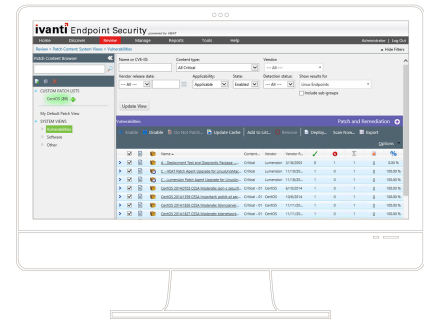


# Schützen Sie Ihre heterogenen Umgebungen

**Sie benötigen eine Patchmanagement-Software, die den heutigen Umgebungen mit gemischten Betriebssystemen gewachsen ist. Das Patching kann heute nicht mehr bei Windows aufhören, sondern muss darüber hinausgehen. Geschieht dies in effizienter Weise mit einer zentralen Konsole und einem automatisierten Tool, sparen Sie nicht nur IT-Zeit, sondern reduzieren auch die Zahl menschlicher Fehler. Zudem verbessern Sie Ihren Schutz.**



## Patching – die Grundlage einer effektiven Sicherheitsaufstellung

Die Zahl der Cyberangriffe nimmt zu. Unternehmen wehren sich, indem sie Programme ins Leben rufen, um Ihre Sicherheitsaufstellung zu verstärken. Der erste Schritt zum Aufbau einer effektiven, mehrschichtigen Sicherheitsstrategie besteht zweifellos im Patching. Doch das Patching stellt immer noch ein Problem dar. Bedrohungsakteure nutzen weiterhin Anfälligkeiten aus, die durch Patching vermeidbar wären.

Patching kann strapaziös sein, wenn das IT-Team durch manuelle, zeitraubende Tools behindert wird, die Zeit beanspruchen, die das Team sonst zur Unterstützung geschäftlicher Ziele einsetzen könnte. Gleichzeitig vergrößert sich dadurch die Fehlerwahrscheinlichkeit. All dies ist umso wahrscheinlicher, wenn mehrere Tools zum Patchen der heterogenen Umgebungen zum Einsatz kommen.

Ivanti® Patch for Linux, UNIX, Mac mit Technologie von Heat erkennt in kürzester Zeit Anfälligkeiten in den Umgebungen von heute, von der Workstation bis hin zum Rechenzentrum. Die Lösung stellt fachkundig vorab getestete Patches automatisch bereit und hilft Unternehmen, das Patching mit größerer Wirksamkeit und Effizienz vorzunehmen.

## Patchen Sie mit Agent – mehr als nur Ihre Windows-Betriebssysteme

Schützen Sie Tausende von Systemen mit einem einzigen Tool, das Patching-Unterstützung für Linux, UNIX, Mac und Drittanbieteranwendungen von Hunderten von Herstellern bietet. Diese eine Konsole mit integrierter Automatisierung reduziert die Fehlerwahrscheinlichkeit und vereinfacht gleichzeitig die Art und Weise, in der Sie Ihre gemischte Umgebung patchen.

## Automatisieren Sie die Bewertung von Anfälligkeiten und das Patchmanagement

Patching ist kein Ereignis, sondern eine Reise. Dank intelligenter, bedarfsgesteuerter Planung bringt Ivanti Patch for Linux, UNIX, Mac Klarheit über die Anfälligkeiten in Ihrer Umgebung. Neue Patchinformationen werden konsistent aktualisiert und zur Bewertung und bei Bedarf auch zur automatischen Reparatur von Anfälligkeiten auf Systemen eingesetzt. Bereitstellungsaufgaben können verwaltet und kontrolliert werden, damit sichergestellt ist, dass die Reparaturen bzw. Korrekturen ohne Störung für Ihre Benutzer und Ihre kritische Infrastruktur durchgeführt werden. In Verbindung mit der Compliance-Berichterstattung gibt dies Ihrem Unternehmen ein klares Bild der Risiken, mit denen es konfrontiert ist.

## Helfen Sie, die Compliance sicherzustellen

Sehen, bewerten und schützen Sie Ihre Workstations und Server, um Sicherheitsstandards wie PCI und HIPAA/HITECH zu erfüllen. Sparen Sie Zeit und Ressourcen, indem Sie Ihre Compliance sicherstellen und Non-Compliance-Strafen vermeiden.

## Stellen Sie die Produktivität der Benutzer sicher

Patching muss die Benutzerproduktivität nicht behindern. Wenn Sie die Bereitstellung von Patches zur richtigen Zeit und unter den richtigen Bedingungen planen, kann sich Ihr Unternehmen weiterentwickeln, ohne dass dadurch die Sicherheit beeinträchtigt wird.

## Schließen Sie die Lücke zwischen Sicherheit und IT-Betrieb

Ivanti Patch for Linux, UNIX, Mac ist in Security Information and Event Management (SIEM)-Systeme integrierbar und sorgt so bei Ihren Sicherheitsteams für Transparenz.

Diese Integration hilft Ihnen ferner, die Kluft zwischen Sicherheit, IT und DevOps zu überbrücken. So können beispielsweise Anfälligkeits- und Patch-Feeds Ihre Risikomanagement- und Risikoregistrierungssysteme auf dem Laufenden halten, damit eine ständige Auswertung von Anfälligkeiten erfolgt.

Ist DevOps mit leistungsstarken Patchmanagement-Lösungen ausgestattet, führt dies zu flexibleren, langlebigeren und konsistenteren Infrastrukturen und Systemen.

- Technik- und Qualitätssicherungsteams können ein konsistentes Patching und einheitliche Drittanbieterbibliotheken in ihren Umgebungen sicherstellen, wodurch sich die Stabilität ihrer Bereitstellungen vergrößert.
- DevOps-Teams können die Bereitstellung von Patches und von Drittanbieterbibliotheken automatisieren, um ein einheitliches Installationserlebnis sicherzustellen und menschliche Fehler bei Bereitstellungen auszuschließen.
- Jeder profitiert vom integrierten Reporting, mit aufbereiteten Informationen, die den aktuellen Status und Konfigurationsabweichungen vom vorgegebenen Patching-Level zusammenfassen.

## Hauptmerkmale

- Zentrale, webgestützte Konsole mit integrierten Berichts- und Alarmfunktionen
- Zentralisierte Patchbereitstellung
- Richtlinienbasierte Konfiguration, Bewertung und Bereitstellung von Patching
- Maßgeschneidertes Echtzeit-Reporting
- Umfassender Patchkatalog



[www.ivanti.de](http://www.ivanti.de)



+49 (0)69 941 757-0



[contact@ivanti.de](mailto:contact@ivanti.de)