



# The New “Insider” Threat

Extending Device and Data Protection  
to the Mobile Workforce

Charles Brown  
Product Manager  
[www.Fiberlink.com](http://www.Fiberlink.com)

**FIBERLINK**  
Simple. Secure. Mobility.

# > Agenda

- Mobility Trends and Their Impact on IT
- Investment Impact on Mobile Security
- Pursuit of a Solution
- Closing the Security Gaps

## > Fiberlink Overview



- **Company** – Founded in 1994. Headquarters in Blue Bell Pennsylvania. Presence in NA, EMEA & Asia. Over 250 employees.
- **Mission** – Make Laptop mobile computing simpler and more secure, so enterprises can realize the full potential of mobile work.
- **Customers** – Over 1,000,000 deployed users across over 700 enterprise customers,
- **Leadership** – Recognized by industry analysts as an innovator and leader in the mobile market.
- **Financial** - Privately held, profitable and growing. Investors include Goldman Sachs, GE and TCV

# > Today Everyone is Mobile and Access is Everywhere

## Road Warriors



*Planes*

*Trains*



*Automobiles*

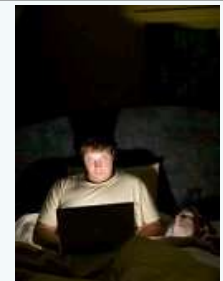
**Highly Mobile Employees: 25%**

## Day Extenders



*Morning*

*Noon*



*Night*

**Employees with Laptops: > 50%**

[Mobility] is not limited to the traditional 'hot' employee categories, who are typically 'road warriors' seeking to access corporate applications while on the move or in public places; increasingly it also includes part-time and full-time home workers and so-called 'day extenders.'

- Jeremy Green & Pauline Trotter, Ovum

## > IT Worries Around Greater Mobility

How and Where are Users Connecting?

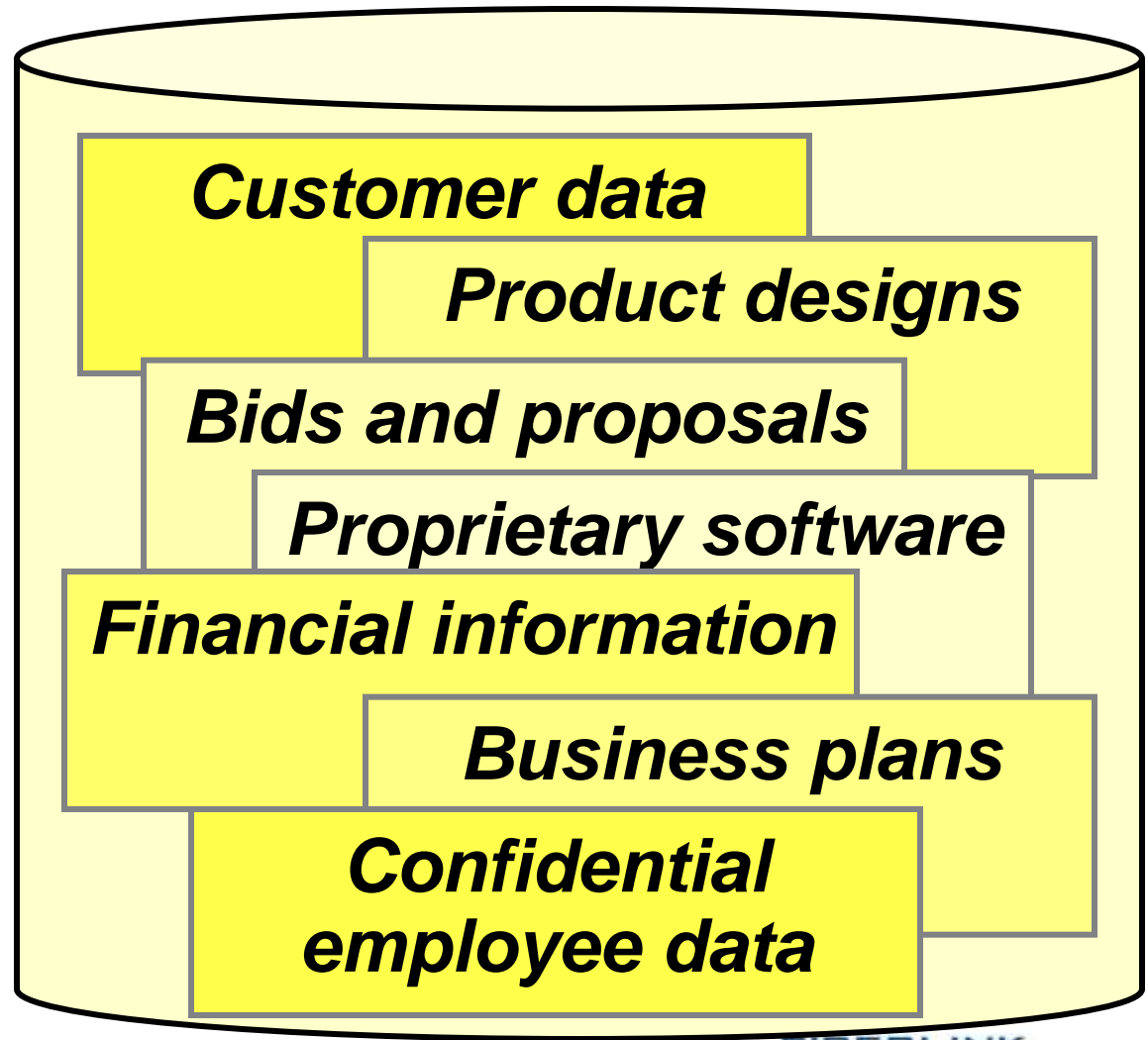
Are Devices Safe for Corporate Connectivity?

Is it Easy and Still Secure?

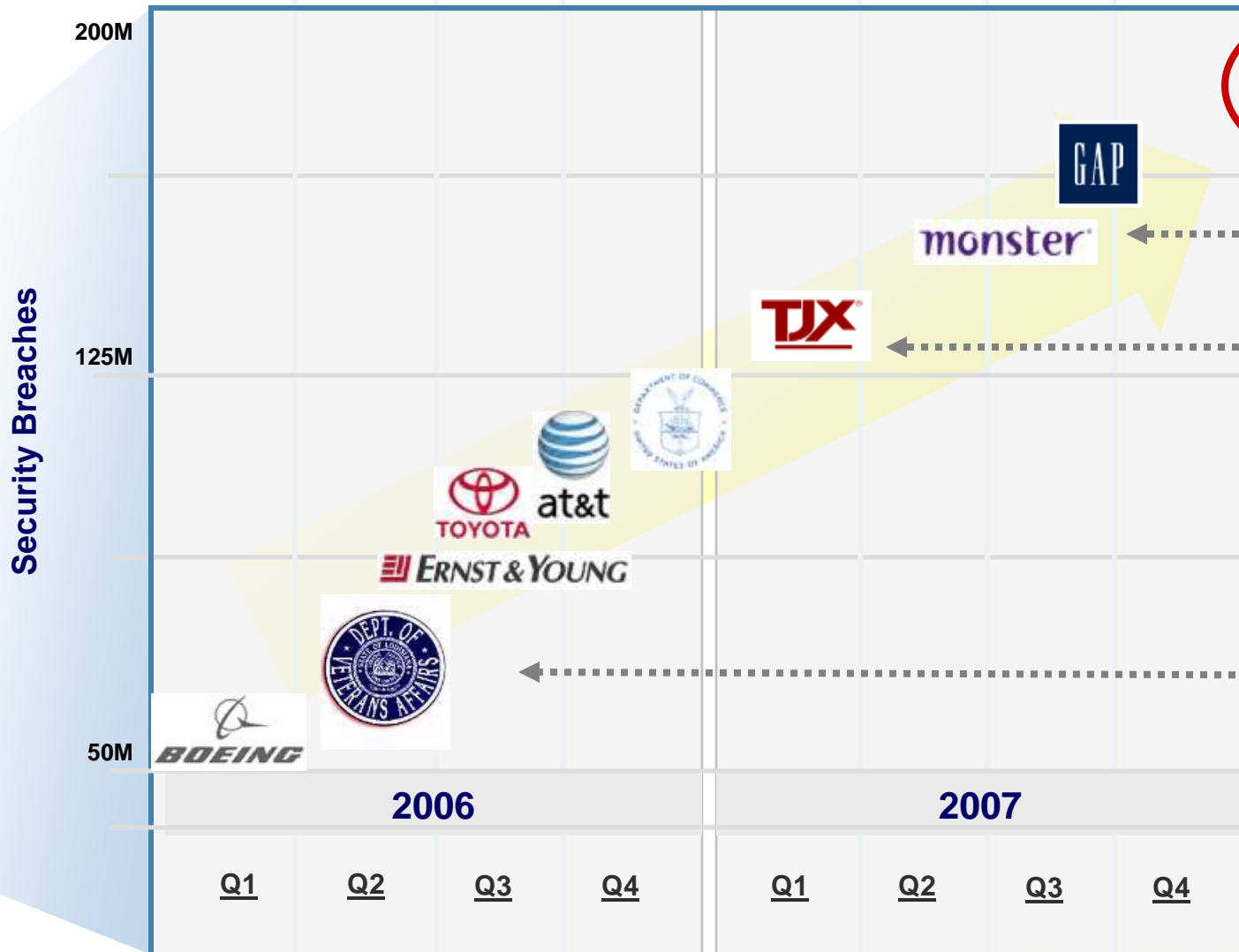
Will Mobility be Cost Effective?

# > More Data is Exposed on Laptops

IDC estimates that 60% of corporate data resides on laptops and PCs



# > Security Breaches Are Growing



**1/1/2008: Over 217 million data records of U.S. residents have been exposed due to security breaches since Feb. 2005.**

**8/23/07:**  
Details of some 1.6 million job seekers had been stolen. Fewer than 5000 were outside the US.

**1/17/06:**  
45,700,000 credit and debit card account numbers through an "unauthorized intrusion" into its computer systems that process and store customer transactions including credit card, debit card, check, and merchandise return transactions.

**5/3/06:**  
Data of all American veterans were stolen from a VA employee's home. Theft of the laptop and computer storage device included data of 26.5 million veterans.

# > Gone Phishing? They are Motivated!

## Recent Information Week Article:

- **\$10 - \$150**
  - Price range on the black market for full set of identity information
- **\$.50 - \$5**
  - Price range per stolen credit card number
- **196,860**
  - Unique phishing messages detected by Symantec for the first half of 2007, up 18% over previous 6 months
- **52,771**
  - Number of active bot-infected computers per day during first half of 2007

**Source: Symantec Internet Security Threat Report Trends, Jan. to June 2007**

# > Targeting the Mobile Device

Data In Motion:



Wireless Hacking:



Lost Device:

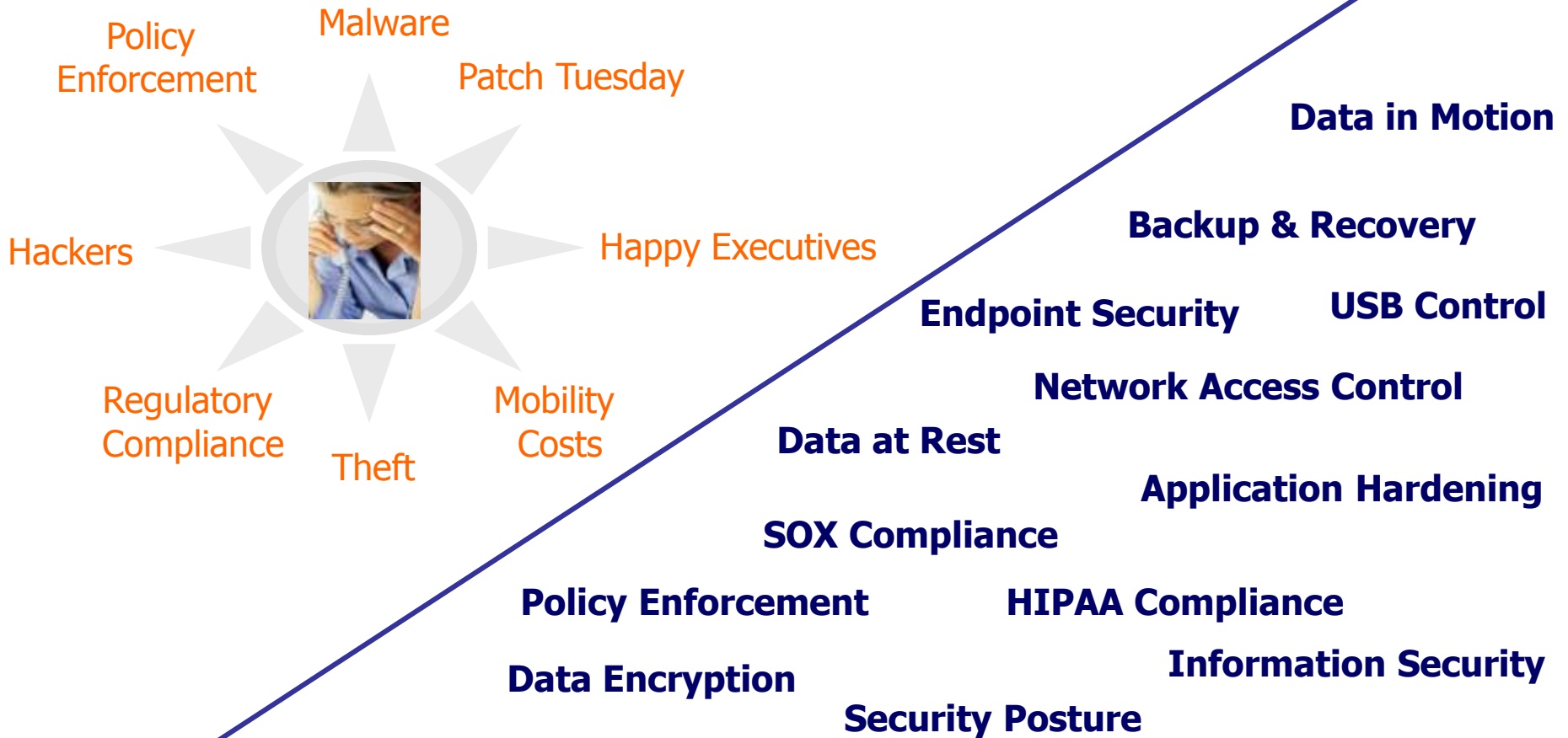


Stolen Laptop:



**Taking Aim**

# > Decisions, Decisions...

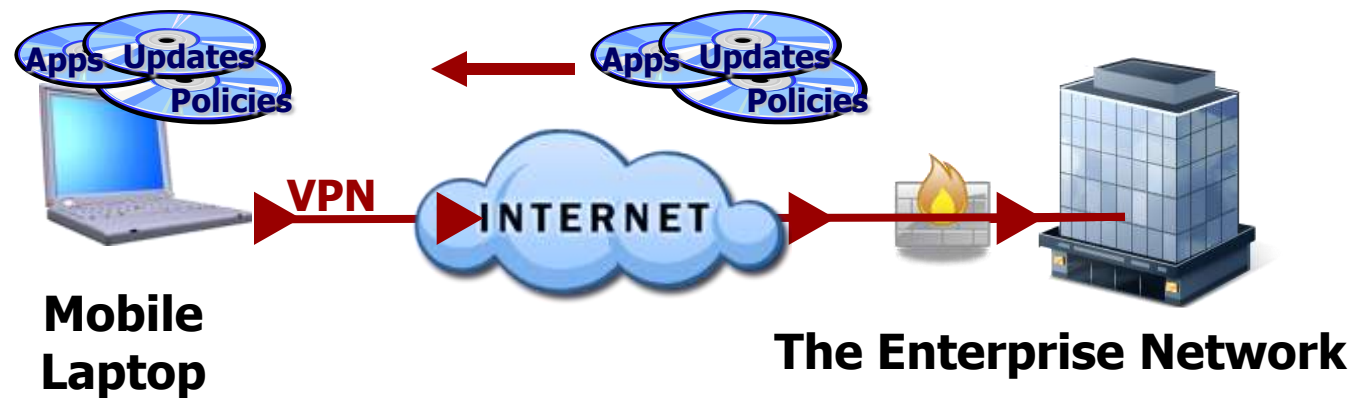


How do you extend this protection to the remote device?

# > Today's Architectures are LAN-Locked

LAN-based solutions rely on a connection to the corporate network to receive updates, new policies, and applications

IT has some Control

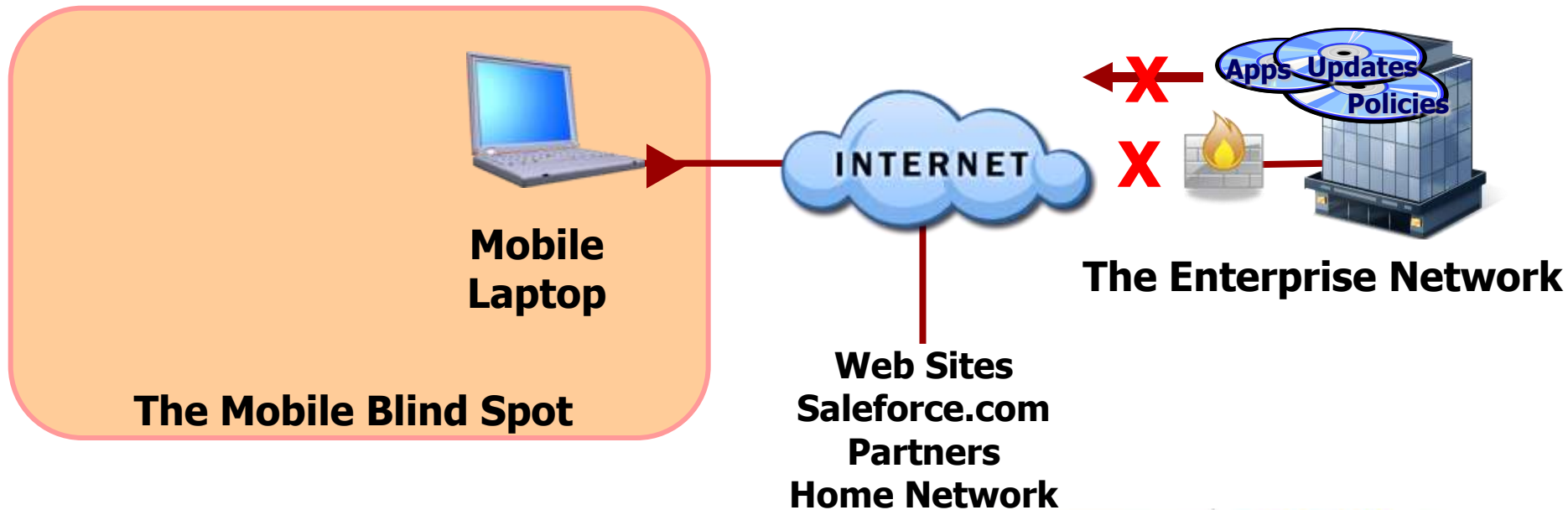


# > Today's Architectures are LAN-Locked

LAN-based architectures rely on a connection to the corporate network to receive updates, new policies, and applications

When the device is not connected to the corporate network, it is in the "Mobile Blind Spot"

IT is not in Control



## > It's a Mobile Paradox ...

***Companies spend more time addressing the least vulnerable devices that they can see, on the network ...***

***... and less time addressing the most vulnerable devices they cannot see, outside the network.***

***This is the "Mobile Blindspot"***

## Case in Point:

# > Are Companies Investing in the Right Area?

- Companies are spending millions in Anti-Virus support
  - When was the last big virus outbreak?
  - Likely a small % increase in protection for the money
- With data replication capabilities, approximately 60% of the data required by the end user is on the PC/laptop already
  - When did you last have a lost or stolen device?
  - Probably much more recent



## SSL VPNs:

### > Expanding The "Mobile Blind Spot"?

"By 2008, SSL VPNs will be the primary remote-access method for more than two-thirds of business teleworking employees, more than three-quarters of contractors and more than 90% of casual employee access (0.8 probability)." *Gartner*

- An SSL VPNs is referred to as an "application layer" technology.
  - Great for email access, the "killer app"
  - IPSec VPNs are Network Layer connections

*The Question: Even if the user connects, will IT have the ability to update this device?*

## > Pursuit Of A Solution – Access Control

- Access control initiatives being considered
  - Cisco NAC, Microsoft NAP, TCG, software suites
- Basic functions of these solutions
  - Policy definition
  - Assessment of the device
  - Quarantine the device
  - Remediation where possible
- The basic concept:
  - Devices that are not in compliance with enterprise security policies should be blocked from accessing corporate networks.

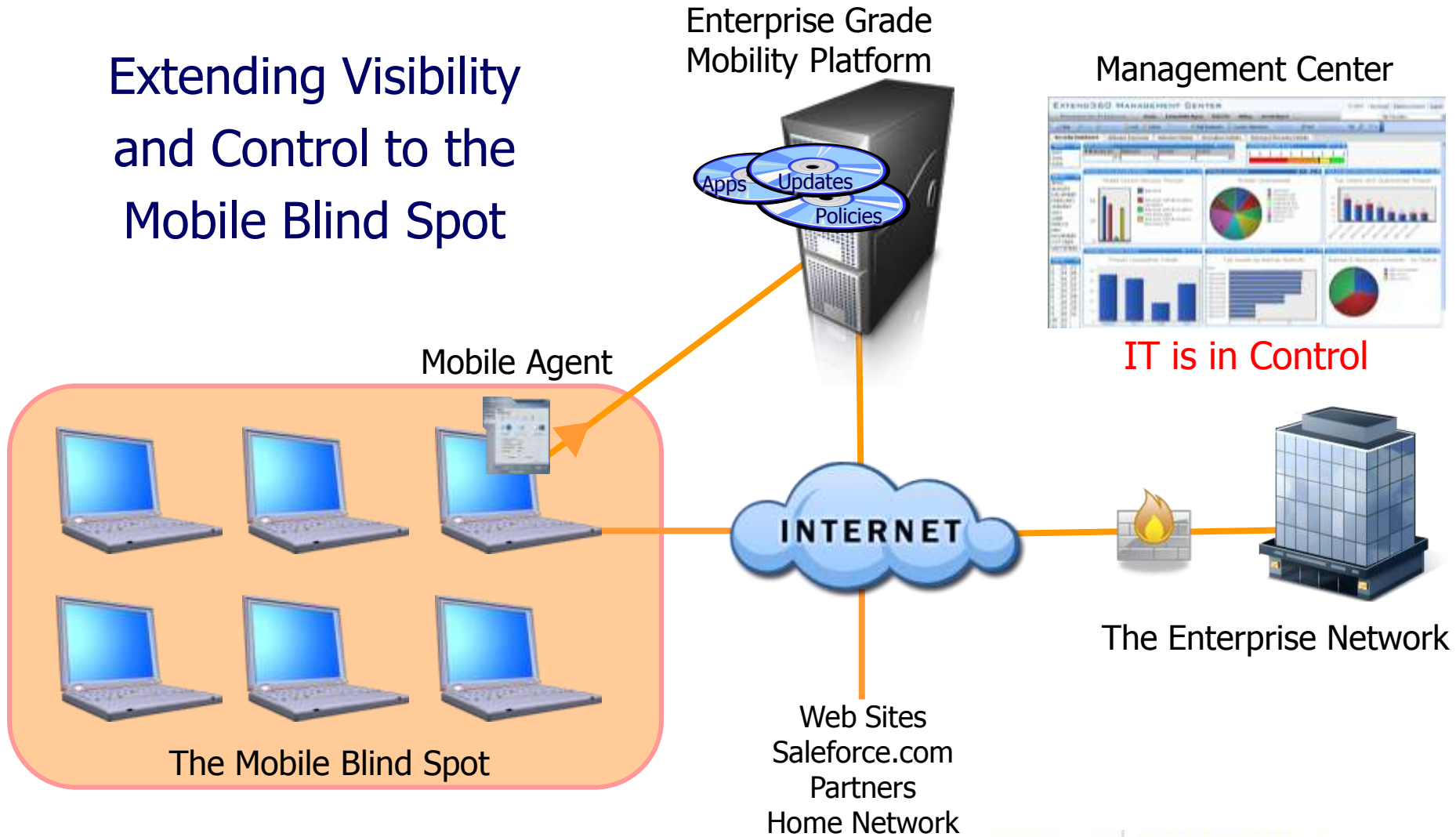
## > Limitations of Access Control

- Fundamental goal: Protect the network, not specifically the data or device
- Users must connect to the LAN (physically or through a VPN)
  - What if they gain Internet access only
- Addressing “baseline” problems
  - AntiVirus, AntiSpyware, Personal FW
  - Not all remediate, many just block the user
- The products do not address “the mobile blind spot” and their unique threats

# > The Mobile Approach – Step 1

Address the Problem & Opportunity Where it Occurs

Extending Visibility and Control to the Mobile Blind Spot



# > The Mobile Approach – Step 2

## Treat All Networks like the Corporate Network

### 1. Corporate Network

### 2. Roaming Network

- 3G
- Wi-Fi
- Hotels
- Dial-up

### 3. Home Network

- Same usability
  - To encourage users to not stray too far
- Enterprise Control
  - Endpoint Security
  - Data Security
  - Updates, etc.
- Universal Access Controls

# > The Mobile Approach – Step 3

## A Phased Approach to Securing Mobility

*Defend against network-based threats and phishing*

- Zero-Day Protection
- Intrusion Prevention
- Anti-Spyware
- Anti-Virus
- Firewall

**2**

*Defend against loss and theft (Data at rest)*

- Data encryption
- Backup and recovery

**3**

*Defend against user policy violations (Incl. data in motion)*

- Device control
- Information protection

**4**

- 1** Endpoint monitoring and remediation, patch management, vulnerability management, inventory management

*Improve administration; Support other defenses*

## > Summary: What's It All Mean To You?

- Increased mobility is creating new device and data threats
  - Insiders are becoming outsiders and are the most vulnerable
- Implement security solutions that reach the “unconnected users” – the Mobile Blind Spot
- Data in motion exposures can occur maliciously or by accident
  - Devices are exposed, with or without the Internet
- An integrated NAC and Mobile NAC solution will provide the overall most compliant and secure solution



**\*\* WiFi Warning \*\***  
**Are You Secure Enough?**

**FIBERLINK**  
Simple. Secure. Mobility.

# Securing WiFi

## > Is it a False Sense of Security?

- Not all WiFi access points are the same
- Public access points don't want security
  - Too painful for the user to manage it
  - Desire simple connection only
- Even secure points are at risk
  - Home and office environments with WEP are exposed
- Let's look at how easy it is to hack...



# A Short “Training” Video

**FIBERLINK**  
Simple. Secure. Mobility.

# > The Internet as a Hacking Source

The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying `http://www.youtube.com/results?search_query=hacking+wep&search_type=`. The page content is the YouTube search results for "hacking wep".

**YouTube - Broadcast Yourself™**

Navigation: [Home](#) [Videos](#) [Channels](#) [Community](#)

Search:  [Videos](#) [Search](#) [Upload](#)

“hacking wep” video results 1 - 20 of about 154

Sort by: [Relevance](#) | Uploaded: [Anytime](#) | Display: [List](#) [Grid](#)

Video Thumbnail	Video Title	Added	From	Views	Rating	Duration	Category
	<b>Hacking WEP Encryption</b> WEP being hacked. MORE: hacks1010.webs.com...hacks hacks1010 hacking wep wpa tsf cell phone upload	Added: 3 months ago	From: <a href="#">sloggyman83</a>	Views: 4,234	★★★★★	01:47	More in <a href="#">Education</a>
	<b>IEFD ep. 2 - Wireless Hacking - Cracking WEP</b> ... To download a High quality version visit our website, www.infinityexists.com...Cracking 128 bit WEP aircrack airodump aireplayhack hacking Infinity Exists (more)	Added: 10 months ago	From: <a href="#">Gregorpm</a>	Views: 131,005	★★★★★	04:42	More in <a href="#">Howto &amp; Style</a>
	<b>Hacking WEP by ĐăĐK</b> Hacking WEP in anyone wireless network....kismet wireless wep aircrack hacking	Added: 1 year ago	From: <a href="#">darkkill666</a>	Views: 66,728	★★★★★	03:36	More in <a href="#">Sports</a>
	<b>Wireless WEP Key Hacking</b> com For a Hacking Guide. This video	Added: 6 months ago	From: <a href="#">jcortes187</a>				

Copyright 2

Done | Internet

# > All You Need to Break a WEP Key

## **Programs Used: (These are all free and easily downloaded online)**

- Backtrack 2 Final- CD Bootable Linux Operating System with built in auditing/cracking tools
- Airodump- Captures wireless packets from access point
- Aireplay- Injects packets at the access point to create traffic and increase cracking speed
- Aircrack- Statistical algorithm to crack WEP 64/128 bit codes. Current version can crack 64bit in 2 minutes and 128bit in < 6.
- Aircrack-ng- Used to create an Evil Twin attack
- Ettercap- Man In the Middle Attacks, can also sniff data and decrypt passwords over the air



# Thank You

Charles Brown  
Product Manager  
[cbrown@Fiberlink.com](mailto:cbrown@Fiberlink.com)

**FIBERLINK**  
Simple. Secure. Mobility.

# A Mobile NAC Approach

## Address the Problem Where it Occurs



Extend360 turns the Internet into your mobile corporate network

Fiberlink Extend360™ Platform



Extend360™ Management Center



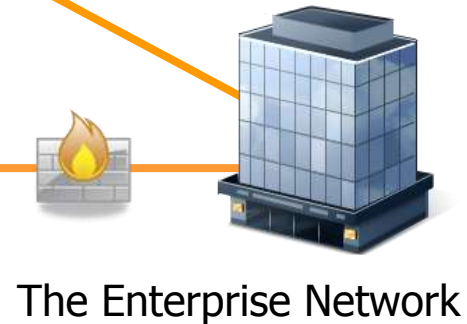
Extend360™ Agent



The Device is Connected



IT is Back in Control



# > Mobile NAC Benefits

- **Protects the corporate network**
  - Blocks non-compliant systems from connecting
- **Addresses the “mobile blind spot”**
  - Monitors, protects and updates mobile computers even when they don’t connect with the corporate LAN
  - Provides protection from start-up to shut-down, anywhere
- **Protects “data at rest” and “data in motion”**
  - Beyond firewalls: data encryption and backup & recovery if devices are lost or stolen
  - Device control and information protection to reduce the risk of internal threats
- **Real-time compliance reporting**
  - Audit trail provides visibility to The Blindspot

# > Recommendation: A Phased Approach to Securing the New Insider Threat

*Defend against network-based threats and phishing*

- Zero-Day Protection
- Intrusion Prevention
- Anti-Spyware
- Anti-Virus
- Firewall

**2**

*Defend against loss and theft (Data at rest)*

- Data encryption
- Backup and recovery

**3**

*Defend against user policy violations (Incl. data in motion)*

- Device control
- Information protection

**4**

- 1** Endpoint monitoring and remediation, patch management, vulnerability management, inventory management

*Improve administration; Support other defenses*

## > Summary: What's It All Mean To You?

- Increased mobility is creating new device and data threats
  - Insiders are becoming outsiders
- Mobile devices are the most vulnerable
- Implement security solutions that reach the “unconnected users” – the Mobile Blind Spot
- Data in motion exposures can occur maliciously or by accident
- Devices are exposed, with or without the Internet
- You will need a blended/layered approach with security
- An integrated NAC and Mobile NAC solution will provide the overall most compliant and secure solution



Thank You

Questions? [cbrown@Fiberlink.com](mailto:cbrown@Fiberlink.com)

**FIBERLINK**  
Simple. Secure. Mobility.