avast business
powered by AVG and Avast

Patch Management in CloudCare

Identify critical vulnerabilities and quickly deploy updates to all endpoints

Patch management plays a critical role in endpoint security, but many businesses are reluctant to patch because there are too many patches, patching often interrupts operations, and they can cause problems with other systems. Avast Business Patch Management takes the guesswork out of patching by identifying critical vulnerabilities and making it easy to deploy patches across all endpoints from one central dashboard.

Stay ahead of vulnerabilities
Keep Windows operating systems and thousands of other third-party applications up to date automatically to prevent possible security gaps.

Ensure compliance
Identify and patch outdated or failed-to-install software to ensure company and regulatory compliance, and prevent security breaches.

Centralize management
Stay in complete control of patches with centralized management that allows you to scan all devices, set schedules, and approve everything from a single page.

DATA SHEET

Features

Automatic patch scans
Automatically run a patch scan daily, weekly, or monthly for all devices in a customer policy, including workstations, and physical and virtual servers.

Centralized patch results
Manage all software patches, view statuses of installed, missing, or failed patches across all devices by customer.

Approve patches
Save time by automatically approving patches by vendor, application, or severity or manually approving patches.

Flexible deployment options
Easily schedule and deploy patches based on approval rules and view ignored patches via the customer policy.

Patches by device
Manually patch individual devices and get a full list of missing patches, so you can run a deep analysis of all existing vulnerabilities on that device.

Roll back patches
Simply uninstall conflicting or unstable patches without any manual intervention all from one platform.

Ignore patches
Ignore individual patches for select devices based on customer policies, so you can test patches prior to deploying them and remediate any issues.

Master policy
Create master policies and apply them across all of your existing customers with just one click.

Clear cache
Save space by setting a timeframe when patches should be deleted once they have been installed on endpoint devices.

System Requirements

Windows 7 (Service Pack 1), Windows 8, Windows 8.1, Windows 10 – Windows 10 Pro, Windows 10 Education, and Windows 10 Enterprise.

Servers

Windows Server 2019 (64-bit version)

Windows Server 2016 (64-bit version)

Windows Server 2012 (64-bit version)

Windows Server 2008 R2 (64-bit version with the latest Service Pack, excl. Server Core Edition)

Microsoft Exchange Server 2016 (64-bit version)

Microsoft Exchange Server 2013 (64-bit version)

Microsoft Exchange Server 2010 Service Pack 2 (64-bit version)

Hardware

Intel Pentium 4 / AMD Athlon 64 CPU supporting SSE2 instructions, 256 MB+ RAM and 2 GB of hard disk space.

Patch is only available for Windows

Complete layered security in one easy-to-use, cloud-based platform

Deploy Patch Management from CloudCare along with our award-winning Avast Business Antivirus and other security services, including Secure Internet Gateway, Email Security, Backup and Recovery, and more for powerful protection. Easily manage and monitor your endpoint and network security from a single cloud-based security platform for seamless protection across all devices.

About Avast Business

Avast Business provides advanced, integrated endpoint and network security solutions for businesses and IT service providers. The result is superior protection that businesses can count on. For more information about our managed security services and cybersecurity solutions, visit **www.avast.com/business**.