

# Cybernut Solutions

## *The Dirty Little Secret About Security In The Emerging Remote Worker Society*

A whitepaper by: Jason Haddad

---

## The Dirty Little Secret About Security In The Emerging Remote Worker Society

For better or for worse, “telecommuting,” “working from home,” “working remotely,” or whatever else it’s called has grown exponentially in the 21<sup>st</sup> century and become a common practice for businesses big and small. A recent study by WorkSimple showed that “61% of Senior Leaders believe their companies will let more people telecommute over the next three years.” Given the rapid growth in laptops and smartphones, this is no surprise. However, the reality that most internal security technologies are network-based has created a significant gap in that they do not typically extend to off-network activity and certainly not to smartphones.

*Accordingly, we now see that*

- *the mobile worker, through the emergence of laptops, tablets, and smartphones, are now exploiting the limitations of said securities*
- *the security must now be placed on the endpoint to ensure complete protection and visibility*

### **Why such remote worker growth?**

Technology, as Gordon E. Moore predicted, has evolved exponentially since the advent of the microprocessor, making high-speed mobile computing available for anyone to consume. Consumer telecommunication services provide access to high-speed LAN and WiFi internet that is nearly as stable and as fast as a corporate offering (since far fewer individuals are straining the network). As of June 2010, 77% of the U.S. population has access to the internet; while 28% or 85.29MM people in the U.S. have access to a broadband internet service (according to the ITU).

It’s not any news that companies are operating globally. To keep up, the global economy requires a mobile workforce equipped with laptops and mobile phones to maintain real-time productivity and reactivity to business needs. It’s not uncommon to have workers within an organization out of the office for 75% of the fiscal year, making them as remote of a worker as an employee telecommuting from their home. Both scenarios offer similar challenges for human resource and IT departments that continue to face structured corporate policies updated quarterly, or the complete opposite in neglect and uncertainty for policy making from upper management.

### **If they can do the same work at home or on the road, why not?**

Technology is a pricey investment, especially at high volumes. It isn’t just something that is bought and not maintained. WorkSimple estimated *26.2MM employees worked remotely in some way in 2010* – that’s a lot of trust being placed in millions of dollars worth of labor and capital. While working, they may have been using secure corporate networks to complete tasks such as updating financial spreadsheets for others in the company to then access and update. What happened, though, when they

left the network environment? What programs did they use? What websites did they visit? Was confidential information leaked outside of the company?

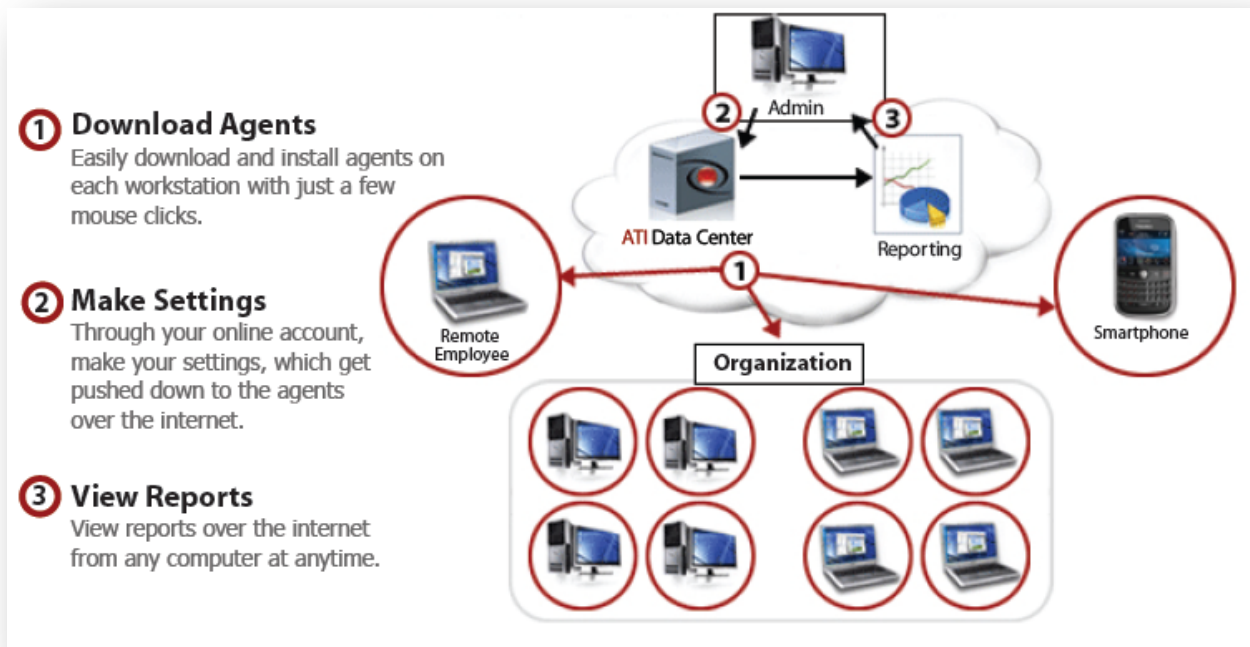
These are the common questions and concerns shared by managers and information technology departments responsible for ensuring that their workers and technology are being productive. Relying on monitoring solutions tethered to a corporate network has drastically limited the visibility into actual uses of company resources, and opened organizations up to new security threats that they haven't faced before.

### So what's the solution?

#### *An EndPoint Security Solution*

Endpoint security has become much more necessary as network based solutions do not adequately account for off-network staff. What information security professionals need is a next generation endpoint solution that focuses on the insider that works everywhere and sees everything. No excuses or exceptions for telecommuters, travelers, and other remote employees. No security gaps missed by lack of visibility across all endpoints, PCs **and** smartphones, regardless of location.

#### *Simple, Complete SaaS Solution*



## InterGuard

Deployed at the endpoint, InterGuard defends your business from all insider threats through a cloud-based delivery model. From one desktop agent and one interface, clients can access 5 technologies including Data Loss Protection, Web Filtering, Employee Monitoring, Laptop Recovery, and Smartphone Monitoring. Our solution is offered as both a complete suite or as five individual modules and is offered through the cloud so there is no hardware to buy, install or manage. Installs are fast and easy with no ongoing management required.

### 1. *Web Filtering*

- Monitors and filters Internet use on and off the network (even on laptops).
- Blocks or limits applications like peer-to-peer and instant messaging.
- All search terms captured
- Screenshots taken whenever an alert word is typed or read on a webpage.

### 2. *Data Loss Prevention*

- Protect and enforce policies governing each employee's computer use, including those that never connect to a network, including laptops.
- Detect and block non-public personal information (NPPI) from leaving your network or organization , either via email (both Outlook and webmail) or USB
- Scan all PCs (including if off-network) for sensitive/confidential data
- Stop the use of removable media.
- Easy intuitive policy creation.

### 3. *Employee Monitoring*

- Records all PC activity including employee communications (email, webmail, and instant messaging) programs used, websites visited, search terms used and keystrokes.
- Screenshots taken whenever an alert word is typed or read on a webpage.
- Blocks or limits applications like peer to peer, webmail and instant messaging.
- Formats all data into easy-to-read reports, making it easy to find and evaluate critical security lapses.
- Ability to search all stored data based on alert words as well as sender or recipient.
- Full individualized reporting on an employee's computer activity.
- Works invisibly and undetectable at each desktop, without impacting central network computer resources.
- Ideal complement to DLP by recording all PC activity. Since DLP is rule-based, you don't know what has been missed. Allows for DLP fine-tuning and forensics in case of data-breach.
- Ideal complement to Web Filtering by recording all PC activity instead of just websites since time wasting activities on a PC extend beyond simple websurfing.

#### 4. *Stolen/Lost Laptop Protection*

- Geo-locate all laptop locations
- Remotely retrieve/delete important files invisibly, using any Internet connection.
- Monitor everything the thief does including all of the files they attempt to access, etc.
- Prevent the thief from being able to access to any desired programs (Excel, Word, etc.)
- Remotely delete files or an entire hard drive.

#### 5. *Smartphone Monitoring*

- Monitor and record smartphone messages, including SMS and email
- Get notified via email when select keywords are found in messages
- Select important keywords to have them highlighted in user-interface for easy access
- Access the account from any web browser along with all other InterGuard services

## Looking For Some Additional Information? Contact Us Today

**CYBERNUT SECURITY TEAM**

**CYBERNUT SOLUTIONS**

**972.216.8800 x5841**

**INFO@CYBERNUT.NET**

**WWW.CYBERNUTSOLUTIONS.COM**

