

Vereinfachung der Sicherheit in der Cloud

Konsistente Sicherheitsfunktionen für Ihre Umgebungen mit Red Hat Enterprise Linux



Konsistente Abläufe in Ihren Cloud-Umgebungen

Red Hat Enterprise Linux enthält viele Optimierungen, die für eine zuverlässige, sicherheitsorientierte Performance in der Cloud sorgen. Es bietet eine konsistente Betriebsbasis für Hybrid Cloud- und Multi-Cloud-Umgebungen, damit Sie Ihre Anwendungen dort ausführen können, wo es am meisten Sinn ergibt.

[Erfahren Sie mehr](#) über den Wert von Red Hat Enterprise Linux in der Cloud.

Cloud-Sicherheit als zentrales Anliegen

Das Thema Sicherheit bleibt bei der Cloud-Einführung ein Hauptanliegen für Unternehmen beliebiger Größe. Tatsächlich geben 85 % der Unternehmen Sicherheit als eines ihrer größten Herausforderungen im Hinblick auf die Cloud an.¹ Und das mit gutem Grund: 45 % der Sicherheitsvorfälle im Jahr 2022 fanden in der Cloud statt.²

Konsistenz ist der Schlüssel zu Best Practices im Bereich Sicherheit und Compliance – unabhängig von der Umgebung. Damit Sie Ihr Unternehmen schützen können, brauchen Sie in der Cloud das gleiche Niveau an Sicherheitsrichtlinien und Zugriffskontrollen wie in Ihren Onsite-Rechenzentren. Die Standardisierung auf einem Betriebssystem mit konsistenten Sicherheitskontrollen für die gesamte Infrastruktur kann Sie dabei unterstützen, die Sicherheit und Compliance unternehmensweit zu verbessern. Mit Red Hat® Enterprise Linux® als Betriebssystem für Ihre Umgebungen können Sie für die Konsistenz sorgen, die für die Sicherheit und Compliance in der Cloud erforderlich ist.

Einführung einer konsistenten Basis für Sicherheit und Compliance in mehreren Umgebungen

[Red Hat Enterprise Linux](#) vereinfacht die Einhaltung von Sicherheits- und Compliance-Anforderungen in lokalen, Cloud- und Edge-Umgebungen. Sicherheit ist ein zentraler Bestandteil der Architektur und des Lifecycles von Red Hat Enterprise Linux. Integrierte Sicherheitsfunktionen sowie Compliance mit Branchen- und Regierungsvorschriften schützen Ihre Systeme in der Cloud. Standardeinstellungen, die auf Best Practices basieren, sorgen dafür, dass Ihre Systeme von Anfang an für erhöhte Sicherheit konfiguriert sind. Minimale Paket-Sets für vorgefertigte Cloud-Images reduzieren Ihre Angriffsfläche bei Cybersicherheitsbedrohungen. Auch Sicherheits-Upgrades und Live-Patches werden im Rahmen Ihrer Red Hat Enterprise Linux Subskription bereitgestellt.

Mit Red Hat Enterprise Linux können Sie Sicherheitsrisiken mindern, eine mehrschichtige Sicherheit implementieren sowie aufrechterhalten und die Compliance in Ihren Hybrid Cloud- und Multi-Cloud-Umgebungen optimieren. Dieser Überblick beschreibt wichtige Features und Funktionen für die Einführung eines konsistenten, cloudübergreifenden Sicherheitsansatzes.

Erkennung und Behebung von Schwachstellen in großem Umfang mit Red Hat Insights

Die Identifizierung und Eindämmung einer Datenpanne dauerte im Jahr 2022 durchschnittlich 277 Tage.² Erfolgt dies in 200 Tagen oder weniger, können die Kosten um durchschnittlich 24 % gesenkt werden.² Eine konsistente, tägliche Überwachung unterstützt Sie dabei, Schwachstellen und Compliance-Risiken zu entdecken, bevor dadurch geschäftliche Abläufe unterbrochen werden oder es zu einer Datenpanne kommt.

¹ Flexera: „[Flexera 2022 State of the Cloud Report](#)“, März 2022.

² IBM Security: „[Cost of a Data Breach 2022](#)“.



Red Hat Enterprise Linux



Beschleunigung von Sicherheits- und Compliance-Prozessen

Mit Red Hat Insights können Sie Ihre Sicherheits- und Compliance-Abläufe beschleunigen:

- ▶ **91 %** schnellere Erkennung von Sicherheitsschwachstellen³
- ▶ **69 %** schnellere Erkennung von Richtlinienverletzungen³

Weitere Informationen zum Management von Sicherheit und Compliance mit Red Hat Enterprise Linux:

- ▶ [Kurzdarstellung „Verwaltung von Sicherheitsrisiken mit Red Hat Insights“](#)
- ▶ [Demo „Behebung von Problemen mit Red Hat Insights“](#)
- ▶ [Live-Demo „Sicherheits-Compliance und Schwachstellenscans mit OpenSCAP“](#)

Red Hat Enterprise Linux beinhaltet den Zugang zu [Red Hat Insights](#). Diese Suite mit in Red Hat Hybrid Cloud Console gehosteten Services analysiert durchgehend Plattformen und Anwendungen, damit Sie Ihre Hybrid Cloud-Umgebungen besser verwalten und optimieren können. Mithilfe von prädiktiven Analysen und einem fundierten Know-how kann Red Hat Insights Sicherheits- und Compliance-Risiken ebenso wie andere operativ Risiken identifizieren, bewerten und entsprechende Behebungsmaßnahmen empfehlen. Er hilft Ihnen außerdem dabei, Maßnahmen anhand des Schweregrads, der Art des Risikos und der Auswirkungen der Änderung zu priorisieren. Außerdem funktioniert Red Hat Insights in mehreren Onsite- und Cloud-Umgebungen, wodurch Sie Ihre verschiedenen Red Hat Enterprise Linux-Systeme in einer einzigen Benutzerschnittstelle verwalten können. Sie können Ihr Red Hat Account sogar mit dem Ihres Cloud-Anbieters verknüpfen, um Ihre cloudbasierten Systeme und Workloads automatisch mit Red Hat Insights und anderen Red Hat Services verbinden, wenn Sie diese provisionieren.

Red Hat Insights beinhaltet Services, die Sie bei der Sicherung Ihrer Hybrid Cloud -und Multi-Cloud-Umgebungen unterstützen.

- ▶ **Schwachstellenservice:** Damit können Sie Ihre Systeme in einer zentralen Oberfläche auf CVEs (Common Vulnerabilities and Exposures) scannen, diese Scanergebnisse sammeln und auf Anleitungen zur Fehlerbehebung zugreifen.
- ▶ **Malware-Service:** Sie können Systeme identifizieren, die aktive Malware-Signaturen enthalten, und so eine langfristige Exposition zu verhindern.

Integrierte Scans und Fehlerbehebung für eine bessere Compliance

Compliance-Verstöße können – abgesehen von Sicherheitsverletzungen – Bußgelder nach sich ziehen, dem Ruf des Unternehmens schaden und zum Verlust von Zertifizierungen führen. Für Unternehmen mit einem hohen Ausmaß an Compliance-Verstößen betrugen die Kosten einer Datenpanne im Jahr 2022 durchschnittlich 5,57 Millionen USD.² Ein hohes Ausmaß an Compliance-Verstößen erhöhte die Kosten einer Datenpanne 2022 um durchschnittlich 258.293 USD.²

Red Hat Enterprise Linux ist nach zentralen behördlichen und Branchenstandards zertifiziert. Dadurch können Sie das System auch für stark regulierte Umgebungen zuversichtlich verwenden. Red Hat Insights beinhaltet Services, die Ihnen die Sicherstellung der Compliance von Hybrid Cloud -und Multi-Cloud-Umgebungen erleichtern.

- ▶ **Compliance-Service:** Damit können Sie die Compliance mithilfe von OpenSCAP-Richtlinien überprüfen, nichtkonforme Systeme anpassen und Berichte für Compliance- und Sicherheitsaudits generieren. Sie können die Standardrichtlinien auch an Ihre Umgebung und Abläufe anpassen, um genauere Ergebnisse zu erzielen. Zu den wichtigsten integrierten Baselines gehören:
 - ▶ PCI-DSS (Payment Card Industry Data Security Standard)
 - ▶ Erweitertes OSPP (Operating System Protection Profile) nach Common Criteria (CC)
 - ▶ Die „Essential Eight“ des ACSC (Australian Cyber Security Centre)
 - ▶ CIS-Benchmark (Center for Internet Security)
 - ▶ HIPAA (Health Insurance Portability and Accountability Act)
 - ▶ DISA STIG (Defense Information Systems Agency Security Technical Implementation Guide)
- ▶ **Richtlinienservice:** Sie können benutzerdefinierte Sicherheitsrichtlinien erstellen, Systeme auf Compliance überwachen und Teams alarmieren, wenn ein System nicht mehr konform ist.

³ Principled Technologies, gesponsert von Red Hat. „[Geringerer Zeit- und Arbeitsaufwand für Administrationsteams durch automatisiertes Monitoring mit Red Hat Insights](#)“, September 2020.

Bereitstellung konsistenter, gehärteter Images in mehreren Clouds mit dem Image Builder Service

89 % der Unternehmen folgen heute einer Multi-Cloud-Strategie.¹ Mit einem Multi-Cloud-Ansatz können Sie zwar für Ihre Workloads die jeweils passende Cloud wählen. Allerdings erhöht sich damit auch die Komplexität und das Risiko von Inkonsistenzen, die zu Sicherheits- und Compliance-Problemen führen können.

Mit dem [Image Builder Service von Red Hat Insights](#) können Sie die Betriebssystem-Images von Red Hat Enterprise Linux in Ihren Hybrid Cloud-Umgebungen schneller und einfacher erstellen, verwalten und bereitstellen. Sie können benutzerdefinierte, sicherheitsgestützte Images erstellen, diese als Vorlagen speichern und dann in die Inventories mehrerer Cloud-Anbieter übertragen, um die Provisionierung zu vereinfachen. So können Sie sicher sein, dass Ihre Systeme in den verschiedenen Clouds konsistent konfiguriert sind.

Überprüfung der Systemintegrität in mehreren Umgebungen durch Remote-Zertifizierung

Die Sicherstellung der Systemintegrität ist in großen, stark verteilten Umgebungen wesentlich. Nicht vertrauenswürdige und kompromittierte Systeme können Ihr Unternehmen für Angriffe durch böswillige Akteure anfällig machen.

Red Hat Enterprise Linux umfasst Remote-Zertifizierungsfunktionen für die Überprüfung des Systemzustands beim Start und die kontinuierliche Überwachung der Integrität von Remote-Systemen. Remote-Zertifizierungen basieren auf dem Open Source-Projekt [Keylime](#) und nutzen eingebettete TPM-Hardware (Trusted Platform Module) und die Linux-Kernel-IMA (Integrity Measurement Architecture), um Systeme in großem Umfang zu überwachen. Außerdem können Sie verschlüsselte Dateien an die überwachten Systeme senden und automatisierte Aktionen festlegen, die ausgeführt werden, wenn der Integritätsstest für ein überwachtes System fehlschlägt.

Schutz Ihrer Daten in der Cloud mit Network Bound Disk Encryption

Ihre Daten sind eine wichtige Unternehmensressource. Es ist daher wesentlich, sie in der Cloud zu schützen.

Red Hat Enterprise Linux unterstützt NBDE (Network Bound Disk Encryption), um die Sicherung von Daten im Ruhezustand zu vereinfachen. NBDE schaltet automatisch Storage Volumes über Verbindungen zu einem oder mehreren Netzwerkservers frei. Dadurch können Sie Volumes entschlüsseln, ohne Verschlüsselungsschlüssel manuell managen zu müssen. Gleichzeitig wird so dafür gesorgt, dass die Volumes nur dann verfügbar sind, wenn sie gesichert sind. Red Hat Enterprise Linux unterstützt auch NBDE über TPMs (Trusted Platform Modules), um die Systemintegrität sicherzustellen, bevor verschlüsselte Volumes freigegeben werden.

Einfachere Implementierung von Zero-Trust-Architekturen mit integriertem Identitäts- und Zugriffsmanagement

Herkömmliche perimeterbasierte Sicherheitsansätze können neue, weit verteilte, cloudbasierte Umgebungen nicht effektiv schützen. Mit [Zero-Trust-Architekturen](#) können Sie Sicherheit auf die einzelnen Assets anwenden statt ausschließlich auf ein Netzwerkperimeter. Die Implementierung von Zero Trust senkt tatsächlich die Kosten von Datenpannen um durchschnittlich 20,5 %.² [Identitäts- und Zugriffsmanagement](#) ist das Kernstück von Zero-Trust-Architekturen.

[Red Hat Identity Management](#) ist in Red Hat Enterprise Linux enthalten und kann Sie dabei unterstützen, das Identitätsmanagement zu zentralisieren, Sicherheitskontrollen durchzusetzen und die Compliance von Sicherheitsstandards in Ihrer gesamten Umgebung einzuhalten. Damit erhalten Sie die Funktionen, die Sie für die Implementierung von Best Practices zu Zero Trust brauchen, und vereinfachen gleichzeitig Ihr Identitätsmanagement-Infrastruktur. Über eine einzige, skalierbare Schnittstelle, die Ihr gesamtes Rechenzentrum umfasst, können Sie Nutzende authentifizieren und richtlinienbasierte Zugriffskontrollen oder RBAC (Role-based Access Controls) implementieren. Red Hat Identity Management kann über Standard-Schnittstellen auch in Microsoft Active Directory, LDAP (Lightweight Directory Access Protocol) und andere Lösungen von Drittanbietern eingebunden werden. Außerdem unterstützt Red Hat Identity Management zertifikatbasierte Authentifizierungs- und Autorisierungsmethoden.



Aufbau einer Zero-Trust-Basis in Linux-Umgebungen

Mit einer Zero-Trust-Architektur können Sie Ihre IT-Umgebung und Ihr Unternehmen besser schützen.

- ▶ [Weitere Informationen](#) über die Implementierung von Zero-Trust mit Red Hat Enterprise Linux
- ▶ [Live-Demo](#) der Benutzerverwaltung in Red Hat Enterprise Linux



Beschleunigtes Sicherheitsmanagement für mehrere Releases

Mithilfe von Automatisierung können Sie manuelle Fehler reduzieren und Ihre Systeme schneller managen.

[Live-Demo](#) zu Systemrollen in Red Hat Enterprise Linux

Optimierte Sicherheitskonfiguration und -verwaltung mit Systemrollen

Je größer und komplexer Ihre Infrastruktur, desto schwieriger wird das manuelle Management. Bei 15 % der Datenpannen setzte der ursprüngliche Angriff bei einer Cloud-Fehlkonfiguration an, was im Jahr 2022 zu Kosten von durchschnittlich 4,14 Millionen USD pro Datenpanne führte.² Mithilfe von Automatisierung können Sie Ihre Systeme schneller, konsistenter und müheloser konfigurieren und verwalten.

Die Systemrollen von Red Hat Enterprise Linux, die auf [Red Hat Ansible® Automation Platform](#) basieren, unterstützen Sie mit Automatisierung dabei, Sicherheitseinstellungen in großem Umfang schnell zu installieren und zu verwalten. Systemrollen funktionieren mit mehreren Red Hat Enterprise Linux-Releases und für Ihre gesamte Infrastruktur. Dadurch können Sie neue Sicherheitseinstellungen über einen einzigen Befehl oder Workflow konfigurieren und für Ihre verschiedenen Systeme beibehalten.

Mehr erfahren

Mit einem konsistenten Sicherheits- und Compliance-Ansatz für Ihre Hybrid Cloud- und Multi-Cloud-Umgebungen können Sie Ihr Unternehmen besser schützen. Red Hat Enterprise Linux bietet Ihnen eine sicherheitsorientierte Basis für die Ausführung von Anwendungen in beliebigen Infrastrukturen, in Ihrem Rechenzentrum, in der Cloud und am Edge.

[Weitere Informationen](#) über das Sicherheitskonzept von Red Hat für die Hybrid Cloud



Über Red Hat

Red Hat, weltweit führender Anbieter von Open-Source-Software-Lösungen für Unternehmen, folgt einem community-basierten Ansatz, um zuverlässige und leistungsstarke Linux-, Hybrid Cloud-, Container- und Kubernetes-Technologien bereitzustellen. Red Hat unterstützt Kunden bei der Entwicklung cloudnativer Applikationen, der Integration neuer und bestehender IT-Anwendungen sowie der Automatisierung, Sicherung und Verwaltung komplexer Umgebungen. [Als bewährter Partner der Fortune 500](#)-Unternehmen stellt Red Hat [vielfach ausgezeichnete](#) Support-, Trainings- und Consulting-Services bereit, die jeder Branche die Vorteile der Innovation mit Open Source erschließen können. Als Mittelpunkt eines globalen Netzwerks aus Unternehmen, Partnern und Communities unterstützt Red Hat Unternehmen bei der Steigerung ihres Wachstums und auf ihrem Weg in die digitale Zukunft.

f facebook.com/redhatinc
t @RedHatDACH
in linkedin.com/company/red-hat

de.redhat.com
275099_0323_KVM

EUROPA, NAHOST, UND AFRIKA (EMEA)

00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI

00800 448820640

ISRAEL

1 809 449548

VAE

8000-4449549