

RocITSafe™ vs. IronClad

Protecting Your Exabytes from Cyber-Thieves in a Mobile Environment

Real Issues - One 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. This means that people might love technology, but are getting the picture that things can go wrong. 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.

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.

Organizations today operate on a slender thread, striking a balance between security as protection, and security as a trust builder. And this thread can snap at a moment's notice. Organizations need to be visible in not merely preventing problems but also inspiring trust.

No data protection strategy is complete unless it takes into account all levels of the security hierarchy - a holistic approach taken from the beginning is the only way to guarantee the design of any solution targeted at security and data protection.

RocITSafe™ Family: Securing, Enabling, Mobilizing

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 keyloggers 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 cheaper, lighter to carry and can be centrally managed. If it is

Secure Mobile Solution

- RocITSafe™ 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
- Data is highly secure throughout entire life cycle
- Guaranteed Data Integrity
- Continuous Data Availability
- Unconscious Business Continuity
- Near-instant Disaster Recovery
- Policy-specific, Granular, Role-based, Access & Control

Solution Brief: RocITSafe vs. IronClad

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.

When companies deploy the device to individuals or groups of workers, they register themselves as users on their networked corporate system where RocITConsole ties their Active Directory details to the unique identifier on their USB stick. It then deploys the virtual desktop software, and thereafter the users are free to take the stick with them and use it from any host machine.

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.

RocITSafe 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. RocITSafe 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 RocITSafe, 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 RocITSafe stack, outside unauthorized access points into the system are eliminated.

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.

Pre-loaded & User Configurable Software

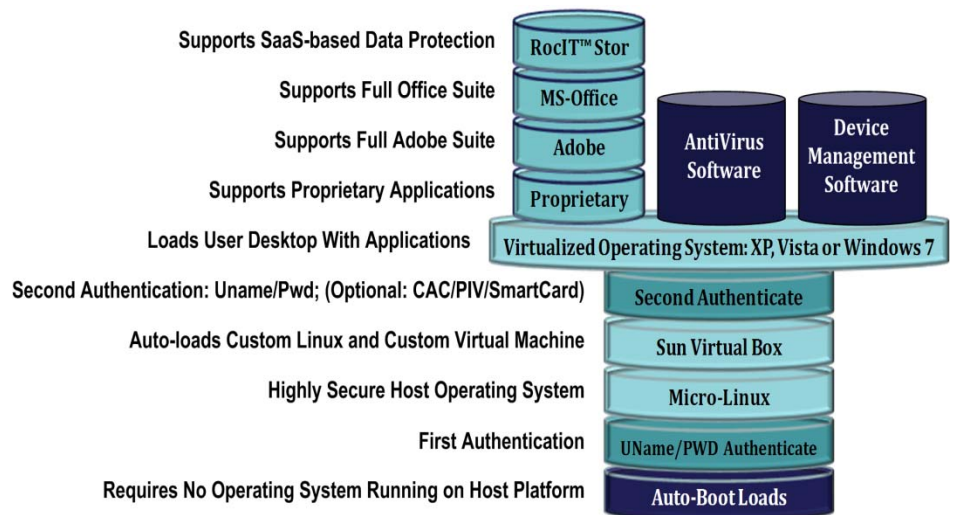
The software stack is designed to provide a high degree of flexibility in configuring the systems according to specific user requirements.

Secure Mobile Solution

*ViSo™ Runtime Environment (VRE)
The VRE is comprised of the Secure Kernel, Boot-loader, First Authentication, Secure Micro-Linux, Virtual Box, and Second Authentication components of the Secure ViSo™ Stack. This configuration is completely locked down and does not change.*

The Virtual OS layer and above are completely user-configurable.

The combination of the VRE and the user-configurable layers creates one of the most secure virtual USB computing platforms ever constructed – the ultimate in secure mobile computing.



RocITSafe™ vs. IronClad: The Comparison

RocITSafe™

Supports XP, Vista, Win7, Linux

CAC/PIV & SmartCard Support – Internally Developed

STIG Tested Software Stack

DIACAP Certified

RocITSafe devices are TAA compliant

Hardware Agnostic (Best of Breed Drive Support - Fast)

Integrated With McAfee eUSB manager

Will Integrate With McAfee ePO

Multiple Images and/or Partitions – Flexibility for User

Provides Multiuser Configurations

ABID Values DoD Business

Direct Support to Government Sector

Single-Device Start-up – Very Portable

24x7x365 Customer Support

RocITSafe footprint is small – 4GB

RocITSafe Software Operates Very Fast

RocITSafe is Affordably Priced

RocITSafe Available on Flash Drives and Spinning Drives

Streamlined Provisioning – Trusted Relationship

RocITSafe provides the tools for the entire enterprise process to take place in house and under full security control of the client without the need of a 3rd party.

IronClad

Only supports Windows XP

No CAC/PIV Support – Would Have to Contract

Not STIG Tested Software Stack

Not DIACAP certified

IronKey devices are TAA compliant

Only works on IronKey 8GB Drives – Very Slow

Not Integrated With McAfee eUSB manager

Will Not Integrate With McAfee ePO

One Image and/or Partition – Inflexible for User

Provides ONLY Single User Configuration

IronKey De-Values DoD Business

Indirect Support to Government Sector

IronClad requires the use of the CDROM in addition to the USB Device – Not Portable

8x5 Customer Support

IronClad footprint is very large – 7.2GB

IronClad is ‘Painfully Slow’

IronClad is Expensive (\$399 licensing fee, \$199 annual maintenance and support)

IronClad Available on USB Flash Drives ONLY

Multi-party Provisioning Process – Creates Holes

IronClad’s Virtual Machine requires outsourcing the image building and provisioning of devices to a 3rd party.

Solution Brief: RocITStor vs. Tape & RAID

RocIT*Safe* provides the ability to fully leverage the host PC's hardware to use it to its full, intended capabilities including full graphics, sound and networking options.

RocIT*Safe* Partners have excellent track record insupporting SEAT type solution such as RocIT*Safe*.

IronClad's VM limits the user to the defined processor power and RAM that is used when the VM is built. Full graphics, sound and networking options are limited in IronClad's virtual machine.

Lockheed does not have much success supporting a SEAT type solution like IronClad.

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