



Control Over Endpoints

Ensure that patches and security software on laptops and distributed PCs are always up to date. Restart applications automatically. Block non-compliant systems from accessing the corporate network.

Visibility in the "Mobile Blind Spot"

View detailed reports about hardware and software inventory, missing patches, firewalls, antivirus packages, and compliance, even when mobile devices don't connect with headquarters.

Savings, Security, Compliance

Reduce management and support costs, improve security, document compliance on endpoints.

Are You in Control?

Can you ensure that...

Patches and anti-virus signature files are always up to date on laptops and PCs?

Personal firewalls and anti-virus packages are restarted automatically if they are turned off by a virus or a user?

Mobile devices are blocked from accessing the corporate network when they are out of compliance with corporate standards?

The new security application you just rolled out has been installed successfully on every system?

You know what software applications are installed on every laptop and PC in the field, down to the release level and installation date?

You can prove to auditors which mobile systems are in compliance with corporate standards?

Conventional software and security management tools work fine inside the office, but can't provide continuous control of devices

Take Command

The MaaS360 Control Service gives you visibility into and control over laptops, distributed PCs and mobile devices. You gain the power to:

- Assess installed hardware and software
- Update patches and anti-virus signature files
- Remediate security applications
- Apply network access controls
- Report on compliance

By taking command of your mobile environment with the MaaS360 Control Service you reduce the cost of manual update processes for laptops and mobile devices, reduce calls to the help desk, keep security applications running, and streamline compliance efforts.

The MaaS360® Control Service

The MaaS360 Control Service gives you power over laptops, PCs and mobile devices in remote offices and in the field.

Subscribers to the MaaS360 Control Service can use Fiberlink's MaaS360 Management Center™ to set and distribute management and security policies, and to view a wide range of reports on installed hardware and software, missing operating system patches, endpoint security applications, and compliance with corporate standards.

A software agent is installed on devices managed by the MaaS360 Control Service. This allows the MaaS360 Control Service to continuously monitor security applications and send security and compliance information back to the MaaS360 Management Center for reporting. The agent also takes actions to bring systems back into compliance with corporate standards, actions that include updating patches and anti-virus signature files, restarting stopped applications, and restricting access to corporate networks for non-compliant systems.

The MaaS360 Control Service also includes an easy-to-use UI that lets employees see what security applications are running on their computers and what applications are causing their systems to fall out of compliance.

Because the MaaS360 Control Service is hosted by MaaS360, it:

- Requires no capital expenditure or staffing for servers.
- Scales quickly and easily
- Is available as an economical, subscription-based service.

The MaaS360 Control Service includes the same reporting capabilities as the MaaS360 Visibility Service, but in addition it provides compliance reporting and management features that further optimize cost savings, improve security, and streamline compliance efforts.



Figure 1: The MaaS360 Control Service includes a UI showing which applications are currently running

Visibility

The MaaS360 Control Service provides IT managers with visibility into mobile endpoints. They can use the MaaS360 Management Center to view detailed reports on hardware and software inventory, missing operating system patches, firewalls, anti-virus packages and other security software, and compliance with corporate standards. These include all of the reports available through the MaaS360 Visibility Service, and additional compliance reports.

INVENTORY AND PATCH STATUS REPORTS

Hardware and software inventory information can be used to troubleshoot problems, help manage software rollouts and upgrades, and save money by redeploying unused software licenses. The MaaS360 Control Service provides detailed reports on hardware (processors, memory and disk) and installed software (operating system and application versions).

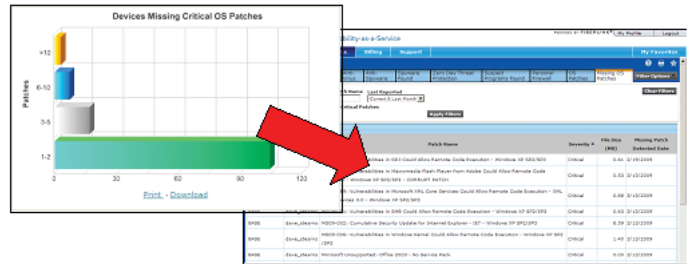


Figure 2: Reports show how many critical patches are missing across the company and on each system.

The MaaS360 Control Service provides detailed information about missing Microsoft operating system patches on laptops and PCs. Summary graphs show at a glance how many systems are missing patches, and what patches are missing from each system.

SECURITY AND COMPLIANCE REPORTS

The MaaS360 Control Service provides summary and detail reports about personal firewalls, anti-virus packages, anti-virus signature files, and compliance. For example:

- Summary graphs show which personal firewalls and anti-virus packages are installed on all laptops and PCs across the organization, and the age of anti-virus signature files.
- Detailed drill-down reports show the firewall and anti-virus software installed on each computer, by vendor, release and installation date.
- If other security applications are installed, reports show details like the hard drives that have been encrypted and how many files have been backed up to remote locations.

Compliance reports show information like what systems are out of compliance with corporate policies, what events are causing them to go out of compliance (such as security applications being disabled), and what remediation actions have been taken. Reports that demonstrate which systems are in compliance can be used to show auditors that your organization is fulfilling its requirements related to SOX, PCI DSS, HIPAA and other government regulations.

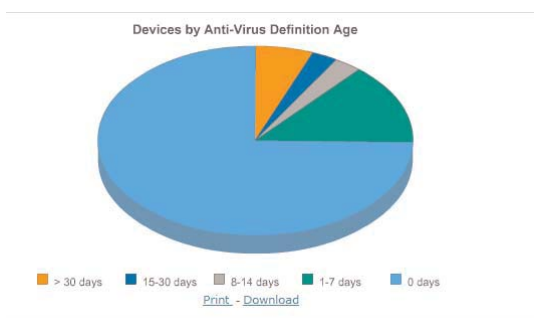


Figure 3: A view of the ages of anti-virus definition files.

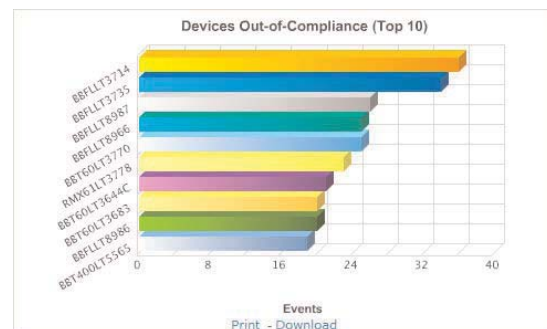


Figure 4: Report showing devices with the most out-of-compliance events.

Control

The MaaS360 Control Service goes well beyond reporting to actually manage software on laptops and distributed PCs. These control features can eliminate inefficient manual patching processes, save money by decreasing calls to the help desk, and reduce the risk of security breaches.

CENTRALIZED POLICY MANAGEMENT

IT managers can use Fiberlink's MaaS360 Management Center to set management and security policies and distribute them to mobile endpoints. For example, administrators can define what firewalls and anti-virus packages to monitor and restart if they are stopped, and what actions to take if a system goes out of compliance with corporate standards.



Figure 5: Centrally manage policies for laptops and PCs in the field

PATCH AND ANTI-VIRUS UPDATES

The MaaS360 Control Service includes patch distribution and anti-virus signature update services. These ensure that Microsoft operating system patches are always kept up to date, and that anti-virus signature files are downloaded on the schedule set by IT managers (for example, no later than every seven days).

APPLICATION MONITORING AND REMEDIATION

The MaaS360 Control Service can be set to monitor and remediate selected security applications. For example, if a virus shuts down the anti-virus package, the MaaS360 Control Service can restart it. Automatic remediation can prevent security breaches and reduce help desk calls by solving problems before the end user is even aware they have occurred.

MOBILE NAC®

Fiberlink's Mobile NAC (Network Access Control) makes corporate networks less vulnerable to viruses and hacker attacks from compromised endpoints. If a laptop or PC falls out of compliance (for example, because the firewall has stopped running, or the anti-virus signature file is out of date), the MaaS360 Control Service attempts to remediate the problem. If automatic remediation fails, then the MaaS360 Control Service can take actions like blocking the system from reaching the corporate network, or restricting access to specified systems such as a remediation server.

Out-of-Compliance Enforcement Actions

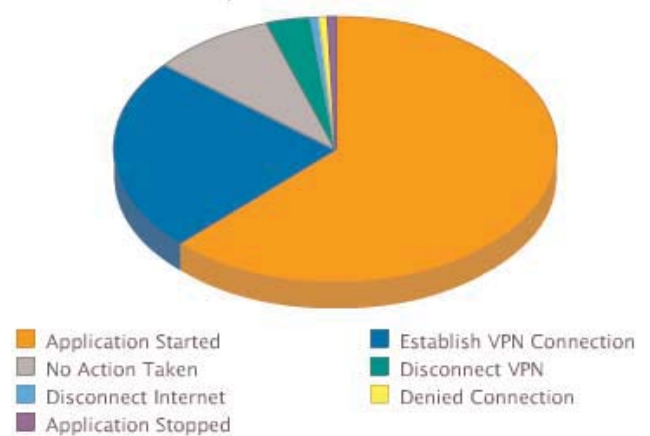


Figure 6: The MaaS360 Control Service enforces policies on mobile devices and remediates when possible.

Compatible with Other Services

Subscribers to the MaaS360 Control Service can add Fiberlink Security Services. These are an extensive menu of managed endpoint security and data protection services such as Data Encryption, Data Leak Prevention, Device (USB) Control and Backup & Recovery.

The MaaS360 Control Service can work in the same environment as Fiberlink’s MaaS360 Visibility Service and MaaS360 Mobile Service, which are summarized in the table below.

MaaS360 Service:	Visibility	Control	Mobile
Designed for:	All managed laptops and PCs	Laptops and PCs with confidential data	“Road warriors”
Includes:			
Visibility and reporting:	Inventory management reports Endpoint security reports Data protection reports	Inventory management reports Endpoint security reports Data protection reports Policy enforcement reports	Inventory management reports Endpoint security reports Data protection reports Policy enforcement reports Connectivity and connectivity cost reports
Control and management:		Centralized policy definition Application monitoring and remediation Patch distribution Anti-virus definition updates Mobile NAC	Centralized policy definition Application monitoring and remediation Patch distribution Anti-virus definition updates Mobile NAC VPN enforcement
Mobile connectivity:			Connectivity manager Intuitive connectivity interface Single password for mobile networking Virtual global network with 98,000 access points
Also Supports:			
Optional:	Visibility Service for Handhelds Any Connection Reporting Fiberlink Security Services Managed VPN services Patch distribution Anti-virus definition updates	Fiberlink Security Services Managed VPN services	Fiberlink Security Services Managed VPN services Access services

FOR MORE INFORMATION

For more information on MaaS360’s technology and services, see www.MaaS360.com or email aholmes@fiberlink.com.

Fiberlink Communications 1787 Sentry Parkway West Building 18 Suite 200 Blue Bell, PA 19422 Phone 215.664.1600 Fax 215.664.1601