



Technology on the Move!



FINANCE SAFE™

OVERVIEW WHITE PAPER



SECURE MOBILE COMPUTING

Introduction

In the 21st Century, we have a global climate, highly mobile and more technologically savvy users than at any other time in history. Individuals and institutions take for granted, the ability to instantly communicate anytime, anyplace with anyone over a worldwide heterogeneous technological environment into which more data is transmitted in a single hour than the sum total of the world's biggest Library, the Library of Congress in the USA. The Internet is a severely under protected network and storage environment where people are lulled into the misplaced belief that their information is safe and secure.

With the rising incidence of threats to sensitive data, and increasing requirements to protect that data, organizations must focus squarely on their security infrastructure. Protecting sensitive and critical data, no matter where it resides, and ensuring that only the appropriate persons have access to that data, must be a core requirement of every company's security strategy.

Ad-ware, spy-ware, mal-ware, etc., are now all more correctly named crime-ware, giving them a more appropriate descriptor. Crime-ware is any computer program or set of programs designed expressly to facilitate illegal activity online. There are many types of attacks including the more pervasive attacks listed below and described in more detail in Appendix of Risks:

- *Phishing*
- *Password Database Theft*
- *Password Stealing and Identity Theft*
- *ManintheMiddle*
- *(MitM) Attacks*
- *ManintheBrowser*
- *(MitB) Attacks*
- *Identity Theft*
- *StuxNet Worm Derivations*

Even today, with all of the public information about how unsafe the Internet has become, individuals and financial institutions alike routinely put their highly cherished "Financial Family Jewels" of information out for the cyber-thief to steal. Whether it's the cost to build the necessary protective environments or the poor deployment of security technology, the result is the same – everyday cyber-thieves add another notch in their data theft belts.

The “REAL” Threat

Crime and technology are getting ever closer. Today’s reports on security risks mostly cover amateur frontal attacks that exploit poor system administration or the latest hole that is not yet patched and are relatively inexpensive to mount. Builders of viruses take a little less direct approach by planting malicious code, but even this can be done nowadays by amateurs with limited means and unserious motives.



Serious hackers are less interested in hacking for fun and more interested in attacking for profit. Organized crime from diverse geographies is devoting extraordinary amounts of energy and resources to online fraud and theft. Technology has created a new super-empowered criminal.

Information warfare professionals are distinguished from the amateurs by objectives, resources, access, and time. A professional is well funded and has adequate resources to research and test the attack in a closed environment – to make its execution flawless and therefore less likely to attract attention. The resulting attacks do not get press coverage because they are not mounted against low value assets; however, in one unguarded instant, you might be facing lost revenues, lost reputation, and even regulatory exposure.

Equipping mobile workers with laptops is expensive and risky. Machines must be secured and patched regularly and if lost, they present a tremendous security risk.

With the increasing availability of high-capacity USB memory sticks, an alternative to traditional mobile business computing is emerging. By creating a virtual desktop on a USB thumb drive, companies can provide employees with the means to communicate safely with corporate systems and work securely from any PC, including a home machine or a device in an Internet café.

If the virtual environment is correctly configured, the user should be protected from any viruses or key loggers that may be lurking on the host machine. And when they close the session and remove the USB stick, users should leave no footprint or clue that they had ever used the machine.

Provided the user can find a PC to use, the advantages are clear. The USB stick is a low cost solution, lighter to carry and can be centrally managed. If it is encrypted, it has zero value to a thief or to someone who finds it in the street. It can also be a useful business continuity measure if employees are suddenly prevented from using their office systems. The rapid distribution of USB devices would allow employees to work from home while maintaining policy control.

FinanceSafe™: Financial Services Solution

FinanceSafe™ focuses on the need to create a secure end-user environment that provides Financial Services Providers (FSP's) with unparalleled management and control of the end-users' desktop environment to ensure the highest degree of security and defence against malicious attacks against FSP financial data and customer records. As online banking and financial trading continue to be more readily accepted and utilized by FSP customers, the number and types of attacks have exponentially grown.

FinanceSafe™ provides an answer to the threats of today and tomorrow by giving the control back to the FSP through the creation of a "closed" end-user client solution that guarantees and protects the identity of the customer through the provisioning of customer and enterprise certificates stored in a secure area of the FinanceSafe drive. Through this solution, the FSP can customize and control who has what rights and privileges to what systems, and track and monitor how the customer works.

FinanceSafe™ is a highly secure VRE and Browser which auto-mounts when plugged into either a PC or Intel-based Mac computer that is running its standard operating system. The Browser is managed inside the secure VRE and the administrator can set a “Whitelist” to define the browsers Internet access permissions. If a user attempts to access any Website other than those “Whitelisted”, an “error” message pops up and the user is prevented from accessing the Website.

FinanceSafe™ solutions are built on an extremely secure Linux-based runtime environment that has been hardened and locked down from end-user access, disabling cyber-attacks from occurring by enabling the control of the environment in which the solution runs. Competitive solutions employ a “defend from attacks” strategy whereby multiple types of control and security measures are taken to defend from the variety of different attacks. However, since their solutions run within an unsecured, hostile uncontrolled environment, this strategy is a continuous battle, where each new security measure is bypassed by malicious attackers, and new security measures in the solution must be continuously upgraded and revised. **FinanceSafe** is built with a highly secure runtime environment at its core that virtually eliminates attacks that could infect the system.