

Patch Management

Identifizieren kritischer Schwachstellen und schnelle Bereitstellung von Updates auf allen Endgeräten

Das Patch Management spielt eine entscheidende Rolle bei der Endgerätesicherheit, doch viele Unternehmen sind zögerlich mit Patches, weil zu viele davon verfügbar sind, die Bereitstellung oft den Betrieb unterbricht und sie Probleme mit anderen Systemen verursachen können. Avast Business Patch Management bereitet dem Ratespiel beim Patching ein Ende, indem es Schwachstellen aufdeckt, die sich durch die Patch-Bereitstellung über ein zentrales Dashboard ohne großen Aufwand beseitigen lassen

Sicherheitslücken immer einen Schritt voraus bleiben

Halten Sie Windows-Betriebssysteme und Tausende von Drittanbieter-Software automatisch auf dem neuesten Stand, um mögliche Sicherheitslücken zu vermeiden.

Compliance sicherstellen

Identifizieren und patchen Sie veraltete Software oder Software mit Installationsproblemen, um Compliance mit firmeninternen und gesetzlichen Vorschriften zu gewährleisten um so Sicherheitsverstößen vorzubeugen.

Zentrale Verwaltung

Die zentrale Verwaltung ermöglicht die Steuerung von Patches und das Scannen aller Geräte, Einrichten von Zeitplänen und Abrufen von Berichten – alles über eine Konsole.



1. Geräte scannen



2. Patches bereitstellen



3. Status überprüfen

Funktionen

Flexible Bereitstellungspläne

Genehmigte Patches können für einen gewünschten Zeitpunkt geplant und bereitgestellt werden oder das Patchen kann manuell für Gruppen oder einzelne Geräte erfolgen.

Intuitives Dashboard

Sie können alle Software-Patches verwalten und erhalten für alle verwalteten Geräte eine grafische Übersicht über alle installierten, fehlenden Patches bzw. fehlgeschlagenen Patches.

Konfigurierbare Patches

Wählen Sie Softwareanbieter, Produkte und den Schweregrad der Patches für den Scan und die Installation aus. Erstellen Sie mühelos Ausnahmen für Anwendungen.

Master-Agent-Funktionen

Laden Sie alle fehlenden Patches auf einen Master-Agent herunter, der sie nahtlos auf alle verwalteten Geräte im Netzwerk verteilt.

Patch-Scan-Ergebnisse

Zeigen Sie detaillierte Ergebnisse von der Verwaltungsplattform an, einschließlich Informationen zu fehlenden Patches, die jeweiligen Schweregrade, Knowledge Base-Links, Veröffentlichungsdaten, Beschreibungen und mehr.

Erweiterte Berichtsfunktionen

Ermitteln Sie einfach und schnell den Zustand und die Sicherheit von Gerätesoftware mit einer Vielzahl leicht konfigurierbarer Berichte.

Automatische Scans

Planen Sie die automatische Ausführung von Patch-Scans alle 24 Stunden und die automatische Bereitstellung von Patches an jedem gewünschten Tag. Diese Standardeinstellungen lassen sich beliebig anpassen.

Tausende Patches

Stellen Sie für umfassenden Schutz Patches für Windows-Betriebssysteme und Tausende weitere Softwareanwendungen von Dritten bereit.

Umfassender Endgeräteschutz über eine benutzerfreundliche, Cloud-basierte Konsole

Durch gemeinsame Bereitstellung der preisgekrönten Produkte Avast Business Antivirus und Patch Management über die Management Console lässt sich die gesamte Endgerätesicherheit nahtlos über eine einzige Plattform verwalten.

Informationen zu Avast Business

Avast Business bietet integrierte, unternehmensweite Endgeräte – und Netzwerk-Sicherheitslösungen für KMU und IT-Dienstleister. Das Sicherheitsportfolio von Avast Business stützt sich auf das größte und umfassendste Netzwerk zur Bedrohungserkennung. Dadurch werden Schutz, Verwaltung und Überwachung komplexer IT-Umgebungen einfach und erschwinglich. Das Resultat ist überlegener Schutz, auf den sich Unternehmen verlassen können.

Weitere Informationen zu verwalteten Sicherheitsdiensten und Cybersicherheit-Lösungen finden Sie auf www.avast.com/business.

Systemvoraussetzungen

Verwaltungskonsole

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

Server

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 mit aktuellem Service Pack außer 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- bzw. AMD Athlon 64 – Prozessor mit Unterstützung von SSE2-Anweisungen, 256 MB RAM und 2 GB Festplattenspeicher.

Patch ist nur für Windows verfügbar