options, their management is still relegated to Kevin.

It is no wonder, then, that according to a recent Forrester report, 77% of IT managers list security as their principal concern and remain to be convinced by Microsoft's 'Trustworthy Computing' security message.

The ArmourSoft Active Security Platform (TAASP), Enterprise FileSafe and SmartAccess

Corporate-wide consistency, manageability, scalability, ease of deployment and management

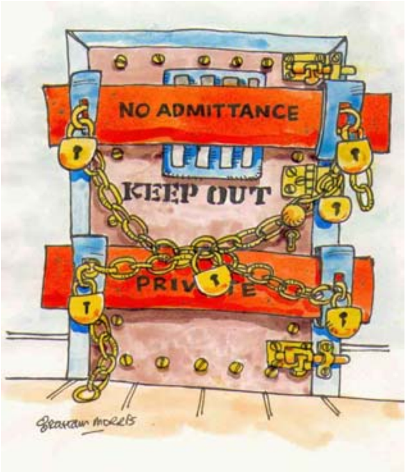
ArmourSoft was formed from a group of renowned IT security specialists who recognised the problems early on. They shared a vision of an enterprise-wide security platform that provided end-to-end, consistent and positive protection. A platform that ensured consistency and transparency to the end user – enhancing their experience at the same time as ratcheting up control. A corporate solution that could support thousands of users, eliminating the overheads and complications of implementation at each workstation

A platform, and related integrated security solutions, that add value while meeting the demands of corporate governance

The result is The ArmourSoft Active Security Platform (TAASP). TAASP is the corollary of the problems we described earlier – a truly scalable, manageable foundation for enterprise-wide security that is easily deployed and managed. A platform, and related integrated security solutions, that add value while meeting the demands of corporate governance.

The purpose of this section of the White Paper is to provide a non-technical overview of TAASP, ArmourSoft's Enterprise FileSafe and SmartAccess solutions.

A technical paper is also available for anyone wanting to look under the covers in more detail.



There is little satisfaction locking the doors (and reporting on it) after the horse has bolted.

Another platform?

Perform a web search on ‘security platform’ and it is possible to identify a number of vendors using the term loosely to describe their offerings. What differentiates ArmourSoft is that, uniquely, we refer to an *active* platform.

Rather than simply monitoring the network for unusual activity, breaches or attempted incursions, we actively *prevent* violations. This is a fundamental difference from the ArmourSoft approach and anything else on the market. There is little satisfaction locking the doors (and providing management reports) after the horse has bolted.

Manageability

ArmourSoft’s platform and its growing family of integrated products can be deployed to tens of thousands of corporate desktops without requiring investment in a large central administrative facility. The products are configured centrally and once deployed require no further configuration changes. Deployment and management are performed silently (without intervention or the need to visit the desktop).

Isolating the data – even from Kevin and third party contractors

TAASP is the <u>only</u> solution that separates *access* to the data from the routine management of the network, backup of files and so on. IT administrators, operators, contractors and other IT staff, however technically devious, are unable to read the encrypted information. They simply do not have access to the encryption keys……

Outsourcing the data, not the access to data

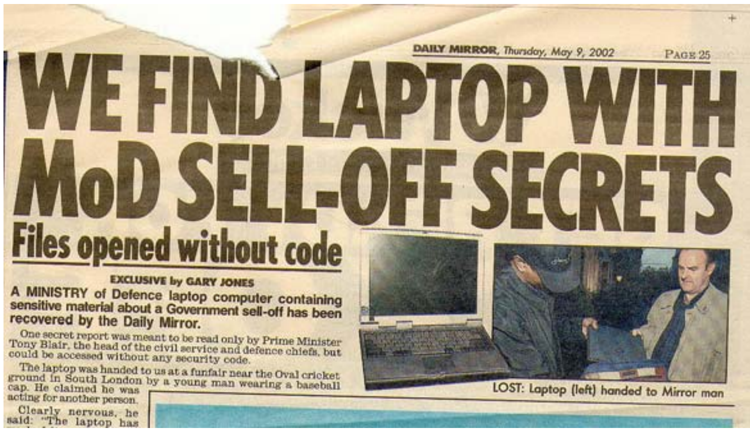
…..Similarly, the enterprises may now decide to outsource its IT infrastructure, secure in the knowledge that no-one employed by the outsourcing company, even the IT administrators responsible for managing the data, is capable of *reading* the data.

With ArmourSoft products, the outsourcer is able to offer full operational backup and recovery whilst not being able to access the contents of the secured data. User names and passwords are still managed in-house, even though the outsourcer is managing the applications.

According to an IDC report asking top company executives about outsourcing, 87% stated that security was top of the agenda when considering issues

Transparency in use

We have explained how deploying applications in an enterprise can lead to significant costs in end-user training and support. ArmourSoft's product suites have been designed explicitly to be invisible to the end user. Apart from entering a single pass-phrase when starting a new session, all the benefits of ArmourSoft's product suite are delivered without further interaction with the end-user.



DAILY MIRROR, Thursday, May 9, 2002 PAGE 25

WE FIND LAPTOP WITH MoD SELL-OFF SECRETS

Files opened without code

EXCLUSIVE by GARY JONES

A MINISTRY of Defence laptop computer containing sensitive material about a Government sell-off has been recovered by the Daily Mirror.

One secret report was meant to be read only by Prime Minister Tony Blair, the head of the civil service and defence chiefs, but could be accessed without any security code.

The laptop was handed to us at a funfair near the Oval cricket ground in South London by a young man wearing a baseball cap. He claimed he was acting for another person.

Clearly nervous, he said: "The laptop has

LOST: Laptop (left) handed to Mirror man

ArmourSoft's FileSafe would have saved the MoD from unwanted press coverage!

Transparent encryption with ArmourSoft's FileSafe

Encryption is universally recognised as essential to data security. So why is it that encryption isn't universally used?

The problem has always been that of operational overhead. Hassle. The need for users to encrypt their files. The ages that busy users have had to spend staring at an egg timer.

That's where ArmourSoft's **FileSafe** solution comes in. FileSafe uses a filter to encrypt files automatically as they are read and written. Again, automatically, each file is encrypted to comply with the established security policy relevant to the individual user or workgroup. Users have no need, or ability, to change encryption policy settings. At their workstations, including laptops, their files are secured without their knowledge or interaction.

Suddenly, encryption is a reality. No more hassle, more user intervention no operational delays.

Securing access with ArmourSoft's SmartAccess

SmartAccess automatically 'learns' each user's many passwords – passwords into legacy systems, into personal productivity system, the intranet, web applications and so on. It then stores them in a secure 'vault', which means that users are now required to remember just a single pass phrase. At a stroke SmartAccess virtually eliminates password re-set calls to the Help Desk (According to HUG, 60% of all calls made to IT Help Desks relate to forgotten or lost passwords).

User 'password vaults' can be stored offline using Smart Cards or USB storage devices small enough to be attached to a key ring. This is particularly relevant for laptop users. Should their system be lost or stolen (and according to Metropolitan Police, computer theft is currently the fastest growing crime) encrypted data is extra secure, as the encryption key is no longer stored on the system.

User 'password vaults' can be stored offline using Smart Cards or USB storage devices small enough to be attached to a key ring.

So, there we have it….

The ArmourSoft active security platform and associated security suite:

- Are the only security offerings designed specifically for the enterprise environment.

- As such, they really do address the growing demands for corporate governance, rather than simply bolting doors

- Allow ease of installation, administration and management without compromising security performance

- Improve the 'user experience' whilst increasing corporate security (no more password re-sets etc)

- Provide a comprehensive enterprise-wide integrated solution, as opposed to an eclectic collection of tools and hardware devices

- Enable secure outsourcing

- Provide a very real return on investment, decimating Help Desk calls, training costs and management overheads