

Bitdefender GravityZone Patch Management

Patch Operating System and Applications

Unpatched systems leave organizations susceptible to malware incidents, outbreaks, and data breaches. GravityZone Patch Management module enables organizations to keep OS and Applications up to date across the entire Windows install base - workstations, physical servers and virtual servers.

Flexible and Simplified Patch Management Workflows

GravityZone Patch Management module supports both automatic and manual patching. It gives organization greater flexibility and efficiency for patch management, with the ability to create a patch inventory, schedule patch scanning, limit automatic patching to admin-preferred applications, vary scheduling for security and non-security patches and postpone reboots for patching requiring a restart.

Reduce risks against advanced attacks and achieve compliance

In the current cybersecurity landscape, patching OS and Applications has become a high priority for the IT team for both security and compliance. GravityZone Patch Management allows verification of patching enterprise-wide to comply with policies and regulations.

The screenshot displays the Bitdefender GravityZone Patch Management interface. On the left is a sidebar menu with categories like Dashboard, Network, Patch Inventory, Application Inventory, Packages, Tools, Alerts, Reports, Quarantine, Accounts, User Activity, Configuration, Updates, and Users. The main area shows a table titled 'Patch inventory in database' with columns for Patch Name, ESM, Patch security, Category, Bulletin ID, Installed / Pending %, Missing / Installation F..., and Affected Products. The table lists various patches such as '751594.exe', 'KB2915411', 'KB2915412', etc., with their respective security levels and affected products.

Patch Name	ESM	Patch security	Category	Bulletin ID	Installed / Pending %	Missing / Installation F...	Affected Products
751594.exe	N/A	None	Non-Security	751594	0 EP / 0 EP	0 EP / 0 EP	0 Products
KB2915411	N/A	Critical	Non-Security	KB2915411	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915412	N/A	Critical	Non-Security	KB2915412	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915413	N/A	Critical	Non-Security	KB2915413	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915414	N/A	Critical	Non-Security	KB2915414	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915415	N/A	Critical	Non-Security	KB2915415	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915416	N/A	Critical	Non-Security	KB2915416	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915417	N/A	Critical	Non-Security	KB2915417	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915418	N/A	Critical	Non-Security	KB2915418	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915419	N/A	Critical	Non-Security	KB2915419	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915420	N/A	Critical	Non-Security	KB2915420	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915421	N/A	Critical	Non-Security	KB2915421	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915422	N/A	Critical	Non-Security	KB2915422	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915423	N/A	Critical	Non-Security	KB2915423	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915424	N/A	Critical	Non-Security	KB2915424	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915425	N/A	Critical	Non-Security	KB2915425	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915426	N/A	Critical	Non-Security	KB2915426	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915427	N/A	Critical	Non-Security	KB2915427	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915428	N/A	Critical	Non-Security	KB2915428	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915429	N/A	Critical	Non-Security	KB2915429	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915430	N/A	Critical	Non-Security	KB2915430	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915431	N/A	Critical	Non-Security	KB2915431	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915432	N/A	Critical	Non-Security	KB2915432	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915433	N/A	Critical	Non-Security	KB2915433	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915434	N/A	Critical	Non-Security	KB2915434	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915435	N/A	Critical	Non-Security	KB2915435	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915436	N/A	Critical	Non-Security	KB2915436	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915437	N/A	Critical	Non-Security	KB2915437	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915438	N/A	Critical	Non-Security	KB2915438	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915439	N/A	Critical	Non-Security	KB2915439	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915440	N/A	Critical	Non-Security	KB2915440	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915441	N/A	Critical	Non-Security	KB2915441	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915442	N/A	Critical	Non-Security	KB2915442	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915443	N/A	Critical	Non-Security	KB2915443	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915444	N/A	Critical	Non-Security	KB2915444	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915445	N/A	Critical	Non-Security	KB2915445	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915446	N/A	Critical	Non-Security	KB2915446	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915447	N/A	Critical	Non-Security	KB2915447	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915448	N/A	Critical	Non-Security	KB2915448	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915449	N/A	Critical	Non-Security	KB2915449	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915450	N/A	Critical	Non-Security	KB2915450	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915451	N/A	Critical	Non-Security	KB2915451	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915452	N/A	Critical	Non-Security	KB2915452	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915453	N/A	Critical	Non-Security	KB2915453	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915454	N/A	Critical	Non-Security	KB2915454	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915455	N/A	Critical	Non-Security	KB2915455	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915456	N/A	Critical	Non-Security	KB2915456	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915457	N/A	Critical	Non-Security	KB2915457	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915458	N/A	Critical	Non-Security	KB2915458	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915459	N/A	Critical	Non-Security	KB2915459	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915460	N/A	Critical	Non-Security	KB2915460	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915461	N/A	Critical	Non-Security	KB2915461	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915462	N/A	Critical	Non-Security	KB2915462	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915463	N/A	Critical	Non-Security	KB2915463	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915464	N/A	Critical	Non-Security	KB2915464	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915465	N/A	Critical	Non-Security	KB2915465	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915466	N/A	Critical	Non-Security	KB2915466	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915467	N/A	Critical	Non-Security	KB2915467	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915468	N/A	Critical	Non-Security	KB2915468	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915469	N/A	Critical	Non-Security	KB2915469	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915470	N/A	Critical	Non-Security	KB2915470	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915471	N/A	Critical	Non-Security	KB2915471	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915472	N/A	Critical	Non-Security	KB2915472	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915473	N/A	Critical	Non-Security	KB2915473	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915474	N/A	Critical	Non-Security	KB2915474	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915475	N/A	Critical	Non-Security	KB2915475	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915476	N/A	Critical	Non-Security	KB2915476	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915477	N/A	Critical	Non-Security	KB2915477	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915478	N/A	Critical	Non-Security	KB2915478	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915479	N/A	Critical	Non-Security	KB2915479	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915480	N/A	Critical	Non-Security	KB2915480	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915481	N/A	Critical	Non-Security	KB2915481	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915482	N/A	Critical	Non-Security	KB2915482	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915483	N/A	Critical	Non-Security	KB2915483	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915484	N/A	Critical	Non-Security	KB2915484	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915485	N/A	Critical	Non-Security	KB2915485	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915486	N/A	Critical	Non-Security	KB2915486	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915487	N/A	Critical	Non-Security	KB2915487	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915488	N/A	Critical	Non-Security	KB2915488	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915489	N/A	Critical	Non-Security	KB2915489	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915490	N/A	Critical	Non-Security	KB2915490	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915491	N/A	Critical	Non-Security	KB2915491	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915492	N/A	Critical	Non-Security	KB2915492	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915493	N/A	Critical	Non-Security	KB2915493	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915494	N/A	Critical	Non-Security	KB2915494	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915495	N/A	Critical	Non-Security	KB2915495	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915496	N/A	Critical	Non-Security	KB2915496	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915497	N/A	Critical	Non-Security	KB2915497	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915498	N/A	Critical	Non-Security	KB2915498	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915499	N/A	Critical	Non-Security	KB2915499	0 EP / 0 EP	0 EP / 0 EP	1 Products
KB2915500	N/A	Critical	Non-Security	KB2915500	0 EP / 0 EP	0 EP / 0 EP	1 Products

Bridging the Great Divide Between IT Security and IT Operations

GravityZone is now a single unified Endpoint Security platform, not only for protecting your endpoints from advanced attacks but also for incident response and patch management. Integration, simplicity, and ease of management will enable IT security and operational personnel to focus and work more efficiently.

Patch Management available as add-on for customers

Patch Management module can be added on top of existing Bitdefender GravityZone Endpoint Security products. The new module is managed from the same GravityZone console that customers use today.

Key features

- Patching for OS and the largest collection of software applications
- Automatic and manual patching
- Detailed information centering patches - CVE, Bulletin ID, Patch Severity, Patch Category
- Ability to set different schedules for security and non-security patches
- Quick deployment of missing patches
- The ability to distribute patches from the relay, reducing network traffic
- Patch specific reports that help companies demonstrate compliance
- Automatically notify IT administrator when security/non-security patches are missing

Bitdefender GravityZone Patch Management Requirements

The Patch Management Module is available for both GravityZone cloud and on-premises deployments.

Patch Management module is compatible with all Microsoft Windows Desktop and Server operating systems supported by the endpoint protection products, starting with Windows 7 and Windows Server 2008 R2. Please check system requirements for endpoint security products.



Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at <http://www.bitdefender.com>.

All Rights Reserved. © 2018 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners.
FOR MORE INFORMATION VISIT: bitdefender.com/business

