

# Stealth ZONE Secures USB Desktops

MXI Security delivers ease of deployment and manageability to secure portable desktops via McAfee<sup>®</sup> Encrypted USB devices

Stealth ZONE from MXI Security leverages industry-leading McAfee<sup>®</sup> Encrypted USB devices to deliver a superior, secure USB desktop. Any computer can be instantly transformed into a standard IT-managed system while maintaining both performance and security.

## McAfee Compatible Solution

MXI Security Stealth ZONE and McAfee Encrypted USB

## Joint Solution Advantages:

- Turn any computer into a fully trusted, IT-managed secure desktop environment
- Provide data mobility without compromising security policies
- Securely provision, deploy, and manage even for very large user populations

The objective of portable work environments is to allow employees to access applications and information while being completely mobile. Users simply plug their USB device into any computer, reboot, authenticate their identity, and gain access to their complete Microsoft Windows desktop wherever they go. When they leave, their desktop leaves with them, and no trace of their presence remains behind.

Stealth ZONE's boot-from-USB technology offers excellent security for protecting enterprise data while delivering exceptional overall performance, mobility, and functionality. The solution also includes an industry-leading provisioning system that enables quick deployment of large numbers of devices in a secure and flexible manner.

## The Demand for Secure USB Desktops

Organizations are finding that many of their employees need to decouple their computing environment from a specific computer. Common usage applications include:

- *Telecommuting*—Users can work securely at home, even on untrusted systems
- *Secure remote access*—A secure environment for VPN authentication without local host installation
- *Separation of desktop environments*—Deploy multiple environments to the same user on a single computer to handle regulatory and policy-driven requirements
- *Secure transactions and online banking*—Combine a portable web browser with a full-featured PKI token for anywhere, anytime certificate-based authentication
- *Safe interaction with hostile systems and networks*—Shield the desktop from even the worst environments, immunizing against any unknown intrusions

Advanced USB security devices such as McAfee Encrypted USB offer hardware-based encryption and multifactor user authentication that allow Stealth ZONE to protect the user's entire portable work environment, including the operating system, applications, and data. McAfee Encrypted USB's PKI token functions can also be leveraged to solve more complex security problems.

## Why Boot from USB?

Portable work environment products typically leverage a variety of desktop delivery technologies. The diagram below illustrates the four most common architectures in use and compares them from the standpoints of security, mobility, and functionality. Booting from USB is the clear winner in all categories.

**Stealth Zone Features**

**Large-scale provisioning**

Dedicated appliance can securely configure many devices at once with the multigigabyte images required for a secure USB desktop

**Pre-boot authentication**

Access to the hardware-encrypted desktop requires up to three-factor authentication (biometric, password, CAC/PIV)

**Host isolation**

The environment is fully isolated from malware and data leakage

**Optional secure portable storage**

A separate, secure partition allows exchange of data between Stealth ZONE and other computing environments

**Optional PKI token operations**

Secure key and certificate stores, hardware key generation, digital signing, and a range of other user PKI operations are possible within the USB desktop

**Traceless departure**

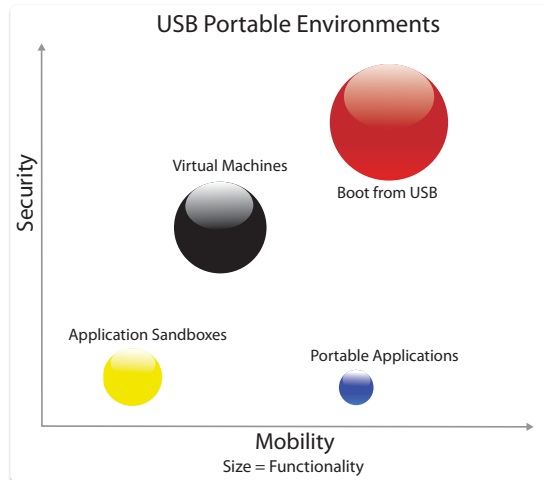
When users leave, they take their environment with them, and no trace of their presence remains on the host

**About MXI Security**

MXI Security develops portable security and computing products for government and enterprise customers. MXI's Stealth products are the best-selling line of secure portable storage devices in the U.S. Government, reaching 75 separate agencies across multiple departments. MXI's partners, including McAfee, extend its reach to security-conscious customers worldwide.

**About McAfee Encrypted USB**

Today's mobile workforce often carries sensitive corporate data on portable USB devices, unaware of the security risk if the drives are lost or stolen. McAfee Encrypted USB devices keep sensitive data safe and secure, wherever it goes. A variety of encrypted device options are available, ranging in storage size from one GB to 32 GB.



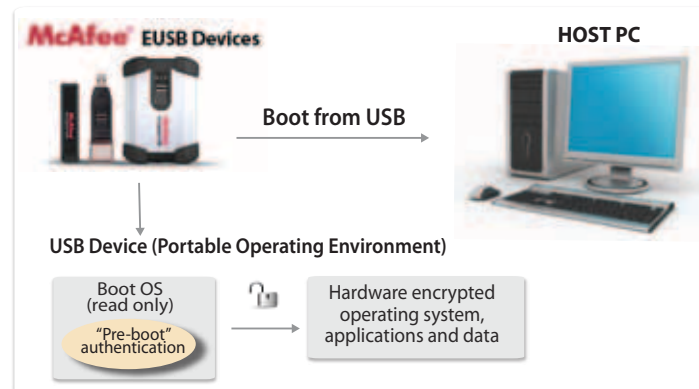
**Advantages: Stealth ZONE and McAfee Encrypted USB**

Until recently, portable work environments have had to compromise on security, mobility, or functionality, and they have also required sizable investments in centralized computing resources. Stealth ZONE avoids these issues by placing a bootable secure portable desktop directly onto McAfee Encrypted USB devices, offering both convenience and low cost.

Unlike secure USB desktops based on virtualization technology, Stealth ZONE allows Microsoft Windows to natively boot on any computer and take full advantage of multicore processors and all available memory.

In addition, Stealth ZONE's tuning technology offers a significant incremental benefit. Instead of a generic desktop, Stealth ZONE allows computers to be auto-configured with the correct device drivers for video, audio, network, and any other peripherals, offering full system functionality and providing an excellent user experience.

The advanced authentication features of McAfee Encrypted USB devices are a critical element of the solution. Before booting the secure USB desktop, a pre-boot environment loads, requiring users to prove their identity. Multiple authentication factors are available individually or combined, including strong password, biometric fingerprint scan, or a U.S. Government Common Access Card or Personal Identity Verification (CAC/PIV) card, all validated in the device hardware itself. Once the user is authenticated, the operating system, applications, and all user data—hardware-encrypted via AES-256—are unlocked and ready for use.



McAfee, Inc.  
2821 Mission College Boulevard  
Santa Clara, CA 95054  
888 847 8766  
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "AS IS" without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.

McAfee and the McAfee logo are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2010 McAfee, Inc. 14601brf\_mxj\_0910\_fnl\_ETMG