

# Check Point Abra: A Virtual Secure Workspace Technical Whitepaper



**Check Point Abra**  
Put your office in your pocket

# Contents

An Increasingly Mobile World .....	3
Threats and Dangers of a Mobile Workforce.....	3
Abra Provides the Solution .....	4
Introduction to Abra Technology .....	6
Applications of Abra Technology (Use Cases) .....	7
At Work .....	7
At Home .....	8
On-the-go.....	8
Summary .....	8



## Workforce Challenges

Over the past several years, enterprises have experienced a significant increase in workforce mobility. Today, employees routinely connect to their offices from home PCs via VPN, use wireless hotspots in airports, and receive work emails on smartphone devices. This mobility has led to unprecedented productivity for enterprises, as employees are able to remain continuously connected — anytime, anywhere.

An increasing number of companies have formally embraced telecommuting as a viable alternative for their workforce. Some employees work from home a few days each week, while others work remotely on a full-time basis. According to *World at Work*, 42 percent of U.S. employers allowed staff to work remotely in 2008 — up from 30 percent the previous year. These employees typically log in from either a company-owned laptop, or from their home computer, via a direct VPN connection.

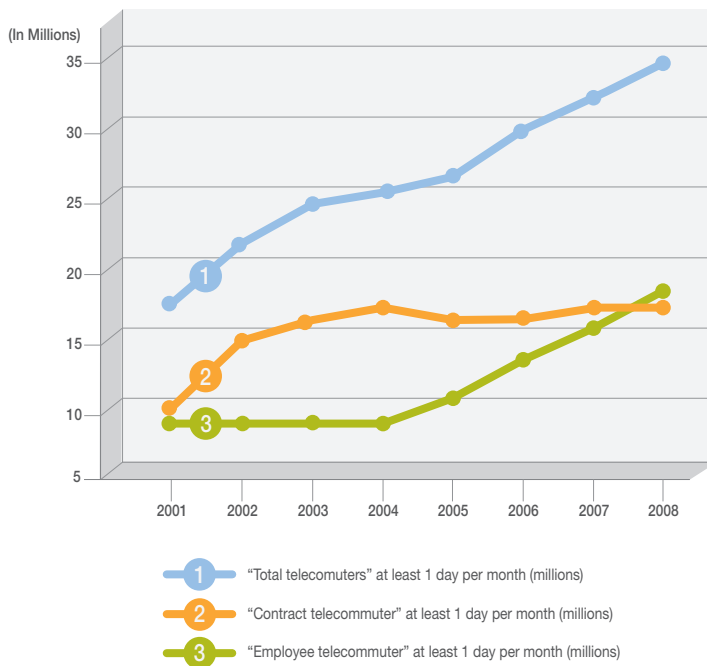


Figure 1. Telecommuter Trendline.  
Source: *Telework Trendlines 2009, WorldatWork*.

Companies are also facing challenges in providing controlled and protected access to contractors and partners. According to Ponemon Institute, over 44% of all cases in this year's data breach study involved third-party mistakes. Providing instant access to the office network for employees who travel has also become a critical requirement for many enterprises. The availability of broadband access, coupled with the efficiency of modern communications, has accelerated the speed at which business is conducted — and fueled expectations of continuous access to workplace resources.

## BY THE NUMBERS:

- 42% US employers allow telecommuting
- 34 Million telecommute at least 1 day a month
- 43% rise in telecommuters

## FACT:

**Growing mobile workforce increases security risks**



## Threats and Dangers of a Mobile Workforce

While providing employees, contractors and partners with instant remote and secure access to the corporate network provides tremendous advantage in terms of productivity and efficiency, it also introduces significant security risks to the enterprise. Laptops containing sensitive company or customer data can be lost or stolen; passwords, login credentials, and sensitive files can be left behind on un-trusted devices at the end of a session, making them readily available to subsequent users. Additionally, employees remotely logging in could be using an un-trusted machine, or a machine with malicious software and open a direct port into the enterprise's network, making it vulnerable to an array of security threats.

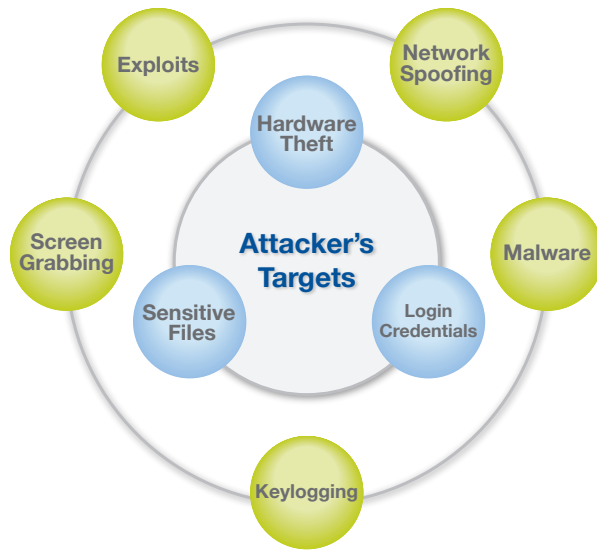


Figure 2. Attacker targets sensitive data using a variety of methods.

For these reasons, mobile users on the go require additional layers of security protection that simply cannot be provided through traditional endpoint solutions.

## Abra Provides the Solution

Abra is a hardware-encrypted flash drive with embedded security software. Abra encrypts data on the flash drive, and provides secure remote access with special policy enforcement, as well as a secure virtual workspace for working with documents and applications. All sensitive user information is encrypted on the flash drive, so user credentials, information contained in documents, and other sensitive data remain protected — even if Abra is lost.

When Abra is inserted into the USB port of any PC, the user will be presented with a new Windows desktop, which contains the user's shortcuts and documents. Abra uses the software installed on the host PC to run applications such as Microsoft Word and Microsoft Excel, but the user's documents will remain secure in the Abra environment — a separate secure workspace that runs parallel to the host environment. Abra opens a secure channel to the applications stored on the host, which enables it to use the applications, but with data neither transferred to, nor available on, the host PC.

## DATA LOSS IS A REAL THREAT:

- Untrusted and unmanaged PCs
- Malicious software
- Keyloggers

## ABRA IS A THREE-IN-ONE SOLUTION:

- Secure virtualization
- Secure connection
- Portable, plug-and-play



Employees routinely utilize a wide range of untrusted computers including home computers or computers in hotel and airport business centers. There is no guarantee that these systems possess latest antivirus software with newly updated signatures, or that they are free from malicious software — this puts company at a significant risk from security threats. Therefore, Abra creates a virtual Secure Workspace — a special environment that provides direct access to the company network in a segregated, secure environment. None of the host system’s processes can gain access, nor any traces are left behind on the host system after the session is over.



Figure 3. Abra controls which applications can run and which cannot.

For an additional layer of security, the enterprise can employ security policies, to determine what applications are allowed to run on Abra, and how secured files should be handled. Administrators can also configure additional settings that would restrict users from printing or accessing host PC.



\* These options can be configured by administrators

Figure 4. Security through segregation.

## ABRA FEATURES:

- Plug-and-Play Operation
- Secure Virtual Workspace
- Standard Windows User Environment
- Integrated VPN Connectivity
- Always-on Hardware and Software Encryption
- File Transfer Control
- Application Control
- User Authentication
- Central Management

## SECURITY THROUGH ACCESS CONTROL:

- Granularly restrict access to host PC
- Printing from Abra can be blocked



## Abra Technology

Once the Abra flash drive is inserted into a PC or laptop, a special program launches and is granted access to the flash drive firmware, where sensitive information is stored. The user is then presented with a login screen, where he or she will be required to enter credentials.

Upon successful login, a new explorer.exe instance is started in the Abra Secure Virtual Workspace. All subsequent processes will be started as child processes of this new explorer, thereby allowing Abra to control applications in the secure workspace.

The Microsoft Windows dynamic-link library (NTDLL) acts as a barrier between the user environment and the system kernel.

Abra performs a special sort of hooking on this border, intercepting the secure application's code execution before it reaches the NTDLL. The enterprise can enforce specific security policies such as forbidding the copying of files from Abra to the host PC, or vice-versa.

All file and registry input/output (I/O) calls for the secure application running inside Abra are redirected to the flash drive. In other words, applications running on the Abra desktop (including the new explorer) operate in a virtual file system and registry. The virtual files and all registry data are written to the flash drive instantly, where they are immediately encrypted.

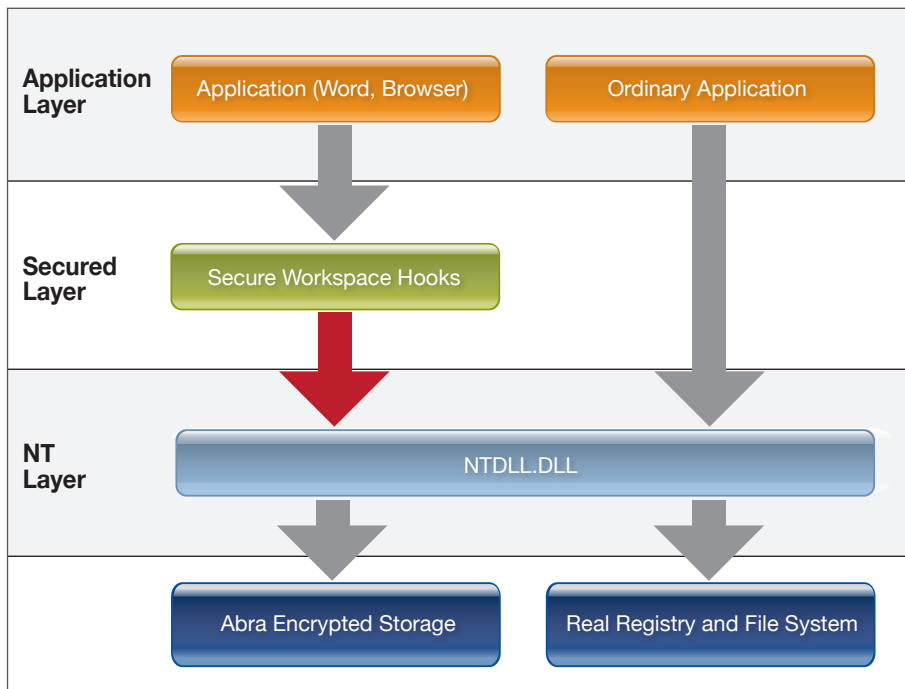


Figure 5. Abra architecture.

## SECURE VIRTUAL WORKSPACE:

- Leverages host operating system – no separate license needed
- Leverages permitted applications on host PC
- Encrypted storage

## SECURE ARCHITECTURE:

**Segregating user workspace from the host PC inherently protects sensitive user data**



When the application requests file creation inside Abra, the CreateFile Win32 API function is called. Abra intercepts the API and the file is actually created within the flash drive file system. Alternatively, file creation inside Abra can be denied by policy, if desired.

This special hooking does not require Abra to install a driver component, which dramatically reduces the potential for conflicts between Abra and the software applications on unmanaged computers. In this architecture, the memory spaces of applications under Abra and those of ordinary applications on the host PC are not separated avoiding memory conflicts. In addition to NTDLL, several other Microsoft Windows dynamic-link libraries are hooked in the same manner, to provide additional security.

Abra also includes an anti-keylogger, to protect applications in the Abra Secure Workspace from malicious software on the host PC that secretly records key-strokes. Such malicious software could capture the user's credentials, which could be employed by malicious users to gain unauthorized access to the corporate network.

### Applications of Abra Technology (Use Cases)

With Abra, enterprises can provide employees, contractors and partners with a consistent, controlled, encrypted and secure virtual workspace that is independent of the host computer. Security administrators have the ability to enforce mandatory access control on all files — stored in a hardware-encrypted, password-protected partition, to enable compliance with privacy regulations.

#### At Work

Abra is portable, so users can take it wherever they go. The entire working environment — including security settings, bookmarks, documents, shortcuts, and VPN connectivity — will remain consistent on every PC.

Abra can be used to provide easy access to partners and guests, or to grant temporary access to contractors who utilize their own computer. In either case, the contractors or guests don't have to install anything on their computer — eliminating the need to purchase additional assets, and significantly reducing support costs.



Figure 6. Easy access for contractors and guests.

## PROTECTION MECHANISMS:

- Virtual keyboard for login to battle keyloggers
- Control over applications and programs

### FACT:

**One solution,  
many use cases**



### At home

The growing number of emails with the subject line “Working From Home Today” makes system administrators nervous. There is a negative correlation between the number of employees working outside the firewall and the control the enterprise has over its information. Increases in the number of employees working from home are met with a corresponding increase in the potential for a security breach.

A simple “snow day” can keep workers at home for a few days. A worldwide pandemic which nearly occurred during the recent H1N1 Flu outbreak, may force people to stay home for weeks at a time. As a result, convenient and secure remote connectivity tools will be required to maintain productivity — without sacrificing security.



Figure 7. Abra provides the ability to work from home in case of natural disaster.

### On-the-go

Employees such as sales professionals who work on the road and from home can carry the pocket-sized Abra to use on any PC, rather than hauling a laptop from place to place. Alternatively, they can supplement their laptop with Abra — for an unparalleled blend of consistency and security.



Figure 8. Abra provides a workspace on the go.

### Summary

Abra provides a convenient secure access to the corporate workspace, while preventing data loss and malicious activity from remote systems — at a significantly reduced cost over traditional endpoints.

## USE CASES:

- Mobile workers
- Partners, contractors or guest access
- Disaster planning

## IDEAL SOLUTION:

**Abra puts  
your office in  
your pocket**



## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

### CHECK POINT OFFICES

#### Worldwide Headquarters

5 Ha'Solelim Street  
Tel Aviv 67897, Israel  
Tel: 972-3-753 4555  
Fax: 972-3-624-1100  
email: [info@checkpoint.com](mailto:info@checkpoint.com)

#### U.S. Headquarters

800 Bridge Parkway  
Redwood City, CA 94065  
Tel: 800-429-4391 ; 650-628-2000  
Fax: 650-654-4233  
URL: <http://www.checkpoint.com>

©2010 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.