

Guardian Managed Patching vs. SCCM

You need to patch everything.
Guardian Managed Patching can help.

NOT JUST WINDOWS

Let's face it: although you may use Microsoft® Manager (SCCM) for managing your physical and virtual workstations, when it comes to patch management and distribution of non-Microsoft updates, things can get complicated.

Yes, you need to use Windows® Server Update Services (WSUS) for patching, and System Center Updates Publisher (SCUP) to import third-party software catalogs. And you only get a bare minimum of pre-built and tested third-party software packages for deployment with SCCM.

And then you have to hope that the target device is not on the road where it isn't connected via VPN.

There are more management systems to handle, more manual effort, and certainly a huge toll on administrative and troubleshooting time.

Guardian Managed Patching provides you with a managed service to keep your devices protected with the latest patches for both Microsoft® and third-party applications. With Fortress Managed Patching, you'll save a ton of time by letting us manage and deploy patches for your environment.

Here are the top 15 reasons why you need to have Fortress patch management standing watch over your environment.

	MICROSOFT® SCCM	GUARDIAN PATCHING
Patching Microsoft	Yes	Yes (no WSUS needed)
Patching Non-Microsoft 3rd Party Software	Limited By using Microsoft SCUP	Yes - Refer to Supported App List in Fortress Product Info
Visibility into Application Inventory	Yes – For System Center Essentials (SCE) environments which uses WSUS natively. Enable the use of the WSUS/ WUAgent. The Extended Inventory collection tool, includes software and hardware inventory	Yes – Microsoft & other 3rd party applications, hardware inventory, disk space & other metrics
On-Demand Patching	No	Yes
Reporting Visibility into Patched & Unpatched Systems & Software	Requires some knowledge of SQL programming as well as administration of SQL Server Reporting Services (SSRS)	Yes – Granular Visibility
Filtered Views	No	Yes
Scheduled Approvals	No	Yes
Notification of Failed Updates	No	Yes – Provides alerting via the portal as to when and why the update failed
Patch Scheduling	Yes	Yes – Push patches at discrete times to accommodate different time zones and network impacts of patching large numbers of endpoints
Deliver Patches across Internet	No	Yes
Third-party Pre-built & Tested Packages	Limited – Only for cataloged patches	Yes – For many common applications
1-click Patch Removal	No	Yes
Client Health Diagnosis & Remediation	Yes – Client Health Data	Yes – Repair WMI, WUAgent, and Fortress Agent Status Reporting
Hardware, Software, and Engineering Costs	Yes	Included with Service
Forced Reboot with User Postponement	No	Yes