Mehr Sicherheit, bessere Compliance

Weniger Risiken durch eine robuste Linux-Plattform, die auf Open Source basiert

Red Hat

Inhaltsverzeichnis

Linux – die Basis für die Zukunft

Linux® ist eines der am weitesten verbreiteten Betriebssysteme der Welt. Es kommt in zahlreichen Branchen und mit vielen Erfolg versprechenden Technologien zum Einsatz.[1] Es wird für hochverfügbare, zuverlässige und betriebswichtige Workloads in Rechenzentren und Cloud Computing-Umgebungen verwendet und unterstützt zahlreiche Use Cases, Zielsysteme und Geräte. Alle wichtigen Public Cloud Provider bieten in ihren Märkten mehrere Linux-Distributionen an.

Allerdings können die Linux-Distribution und die Managementtools, für die Sie sich entscheiden, einen großen Einfluss auf die Effizienz, Sicherheit und Interoperabilität Ihrer IT-Umgebung haben. In diesem E-Book erhalten Sie wichtige Informationen und Tipps zu Sicherheit und Compliance in Linux-Umgebungen.

Sicherheit und Compliance sind der Kern Ihrer IT

IT-Sicherheit und Compliance sind ein aktuelles Thema in jedem Unternehmen. 33 % der CEOs betrachten Cyberattacken als größte Bedrohung für den wirtschaftlichen Erfolg Ihres Unternehmens.[2] Und Sicherheitslücken können sich als kostspielig erweisen. Eine Datenpanne kostet durchschnittlich 3,86 Millionen USD.[3]

Die Branchen- und Verwaltungsvorschriften ändern sich ständig. Stets auf dem aktuellen Stand zu sein, ist nicht einfach. Bei mangelnder Compliance steigen die Kosten einer Datenpanne im Schnitt um 6 %.[3]

Bekannte Herausforderungen in Sachen Sicherheit und Compliance

Mehrere Faktoren machen Sicherheitslücken und Compliance-Management schwierig.

Auswirkungen ineffizienter Sicherheitsmaßnahmen

Bei der Reduzierung von Risiken und den Auswirkungen von Datenpannen kommt es auf Geschwindigkeit an.

3,86 Mio. USD
durchschnittliche Kosten von Datenpannen im Jahr 2020[3]

280 Tage
durchschnittlicher Zeitraum zur Erkennung und Eindämmung einer Datenpanne im Jahr 2020[3]

1,12 Mio. USD
Kosteneinsparungen, wenn die Erkennung und Eindämmung einer Datenpanne in maximal 200 Tagen erfolgt[3]

Sich verändernde Sicherheits- und Compliance-Landschaften

Sicherheitsbedrohungen und Compliance-Änderungen entwickeln sich schnell und erfordern eine unmittelbare Reaktion auf neue Bedrohungen und sich ändernde Vorschriften.

Verteilte Hybrid Cloud- und Multi-Cloud-Umgebungen

Geografisch und logisch verteilte Umgebungen können Ihr IT-System unübersichtlich machen.

Große und komplexe Umgebungen

Große Infrastrukturen verfügen oft über zahlreiche Sicherheits- und Compliance-Tools, die das Risikomanagement erschweren.

Wenig Personal und Möglichkeiten zur Remote-Arbeit

Den meisten Unternehmen fehlen die Mitarbeiter, die sich um das Management manueller Sicherheits- und Compliance-Aufgaben kümmern.

1 *The Linux Foundation.* **Linux ist das erfolgreichste Open Source-Projekt aller Zeiten**, *vom 24. September 2020.*

2 *PWC.* **23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty**, *2020.*

3 *IBM Security.* **Bericht „Kosten einer Datenschutzverletzung“**, *2020.*

Einführung eines effektiven Konzepts für Sicherheit und Compliance

Das Risiko-Management von Sicherheit und Compliance erfordert die Überwachung und Analyse von Systemen, um sicherzustellen, dass Sicherheitsrichtlinien und gesetzliche Vorgaben eingehalten werden. Bei einem idealen Konzept für Sicherheits- und Compliance-Management werden konsistente, wiederholbare Prozesse für die gesamte Umgebung entwickelt:

Analyse
Identifizieren Sie Systeme, die nicht konform sind oder Sicherheitslücken aufweisen. Sie können den aktuellen Sicherheitsstatus Ihrer Umgebung von der Infrastruktur bis zum Workload im Handumdrehen ermitteln. Finden Sie heraus, welche der zahlreichen Sicherheitsvorgaben tatsächlich für Ihre Systeme und Ihre Umgebung angewendet werden sollten.

Priorisierung
Planen Sie Korrekturmaßnahmen nach Aufwand, Auswirkungen und Schweregrad des Problems. Ermitteln Sie anhand von Techniken zum Risikomanagement das konkrete Geschäftsrisiko eines jeden Problems und planen Sie entsprechende Maßnahmen zu dessen Behebung. Ein Risiko beinhaltet die Wahrscheinlichkeit, dass ein Problem zu einer Datenpanne führt, die potenzielle Schwere einer Panne und die Folgen der Fehlerbehebung. Es ist unter Umständen gar nicht sinnvoll, ein bestimmtes Problem in Entwicklungs- und Testsystemen zu beheben. Es ist allerdings möglich, dass dasselbe Problem für Produktionssysteme von großer Bedeutung ist.

Behebung
Patchen Sie alle Systeme, die Maßnahmen erfordern, schnell und auf einfache Weise, und konfigurieren Sie sie neu. Automatisieren Sie Konfigurations- und Patching-Prozesse, um die Behebung zu beschleunigen, systemübergreifende Konsistenz sicherzustellen und um das Risiko menschlicher Fehler zu reduzieren. Durch den effektiven Einsatz automatisierter Tools erreichen Sie einen Zustand, in dem Sie Probleme schnell beheben und die Sicherheit Ihrer Umgebung und Ihres Unternehmens verbessern können.

Berichte
Für optimales Auditing prüfen Sie, ob Änderungen vorgenommen wurden, und automatisieren die Berichte zur Fehlerbehebung. Eine effiziente Berichterstellung hilft Ihnen dabei, die jeweils passenden Informationen an Geschäftsleitung, Betriebsprüfer und technische Teams weiterzugeben, damit sich diese einen Eindruck von den aktuellen Sicherheitsrisiken machen können.

Dieses Konzept bereitet Ihr Unternehmen gleichzeitig auf moderne und schnelle Entwicklungs- und Managementtechniken wie **DevSecOps** vor. 38 % der Unternehmen betrachten die Analyse von Sicherheitslücken sogar als das entscheidende Sicherheitselement ihres DevOps-Workflows.[4]

In den folgenden Abschnitten werden wichtige Aspekte und Maßnahmen für ein effektives Management Ihrer Sicherheits- und Compliance-Risiken behandelt.

4 451 Research, Teil von S&P Global Market Intelligence – Voice of the Enterprise, DevOps H2 2019.

Identifizierung von Sicherheitslücken und ihre Behebung in Linux-Umgebungen

Die Erkennung von Sicherheitslücken und ihre Behebung sind Bestandteile der Infrastrukturanalyse. Dabei werden Systeme erkannt und repariert, die für Angriffe anfällig sind. Diese Sicherheitslücken können durch neue Bedrohungen, veraltete oder fehlende Patches oder eine fehlerhafte Systemkonfiguration entstehen. Zu den Maßnahmen für die Fehlerbehebung zählen häufig Patches, Updates und die Neukonfiguration von Systemen, um die Sicherheitslücke zu schließen.

Warum ist das wichtig?

Sicherheitslücken können zu kostspieligen Datenpannen führen, was wiederum negative Folgen für das Vertrauen der Kunden, den Ruf des Unternehmens und den Umsatz haben kann. Umsatzeinbußen machen 39,4 % der durchschnittlichen Kosten einer Datenpanne aus.[5]

Herausforderungen bei der effektiven Erkennung von Sicherheitslücken und ihrer Behebung

Die meisten Unternehmen verfügen über keine konsistente Sicherheitsstrategie für Operationen in großem Umfang.

- Die Zahl der Mitarbeiter ist begrenzt, diese sind überlastet oder verfügen möglicherweise nicht über die Kompetenzen, die für die Entwicklung und Umsetzung einer vollständigen Sicherheitsstrategie nötig wären.
- Tools für allgemeine Sicherheitsscans generieren lange Listen von potenziellen Sicherheitslücken, aber längst nicht alle treffen auf Ihre Umgebung zu. Mitarbeiter sind daher gezwungen, sehr viel Zeit in die Prüfung von Sicherheitslücken und deren Behebung zu investieren.
- Manuelle Prozesse zur Erkennung, Behebung und Verfolgung verlangsamen den Betrieb, und bekannte Sicherheitslücken werden häufig nicht behoben.
- Methoden zur Adhoc-Behebung führen zur inkonsistenten Anwendung von Patches und zu potenziell höheren Sicherheitsrisiken.

Wichtige Funktionen von Tools für das Sicherheitsmanagement

Die größte Effektivität erreichen Sie, wenn Sie Sicherheitslücken von Systemen schnell erkennen und beheben, bevor diese zu einer Datenpanne führen. Die geeigneten Tools für das Sicherheitsmanagement sollten:

Systeme analysieren, um Risiken in Systemen und Instanzen in Ihrer Umgebung zu erkennen – sowohl auf Betriebssystem- als auch auf Workload-Ebene.

Die Fehlerbehebung automatisieren, um bei erkannten Risiken die Schnelligkeit, Genauigkeit und Effizienz der IT- und Sicherheitsteams zu erhöhen.

Das Fachwissen von Anbietern nutzen, die Anleitungen zur Fehlerbehebung für ihre Produkte bereitstellen. Möglicherweise lassen sich Risiken schon durch einfache Maßnahmen reduzieren.

Regelmäßig aktuelle Daten abrufen, sobald diese zu bekannten Sicherheitslücken und Risiken vorliegen – und zwar aus Ihrem Betriebssystem und von den Anwendungsanbietern.

Berichte generieren, die potenzielle Risiken, Maßnahmen zur Fehlerbehebung und Auditing passend für die jeweilige Zielgruppe zusammenstellen.

5 *IBM Security.* **Bericht „Kosten einer Datenschutzverletzung“**, *2020.*

Compliance-Management in Linux-Umgebungen

Durch Compliance-Management wird sichergestellt, dass Systeme nicht gegen Unternehmensrichtlinien, Branchenstandards und geltende Vorschriften verstoßen. Dazu gehört eine Infrastrukturbewertung zur Identifizierung von Systemen, die aufgrund von geänderten Vorschriften, Richtlinien oder Standards, Fehlkonfigurationen oder aus anderen Gründen nicht konform sind.

Warum ist das wichtig?

Compliance-Verstöße können – abgesehen von Sicherheitsverletzungen – Bußgelder nach sich ziehen, dem Ruf des Unternehmens schaden und zum Verlust von Zertifizierungen führen. Compliance-Verstöße führen im Schnitt zu noch höheren Kosten von Datenpannen.[6]

Herausforderungen für effektives Compliance-Management

Zahlreiche Unternehmen managen Compliance mithilfe von manuellen Operationen und benutzerdefinierten Skripts. Doch in einer modernen Welt, die sich in rasantem Tempo verändert, sind diese Prozesse zu langsam und zu eingeschränkt.

- Die Vielzahl allgemeiner Standards und Baselines macht es schwer, die Relevanz und die Auswirkungen für Ihre Umgebung nachzuvollziehen.
- Manuelle Prozesse verlangsamen Compliance-Monitoring, Fehlerbehebung und Auditing. Dies führt zum ineffizienten Einsatz von Mitarbeitern, inkonsistenter Anwendung von Richtlinien und macht Compliance-Probleme noch wahrscheinlicher.
- Zahlreiche Unternehmen verwenden unterschiedliche Tools für das Sicherheits- und das Compliance-Management. Dies führt zu einer schlechteren operativen Effizienz, und die Einrichtung konsistenter und benutzerdefinierter Richtlinien wird erschwert.

Wichtige Funktionen von Tools für das Compliance-Management

Die größte Effektivität erreichen Sie, wenn Sie Folgendes umsetzen können: kontextbezogene Richtlinien definieren und anwenden, die Einhaltung dieser Richtlinien in allen Systemen sicherstellen und Compliance-Berichte für das Auditierung schnell generieren und managen. Die geeigneten Tools für das Compliance-Management sollten:

Analysen verwenden, um Compliance-Risiken zeitnah und konsistent zu identifizieren.

Automatisch Fehler beheben, die in Systemen mit Compliance-Verstößen vorliegen.

Einen vollständigen Überblick geben über den Compliance-Status Ihrer Umgebung.

Automatisch Compliance-Berichte generieren, die Ihren Auditing- und Zielgruppenanforderungen entsprechen.

Zuverlässige Empfehlungen geben, die kontextbezogene Anweisungen zur Behebung von Compliance-Verstößen in Systemen Ihrer Umgebung enthalten.

6 *IBM Security.* **Bericht „Kosten einer Datenschutzverletzung“**, *2020.*

Best Practices

Regelmäßige Systemanalysen

Durch tägliches Monitoring können Sie Sicherheitslücken und Compliance-Risiken erkennen, bevor diese Ihren Geschäftsbetrieb unterbrechen oder zu einer Datenpanne führen. Achten Sie darauf, dass Sie die aktuellen Sicherheitsdaten aus Ihrem Betriebssystem und von Ihren Anwendungsanbietern verwenden, um die Analysegenauigkeit zu optimieren. Richten Sie außerdem benutzerdefinierte Sicherheitsrichtlinien ein, die auf Ihre Umgebung und Ihre Abläufe zugeschnitten sind, damit genauere Compliance-Ergebnisse erzielt werden.

Wenn Sie eine Datenpanne innerhalb von **200 Tagen** oder weniger erkennen und beheben, können Sie die entstehenden Kosten erheblich reduzieren.[7]

Häufige Patches, zahlreiche Tests

Wenn die Systeme auf dem neuesten Stand sind, wirkt sich das positiv auf die Sicherheit, Zuverlässigkeit, Performance und Compliance aus. Installieren Sie regelmäßig Patches, damit Sie in Bezug auf wichtige allgemeine Probleme immer auf dem neuesten Stand sind. Installieren Sie Patches für kritische Fehler und Defekte so schnell wie möglich. Führen Sie für gepatchte Systeme einen Abnahmetest durch, bevor Sie diese wieder in den Produktivmodus versetzen.

Mit einem effektiven Tool für das Patch-Management können Sie Systeme bis zu **88,9 % schneller** patchen.[8]

Automatisierung

Je größer und komplexer Ihre Infrastruktur, desto schwieriger wird das manuelle Management. Nutzen Sie Automatisierung, um das Monitoring zu optimieren, die Fehlerbehebung zu beschleunigen, die Konsistenz zu erhöhen und regelmäßige Berichte sicherzustellen.

Automatisierte Sicherheitsprozesse können die durchschnittlichen Kosten einer Datenpanne um **93 %** senken.[7]

Vernetzte Tools und angepasste Prozesse

Verteilte Umgebungen beinhalten häufig unterschiedliche Verwaltungstools für die einzelnen Plattformen. Integrieren Sie diese Tools durch APIs (Application Programming Interfaces) und verwenden Sie Ihre bevorzugten Oberflächen, um Aufgaben in anderen Tools zu erledigen. Mit einer geringeren Anzahl von Oberflächen können Sie die Betriebsabläufe optimieren und die Übersicht über den Sicherheits- und Compliance-Status aller Systeme in Ihrer Umgebung verbessern. Stimmen Sie außerdem Ihre Prozesse in allen Umgebungen aufeinander ab, um die Konsistenz und Zuverlässigkeit zu erhöhen.

52 % der Unternehmen optimieren ihre IT-Infrastruktur und IT-Prozesse, um die Sicherheit zu erhöhen.[9]

Eine konsistente, kontinuierliche Sicherheitsstrategie

Eine effektive Sicherheit erfordert einen ganzheitlichen Ansatz, bei dem die Prozesse, Technologien und die Menschen berücksichtigt werden. Eine kontinuierliche Sicherheitsstrategie basiert auf Feedback und Anpassungen, um moderne Entwicklungstechniken, DevSecOps und digitale geschäftliche Anforderungen zu unterstützen. Führen Sie eine Sicherheitsstrategie ein, die die Funktionen aller Schichten in Ihrer Umgebung umfasst – wie Betriebssysteme, Container-Plattformen, Automatisierungstools, SaaS-Assets (Software-as-a-Service) und Cloud-Services.

Durch die Einführung eines DevSecOps-Konzepts können die durchschnittlichen Kosten einer Datenpanne um **5 %** reduziert werden.[7]

7 *IBM Security.* **Bericht „Kosten einer Datenschutzverletzung“**, *2020.*

8 *Principled Technologies, gesponsert von Red Hat.* **Save administrator time and effort by activating Red Hat Insights to automate monitoring**, *September 2020.*

9 *Qualtrics und Red Hat. Studie zur IT-Optimierung, Februar 2020.*

Empfohlene Tools

Ideale Sicherheits- und Compliance-Tools haben mehrere wichtige Funktionen.

Proaktive Analyse

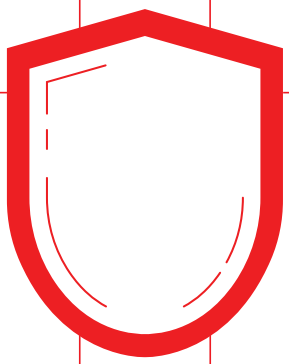
Der erste Schritt zur Optimierung von Sicherheit und Compliance besteht darin, sich einen guten Überblick zu verschaffen. Durch Tools für automatische Analysen kann sichergestellt werden, dass Systeme in regelmäßigen Abständen überwacht werden. So werden Sie ohne großen Zeit- und Kostenaufwand auf Probleme aufmerksam gemacht.

Priorisierte Fehlerbehebung

Durch Tools, die definierte Fehlerbehebungen bereitstellen, entfällt die Notwendigkeit, selbst nach Maßnahmen zu suchen, was Zeit spart und das Fehlerrisiko verringert. Durch die Priorisierung von Maßnahmen basierend auf potenziellen Auswirkungen und betroffenen Systemen können Sie begrenzte Patch-Fenster optimal nutzen.

Anpassbare Ergebnisse

Einige Sicherheits- und Compliance-Prüfungen sind aufgrund ihrer besonderen Konfiguration, ihrer Nutzung oder Workload unter Umständen nicht mit bestimmten Systemen kompatibel. Tools, mit denen Sie den Geschäftskontext definieren können, sind ideal geeignet, um falsch-positive Ergebnisse zu reduzieren, Geschäftsrisiken zu managen und Ihnen so eine realistischere Sicht auf Ihren Sicherheits- und Compliance-Status zu liefern.



Verständliche Berichte

Tools, die klar verständliche Berichte dazu erstellen, welche Systeme gepatcht sind, welche gepatcht werden müssen und welche nicht den Sicherheits- und Gesetzesrichtlinien entsprechen, erhöhen die Auditierbarkeit und ermöglichen einen besseren Überblick über den Status Ihrer Umgebung.

Einheitliche Oberfläche

Tools, die über das Management einer einzelnen Komponente oder Schicht Ihrer Umgebung hinausgehen, können Ihnen dabei helfen, Sicherheitsabläufe zu vereinfachen und einen besseren Überblick über Ihren Sicherheits- und Compliance-Status zu erhalten. Einheitliche Tools können darüber hinaus einen breiteren Kontext für Scans sowie nützliche Informationen für die Fehlerbehebung liefern.

Verwertbare Erkenntnisse

Mit Tools, die auf Ihre Umgebung zugeschnittene Informationen liefern, können Sie schneller erkennen, welche Compliance-Probleme und Sicherheitslücken vorliegen, welche Systeme betroffen sind und welche potenziellen Auswirkungen Sie erwarten können. Mit diesen Tools können Sie außerdem Korrekturen priorisieren und planen.

Mehr Sicherheit und bessere Compliance mit Red Hat

Red Hat verwendet einen ganzheitlichen Ansatz für das Risikomanagement von Sicherheit und Compliance, mit dem Sie die Schnelligkeit, Skalierbarkeit und Stabilität Ihrer gesamten IT-Umgebung steigern können – von Bare Metal- und virtualisierten Servern bis hin zu Private, Public und Hybrid Cloud-Infrastruktur. Red Hat® Plattformen stellen durch die Integration von Mitarbeitern, Prozessen und Technologie die betriebliche Effizienz sicher, fördern Innovationen und steigern die Zufriedenheit der Mitarbeiter.

Im Zentrum dieser Strategie steht **Red Hat Enterprise Linux**. Red Hat Enterprise Linux ist eine konsistente, intelligente Basis für moderne geschäftliche IT-Systeme und Hybrid Cloud-Deployments. Sie bietet optimale Vorteile für Ihr Unternehmen. Dank der Einheitlichkeit zwischen Infrastrukturen können Sie Anwendungen, Workloads und Services mit den gleichen Tools bereitstellen, unabhängig vom Standort.

Sicherheit ist ein zentraler Bestandteil der Architektur und des Lifecycles von Red Hat Enterprise Linux. Der mehrschichtige Schutz vor Datenpannen verwendet automatisierte, wiederholbare Sicherheitskontrollen, um das Risiko von Sicherheitslücken so gering wie möglich zu halten. Wichtige Sicherheits-Upgrades und Live-Patches werden im Rahmen Ihrer Red Hat Enterprise Linux Subskription bereitgestellt. Sie sorgen nicht nur dafür, dass Ihre Umgebung immer auf dem neuesten Stand ist, sondern erhöhen auch die Sicherheit.

Red Hat Management Tools können in Red Hat Enterprise Linux eingebunden werden und bieten die Funktionen, die Sie benötigen, um das Risiko von Sicherheitslücken und die Compliance effektiv zu managen.

- Konfigurierbare Tools und Baselines reduzieren die Anzahl von falsch-positiven Ergebnissen und verschaffen Ihnen einen genauen Überblick über den Status Ihrer Infrastruktur.
- Durch Automatisierungsfunktionen wird die Konfigurations- und Patching-Genauigkeit erhöht und die Anzahl von menschlichen Fehlern reduziert.
- Anpassbare Ansichten liefern im Handumdrehen die richtigen Informationen zum richtigen Zeitpunkt.
- Mit automatisierten und proaktiven Korrekturmaßnahmen können Sie Probleme schneller beheben, ohne den Support zu kontaktieren.
- Detaillierte, gezielte Informationen erhalten Sie rund um die Uhr in einer umfangreichen Ressourcen-Library.
- Dank Onsite- und SaaS-Optionen können Sie stets die Tools einsetzen, die Sie benötigen.

„Die Konfiguration von Servern, die ab dem ersten Tag einsatzbereit und sicher sind, ist eine der wichtigsten Anforderungen für unsere IT-Organisation. Red Hat Enterprise Linux mit Red Hat Insights verleiht uns genau diese Fähigkeit. So sind wir in der Lage, Server bereitzustellen, die wir sofort nutzen können und die unsere speziellen Anforderungen erfüllen, sobald sie den Regelbetrieb aufnehmen.“[10]

Steve Short
Platforms Manager, Unix, Kingfisher PLC

10 *Red Hat Pressemitteilung.* **Red Hat Delivers Force Multiplier for Enterprise IT with Enhanced Intelligent Monitoring, Unveils Latest Version of Red Hat Enterprise Linux 8**, *21. April 2020.*

Vorteile integrierter Managementtools

Die Managementtools von Red Hat basieren auf jahrelanger Linux-Entwicklung und Support-Erfahrung. Die einzelnen Tools funktionieren Hand in Hand, um die IT-Administration zu optimieren. Hiervon profitiert Ihr Team, das Zeit und Mühen spart, aber auch Ihre Umgebung, die sicherer und zuverlässiger wird.

Red Hat Insights

Prädiktive Analysen von IT-Risiken

Red Hat Insights ist in allen aktiven Red Hat Enterprise Linux Subskriptionen enthalten und unterstützt IT-Teams proaktiv bei der Erkennung und Behebung verschiedener Bedrohungen, um Systemfehler, ungeplante Ausfallzeiten sowie Risiken für Sicherheit und Compliance zu vermeiden.

- Gründliche Analyse von Systemen, um proaktiv Sicherheitslücken, Compliance-Probleme und Richtlinienverstöße zu erkennen
- Definition und Priorisierung von Korrekturmaßnahmen und Generierung von Red Hat Ansible® Automation Platform Playbooks
- Vergleich von Systemen mit Baselines, Verläufen und anderen Systemen
- Einfaches Deployment lokal und in Cloud-Umgebungen

96 % schnellere Erkennung App-spezifischer Probleme[11]

91 % schnellere Erkennung von Sicherheitslücken[11]

89 % schnellere Erkennung von Konfigurations-abweichungen[11]

Mehr erfahren

Red Hat Smart Management

Maßnahmenmanagement und Fehlerbehebung

Red Hat® Smart Management vereint die leistungsstarken Funktionen zur Infrastrukturverwaltung von Red Hat Satellite mit dem einfachen Management der Cloud, um die Funktionen von Red Hat Insights zu optimieren und zu ergänzen.

- Mit Red Hat Satellite können Sie Ihre Red Hat Enterprise Linux Hosts patchen, provisionieren und kontrollieren und darüber hinaus allgemeine detaillierte Berichte erstellen.
- Unter cloud.redhat.com können Sie in Verbindung mit Red Hat Insights Probleme erkennen und beheben.
- Über Cloud Connector können Sie von Red Hat Insights erkannte Probleme per Knopfdruck beheben.

56 % effizienteres System-Patching[12]

14 % effizientere IT-Sicherheits-teams[12]

23 % produktivere Compliance-Teams[12]

Mehr erfahren

11 *Principled Technologies, gesponsert von Red Hat.* **Save administrator time and effort by activating Red Hat Insights to automate monitoring**, *September 2020.*

12 *IDC White Paper, gesponsert von Red Hat.* **Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools**, *März 2020. Document #US46109220.*

Customer Success Highlight

Metalloinvest

Mit Daten-Insights und prädiktiven Risikoanalysen die Performance zentraler Systeme sicherstellen

Herausforderung

Metalloinvest ist ein weltweit führender Hersteller und Lieferant von heißbrikettiertem Eisen (HBI) und Eisenerzprodukten sowie ein regionaler Produzent von hochwertigem Stahl. Nach mehreren Jahrzehnten des Betriebs sah sich Metalloinvest einer neuen Herausforderung gegenüber: Industry 4.0, der Wandel der Fertigungsindustrie in Richtung eines automatisierten, datenzentrierten Betriebs. Durch die Automatisierung und Digitalisierung der Produktion sollen nun Betrieb und Nutzung von Ressourcen effizienter gestaltet werden. Das Ziel besteht nicht nur darin, das größte Bergbauunternehmen der Welt zu werden, sondern auch das produktivste. Als Basis für Industry 4.0 wollte das Unternehmen seine komplexe SAP®-Umgebung integrieren und optimieren.

Lösung

Mit der Hilfe des Anbieters für gemanagte Services, der JSA-Group, führte Metalloinvest Red Hat Enterprise Linux for SAP Solutions ein, um eine robuste Unternehmensbasis für seine SAP S/4HANA®-Umgebung zu schaffen. Red Hat Enterprise Linux for SAP Solutions wurde von **Red Hat und SAP** gemeinsam entwickelt. Die Lösung enthält Red Hat Insights für prädiktive Analysen und Red Hat Smart Management, womit das Management von Red Hat Enterprise Linux-Umgebungen durch Red Hat Satellite und Cloud-Management-Services vereinfacht wird. Mit nur einer Subskription werden so die Zuverlässigkeit, Skalierbarkeit und hohe Leistungsfähigkeit von Linux mit den Technologien kombiniert, die die spezifischen Anforderungen von SAP-Anwendungen erfüllen.

Metalloinvest führt nun seine gesamte SAP S/4HANA-Produktivumgebung in Red Hat Enterprise Linux for SAP Solutions aus. Das Unternehmen kann nun umfangreiche Daten-Insights und prädiktive Risikoanalysen nutzen, um eine zuverlässige und stabile Performance seiner zentralen Systeme sicherzustellen, während es sich auf die Digitalisierung seiner Produktivumgebung vorbereitet.

„Dank Red Hat verfügen wir nun über Tools, mit denen wir die Produktivität unserer Mitarbeiter und Prozesse steigern können."

Konstantin Zelenkov
Chief Technology Officer, JSA Group

Höhere Zuverlässigkeit und Performance für zentrale Betriebssysteme

Umfassendere Daten durch bessere SAP-Integration

Weniger Risiken durch Sicherheitsmanagement und umfangreichen Support

Success Story lesen

Bereit für mehr Sicherheit und bessere Compliance?

Ihr Geschäft hängt von Ihrer IT-Infrastruktur und Ihren Anwendungen ab. Durch die Einführung effektiver Konzepte und Tools zur Erkennung von Sicherheitslücken und für Compliance-Risikomanagement können Sie Ihr Unternehmen schützen. Red Hat stellt die Linux-Plattform sowie integrierte Managementtools bereit, die Sie für sichere Abläufe und Innovationen benötigen.

Starten Sie noch heute mit Red Hat Insights:

redhat.com/insights

Wie Sie Ihre IT-Workflows mit Red Hat Insights beschleunigen:

red.ht/insights_savetime

Lesen Sie die Kurzdarstellung „Manage security risks with Red Hat Insights“:

red.ht/insights-security-brief

Sehen Sie sich die Demo von Red Hat Insights zum Risikomanagement an:

red.ht/insights-security-demo

F26049_1120_KVM

Red Hat