



FIBERLINK

**MOBILITY AS A SERVICE: BEST PRACTICES
FOR MANAGING MOBILE WORK**

Contents

- OVERVIEW.....1**

- THE CHALLENGES OF MOBILE COMPUTING.....2**
 - The Connectivity Conundrum.....2
 - Lan-Locked Management Tools.....2
 - Security Shortcomings.....2
 - Hide and Seek.....2
 - The Danger Within.....3
 - Data Disasters.....3
 - Summary: Overlooked and Vulnerable.....3

- BEST PRACTICES FOR A MOBILE COMPUTING ENVIRONMENT.....4**

- MOBILITY AS A SERVICE.....5**

- THE FIBERLINK SOLUTION.....6**

- THE AGENTS.....7**
 - MaaS360.....7**
 - Get Control.....8
 - Get Visibility.....10
 - No Longer Overlooked and Vulnerable.....12

- SUMMARY.....13**

- APPENDIX I: COMPLEMENTARY FIBERLINK SERVICES.....14**

- APPENDIX II: HOW ONE COMPANY COULD BENEFIT FROM THE MAAS360 MOBILITY PLATFORM.....15**

Overview

Businesses today have reached a tipping point where a majority of the workers are mobile, or soon will be. It's time now for a set of best practices and solutions specifically aimed at managing the mobile computing environment.

Our lives are becoming more flexible and mobile, so are our work lives. Mobility isn't limited to classic road warriors. Mobile work practices now encompass telecommuters who work from home; office workers who carry notebook PCs into conference rooms for meetings; employees in remote field offices; and day extenders who put in a few extra hours of work at home. According to The Yankee Group, nearly 50% of today's enterprise workers are considered to be "mobile." By the year 2011, IDC predicts that 75% of the U.S. workforce will be mobile.

People now use the Internet and the World Wide Web as their office resources. Workers use their portable PCs to connect to "the office" to catch up on email and perform other important tasks. Web based applications are mission-critical for many businesses. Without a doubt, the Internet has become a necessary extension of the corporate network.

But while business mobility initiatives enhance productivity and flexibility, they have a few drawbacks as well. Workers often have difficulty connecting to the corporate network or the Internet securely and conveniently. Once they do connect, data downloaded to the notebook hard drive is vulnerable to theft or loss. As soon as the umbilical cord of the LAN cable is disconnected, the mobile PC is subject to haphazard enforcement of policies and procedures. This is the "mobile blind spot."

The challenges posed by mobility lead to operational inefficiencies, higher support costs, and increased vulnerabilities to attacks targeting company computing assets and data.

So how can all of the mobile (and remote) devices that access the corporate network and resources such as Web-based applications be given the same level of attention as the wired world when it comes to connectivity, security, productivity and compliance?

This paper discusses the inherent risks of the mobile blind spot, best practices for managing a mobile environment, the concept of "Mobility as a Service," and how Fiberlink Communications helps organizations control mobile devices and data with the MaaS Mobility Platform™.

The Challenges of Mobile Computing

With the growth in mobile computing comes a new set of complexities for companies trying to make it simple and seamless for their end users to connect, while at the same time protecting their network, their information assets and the reputation of their business.

THE CONNECTIVITY CONUNDRUM

Why can't remote connectivity be as simple as plugging the office LAN cable into a notebook PC?

It seems that as soon as an office worker disconnects his notebook PC from the LAN cable, he's looking for a way to connect again to the company network. Whether he uses Wi-Fi, dial-up, ISDN, broadband, or mobile wireless, he wants to connect easily to the network hosting the resources he needs to do his job. This certainly seems like a reasonable expectation.

The fact is, it practically requires a degree in telecommunications to connect from a mobile or remote location - especially a public location like an Internet café. The average worker can't be expected to learn about ISPs, firewalls, modems, wireless networks, protocols, IP addresses, and all the strange configuration settings that will ultimately allow him to connect in a secure fashion.

LAN-LOCKED MANAGEMENT TOOLS

Most mid- to large-sized companies have mastered the science of managing PCs that are directly connected to the company network. There are numerous asset management and systems management tools that automate the "care and feeding" processes of "wired" PCs. These processes include - among many other things - applying timely security patches and software updates; monitoring the PC for anomalous activities; preventing an infected PC from attaching to the network; backing up or encrypting sensitive data; ensuring that corporate policies are enforced, and so on. Typically a central console ensures the security and well being of the connected devices and the data on them.

However, these tools are "LAN-locked"; they don't work well (and sometimes, not at all) on devices that don't maintain a constant touch with the management console. Once a notebook PC is disconnected from the corporate network, the centralized controls and policies are unable to reach the notebook to do their jobs. For example, a disconnected device misses a critical patch to its operating system, leaving the PC susceptible to a known vulnerability.

SECURITY SHORTCOMINGS

Mobile devices create new types of exposure and risk. They are not protected by central firewalls and intrusion detection systems. They frequently communicate over insecure networks, often including public access points in hotels, airports and metro locations. The devices are light weight and portable, making them vulnerable to loss, theft and damage.

Once taken off the network, a notebook PC often has no automated enforcement of corporate security policies. Security, then, is in the hands of the notebook user, whose primary job and expertise is not in computer security. Consequently, he's more concerned with getting a job done than with the risks associated with his actions. In the end, relying on old security measures for new mobile technologies is like locking the bank vault and leaving the cash on the sidewalk.

HIDE AND SEEK

The IT department has little visibility into what is happening on a disconnected mobile PC. For example, there's a lack of log monitoring and intrusion detection system data. When the PC doesn't "phone home,"

THE DANGER WITHIN

Due to potentially lax security procedures, a notebook PC is quite susceptible to getting infected by a virus or other malware. Having one infected computer is bad enough, but when the compromised device is reconnected to the corporate network, it can propagate the malware throughout the network.

DATA DISASTERS

As more workers move to a mobile platform to conduct their work, they often bring their critical data with them. According to IDC, 60% of corporate data resides on desktop PCs and notebooks. Few workers take the necessary steps to protect the data. Steps like backing up the data to a secure location, making sure the data is encrypted when it is "at rest" on the hard drive, or even not possessing the data at all if it is too sensitive. It's difficult to enforce data usage policies and procedures on a mobile PC.

SUMMARY: OVERLOOKED AND VULNERABLE

In summary, mobility introduces challenges that don't exist in the "constant touch" world of a wired corporate network. As a result, security policies and best practices that are rigorously enforced for continuously connected computers are often overlooked for mobile and remote users. Mobile devices and the confidential data on them remain vulnerable much of the time, even after the traditional LAN-based systems management solutions have been implemented.

Best Practices for a Mobile Computing Environment

Eliminating the mobile blind spot - those areas that can't be reached by traditional systems management tools and techniques - requires a different strategy. While there isn't a definitive list of best practices to simplify connectivity and improve systems management and security for a mobile environment, the National Institute of Science and Technology (NIST) does offer these guidelines in its publication *User's Guide to Securing External Devices for Telework and Remote Access* (NIST Special Publication 800-114). According to NIST, securing a mobile PC includes the following actions:

- Use a combination of security software, such as anti-virus and anti-spyware software, personal firewalls, spam and Web content filtering, and popup blocking, to stop most attacks, particularly malware.
- Restrict who can use the PC by having a separate standard user account for each person, assigning a password to each user account, using the standard user accounts for daily use, and protecting user sessions from unauthorized physical access.
- Ensure that updates are regularly applied to the operating system and primary applications, such as Web browsers, email clients, instant messaging clients, and security software.
- Disable unneeded networking features on the PC and configure wireless networking securely.
- Configure primary applications to filter content and stop other activity that is likely to be malicious.
- Install and use only known and trusted software.
- Configure remote access software based on the organization's requirements and recommendations.
- Maintain the PC's security on an ongoing basis, such as changing passwords regularly and checking the status of security software periodically.

Source: *User's Guide to Securing External Devices for Telework and Remote Access* (NIST Special Publication 800-114)

The NIST guidelines are simply the basic tenets of good security for mobile and remote computing. The following additional activities will further strengthen the management and security posture for a mobile platform:

- Build, implement and maintain policies and procedures that are enforced even when the device is off the corporate network.
- Protect the data through automated techniques that include encryption, backup and authorization validation.
- Control hardware and software settings and configurations to prevent unauthorized or undesired changes or compromise.
- Provide a simple, secure connection to the Internet and to the corporate network regardless of location and connectivity medium.
- Deliver timely patches and other software updates to reduce vulnerabilities and enhance productivity. Turn off automatic updates that are not issued in accordance with corporate policy.
- Isolate compromised or suspect mobile devices from the corporate network until the risk can be mitigated to prevent further harm to the business.
- Collect and analyze the appropriate log data from the mobile devices to be aware of their health and status.

And most businesses would add a few additional conditions: do all of the activities above without impacting the end user or his productivity; without overwhelming the IT staff; and at a reasonable and predictable cost.

Mobility as a Service

Reviewing the combined lists of best practices, it's easy to see how mobile management and security can slip through the cracks; it's difficult and expensive to do it all by assembling the policies, procedures, technologies and services from scratch. What's needed is a comprehensive, unified solution that reduces the risks and costs of supporting the growing mobile workforce. What's needed is "Mobility as a Service."

Mobility as a Service is a new paradigm for managing mobile workers, devices and data. In this model an Internet-based mobility management platform allows IT administrators to use a single web-based console to control many types of connectivity and security software on hundreds of mobile devices. They can manage in one place operational tasks such as deploying and updating software, and reporting on compliance status and security events.

Because Mobility as a Service platforms are hosted on the web, enterprises do not need to invest in hardware, administer servers, or worry about new releases of the software.

A web-based service model is particularly appropriate to mobile technology, because the management application can work with devices over the Internet. This contrasts with "LAN-locked" tools that are not fully effective until the mobile devices VPN into the corporate network.

A well-devised Mobility as a Service platform will help organizations:

- *Address the "Internet everywhere" reality.* As more and more people choose to work whenever and wherever they need or want to, and as applications and services move out of the data center and into "the cloud," the Internet grows in importance as the corporate network.
- *Consolidate mobile technologies into a single endpoint-based solution.* The platform to manage and control mobile devices must be easy for IT to implement and administer and seamless to the end user.
- *Improve risk management.* Mobile devices and the data on them pose a very high risk to companies. At the same time, the techniques to manage the devices and mitigate the risks can be costly. An effective Mobility Management Platform must help an organization manage its risk posture while also controlling operating costs.
- *Address the most serious mobile threat: loss of data.* The platform must automatically encrypt and backup data to protect this soft asset during loss or theft of the mobile device or other malicious activity.
- *Simplify network access.* Workers need to be given the means to easily and securely access the network, just as if it were another application invoked by clicking an icon on the PC screen. Making workers "think" about network access detracts from their productivity.
- *Facilitate reporting.* Operations, Security, Audit, and Compliance teams require on-demand reporting to assess and monitor the health and policy compliance posture of mobile endpoints.

The Fiberlink Solution

Fiberlink offers the world's leading Mobility as a Service solution: the MaaS Mobility Platform™. As shown in Figure 1, this platform consists of two types of components, laptop- and PC-based agents (Extend360™ and Secure360™) and a web-based management and reporting application (MaaS360™).

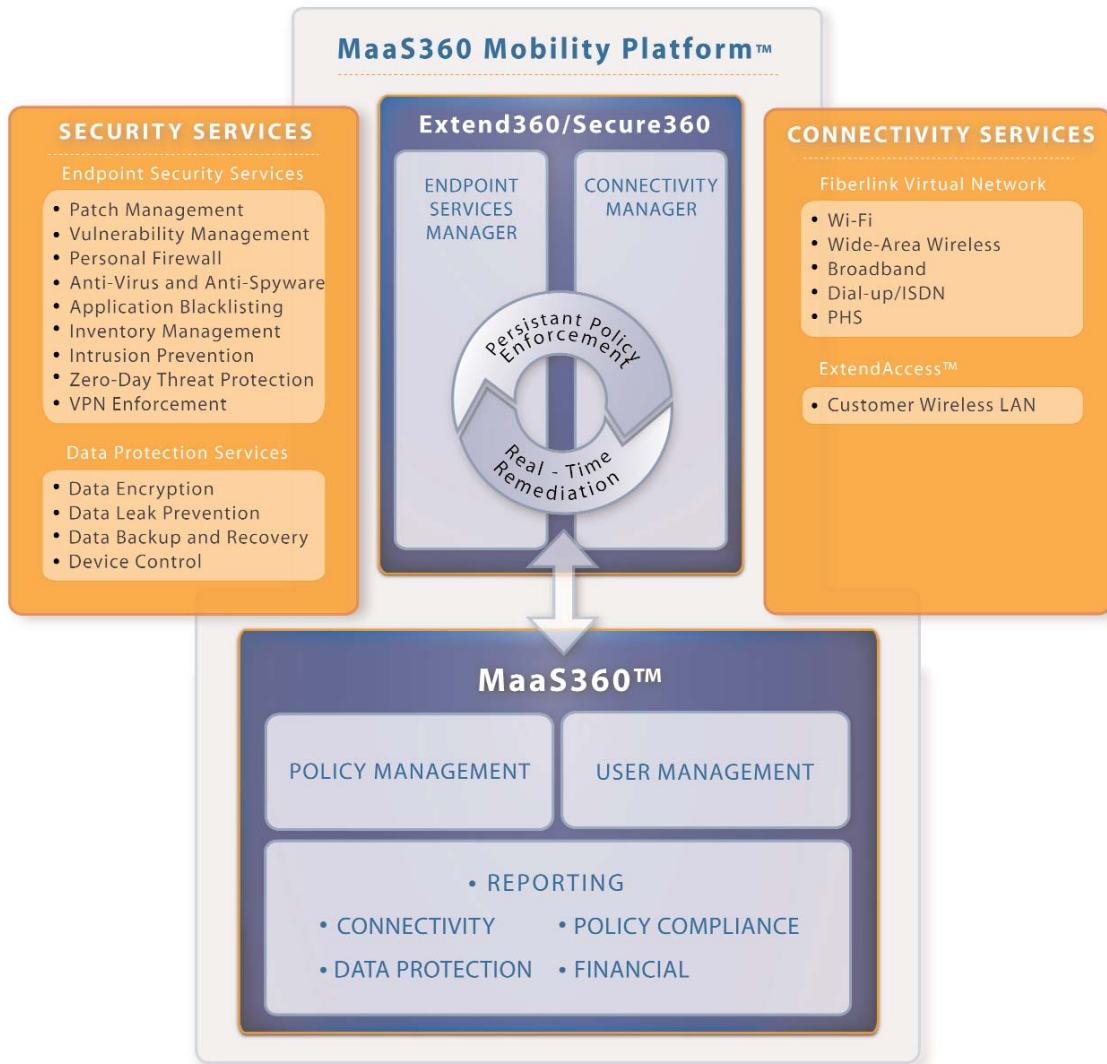


Figure 1: The MaaS Mobility Platform

The Agents

Extend360 and Secure360 are software agents that run on PCs and other endpoint devices.

Extend360 is designed for notebooks and other mobile devices. It includes:

- An **Endpoint Services Manager** that can install, monitor, update and remediate a variety of security, data protection, and endpoint control applications.
- An easy to use **Connectivity Manager** that allows employees to access the Internet with a single click, using any available connection type, including Wi-Fi, 3G mobile data, broadband and dial-up connections.

Secure360 is tailored for desktop (non-mobile) PCs. It includes the Endpoint Services Manager, and provides security and management functions while remaining unobtrusive to PC users.

MaaS360

MaaS360 is the world's leading Mobility Management Platform. It is hosted by Fiberlink in the company's secure and highly reliable data centers. Administrators can access management tools and reports anytime, anywhere from a browser, and don't need to invest in hardware or upgrade software.

A Web portal allows network, IT operations and security personnel to set policies for connectivity and security applications and distribute them quickly to notebooks and other mobile devices. Four optional reporting modules provide visibility into connectivity, policy compliance, security and cost data on distant systems.

MaaS360 gives administrators a single tool to manage the deployment, configuration, monitoring and remediation of a wide range of endpoint security and connectivity services. Compared to using a patchwork of different management and reporting tools, this unified approach reduces administrative costs, provides more consistent security, and makes it easier to comply with regulatory requirements. What's more, an on-demand Mobility-as-a-Service architecture makes deployment fast and economical, reduces on-going management costs, and provides a global mobility infrastructure with no up-front investment.

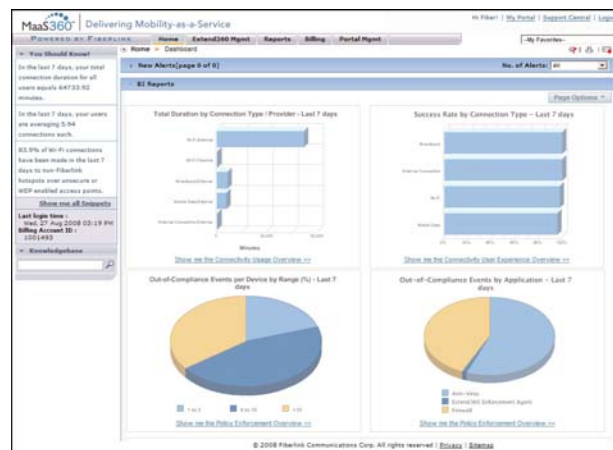


Figure 2: The MaaS360 home page

GET CONTROL

Administrators can control connectivity and security software packages on thousands of mobile devices to keep them in compliance with corporate standards. The unified Web based console makes it easy to manage hundreds of policies and configuration settings and distribute them to systems in the field via the Internet.

Control: Connectivity

Network and IT operations staff can determine what connectivity and remote access services are available to each user group (see Figure 3). For example, top executives and sales "road warriors" can be given access to Wi-Fi, mobile data, broadband and dial-up services worldwide, while other groups are restricted to limited sets of services and regional carriers. Authentication services and policy settings can ensure secure connectivity and data protection for all mobile workers. This helps to make connecting to the corporate network and the Internet easy and intuitive for the workers, and it provides peace of mind to those charged with protecting the network and the data assets.

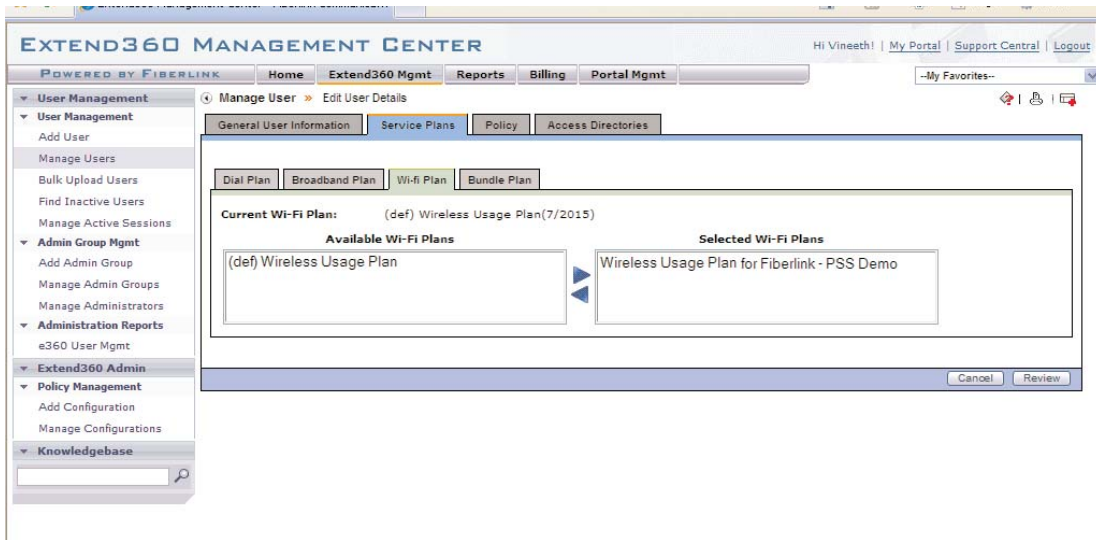


Figure 3: Setting connectivity options

Control: Security

Maa360 allows IT operations and Fiberlink staff to set policies for dozens of endpoint security and control applications on laptops, including:

- Personal firewalls
- Anti-virus and anti-spyware packages
- Data encryption
- Data leak prevention
- Zero-day malware protection
- Intrusion prevention
- Backup and recovery
- Device control

Maa360 can also configure Extend360 and Secure360 agents on laptops and PCs to continuously monitor and remediate security applications. This helps reduce support issues as well as the risks of mobile computing (see Figure 4).

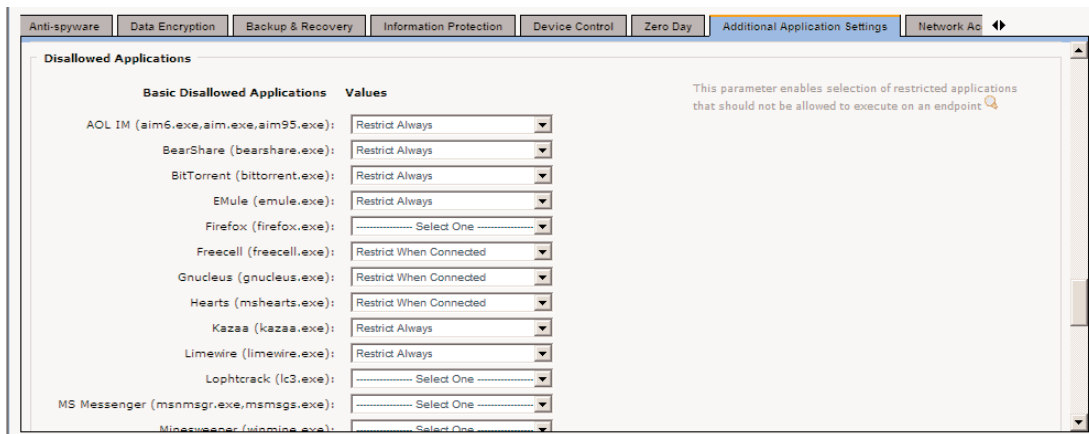


Figure 4: Setting security policies

Control: Network Access Control (NAC) Settings

Fiberlink's Mobile NAC™ technology prevents mobile systems that do not comply with corporate policies from infecting corporate networks. Administrators can define what constitutes compliance and what actions to take with non-compliant systems, actions such as blocking access to the corporate network entirely, or restricting access to specific IP ranges.

GET VISIBILITY

If what you can't see can hurt you, then it's imperative to gain visibility to what is happening on the fleet of mobile devices. MaaS360 collects data from notebooks and mobile devices in the field and provides administrators with visibility into connectivity, policy compliance, security and cost data that otherwise might take days or weeks to compile.

Visibility: Connectivity Reports

Detailed reports correlate connectivity data across corporate wireless LANs, public hot spots, mobile data networks, and broadband and dial-up connections (see Figure 5). Data on types of connections used, connection problems, and session duration can be broken down by departments, regions, and even individual users. Administrators can use these reports to troubleshoot connection difficulties, analyze usage patterns, and save money by moving workers to cost-effective networking plans.

Visibility: Policy Enforcement and Compliance

MaaS360 allows administrators to define compliance with government regulations and industry standards and then track which devices are in compliance with corporate policies, which ones are out of compliance, and what remediation actions that have been taken to restore compliance. They can observe trends, and identify specific devices and applications associated with the most policy violations. These reports facilitate audits and reduce the time and cost it takes to conduct them (see Figure 6).

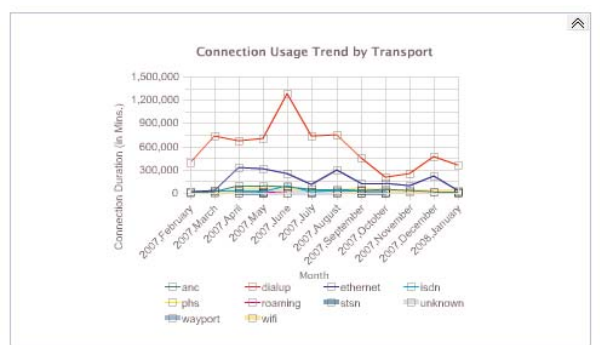


Figure 5: Track connectivity by transport type, region and department

Visibility: Security Reports

MaaS360 provides a single location to find detailed reports from a wide range of endpoint security and control applications. This helps an administrator pinpoint security issues and take steps to remediate them before the problems become damaging and costly (see Figure 6).



Figure 6: Compliance dashboard

Visibility: Data Protection Reports

MaaS360 provides detailed reports on data encryption, data loss prevention, and backup and recovery security applications. This helps an administrator pinpoint security issues and take steps to remediate them before the problems become damaging and costly (see Figure 7).

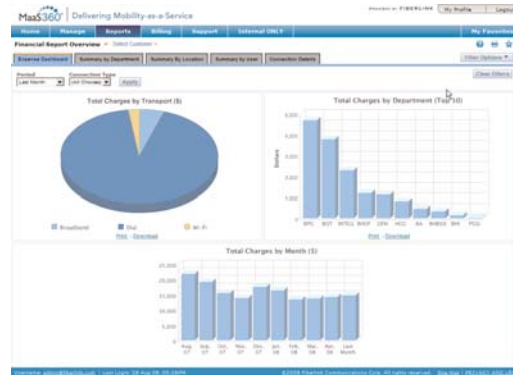


Figure 7: Data protection reports ensure security applications are working

Visibility: Financial Reports

Financial reports can help network and financial staff track connectivity expenses, identify high-cost practices, and charge remote access costs back to departments (see Figure 8).

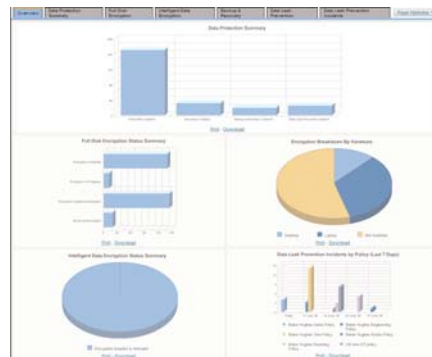


Figure 8: Networking costs are broken down by department and transport type

NO LONGER OVERLOOKED AND VULNERABLE

MaaS360 dramatically reduces the cost of managing mobile workers because it provides a single management console for many connectivity and security applications, automates routine administrative tasks, and centralizes reporting. Companies can roll out new connectivity and security technologies in weeks instead of months, because they can quickly set policies, distribute software to thousands of mobile devices, and track the progress of deployments. And the MaaS360 improves the reliability and consistency of mobile work, because Fiberlink tests a wide range of connectivity services, mobile data cards, VPN clients, and endpoint security applications and ensures that they all work smoothly together.

Summary

Information technology and networking departments are hard-pressed to provide the security, connectivity and control needed to make mobile computing safe and convenient. Fiberlink Communications studied the challenges of mobile computing as well as the best practices for the management, control and operations of a mobile platform. As a result, Fiberlink has selected and integrated the technologies that best address those challenges into the MaaS360 Mobility Platform, as well as complementary security and connectivity services (described in Appendix I).

Fiberlink offers:

- The world's best Mobility as a Service platform.
- The most complete endpoint security available from one source.
- The simplest, anytime/anywhere network connectivity.

Fiberlink's products and services allow IT departments to:

- Improve the security of mobile computers.
- Protect sensitive data.
- Improve the connectivity experience of mobile employees.
- Reduce networking costs.
- Reduce support and administration costs.
- Prove compliance with government regulations and enterprise security policies.

These achievements can increase the productivity and satisfaction of mobile employees, and improve the efficiency and competitiveness of the entire enterprise.

FOR MORE INFORMATION

For more information on Fiberlink's technology and services, contact Fiberlink at:
1787 Sentry Parkway West, Building 18, Suite 200; Blue Bell, PA 19422
Phone 215.664.1600; Fax 215.664.1601
www.fiberlink.com

Appendix I: Complementary Fiberlink Services

Fiberlink Solution Component	Benefits
<p>The MaaS360 Mobility Platform™, a Mobility as a Service platform for managing security and connectivity applications. It includes the Extend360 and Secure360 agents, which manage security and connectivity services on mobile devices, and the MaaS360™, a centralized management and reporting system that facilitates security policy and user management.</p>	<p>This comprehensive mobility management platform...</p> <ul style="list-style-type: none"> • Reduces security risks associated with unmanaged and unprotected mobile computers • Improves a company's compliance posture (Sarbanes-Oxley, HIPAA, PCI, etc.) • Lessens the administrative burden for IT departments • Increases productivity for end users by giving them a stable, secure, easy-to-connect PC • Reduces the overall cost of managing and operating a fleet of mobile computers
<p>Fiberlink Security Services, a set of services to deploy and manage endpoint security and data protection applications on mobile devices.</p>	<p>These world-class security services...</p> <ul style="list-style-type: none"> • Protect mobile devices against hackers, viruses, spyware, and other network threats • Protect data on the devices • Prevent hackers from using remote systems to infiltrate enterprise networks
<p>Fiberlink Connectivity Services, a universal wireless client and an aggregated virtual network that provide Internet connectivity through 85,000 access points round the world using dial-up, broadband, Wi-Fi and other connection types.</p>	<p>These unmatched global communication services...</p> <ul style="list-style-type: none"> • Guarantee ubiquitous access to the Internet through all types of connections around the world • Allow mobile workers to connect to any available network with one or two clicks • Improve the consistency, reliability and security of the connections • Provide cost-effective and simple administration of a global connectivity infrastructure
<p>Fiberlink Professional Services, a range of customized services to help customers deploy and manage an effective mobile computing infrastructure.</p>	<p>These services provided by business and technical experts...</p> <ul style="list-style-type: none"> • Provide for smooth implementation of the MaaS360 Mobility Platform, the Fiberlink Security Services, and the Fiberlink Connectivity Services • Accelerate the adoption and usage of the security and connectivity services through training and education • Help companies optimize their mobile business initiatives

Appendix II: How one company could benefit from the MaaS360 Mobility Platform

<p>Customer Profile</p>	<p>This travel industry organization has 2,000 employees, 40% of whom use notebook PCs. The company encourages employees to work wirelessly on the company campus, while traveling and at home.</p> <p>The company processes customer transactions where personal information and credit card data is captured to secure the travel services. This makes data security an imperative to protect sensitive information, maintain compliance with mandates like PCI, and preserve the company's reputation and customer trust.</p>
<p>Regulations that impact the business</p>	<ul style="list-style-type: none"> • PCI DSS • Sarbanes-Oxley • California SB-1386
<p>Risks exacerbated by mobility</p>	<ul style="list-style-type: none"> • Data Leakage • Problems with network remote access • Difficulty updating tools such as anti-virus, firewall, and data leak prevention software
<p>Concerns about managing the mobile environment</p>	<ul style="list-style-type: none"> • Balancing the benefits of mobility while protecting customer data • Multiple tools and processes were required to manage and control notebook PCs • The timeliness and completeness of patches • Ensuring data encryption • Maintaining a continuous secure Internet connection • Cost
<p>The Solution and Results</p>	<p>The customer deployed the MaaS360 Mobility Platform to all its notebook computers. This allows the company to address the operational and control realities of mobility by:</p> <ul style="list-style-type: none"> • Delivering a unified compliance dashboard and detailed reporting capabilities used by the risk management and security teams to regularly review the organization's mobile compliance and risk postures. • Establishing an Endpoint Control architecture that facilitated the creation of potentially unique policies for each endpoint, via the Mobile NAC module. Once established and published to the endpoints, the policies enforce everything from encryption to secure connectivity, and from patch management to remediation of policy violations while off the corporate network. • Establishing controlled Internet access methodologies so as to reduce the risk of insecure communication to the Internet. • Enabling encryption by file type (e.g. Microsoft Word, Microsoft Excel, etc.) and by business application to ensure that sensitive customer data is protected and secure. • Consolidating disparate mobile operations and control functions/processes into one unified mobile management platform to seamlessly manage risk, reduce the provisioning time lag, and reduce the overall operating cost to the organization.