

Secure Enterprise IT Support Tool

Secure, Manageable and Flexible - Anytime, Anywhere Computing Platform

Secure Mobile IT Support Tool

- SupportSafe™ system is highly secure
- Complete data protection solution
- Configurable and flexible operating environment
- Easily integrate into existing IT infrastructure
- Supports FIPS certified devices
- Minimal host hardware required
- Restricts access to local host resources (i.e. Hard Drive, Printers, etc.)
- No hard drive required on host platform
- Requires use of at least one free USB port
- Multi-factor authentication support
- Supports CAC, PIV and Smart Cards
- Multi-OS support
- Standard web browser support
- Broadband support
- Standard applications software support
- Supports full e-mail client (i.e. Outlook)
- Supports proprietary user software
- Approved for Government & DoD use

SupportSafe™ - Bare-Metal-Boot Virtual System on a Stick is designed from the ground up to provide one of the most secure virtual USB computing platforms ever constructed – the ultimate in secure mobile computing. SupportSafe leverages virtually any PC-based laptop or desktop computer system as the host platform. Then it seamlessly incorporates device management within the SupportSafe guest operating system, supports industry standard software packages and proprietary packages that run within the SupportSafe guest operating system(s) (Windows XP; Windows 7) providing users the flexibility to customize their individual SupportSafe platform according to specific needs or desires without compromising security and data protection within the SupportSafe computing system. SupportSafe supports everyone from the casual user to the sophisticated IT Super-user.

Problem Statement

Today, over 8,200 information security executives in 63 countries struggle to hold the line against security threats and incidents, according to the State of Information Security, the world's largest information security study by IDG's CIO magazine and PricewaterhouseCoopers. It is a constant and never ending battle between the IT Experts responsible for the organizations life blood and the Cyber-thieves.

Even today, with all of the public information about how unsafe the Internet has become, individuals and corporations alike have little choice but to routinely put their highly cherished "Family Jewels" of information out for the cyber-thief to steal. In one unguarded instant, you might be facing lost revenues, lost reputation, and even regulatory exposure. 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.

Crime and technology are getting ever closer. 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. But 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 keep adding notches in their data theft belts.

Real Threats – Real Solution

Surely, for any organization there is nothing more important than trust. Breach that trust and you may face legal, governmental, financial, and reputational consequences. For enterprises, this means that people might love technology, but are getting the picture that things can go wrong.

We believe security will become another yardstick of corporate social responsibility. How companies are seen to manage these issues will become central to corporate reputation. In other words, security will become the new reputation bellwether. It all starts with fully maintained IT environments including central servers and most importantly, desktops, laptops, mobile platforms and remote workers.

SupportSafe™ - Complete IT Support Tools on Ultra-Mobile Platforms

SupportSafe combines technologies to provide a standardized method to secure information on Ultra-mobile devices – technology that allows the information to protect itself. SupportSafe technology is highly portable and standards based so can comply with local, state, federal and international data protection standards as they are adopted around the country and around the globe.

SupportSafe is a Portable IT Device which can be plugged into problem computers and Restore, Update, Repair, or Maintain them from within a completely protected drive. IT professionals are able to access an infected drive with the bootable EUSB, mount the drive in the target computer system (Host Computer) use utilities to scan the drive, remove the bad stuff and make it work.



Depending on which of the various IT support tools are installed on the SupportSafe solution, IT professionals can recover lost files and/or move critical files to remote storage using the RocITStor application installed on SupportSafe. Using SupportSafe beats other alternatives including having to crack open the laptop to gain access to the hard drive to repair and/or bootable CD.

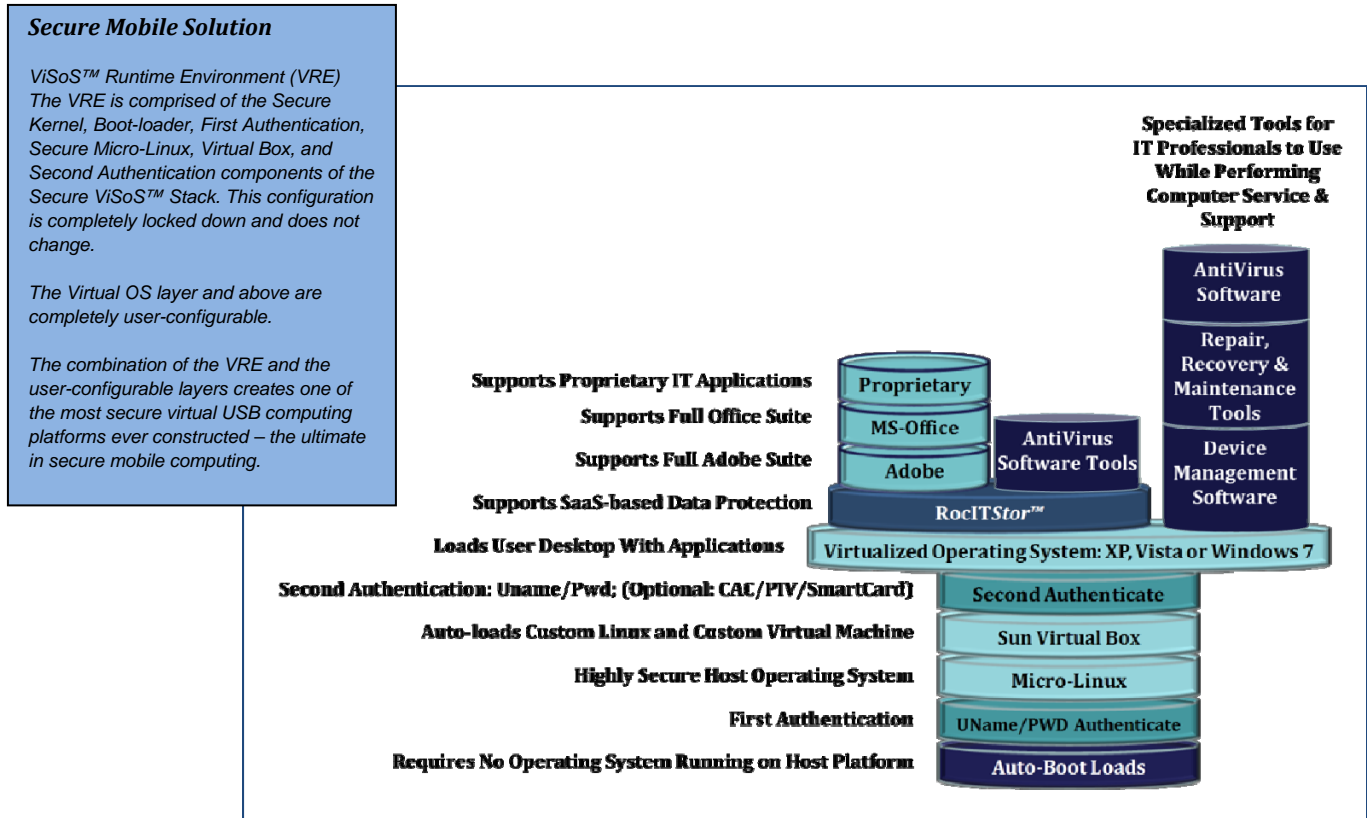
SupportSafe is available today on multiple sizes of FIPS and non-FIPS certified thumb drives as well as FIPS and non-FIPS certified USB spinning hard drives in sizes to over 500GB. SupportSafe creates a highly secure and ultra-mobile container in which the user environment resides including a user-specified OS, user-specific application software, device management tools and Anti-Virus software as well as user-generated data.

By adding CAC/PIV/Smartcard fully integrated login support within SupportSafe, the system has multi-factor authentication, which virtually guarantees your system cannot be compromised through unauthorized access and because of the unique design characteristics of the SupportSafe stack, outside unauthorized access points into the system are eliminated.

SupportSafe supports standard methods for connecting to the network including landlines, basic WiFi, WiMax, Mobile Intelligent MiFi hubs, VPN access and others to support mobile computing while maintaining smaller functional coherent workgroups which allow the users to lock down an open Internet connection, create a highly mobile and secure endpoint to safely connect to critical resources and use a uniform tool set that is easily maintained by IT organizations.

Pre-loaded & User Configurable Software

The software stack is designed to provide a high degree of flexibility in configuring the systems according to specific user requirements. Specific policies governing Disaster Recovery and Business Continuity within the organization can be included, managed and enforced within the SupportSafe solution.



- **Auto-Boot Load:** Proprietary software that auto-sets the hardware into a secure configuration and auto-boots the virtualized software stack.
- **UName/PWD or Biometric Authenticate:** Proprietary software to authenticate user name, password or fingerprints – match-on device. Users can enroll multiple fingers at initial start-up.
- **Micro-Linux:** Custom Linux distribution including open office suite and Firefox Internet browser.
- **Sun V-Box:** Virtual middleware layer to provide the foundation for a virtualized OS.
- **Second Authenticate:** Proprietary software integration that supports user name, password and/or all major CAC/PIV cards. With this authentication, SupportSafe complies with Multi-factor Authentication requirements from Government DoD.
- **Virtual Operating System:** Users can have multiple virtual machines running within the virtualized middleware to create multiple users and/or personalities including custom user environments with applications and user settings that reside inside a virtual space, then lock them to specific user credentials and securely store your entire virtual desktop environment so that it is protected.
- **RocITStor™:** Proprietary software application which provides data protection, high data availability, business continuity and disaster recovery using a proprietary FIPS certified user credential to cryptographically sign, encrypt and manage user data in the Federated Data Cloud.
- **Device Management:** With its single agent and single-console architecture, the software provides security and compliance management that is intelligent, automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

About RocITSafe™ Family: Securing, Enabling, Mobilizing

The RocITSafe bare-metal-boot (BMB) solutions are best suited to companies that want to virtualize the entire user's desktop, while RocITSafe Pluggable (PG) is better suited to deploying certain applications that the users need all the time, such as a VPN connection or certain desktop applications. PG collaborates with the operating system on the PC, while BMB runs with its own standalone highly secure operating system.

Under central administrative control, both versions can restrict what executables can run within the virtual desktop, and thus prevent data leakage via malware on the host PC.

Absolute Identification's RocITSafe family of products are designed and developed from the core with the highest level of security in mind. Every RocITSafe solution contains a fully integrated and highly secure operating environment that dramatically enhances the ability to protect the user against Cyber-theft.

Headquarters

5353 Scotts Valley Dr.
Suite D
Scotts Valley, CA 95066
Phone: (831)459-8199
Toll Free: (888)459-8199
Fax: (831)480-5886
Info@absolute-id.com

ABID International

114 France St.
DDO, Quebec
Canada, H9A 1K1
Phone: (831)278-0957
Fax: (831)515-5256
Canada@absolute-id.com

ABID Federal

22 East 35th Place
Steger, IL 60475
Phone: (708)755-1583
Phone: (831)278-0952
Fax: (831)515-5215
Federal@absolute-id.com