



IRONCLAD™

A Secure, Portable "PC on a Stick"

LOCKHEED MARTIN 
We never forget who we're working for®

The IronClad Solution to the Challenges of Teleworking

Teleworking is an easy and affordable solution to a number of challenges faced by companies and government agencies. It lets employees stay connected during emergencies and major storms, supporting Continuity of Operations (COOP) year-round. It slashes commute times, cutting carbon emissions and helping employers meet green goals. And it's proven to increase productivity and employee satisfaction across the board. One need look no further than the statistics below to see the value of telework to today's on-the-go organizations:

40% HHS anticipated absentee rate in pandemic ¹	73% Number of Feds who say they will stay home in emergency ²	71% Increase in productivity for teleworking employees at DOJ ³	2,299 Tons of emissions saved through teleworking at GSA ³
90% Number of teleworkers who say they are happier and more productive ⁴	91% Number of Feds who say teleworking makes it easier to care for kids ⁴	100% Number of agencies required to have telework plans under S.707 ⁵	<10% Number of eligible Feds who telework regularly ⁶
57% Number of private workers who would telework if it was an option ⁷	69% Number of private sector employers providing telework equipment ⁷	\$24.5M Savings by Nortel Networks by instituting teleworking ⁸	Zero Minutes travel time for the teleworker to get to work ⁹

1 "HHS Pandemic Influenza Implementation Plan." Health and Human Services. 12/15/06.

2 "Federal Contact: Bird Flu in America." Telework Exchange. 5/11/06.

3 "The benefits of Telework." General Services Administration. 2009.

4 "Is Standard Practice Best Practice?" General Services Administration. 8/3/2006

5 "Telework: Senate Gives Unanimous Thumbs Up." Federal Computer Week. 5/25/2010

6 "Status of Telework in the Federal Government." Office of Personnel Management. 8/2009

7 "2008 CDW Telework Report: Feds stuck in Second Gear; Private Sector Puts the Pedal to the Metal." CDW 8/31/2008

8 "Nortel on Nortel: Teleworking and its Positive Benefits." Nortel Networks 2008

9 "Improving Quality of Life Through Telecommuting." The Information Technology & Innovation Foundation. 1/2009.

But teleworking faces an uphill battle in many organizations, for three primary reasons: technological, financial, and social.

The Challenges of Telework

The concept of telework is to bring the work to the employee, not the employee to work. The methodology for telework is to provide workers the tools they need and to enable them to work productively. At the same time, employers must ensure the security of their networks and data. Telework has experienced a recent resurgence due to a greater focus on environmental concerns, and increased technological capabilities – such as mobile devices and the increasing penetration of residential high speed internet connectivity. Telework Centers

are now available throughout the Washington, DC region (<http://www.gsa.gov/portal/content/102788>). Additionally, the Federal Government is currently completing legislation to provide, enable, and encourage telework amongst its workforce.

While there is an increased focus on telework, there remain many challenges and barriers to the broader adoption and implementation of telework. These challenges include social, technological, and financial constraints. However, for each challenge, there is a solution.



IRONCLAD™

Carry Your Computer on a Keychain - with Complete Security

The IT Challenges of Telework

Information Technology (IT) departments must ensure a reasonable level of access for remote workers to enterprise systems. They must also maintain multiple remote IT baselines and support functions. Meanwhile, the Chief Information Officer (CIO) must ensure continuous refresh and recapitalization of deployed equipment. All of the above lead to increased costs, complexity, vulnerabilities, and maintenance costs. In addition to the complexities and costs of the IT infrastructure, the loss of a single IT asset (such as a laptop computer) can have a tremendous financial impact as well as the loss of company or customer confidence.

The User Challenges of Telework

Users who are fortunate enough to be issued IT assets such as a laptop from their work complain of many issues with them. For example, lugging the equipment to and from work, providing safety and security for it, enabling administrator access to it, and ensuring updates to the system are completed in a timely manner. Users tend to find the requirement to carry the laptop back and forth to work a burden and would prefer something much more convenient.

The Security Challenges of Telework

The compromise (such as theft or malware infection) of a laptop has been estimated to cost an employer \$50,000 per device (Ponemon Institute, 2009) and the associated loss of customer confidence is incalculable. In addition to the threats to the laptop themselves, there is little to no control over the threats existing on a home computer. Organizations cannot control a compromised home computer and files or the potential danger to company and customer data by enabling a remote connection to the home computer.

The Financial Challenges of Telework

IT departments in conjunction with the financial departments of organizations must maintain a constant refresh cycle of IT equipment. Typical laptop deployments cost several thousand dollars per

machine including costs such as the hardware, configuration, deployment, maintenance, and training. Due to phased refresh cycles, these costs are continuous year to year.

The IronClad Solution to Safe, Secure, Reliable and Portable Telework

- **IronClad** secure USB is the solution to a mobile telecommuting workforce
- **Convenience** – Instead of lugging a laptop around, customers can slip their IronClad into their pocket and be very mobile
- **Cost** – Many organizations already provide their users a desktop. Instead of providing them a laptop as well, IronClad is a cost-effective alternative. Additionally, organizations do not need to provide a second laptop to contractors who already have one – they can simply provide an IronClad and allow the contractor to use their existing laptop
- **Secure Remote Access** – Using IronClad, an organization can provide a secure endpoint and remote access to their network from anywhere. IronClad effectively converts an untrusted computer into a trusted computer

The IronClad Solution to Telework

IronClad™ is a secure “PC on a Stick”™ from Lockheed Martin. IronClad is a new technology that shrinks a laptop’s hard drive – including the entire operating system, software applications, and files – onto a secure USB flash drive. Users on-the-go can plug the flash drive into just about any computer or laptop in the world, and have instant, secure access to their own work desktop and files. IronClad addresses all of the challenges of Telework in one pocket-size, indestructible, configurable, and secure device. The IronClad solution prevents inadvertently or intentionally infected files and devices from compromising a work network through its inherent security architecture and mitigations.

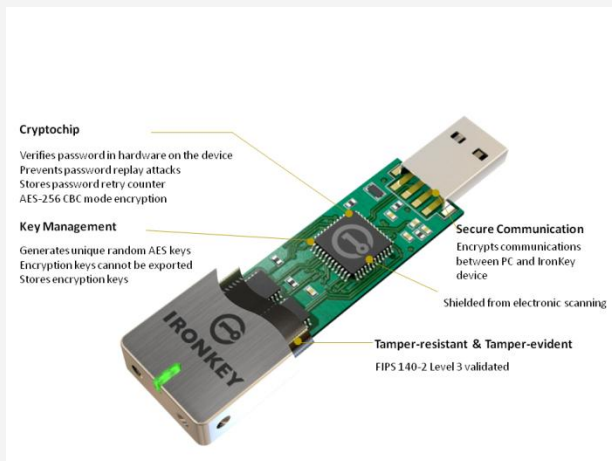


IRONCLAD™

Carry Your Computer on a Keychain - with Complete Security

The IronClad Solution to Malware, Viruses, and Other Threats

The Lockheed Martin IronClad device is manufactured on the IronKey S200 Enterprise USB drive, which is validated by the National Institute of Standards and Technology (NIST) as FIPS 140-2 Level 3 (Tamper-Resistant) offering Advanced Encryption Standard (AES) 256 bit military grade encryption. Because this drive is hardware encrypted, the client's desktop image and data on the drive are secure. In addition to the electronic security of the IronClad device, the IronKey hardware is resistant to heat, cold, water, sand and is epoxy filled to prevent physical tampering. Finally, when the user boots from the IronClad device, it will completely bypass any host computer's local hard drive, thus protecting the information on your desktop from any viruses and malware that the host machine's hard drive may contain.



Therefore, threats from a compromised computer are completely sidestepped. There is no need for IronClad to access or use the local hard drive, so it is never activated and compromised files or applications have no chance to infect the IronClad - period. Even RAM based attacks are mitigated through a final wipe of on-board system memory following shutdown.

IronClad Defense in Depth

- 256-bit hardware encryption and a tamper-proof design
- Whitelisting allows an organization to clearly specify which applications can or can't run on IronClad
- Application wrapping is a feature that quarantines and isolates any viruses that are inadvertently introduced through infected e-mails or files
- Enterprise antivirus and antimalware are applications and policies in place to prevent infection and exploitation of application security holes

The IronClad Solution to IT Management

IronClad is centrally managed in the same way as Enterprise devices such as laptops are currently managed. Typically, software updates and security patches are "pushed" to devices using software such as Microsoft's Systems Management Server (SMS). IronClad leverages existing enterprise operations processes and tools, such as SMS, thereby reducing cost of ownership. Overall support requirements of an IT organization may decrease, as there is only one build of IronClad with policies managed by "whitelisting," as compared to many different builds in support of different makes and models of laptop computers within the Enterprise. All of the IronClad profiles are centrally managed and configured through a simple web interface.

The IronClad Solution to Protecting Sensitive Information

In addition to the protection against infection coming from a compromised end point, there is no possibility of losing sensitive data to a home computer. For example, in a non-IronClad solution a worker may open a sensitive file on their home computer to work on. Upon opening that file, there is typically a "temp" file saved locally as well as the potential for the user to save the original to their



IRONCLAD™

Carry Your Computer on a Keychain - with Complete Security

local hard drive. With IronClad, all files are saved to the 256-bit AES encrypted partition of the IronClad itself and **NEVER** touch the local machine hard drive.

The IronClad Solution to the Financial Challenges of Telework

IronClad offers an affordable safe and secure alternative to the purchase of IT devices such as laptops. The cost of an IronClad device and its support is less than half of that of a mid-level laptop. Coupled with the cost of configuration, maintenance, break/fix, and refresh the costs, the difference between IronClad and laptop solutions is even greater.

The IronClad Solution to the User Experience

From the user's perspective, IronClad is a plug and play device. The user simply plugs the IronClad USB stick into an available computer port on virtually any machine, selects the device from the boot menu and then logs in as normal from a work computer. The user will connect to the work network using their standard Virtual Private Network (VPN) client as if they were connecting via a laptop. ***THAT IS IT.*** From the moment of login through the final shut down, the user interface is identical to their work computer. They have the same levels of access, applications, and files available to them. They can connect to the work networks and collaborate with their peers and customers from virtually anywhere in the world all via a simple yet powerful USB stick.

Make IronClad Your Telework Solution



Lockheed Martin's IronClad provides a safe, secure, portable solution to the challenges of telework. For more information on how you can implement the IronClad telework solution in your environment, please contact Lockheed Martin at 1-888-9-IRONCLAD (947-6625).

<http://www.lockheedmartin.com/products/ironclad/index.html>.

© 2010 Lockheed Martin Corporation. All Rights Reserved.



IRONCLAD™

Carry Your Computer on a Keychain - with Complete Security