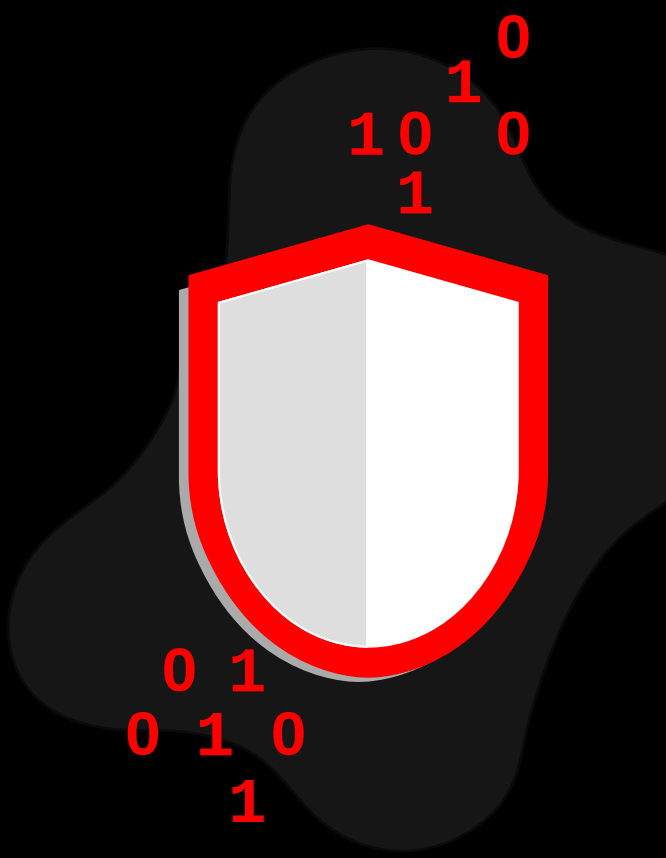
Red Hat

Verbesserung von Sicherheit und Compliance

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

Inhalt



Linux – die Basis für die Zukunft

Als eines der verbreitetsten Betriebssysteme weltweit bietet Linux® eine ideale Plattform für moderne, innovative IT. Es wird für hochverfügbare, zuverlässige und betriebswichtige Workloads in Rechenzentren und Cloud Computing-Umgebungen verwendet und unterstützt zahlreiche Use Cases, Zielsysteme und Geräte. Die wichtigen Public Cloud-Anbieter bieten in ihren Märkten mehrere Linux-Distributionen an.

Dennoch können die von Ihnen gewählte Linux-Distribution und Managementtools die Effizienz, Sicherheit und Interoperabilität Ihrer IT-Umgebung erheblich beeinflussen. In diesem E-Book erhalten Sie wichtige Informationen und Tipps zu Sicherheit und Compliance in Linux-Umgebungen.

Sicherheit und Compliance stehen an erster Stelle

IT-Sicherheit und Compliance sind in den meisten Unternehmen ein wichtiges Thema. Tatsächlich waren 23 % der Unternehmen in den letzten 2 Jahren von einem größeren Angriff auf die Cybersicherheit betroffen.[1] Dazu können Sicherheitsverletzungen sehr kostspielig sein. Eine Datenpanne kostet durchschnittlich 4,45 Millionen USD.[2]

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 5 %.[2]

Vermeiden der Konsequenzen ineffizienter Sicherheitsmaßnahmen

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

4,45 Mio USD
durchschnittliche Kosten für Datenpannen im Jahr 2023.[2]

277 Tage
durchschnittlicher Zeitraum zur Erkennung und Eindämmung einer Datenpanne im Jahr 2023.[2]

1,02 Mio. USD
Kosteneinsparungen, wenn die Erkennung und Eindämmung einer Datenpanne in maximal 200 Tagen erfolgt[2]

1 Nash Squared: „2023 Nash Squared digital leadership report", November 2023.
2 IBM Security. Bericht „Kosten einer Datenpanne", 2023.

Bekannte Herausforderungen in Sachen Sicherheit und Compliance

Mehrere Faktoren machen Sicherheitslücken und Compliance-Management schwierig.

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.

23 %
der Unternehmen sämtlicher Größenordnungen waren in den letzten 2 Jahren von einem größeren Angriff auf die Cybersicherheit betroffen.[3]

82 %
der Datenpannen im Jahr 2023 betrafen Daten, die in Cloud-Umgebungen oder in mehreren Umgebungen gespeichert waren.[4]

Verteilte Cloud-Umgebungen

Geografisch und logistisch verteilte Hybrid- und Multi-Cloud-Umgebungen können verhindern, dass Sie einen vollständigen Überblick über Ihre IT-Infrastruktur erhalten. Das erschwert die Aufrechterhaltung konsistenter Konfigurationen in den verschiedenen Systemen.

Große und komplexe IT-Umgebungen

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

Durch die Komplexität des Sicherheitssystems erhöhen sich die Kosten von Datenpannen um

240.889 USD.[4]

Remote-Mitarbeitende erhöhen die durchschnittlichen Kosten einer Datenpanne um

173.074 USD

im Vergleich zu Vorfällen, bei denen die Remote-Arbeit keine Rolle spielte.[4]

Wenig Personal und Möglichkeiten zur Remote-Arbeit

Die meisten Unternehmen verfügen nicht über die nötige Anzahl an Mitarbeitenden, um Sicherheits- und Compliance-Aufgaben manuell zu verwalten. Darüber hinaus kann die Arbeit an entfernten Standorten den Aufwand für den Schutz von Geräten und Zugriffspunkten auf die digitalen Ressourcen eines Unternehmens erhöhen.

*3 Nash Squared: „**2023 Nash Squared digital leadership report**“, November 2023.*
*4 IBM Security. **Bericht „Kosten einer Datenpanne“**, 2023.*

Einführen eines effektiven Konzepts für Sicherheits- und Compliance-Management

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. Analysieren Sie den aktuellen Sicherheitsstatus Ihrer Umgebung von der Infrastruktur bis zur Workload. 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. Setzen Sie Techniken zum Risikomanagement ein, um das tatsächliche Geschäftsrisiko für jedes Problem zu ermitteln und die Abhilfemaßnahmen entsprechend zu planen. 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 und rekonfigurieren Sie Systeme, die eine schnelle Reaktion erfordern. Automatisieren Sie Konfigurations- und Patching-Prozesse, um die Behebung zu beschleunigen, systemübergreifende Konsistenz sicherzustellen und um das Risiko menschlicher Fehler zu reduzieren. Durch effektiven Einsatz automatisierter Tools können Sie Probleme schnell beheben, um die Sicherheit Ihrer Umgebung und Ihres Unternehmens zu verbessern.

Bericht

Überprüfen Sie, ob Änderungen umgesetzt wurden, und automatisieren Sie die Berichterstattung für optimierte Audits. 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. In den folgenden Abschnitten werden wichtige Aspekte und Maßnahmen für ein effektives Management Ihrer Sicherheits- und Compliance-Risiken behandelt.

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 29,2 % 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 Ad-hoc-Behebung führen zur inkonsistenten Anwendung von Patches und zu potenziell höheren Sicherheitsrisiken.

5 *IBM Security.* **Bericht „Kosten einer Datenpanne“**, *2023.*

Wichtige Funktionen von Tools für das Sicherheitsmanagement

Für Effizienz müssen Sie in der Lage sein, Systemschwachstellen schnell zu erkennen und zu beheben, bevor sie zu einer Datenpanne führen. Die geeigneten Tools für das Sicherheitsmanagement sollten:

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

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.

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 Mitarbeitenden, 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

Damit Sie effektiv arbeiten können, müssen Sie kontextbezogene Richtlinien definieren und anwenden, die Konformität der Systeme sicherstellen und schnell Berichte für Audits erstellen und verwalten. 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 Datenpanne“**, *2023.*

Best Practices und Empfehlungen für Tools

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.

Das Identifizieren und Beheben einer Datenpanne in

200 Tagen

oder weniger kann die dadurch verursachten 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.

Ein effektives Management-Tool kann das Patchen von Systemen beschleunigen, und zwar um bis zu

56 %.[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.

Sicherheitsautomatisierung und künstliche Intelligenz (KI) können die Kosten für Datenpannen senken, um etwa

39.3%.[7]

7 IBM Security. **Bericht „Kosten einer Datenpanne“**, *2023.*

8 IDC White Paper, gesponsert von Red Hat. **„Red Hat Satellite unterstützt Unternehmen mit Automatisierungstools beim Optimieren der Infrastruktur“**. *Dokument Nr. US46109220. August 2021.*

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.

Ein hohes Maß an Komplexität des Sicherheitssystems kann die durchschnittlichen Kosten einer Datenpanne erhöhen, und zwar um

31.6%.[9]

Einsatz einer konsistenten, kontinuierlichen 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.

Das Einführen eines DevSecOps-Konzepts kann die durchschnittlichen Kosten einer Datenpanne reduzieren, um etwa

38,4 %.[9]

9 *IBM Security.* **Bericht „Kosten einer Datenpanne“**, *2023.*

Ideale Sicherheits- und Compliance-Tools verfügen über 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 Reaktion

Tools, die präskriptive Behebungsmaßnahmen anbieten, machen es überflüssig, selbst nach Maßnahmen zu suchen. Das spart Zeit und verringert das Risiko von Fehlern. Durch die Priorisierung von Maßnahmen basierend auf potenziellen Auswirkungen und betroffenen Systemen können Sie begrenzte Patch-Fenster optimal nutzen.

Anpassbare Ergebnisse

Einige Schwachstellen- und Compliance-Prüfungen gelten möglicherweise nicht für bestimmte Systeme aufgrund ihrer Verwendung, Konfiguration oder Workload. Mit den idealen Tools können Sie den geschäftlichen Kontext definieren, um Fehlalarme zu reduzieren, Risiken zu verwalten und einen realistischen Überblick über Ihren Sicherheits- und Compliance-Status zu erhalten.

Verständliche Berichte

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

Einheitliche Oberfläche

Mit Tools, die über die Verwaltung einzelner Komponenten oder Schichten Ihrer Umgebung hinausgehen, können Sie die Sicherheitsabläufe vereinfachen und einen besseren Überblick über Ihre Sicherheits- und Compliance-Situation gewinnen. 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 verfolgt einen ganzheitlichen Ansatz für das Sicherheits- und Compliance-Risikomanagement, der die Geschwindigkeit, Skalierbarkeit und Stabilität Ihrer gesamten IT-Umgebung verbessert – von Bare Metal- und virtualisierten Servern über Private, Public und Hybrid Cloud-Infrastrukturen bis hin zu Edge Deployments. Red Hat® Plattformen stellen durch die Integration von Mitarbeitenden, 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 Sicherheitsverletzungen nutzt automatisierte, wiederholbare Sicherheitskontrollen, um Ihr Anfälligkeitsrisiko zu minimieren. Kritische Sicherheitsupgrades und Live-Patches, die im Rahmen Ihrer Subskription für Red Hat Enterprise Linux bereitgestellt werden, unterstützen Sie beim Aktualisieren und Verbessern der Sicherheit in Ihrer Umgebung.

> „Seit wir zu Red Hat Enterprise Linux gewechselt sind, können wir **schneller Bugs und andere Schwachstellen** finden und untersuchen, als bei der Linux-Distribution, die wir vorher verwendet haben."[10]
>
> **Yuki Miyamoto**
> IT Infrastructure/Business Online Infrastructure System, Information Technology Division, Square Enix Co., Ltd.

*10 Red Hat Case Study. „**Square Enix vereinfacht das Infrastrukturmanagement für Online Gaming**," Mai 2023.*

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 die richtigen Informationen für die richtige Zielgruppe schnell und zur richtigen Zeit.

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.

APIs stellen eine Verbindung zu Ihren vorhandenen und bevorzugten Sicherheits-, Compliance- und Management-Tools und Schnittstellen her.

Funktionen zur Erkennung von Schwachstellen und Malware scannen Systeme auf häufige Schwachstellen und CVEs (Common Vulnerabilities and Exposures) und Malware-Signaturen.

Funktionen zur Ressourcenoptimierung unterstützen Sie bei der richtigen Dimensionierung Ihrer Public Cloud Deployments anhand von Rechen-, Speicher- und Performance-Metriken.

Vorteile integrierter Tools

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

Analysieren, Überwachen und Verwalten von Red Hat Systemen

Red Hat Insights ist im Lieferumfang von Red Hat Enterprise Linux enthalten und wird als Service bereitgestellt. Red Hat Insights analysiert kontinuierlich Plattformen und Anwendungen, um Risiken zu erkennen, Maßnahmen zu empfehlen und Kosten zu verfolgen, damit Sie Hybrid Cloud-Umgebungen besser verwalten können. Mit Insights können Sie die Effizienz, Stabilität und Performance Ihrer IT überwachen, Sicherheits- und Compliance-Risiken managen und Ausgaben für verschiedene Clouds verfolgen und optimieren.

Mehr über Insights erfahren

26 % schnellere Lösung von Sicherheitsvorfällen[11]

24 % mehr Effizienz bei den Teams der IT-Sicherheit[11]

76 % weniger ungeplante Ausfallzeiten[11]

Red Hat Satellite

Optimieren und Automatisieren des Systemmanagements

Red Hat Satellite ist eine Lösung für das Infrastrukturmanagement, mit der Systeme von Red Hat Enterprise Linux bereitgestellt und verwaltet werden können, und zwar standortunabhängig – in physischen, virtuellen, Cloud- oder Edge-Umgebungen. Satellite optimiert das Provisionieren, Patchen und andere sich wiederholende Systemverwaltungsaufgaben in großem Umfang, um die operative Effizienz zu steigern und gleichzeitig die Systemsicherheit, Verfügbarkeit und Compliance mit Richtlinien zu gewährleisten.

Mehr über Satellite erfahren

56 % effizientere Patching-Operationen[12]

56 % effizientere IT-Infrastruktur[12]

28 % niedrigere Gesamtbetriebskosten[12]

11 IDC Business Value Snapshot, gesponsert von Red Hat: „Der Geschäftswert von Red Hat Insights". Dokument #US51795124. Februar 2024

12 IDC White Paper, gesponsert von Red Hat. „Red Hat Satellite unterstützt Unternehmen mit Automatisierungstools beim Optimieren der Infrastruktur". Dokument Nr. US46109220. August 2021.

Erfolgsbeispiele aus der Praxis

Das Met Office

Das Meteorological Office, der nationale Wetterdienst des Vereinigten Königreichs, bietet täglich wetter- und klimabezogene Services für Menschen in der ganzen Welt an. Auf der Suche nach einem umfassenden Ansatz für die Serververwaltung entschied sich das Met Office neben der Verwendung von Red Hat Satellite auch für Red Hat Insights. Mit dem Support eines Technical Account Managers von Red Hat verfügt das Met Office nun über erheblich mehr Transparenz in seiner Serverumgebung.

Das Met Office testete Insights zunächst auf mehreren seiner Rechner mit bereits bekannten Schwierigkeiten. Die Probleme wurden sofort erkannt, und das IT-Team beschloss, mit einem umfassenderen Deployment fortzufahren. Das Team nutzte Satellite – in Übereinstimmung mit den internen Prozessen zum Änderungsmanagement – um die Installation von Insights im gesamten Unternehmen zu vereinfachen.

Mit Insights kann das Team nun viel leichter Aufgaben priorisieren, feststellen, ob es Probleme gibt, und verstehen, welche Systeme betroffen sind und wie schwerwiegend das Problem ist. Zudem konnte das Met Office seinen Serverbestand auf den gewünschten Standard bringen, da sich Konfigurationsprobleme identifizieren und beheben ließen.

Das Met Office plant, Insights und Satellite weiterhin zu nutzen, um seine gesamte Umgebung zu verwalten und seine Sicherheitslage proaktiv zu verbessern.

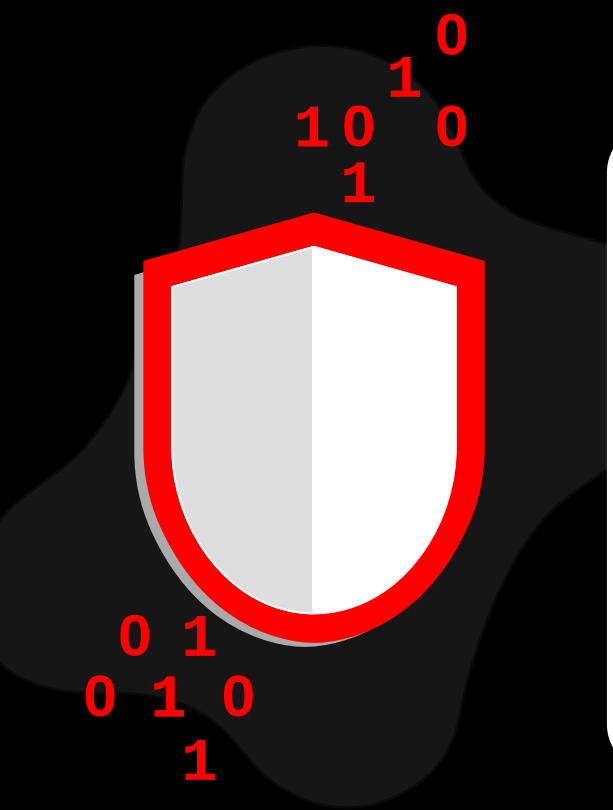
> Ich stellte fest, dass RedHat Insights uns dabei unterstützen könnte, einen Top-Down-Überblick zu erhalten und einen **ganzheitlicheren Ansatz für unser Bestandsmanagement zu wählen**. Red Hat Satellite kann gut Probleme auf einzelnen Rechnern aufdecken, während die Stärke von Red Hat Insights darin liegt, häufige Probleme in der gesamten Anlage zu finden, anstatt sie auf den einzelnen Rechnern zu beheben.
>
> **Chris Wilkinson**
> Senior Systems Engineer,
> The Meteorological Office, Vereinigtes Königreich

Success Story lesen

Bereit für den Einstieg?

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 bewährte Linux-Plattform sowie integrierte Managementtools und Services bereit, die Sie für sichere Abläufe und Innovationen benötigen.



Risikoanalyse mit Red Hat Insights

- **Erfahren** Sie mehr über Red Hat Insights
- **Erfahren Sie, was Analysten** über Red Hat Insights sagen

Management in großem Umfang mit Red Hat Satellite

- **Erfahren** Sie mehr über Red Hat Satellite
- **Erfahren Sie, was Analysten** über Red Hat Satellite sagen

1156696_0524_KVM

Red Hat