



Services > Overview

MaaS360 Financial IT Reg Enforcement Service



Ensure Technical Safeguards for Regulations are Working

Monitor firewalls, anti-virus packages, data encryption solutions, VPN clients and other security applications to ensure that technical safeguards for electronic protected financial information are in place and working as expected.

Watch List for Compliance

Receive daily notification of exactly which systems are out of compliance with endpoint security policies.

Reduce the Burden of Audits

Produce reports documenting that laptops, netbooks and distributed PCs are in compliance with regulations and corporate policies.

Automate Management of Laptops and PCs

Prevent data breaches by using automated services to distribute operating system patches, update anti-virus signature files, provide network access control (NAC), and enforce the use of VPNs. Utilize data on Internet connections and VPN usage to reduce networking costs and identify unencrypted wireless connections.

Use the MaaS360® Financial IT Reg Enforcement Service to Demonstrate Compliance

Unfortunately, merely implementing security best practices is not enough. Organizations must be able to prove compliance to satisfy auditors. However, few tools exist to demonstrate that policies are being followed for laptops, distributed PCs, and other endpoints.

In this section of the white paper, we will examine how the MaaS360 Financial IT Reg Enforcement Service can help financial firms implement the technologies and best practices recommended in the FFIEC Information Security Handbook.

THE MAAS360 FINANCIAL IT REG ENFORCEMENT SERVICE

The MaaS360 Financial IT Reg Enforcement Service is a hosted service designed to help financial firms safeguard data on mobile and distributed computers, and to demonstrate that best practice security technologies are in place and working.

It collects data from laptops, netbooks and distributed PCs, and sends the data to a centralized management portal. Data collected includes: installed hardware and software, the state of endpoint and data security applications, versions and dates for patches and anti-virus signature files, and information about VPN usage and connections to the Internet.



Figure 1: MaaS360 Financial IT Reg Enforcement Service Infrastructure

Data is collected from laptops, netbooks and distributed PCs, and it is presented in the MaaS360 Platform.

Information about non-compliant endpoints is collected in a convenient “My Reg Watch List” that is updated daily. Dashboards and reports, accessed through a secure browser connection, help administrators identify vulnerabilities, troubleshoot problems, demonstrate compliance with regulations and corporate policies, identify opportunities to improve operating processes, and reduce networking costs.

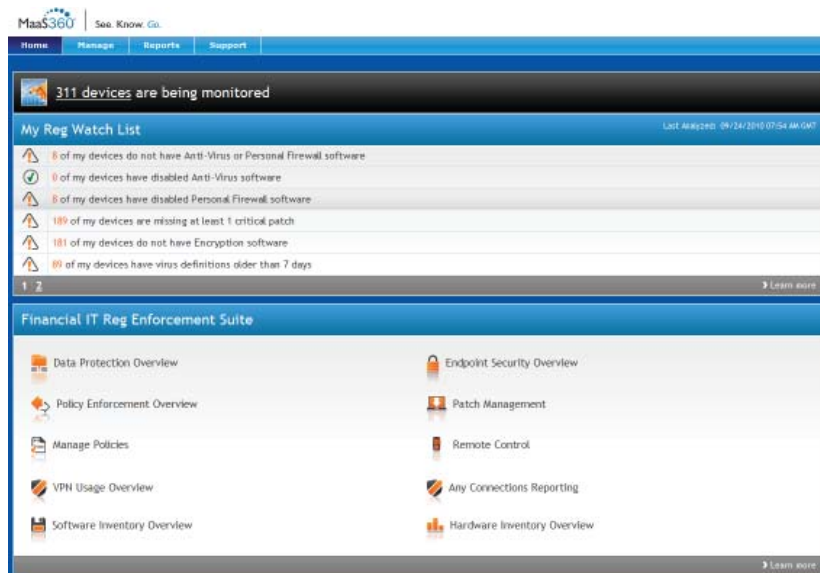


Figure 2: The MaaS360 Watch List and the Management and Reporting Modules

The MaaS360 Financial IT Reg Enforcement Service also includes management services that update and remediate selected software on distributed computers. These services reduce operations costs and improve security by ensuring that key files are up to date.

Because it is a hosted “Mobility-as-a-Service” offering, customers can start small and scale quickly, with no capital costs or new infrastructure to manage.

PATCH MANAGEMENT

The FFIEC Information Security Handbook recommends implementing comprehensive processes to update operating system patches and create an audit trail of patches applied.

The MaaS360 Financial IT Reg Enforcement Service provides detailed information about missing and applied Microsoft® operating system patches, as well as popular Windows Applications Update Reporting. Summary graphs show at a glance how many systems are missing patches. Detailed reports list what patches are missing from each system. Inventory reports show which patches are installed.

It also includes a hosted service to deploy Microsoft Windows® security patches and Windows Application Updates.

The combination of an automated patching service and detailed reports on missing patches can save a tremendous amount of time for operations managers, as well as security and compliance staff.

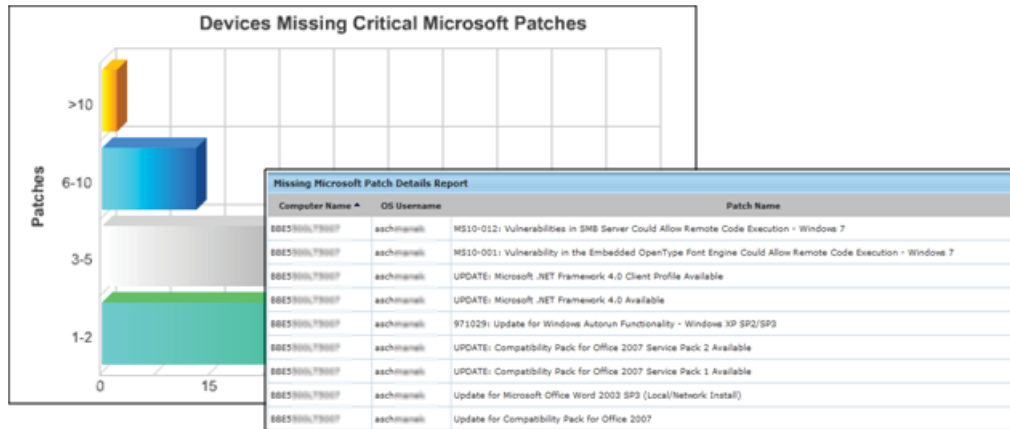


Figure 3: Patch Management
Graphs and reports show missing operating system patches in summary and in detail.

CONFIGURATION MANAGEMENT

The FFIEC authors highlight the importance of appropriately configuring remote devices, periodically auditing the configurations, and monitoring computers to identify unauthorized configurations.

The MaaS360 Financial IT Reg Enforcement Service provides complete hardware and software inventory information for endpoints. This information can be used to demonstrate that system configurations comply with corporate policies. Administrators can also use this information to troubleshoot problems, identify dangerous software, track software implementations and upgrades, and redeploy unused software licenses to save money.

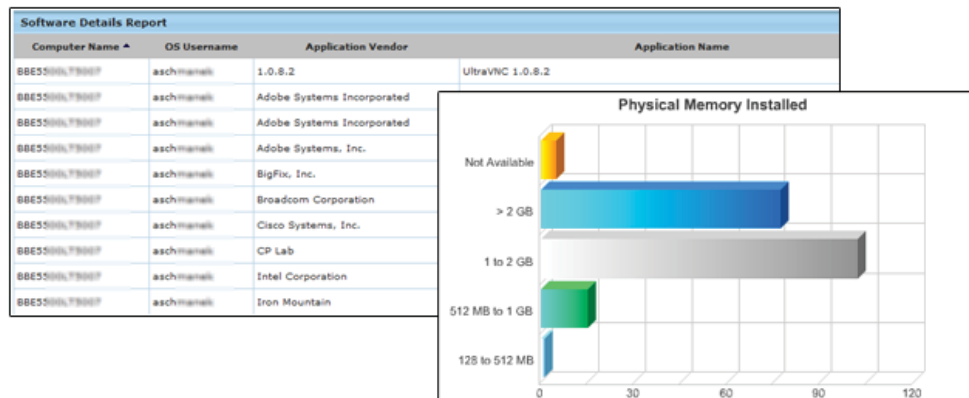



Figure 4: Configuration Management
Reports and charts show details of installed software and hardware configurations

The Service also provides detailed information on the status and health of a wide range of popular firewall and anti-malware software packages. Reports can be used to identify which systems are missing required security software, and which security applications have stopped running because of user intervention or malware attacks. They can also be used to show auditors that security applications are in fact installed and running on systems across the world.



Endpoint Security Details Report					
Computer Name	OS Username	Last Reported	Anti-Virus Detected	Personal Firewall Detected	
00E55HL78007	aschmahel	6/23/2010	Yes	Yes	
00E55HL78008	bcampbell	6/23/2010	Yes	Yes	
00E55HL78009	btan	6/23/2010	Yes	Yes	
00E55HL78010	phood	6/23/2010	No	No	
00E55HL78011	modonell	6/23/2010	Yes	Yes	
00E55HL78012	jplatt	6/23/2010	Yes	Yes	
00E55HL78013	ddiblane	6/23/2010	Yes	Yes	
00E55HL78014	jprice	6/24/2010	Yes	Yes	
00E55HL78015	fapignola	5/30/2010	Yes	Yes	
00E55HL78016	nbrant	6/23/2010	Yes	Yes	

Figure 5: Anti-Malware and Firewall Management Reports show when endpoint security applications are missing or not running.

SECURITY AGAINST MALWARE

The FFIEC Information Security Handbook notes the importance of securing remote access devices against malware, implementing strict change controls, and keeping anti-virus definitions up to date.

The MaaS360 Financial IT Reg Enforcement Service provides detailed information on the status of a wide range of popular anti-malware software packages, allowing administrators to demonstrate to auditors that these packages are installed and working. It also includes:

- Reports that show the “age” of installed anti-virus signature files on all endpoints.
- A hosted service to update anti-virus signature files.

The combination of the update service and the signature file reports helps administrators protect endpoints from malware and provides key reports to auditors.

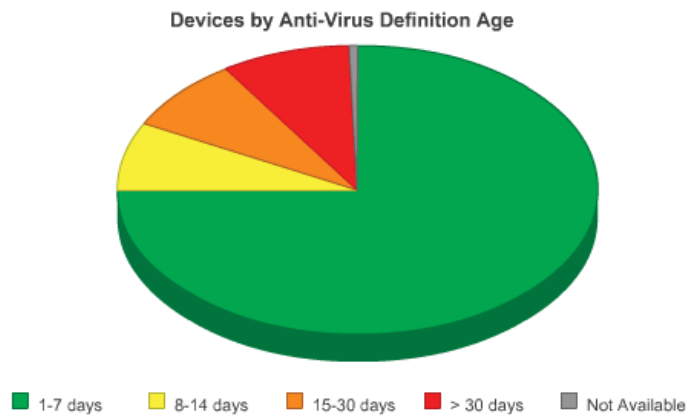


Figure 6: Anti-virus reports identify systems with out-of-date anti-virus signature files, and a hosted service can update signature files automatically.

ENCRYPTION

The FFIEC authors strongly emphasize the importance of encryption to secure data transmitted over wireless networks and data stored on distributed devices.

Disk Encryption (Data at Rest)

The MaaS360 Financial IT Reg Enforcement Service provides detailed information on the status and health of data and disk encryption applications, down to the level of showing which disks have been successfully encrypted and where encryption has failed. Similar reports are available to show the health of data leak prevention (DLP), backup and recovery, and other data protection applications on distributed endpoints.

These reports can potentially save millions of dollars by allowing organizations to demonstrate that lost and stolen devices were encrypted at the time of loss, and so come under the "safe harbor" clause in California SB 1386 and similar data breach laws.

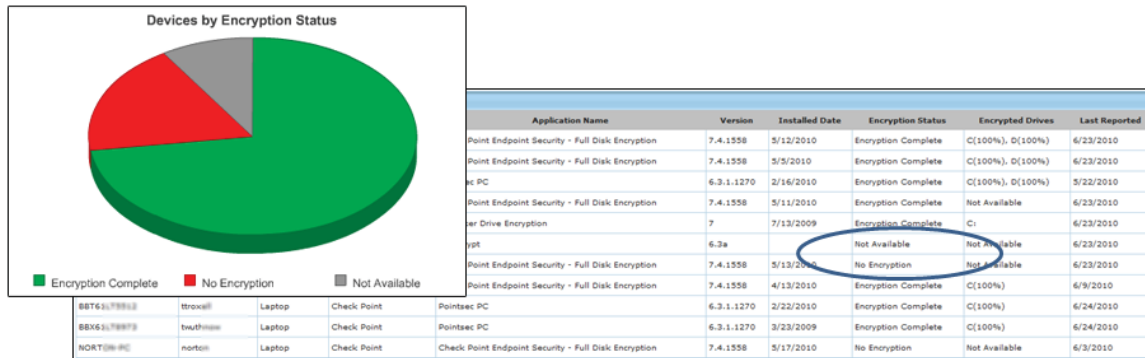


Figure 7: Data at Rest Management

Graphs and reports provide information on data protection applications, down to the level of which disks are encrypted.

Monitoring Wireless Connections (Data in Motion)

Reports show open and wireless connections. Administrators can use this information to identify employees making unencrypted connections, in order to educate the employees, or to enforce the use of VPNs by technical means.

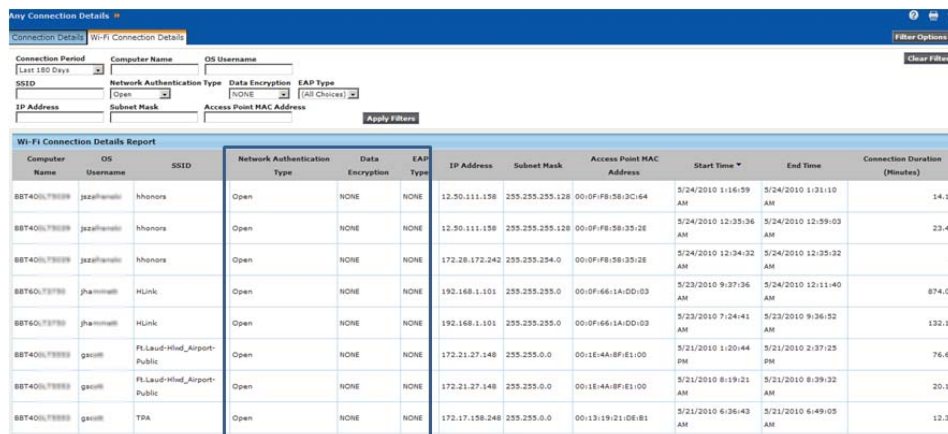


Figure 8: Managing Data in Motion
Reports identify employees making unencrypted Wi-Fi connections.

Recap and Business Impact

The regulatory environment for financial firms exhibits a clear trend toward increasing concern about sensitive data stored on distributed endpoints and transmitted over wireless networks. Financial firms are challenged with the following:

- To implement security measures for mobile systems, both those explicitly required by regulations and those indicated by general guidelines such as “protecting against foreseeable risks.”
- To demonstrate that security software is, in fact, installed and working properly on mobile and remote devices.

To address the first challenge, we suggest that the FFIEC Information Security Handbook is an important reference document, because it provides detailed, concrete, and well-considered guidance for financial companies.

To address the second challenge, we suggest that there is no better solution than the MaaS360 Financial IT Reg Enforcement Service.

It helps financial firms:

- Deploy, monitor, and manage required security applications such as data encryption, firewalls, and anti-virus packages.
- Implement additional “best practices” recommended by the FFIEC, and other authorities like the FSA in the United Kingdom, including patch management, configuration management, logging and monitoring, and network access controls.
- Dramatically reduce the cost of preparing for audits.
- Simplify IT management processes and reduce the cost of PC and mobile operations.

By using the FFIEC Information Security Handbook for guidance, and the MaaS360 Financial IT Reg Enforcement Service as a tool, financial institutions can:

- Reduce the number of security breaches.
- Avoid regulatory fines and customer notification costs.
- Avoid damage to reputation and revenue.
- Reduce the cost of complying with audits.
- Improve IT operations processes.
- Reduce networking and help desk costs.

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