

Supporting Contract Workers, Outsource Workers & Consultants

Secure, Manageable and Flexible - Anytime, Anywhere Computing Platform

Characteristics of Contract Workers & Consultants

- Highly dispersed virtualized workforce.
- Little minute-by-minute control over activities.
- Much more likely to “surf” hitting malicious sites on the Internet.
- Heterogeneous operating environment – little IT control.
- Corporate data highly dispersed and virtually unmanageable.
- Workforce can work for multiple companies at the same time.
- Up to 40% of a workforce may be unavailable at one time.

RocITSafe™ - 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. RocITSafe leverages virtually any PC-based laptop or desktop computer system as the host platform. Then it seamlessly incorporates device management within the RocITSafe guest operating system, supports industry standard software packages and proprietary packages that run within the RocITSafe guest operating system(s) (Windows XP; Windows 7) providing users the flexibility to customize their individual RocITSafe platform according to specific needs or desires without compromising security and data protection within the RocITSafe computing system. RocITSafe supports everyone from the casual user to the sophisticated Super-user.

Problem Statement

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

Even today, with all of the public information about how unsafe the Internet has become, individuals and corporations alike routinely put their highly cherished “Family Jewels” of information out for the cyber-thief to steal.

This problem is further exacerbated as enterprises hire Contract workers, Consultants, and Outsourced Remote site workers. Often, these individuals are provided with some of the most cherished enterprise data which is necessary to perform their jobs. This opens additional holes in the secure fabric within the enterprise.

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.

RocITSafe™ - complete data protection on Ultra-mobile platforms

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

Solution Brief: Contract Worker Support

drives in sizes to over 500GB. RocIT*Safe* 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 RocIT*Safe*, 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 RocIT*Safe* stack, outside unauthorized access points into the system are eliminated.

Real Issues – 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 financial services, 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.

Nowadays, it's accepted wisdom that modern organizations must address issues of corporate social responsibility - their effect on the environment, their engagement with the community, as well as their financial performance. But, 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.

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 data protection.

Contract & Outsourced Worker Solution

RocIT*Safe* combines technologies to provide a standardized method to secure information on Ultra-mobile devices – technology that allows the information to protect itself. RocIT*Safe* 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.

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 RocIT*Safe* stack.

RocIT*Safe* provides a highly secure computing platform that supports Contract workers, Consultants, and Outsourced Remote site workers. Enterprise Administrators are able to define the “Gold Image” of the teleworker’s platform and then monitor the efficiencies and behaviors of the teleworker throughout the business day. Remote device management provides administrators with the ability to shut down devices of teleworkers who are abusing the system.

RocIT*Safe* supports standard methods for connecting to the network including landlines, basic WiFi, WiMax, Mobile Intelligent MiFi hubs, VPN access and others to supports Social Distancing while maintaining smaller functional coherent workgroups which allow the users to lock down an open Internet connection, create a



Solution Brief: Contract Worker Support

highly mobile and secure endpoint to safely connect to critical resources and use a uniform tool set that is easily maintained by small IT organizations before, during and after a major catastrophic event.

Contract workers, Consultants, and Outsourced Remote site workers can connect to the secure RocITSafe solution using their Smart Card ID's and a portable CAC/PIV or Smart Card Reader.

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-