



The New “Insider” Threat

Extending Device and Data Protection
to the Mobile Workforce

Jon Friedman
Director of Marketing
jfriedman@fiberlink.com

FIBERLINK
Simple. Secure. Mobility.

> Agenda

- Mobility – benefits, threats and challenges
- Technologies you should consider
- Setting priorities
- Mobility-as-a-Service

> Fiberlink corporate overview

- **Company:**
 - Founded in 1994; headquartered in Blue Bell, Pennsylvania
 - Presence in North America, Europe, and Asia
- **Legacy of Leadership and Innovation:**
 - Mobility as a Service (MaaS)
 - Gartner Leadership Quadrant for 7 years in a row
- **Mobility as a Service:**
 - The MaaS360 Platform
 - Visibility, control and connectivity for laptops, distributed PCs and mobile devices
 - A menu of managed security services



> Fiberlink customers

Automotive



Consulting



Consumer Goods



Energy



Finance



Healthcare



Insurance



Media



Retail



Technology



Travel



Other



> Mobility helps employees...

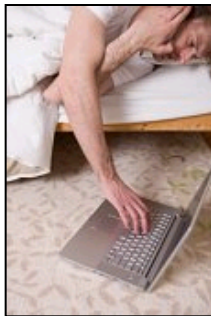
Be more productive



Get closer to customers



Work more hours



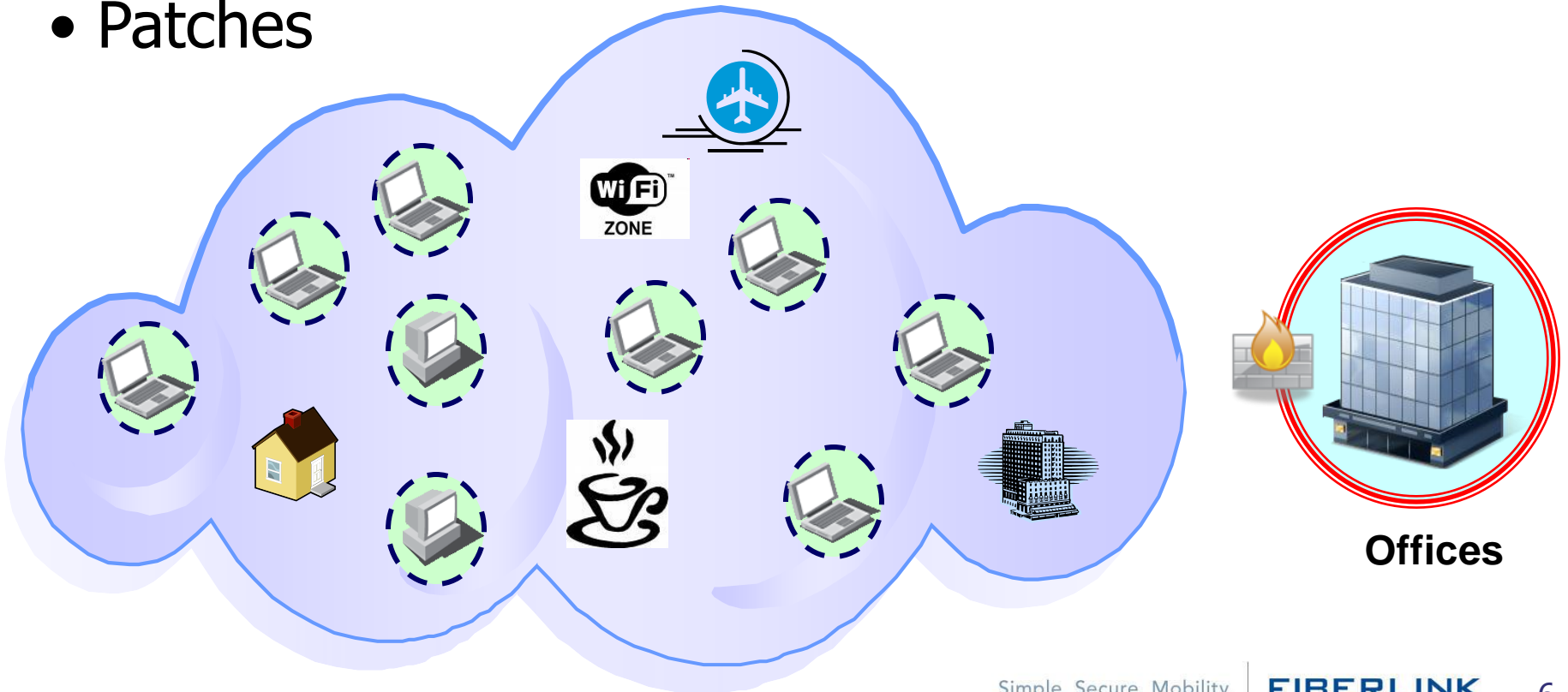
Enjoy flexible lifestyles



...but mobility also brings new challenges...

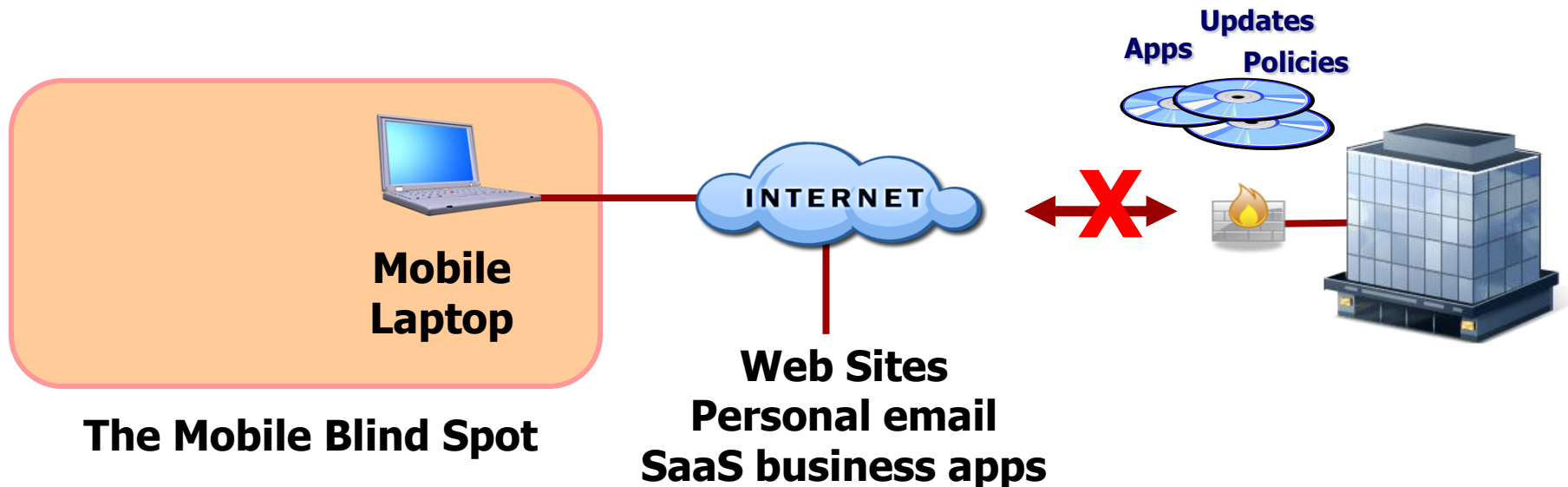
> Managing endpoint security

- Applications
 - Personal firewall
 - Anti-virus
 - Others
- Patches
- Visibility
- Updates
- Remediation



> The “Mobile Blind Spot”

- Employees don't log onto the corporate network for hours, days or weeks
- No patches, no updates, no visibility
- Exposed to hackers and zero-day malware
- No compliance reporting



> Loss and theft of devices



> Lost devices

- 600,000 laptops are reported missing every year just at U.S. airports. (Ponemon Institute)
- In Chicago alone, 160,000 portable devices are left in taxicabs every year. (Washington Post)
- 37% of smart-phone users store confidential business data on their phones. (Washington Post)



> 9,000 USB drives left at UK dry cleaners

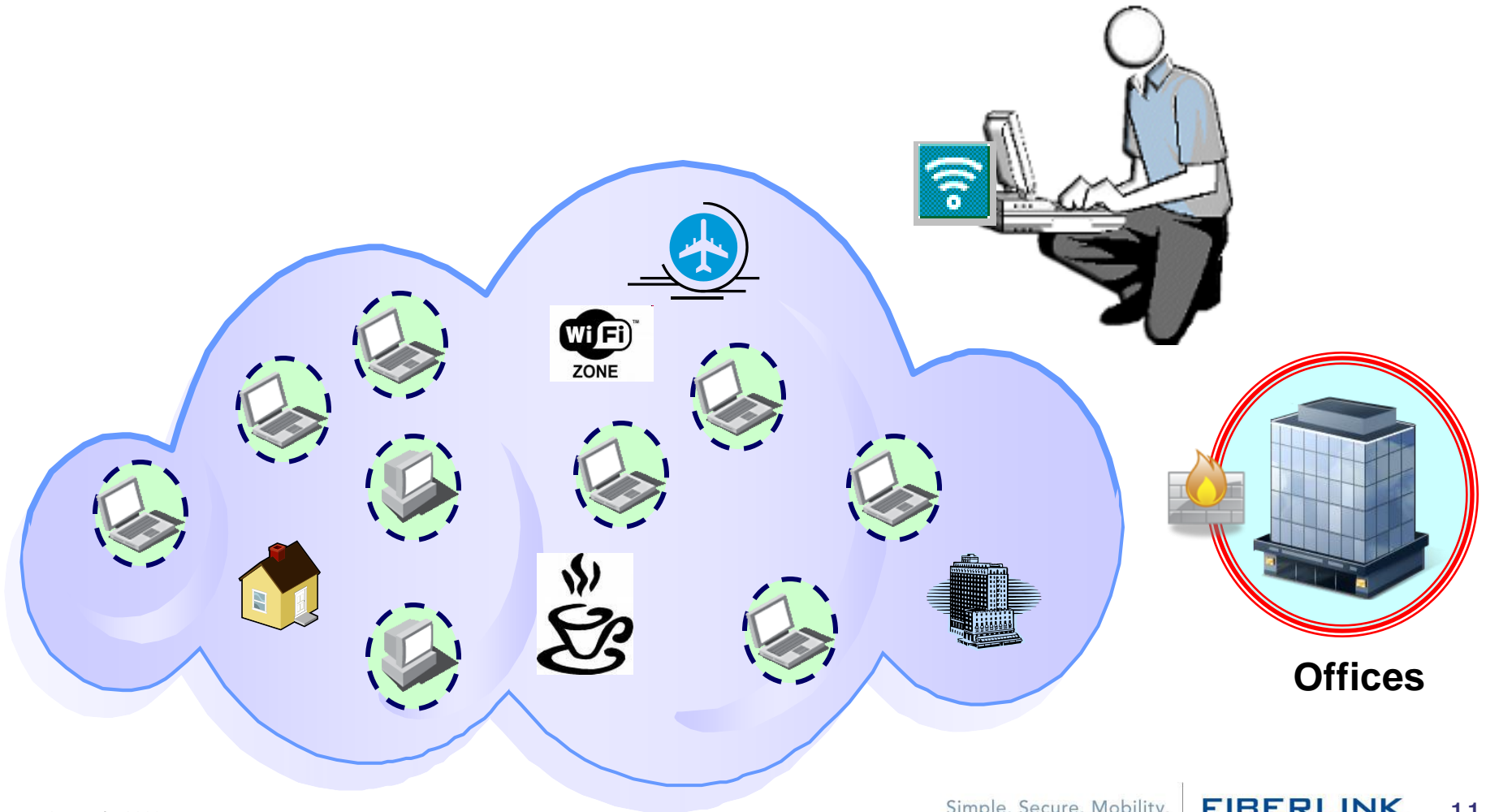
by Steve Ragan - Jan 26 2009, 15:00



Forgotten USB sticks at the dry cleaners leaves data hung out to dry (IMG: courtesy of [Computer Zeitung](#))

> Insecure communications

- Eavesdropping
- “Man in the middle” attacks



> Insecure communications

“Many firms were simply turning on their wireless net access points and use default settings that anyone familiar with wi-fi could easily find out...RSA said that 26% of wi-fi networks found London used default settings compared to 30% in Frankfurt, 31% in New York and 28% in San Francisco.”

> WEP is not very secure

YouTube - Broadcast Yourself. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address http://www.youtube.com/results?search_query=hacking+wep&search_type= Go Links >>

Google Go Bookmarks 156 blocked Check AutoLink AutoFill Send to Settings

You Tube
Broadcast Yourself™




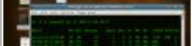
Sign Up QuickList (0) Help Log In Site


Home Videos Channels Community

hacking wep Videos Search Upload

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

Videos Channels Sort by: Relevance Uploaded: Anytime Display: [List] [Grid]

	Hacking WEP Encryption WEP being hacked. MORE: hacks1010.webs.com...hacks hacks1010 hacking wep wpa tsf cell phone upload	Added: 3 months ago From: sloggyman83 Views: 4,234 ★★★★★ 01:47 More in Education
	IEFD ep. 2 - Wireless Hacking - Cracking WEP 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: Gregorpm Views: 131,005 ★★★★★ 04:42 More in Howto & Style
	Hacking WEP by ĐăĐK Hacking WEP in anyone wireless network....kismet wireless wep aircrack hacking	Added: 1 year ago From: darkkill666 Views: 66,728 ★★★★★ 03:36 More in Sports
	Wireless WEP Key Hacking com For a Hacking Guide. This video	Added: 6 months ago From: jortes187



better than flowers
Give mom a FREE* Nokia 6085 camera phone
Get a free phone
*Signif. restrict. apply

Copyright 2

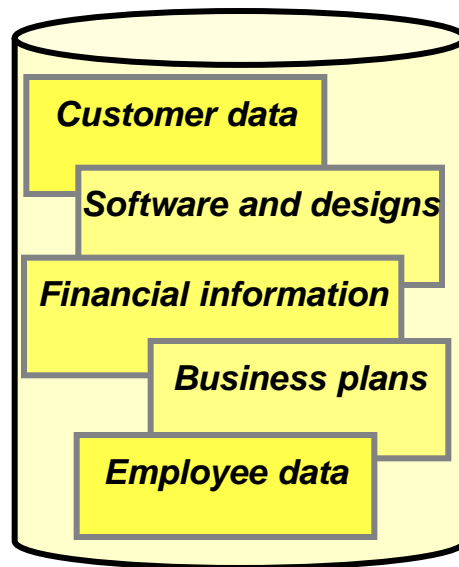
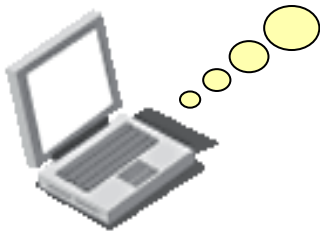
Done Internet

> Employee "data leakage"

- Disgruntled employees
- Inadvertent policy violations

60% of corporate data resides on laptops and PCs

- IDC



- Social security #s
- Credit card #s
- Bank/account #s
- Protected health info



> Employee “data leakage”

- **61% of respondents said that accidental data leaks occur frequently or very frequently. (Ponemon Institute)**
- **79% of respondents said one or more insider-related security breaches at their companies go unreported. (Ponemon Institute)**



> Compliance – does it affect me?

- Yes, if you store credit card numbers or social security numbers
- Yes, if you store confidential employee information
- Probably, if your business customers are regulated
- In the future, if you store any confidential customer information
 - Massachusetts 201 CAR 17.00, effective 1/1/2010 (<http://www.fiberlink.com/fiberlink/en-US/utility/Mass201.html>)

A blurred background image of a business meeting. In the foreground, a laptop is open on a table. In the background, several people in business attire are seated around a table, engaged in conversation.

So What Should We Do?

FIBERLINK

Simple. Secure. Mobility.

> Review key technologies

Endpoint Security

- Personal firewall
- Anti-virus and anti-spyware
- Patch management
- Zero-day threat protection/intrusion protection

Data Protection

- Data encryption
- Data leak prevention
- Device (USB) control
- Back-up and recovery

Communications

- VPN

> Include visibility/management tools

- What laptops are missing a critical patch?
- How many systems have the standard firewall in the current release?
- How old are the anti-virus signature files?
- What unsafe applications are installed?
- Has the new security application been installed properly?
- How many systems have enough capacity to upgrade?

> Set priorities

- **Identify risks**
 - Legal and regulatory exposure
 - Loss of reputation
- **Identify who is carrying the data**
 - Credit card and banking numbers
 - Employee data (SS #s, contact information, health information)
 - Confidential business information: Business plans, product designs, software code, etc.

> Set priorities, cont.

- Tighten up access and auditing
 - May require rewriting policies
- Use “thin client” technology and SSL VPNs where applicable
 - Better for “functional” workers and database-oriented applications,
 - Usually not good for knowledge workers and “personal productivity” applications

> Set priorities, cont.

- Set up a mobile security “baseline” configuration
 - Personal firewall
 - Anti-virus
 - Patch management
 - Data encryption?
- Create a “plus” configuration for key employees
 - Data encryption (if not in baseline)
 - Device (USB) control
 - Data leak prevention
 - Back-up and recovery

> Mobility as a Service (MaaS)

1. Collect and submit data from endpoints

- Inventory data
- Device status
- Compliance status

2. Enforce policies on endpoints

- Stop applications
- Restart applications
- Download files
- Cut network access

Management Portal

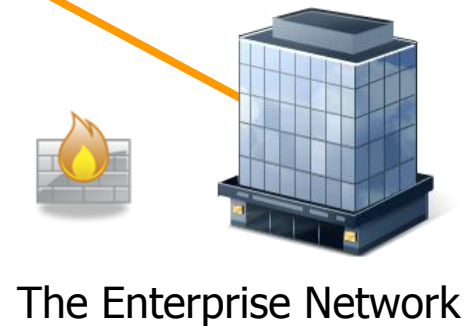


3. Report on inventory, status, compliance, cost

4. Define and distribute policies, document that policies were enforced

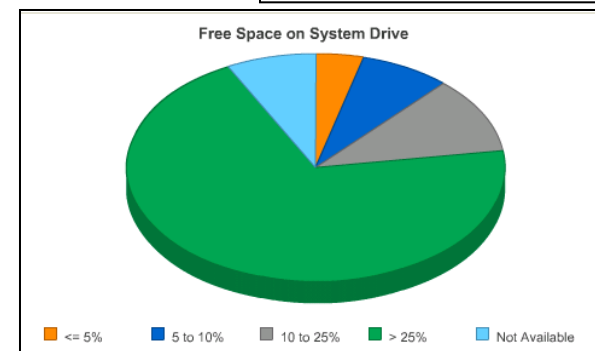
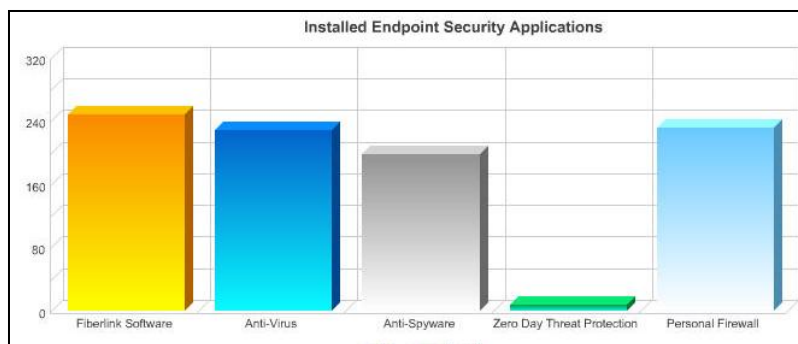
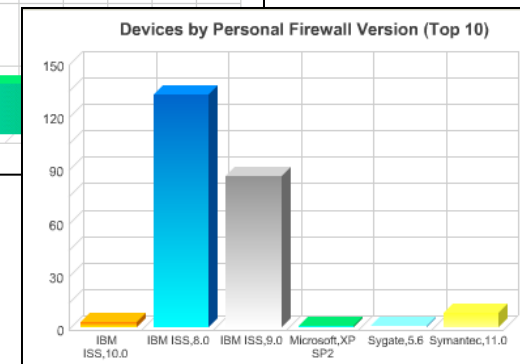
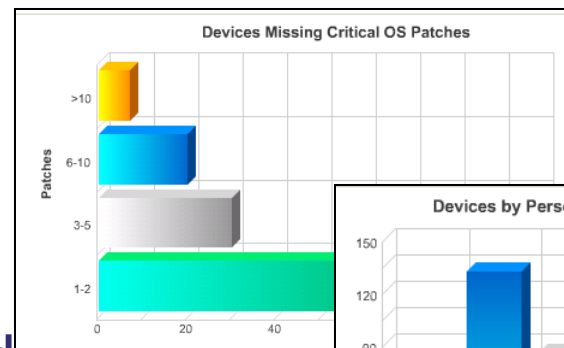


Web Sites
Personal email
SaaS business apps



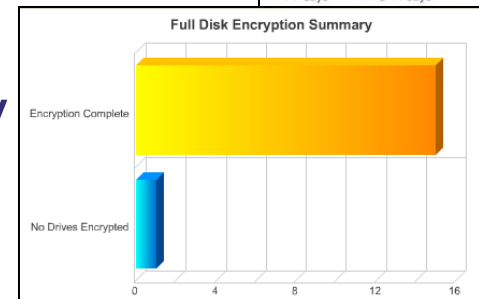
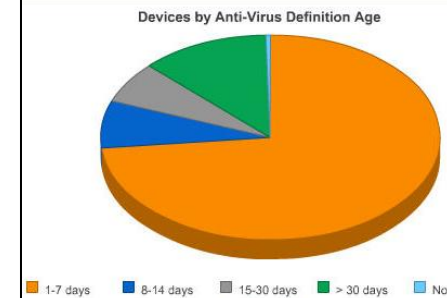
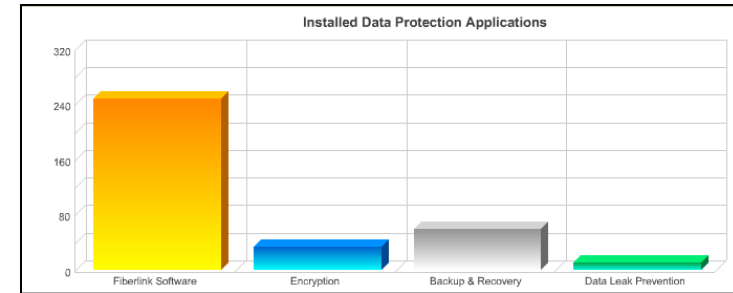
> Improve operational efficiency

- A single management console giving a comprehensive view of software and security applications on endpoints
 - Installed hardware and software
 - Operating system patches
 - Firewalls and anti-virus packages
- Identify gaps and problems
- Know what needs to be updated
- Document compliance
- Plan for upgrades and migrations



> Manage and protect corporate data

- One console to view and control multiple endpoint security and data protection applications
- Automatically update OS patches and anti-virus signature files
- Monitor and remediate security software
- Block non-compliant systems (NAC)
- Speed up deployment of new security applications
 - Data encryption,
 - DLP
 - Device (USB) control
 - Others



Action When Out of Compliance

Warn But Do Not Enforce

----- Select One -----

Disconnect Extend360 Established

Disconnect Extend360 Established

Restrict Internet Access based on

Warn But Do Not Enforce

Disconnect Extend360 Established Internet and VPN Connections

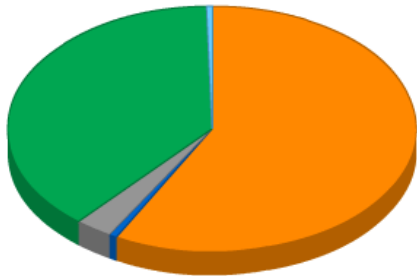
Select the action to be taken when a device is out of compliance. Firewall applications being installed but not been installed.

> Reduce risk by enforcing compliance

Provides a comprehensive picture of:

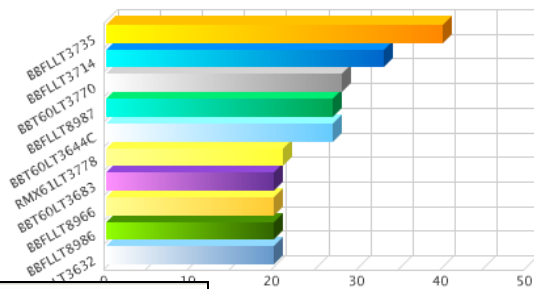
- Software installed
- Patches applied
- Devices in compliance
- Devices out of compliance
- Reasons for falling out of compliance
- Enforcement and remediation actions taken

Out-of-Compliance Events by Application



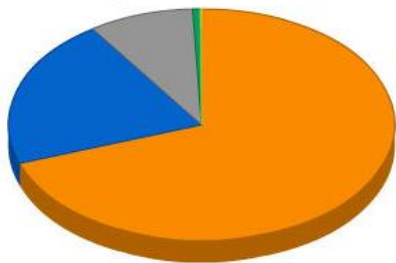
Anti-Virus
Extend360 Enforcement Agent
Generic Applications
Data Encryption
Firewall

Devices Out-of-Compliance (Top 10)



Events
Print Download

Out-of-Compliance Enforcement Actions



Application Started
Establish VPN Connection
Application Stopped
No Action Taken
Disconnect Internet
Denied Connection

> Mobility management is a “Smart Spend”

Q. What is a “**Smart Spend**”

- A. An investment that impacts multiple initiatives
- **Reduce capital expenses**
 - Hosted solutions reduce data center and hardware expenses
- **Lower direct and indirect costs of mobility**
 - Reduce administration, help desk, security and training costs; support telework
- **Increase the value of existing investments**
 - Manage existing security applications better.



> What does it mean to you?

- Increased mobility is creating new device and data threats
- Mobile devices are the most vulnerable
- Implement security solutions that reach the “unconnected users” – the Mobile Blind Spot
- Consider a cloud-based solution to improve overall visibility where mobility is most vulnerable
 - Fewer resources to support
 - Better overall economics



Thank You!

Please stop by our display
for more details

Questions? jfriedman@Fiberlink.com

FIBERLINK

Simple. Secure. Mobility.