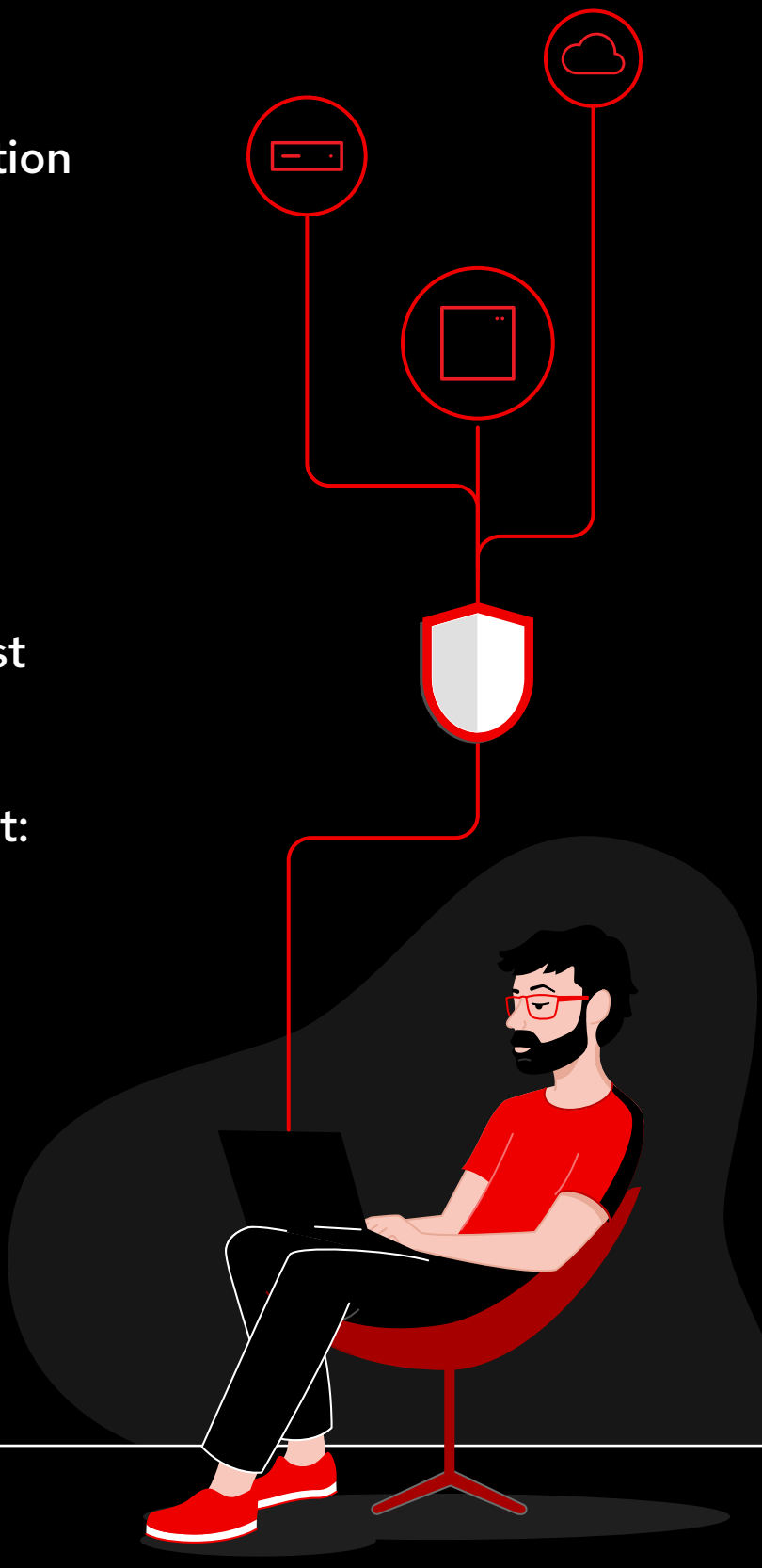
Red Hat
Enterprise Linux

Die wichtigsten Funktionen von Red Hat Enterprise Linux für das Implementieren von Zero Trust-Architekturen

Inhalt



Schutz Ihrer Organisation mit Zero Trust

Da Organisationen zunehmend Public Clouds, mobile Geräte und Remote-Arbeit nutzen, fragmentieren sich die traditionellen Netzwerkgrenzen. Dadurch entstehen neue Sicherheitsherausforderungen für IT-Umgebungen.

Organisationen sehen sich zunehmend mit kriminellen Akteuren konfrontiert, die Schwachstellen nutzen, welche aufgrund veralteter Sicherheitsparadigmen wie Ein-Faktor-Authentifizierung, implizites Vertrauen, perimeterbasierte Architekturen sowie unzureichende Verfolgung des Verhaltens von Nutzenden und Events bestehen. Da Sicherheitsbedrohungen und die Auswirkungen von Sicherheitsverletzungen weiter zunehmen, setzen sich Organisationen zunehmend für eine robustere und proaktivere Sicherheitsstrategie ein. Tatsächlich betrachten mehr als 50 % der Fachkräfte für Cybersicherheit ein verbessertes Identitäts- und Zugriffsmanagement sowie einen sicheren Zugriff auf Anwendungen als aktuelle Sicherheitsprioritäten.[1]

Zero Trust steht für einen grundlegenden Wandel darin, wie wir Vertrauen innerhalb eines Netzwerks wahrnehmen und aufbauen, und lehnt die Annahme ab, dass innerhalb des Netzwerks eine sichere Umgebung vorliegt und außerhalb des Netzwerks nicht. Das Konzept stellt das traditionelle Modell in Frage, indem es davon ausgeht, dass innerhalb oder außerhalb eines Netzwerkperimeters keinen einzelnen Nutzenden oder Ressourcen grundsätzlich vertraut werden kann. Stattdessen müssen Nutzende und Ressourcen unabhängig von ihrem Standort oder Netzwerkzugang kontinuierlich authentifiziert und autorisiert werden.

Dieses E-Book befasst sich mit Aspekten zum Aufbau von Zero Trust-Architekturen in Linux®-Umgebungen und damit, wie Red Hat® Enterprise Linux Sie beim Schutz Ihrer IT-Umgebung und Organisation unterstützen kann.

Die hohen Kosten einer sich verändernden Bedrohungslandschaft

4.45 Mio. USD

Durchschnittliche Kosten einer Datenpanne in verschiedenen Branchen und Regionen im Jahr 2023[2]

180.358 US-Dollar

Durchschnittliche Kostensenkung bei Datenpannen durch effektives Identitäts- und Zugriffsmanagement[2]

82 %

der Datenpannen im Jahr 2023 betrafen Daten, die in Cloud-Umgebungen oder in mehreren Umgebungen gespeichert waren.[2]

51 %

der Organisationen planen, ihre Investitionen in die Sicherheit infolge einer Datenpanne zu erhöhen[2]

1 *Cybersecurity Insiders, gesponsert von Fortra. „2023 Zero Trust Security Report," 2023.*

2 *IBM Security: Bericht von 2023 „Kosten einer Datenschutzverletzung", Juli 2023.*

Was ist Zero Trust?

Zero Trust ist ein Architektur-Pattern, bei dem die Sicherheit auf die einzelnen Ressourcen angewendet wird, anstatt die Sicherheit ausschließlich am Netzwerkrand oder über eine zentralisierte Sicherheitsmanagement-Lösung zu verwalten. Die Basis des Zero Trust-Modells besteht darin, dass keinem Akteur, System, Netzwerk oder Service, der innerhalb oder außerhalb des Sicherheitsperimeters operiert, implizit vertraut wird. Damit eine Ressource eine Verbindung zu einer anderen Ressource herstellen kann, muss die Verbindung sowohl authentifiziert als auch autorisiert sein, um explizites Vertrauen zu schaffen.

Wie funktioniert Zero Trust?

Das Identitäts- und Zugangsmanagement ist der zentrale Bestandteil von Zero Trust-Architekturen. Zero Trust-Architekturen sollten den Zugang zu Ressourcen standardmäßig verweigern. Jedes Subjekt, das mit einer Ressource interagieren möchte, muss für diese spezifische Interaktion ausdrücklich Zugang beantragen. Außerdem sollte das Risiko dieser Interaktion bewertet werden, bevor der Zugang gewährt wird. Deshalb ist ein Verständnis der Identität und der Eigenschaften des Subjekts von entscheidender Bedeutung. Sie müssen festlegen, wer den Zugriff beantragt, auf welche Ressourcen diese Person zugreifen muss, welchen Zweck die Transaktion hat und wie der Zugriff zeitlich, methodisch und funktional eingeschränkt werden soll.

Sobald die Zugriffsentscheidungen getroffen sind, müssen Sie Identitäten und Identitätsattribute geschützt und konsistent speichern, verwalten, kuratieren und aktualisieren. Die meisten Unternehmen verwenden ein oder mehrere Identitätsmanagement-, Directory Server- und Credential Management-Systeme zum Verwalten dieser Informationen. Außerdem sollten Sie diese Zugangsentscheidungen immer wieder überprüfen, um sicherzustellen, dass sie weiterhin gültig sind.

Eine Zero Trust-Architektur, die auf diesen Grundprinzipien basiert, kann Sie beim Schutz Ihrer IT-Umgebung und Organisation unterstützen:

1. Kein implizites Vertrauen in Akteure
2. Strategie der geringsten Berechtigung beim Zugriff
3. Standardmäßige Annahme, dass Netzwerke und Netzwerkverkehr kompromittiert sind

Dies sind die wichtigsten Grundprinzipien, die Red Hat im gesamten Red Hat Portfolio, einschließlich Red Hat Enterprise Linux, Red Hat Insights und Red Hat Identity Management als Guide für Zero Trust-Funktionen verwendet.

Was ist eine Vertrauensgrenze?

Als Vertrauensgrenze wird eine logische Trennung zwischen Komponenten bezeichnet, bei denen die teilnehmenden Subjekte einer Interaktion ihren Vertrauenszustand ändern. Diese Trennung erfolgt üblicherweise zwischen den beiden Zuständen *vertrauenswürdig* und *nicht vertrauenswürdig*. Im Allgemeinen erfordert der Übergang von *nicht vertrauenswürdig* zu *vertrauenswürdig* sowohl die Authentifizierung der Identität des Subjekts als auch die Autorisierung des Zugriffsrechts sowie der Notwendigkeit des Subjekts, auf eine bestimmte Ressource zuzugreifen.

Betriebssysteme: Die Basis für Zero Trust

Ihr Betriebssystem bildet die Basis für Ihre IT-Umgebung und Ihre Zero Trust-Architektur. Es bietet wesentliche Sicherheitsfunktionen, kontrolliert den Zugriff von Nutzenden und Anwendungen, verschlüsselt sensible Informationen und schützt Secrets, um eine sicherheitsorientierte Computerumgebung zu schaffen und zu erhalten.

Dieses Kapitel erläutert die wichtigsten Funktionen des Betriebssystems für die Einführung von Zero Trust.

Bewährte Betriebssystem-Lieferkette

Zero Trust-Modelle setzen voraus, dass Ihr Betriebssystem so sicher wie möglich ist. Zum Verringern des Risikos von Sicherheitslücken im Betriebssystem erfolgt die Bereitstellung von Red Hat Enterprise Linux über eine vertrauenswürdige Software-Lieferkette. Die statische Code-Analyse des gesamten Betriebssystems identifiziert Fehler in der Programmierung, der Speicherreferenzierung und der Validierung des Input-Streams und stellt die Compliance mit den Standardverfahren für die Programmierung sicher. Umfangreiche QE-Tests (Quality Engineering) minimieren Sicherheitsmängel vor der Auslieferung. Regelmäßige Patches für Schwachstellen bieten Abhilfe bei bekannten Problemen. Mit veröffentlichten SBOMs (Software Bills of Materials) können Sie die kuratierten, getesteten Komponenten, die Teil von Red Hat Enterprise Linux sind – einschließlich Quellcode, Open Source-Software und Libraries, Middleware und Entwicklungs-Frameworks – prüfen und bewerten.

Mandatory Access Control

Zum Implementieren einer Zero Trust-Architektur muss Ihr Betriebssystem den Zugriff auf Ressourcen auf individueller Basis isolieren und kontrollieren können. Red Hat Enterprise Linux verfügt über integrierte MAC-Funktionen (Mandatory Access Controls) mit SELinux (Security-Enhanced Linux), einer Technologie, die den Zugriff mithilfe zentralisierter Sicherheitsrichtlinien verwaltet. Granulare, anpassbare Kontrolle über Dateien, Prozesse, Nutzende und Anwendungen minimiert das Risiko einer unangemessenen Berechtigungseskalation, während Prozessisolation und Container-Trennung Angriffe durch Berechtigungseskalation abschwächen. Zudem steht die Möglichkeit, standardmäßig jeglichen Zugriff zu verweigern, im Einklang mit den Grundsätzen von Zero Trust und Least Privilege.

Testen Sie das Generieren benutzerdefinierter SELinux-Sicherheitsprofile für containerisierte Anwendungen.

Zu den **interaktiven Labs**.

Allowlists für Anwendungen

Die Verwendung von Allowlists für Anwendungen erstellt einen Index genehmigter Anwendungen und ausführbarer Dateien, die von bestimmten einzelnen Nutzenden auf einem System ausgeführt werden dürfen. Diese Praxis ergänzt die obligatorischen Zugangskontrollen, die das Verhalten von Anwendungen kontrollieren können, aber nicht wissen, welche Anwendungen vertrauenswürdig sind. Red Hat Enterprise Linux bietet integrierte Whitelists für Anwendungen, die mithilfe von File Access Policy Daemon (fapolicyd) nicht autorisierte Anwendungen erkennen und deren Ausführung auf Systemen oder in Netzwerken verhindern. Dazu haben Systemadmins mit vordefinierten und anpassbaren Richtlinien für die Allowlists mehr Kontrolle über die Anwendungen, die auf ihren Servern und in ihren Netzwerken ausgeführt werden.

Erfahren Sie, wie Sie Anwendungen mit fapolicyd zulassen können.

Zu den **interaktiven Labs**.

Moderne, skalierbare und richtlinienbasierte Verschlüsselung

Die Verschlüsselung des Daten- und Netzwerkverkehrs erhöht den Schutz für Ihre IT-Umgebung und Ihr Unternehmen. Mehrere Industriestandards, darunter National Institute of Standards and Technology (NIST) und Federal Information Processing Standard (FIPS) 140, schreiben systemweite Verschlüsselungseinstellungen vor. Mit den anpassbaren, richtlinienbasierten Kontrollfunktionen für die Datenverschlüsselung in Red Hat Enterprise Linux können Sie konsistente Konfigurationen auf Ihren Systemen anwenden, um Ihre Anforderungen zu erfüllen. Standardprofile für gängige Sicherheitsstandards vereinfachen die Compliance. Darüber hinaus optimieren automatisierte Anwendungen und Durchsetzung von Richtlinien das Management, reduzieren Fehler und kontrollieren die Entschlüsselung von Dateien und Software-Volumes.

Erfahren Sie, wie Sie systemweite kryptografische Richtlinien anwenden.

Zu den **interaktiven Labs**.

Greifen Sie auf das **interaktive Lab für individuelle Anpassungen** zu.

Datenschutz in sämtlichen Phasen

Zero Trust-Modelle erfordern, dass Daten stets gesichert sind – bei der Nutzung, der Übertragung und im Ruhezustand. Red Hat Enterprise Linux unterstützt Technologien und Funktionen, die einen kontinuierlichen Schutz Ihrer Daten bieten. Die Funktionen und der Support von Trusted Execution Environment (TEE) für AMD Secure Encrypted Virtualization (SEV) und Intel Software Guard Extensions (SGX) tragen zum Schutz der verwendeten Workloads und Daten bei. Die zentralisierte, automatisierte Einrichtung und Verwaltung verschlüsselter TLS-Verbindungen (Transport Layer Security) erhöht die Sicherheit von Daten bei der Übertragung. Dazu bieten Linux Unified Key Setup (LUKS) und Network Bound Disk Encryption (NBDE) einen konsistenten Datenschutz in sämtlichen Hybrid Cloud-Umgebungen.

Hardware-basierte Root-of-Trust

Hardwarebasierte Root-of-Trust-, Remote-Bestätigungs- und Measured-Boot-Technologien unterstützen Sie beim Überprüfen der Systemintegrität und stellen sicher, dass Ihre Systeme nicht verändert oder manipuliert wurden. Red Hat Enterprise Linux bietet wichtige Funktionen, die diese Technologien unterstützen.

- Verschieben Sie Ihre verschlüsselten Secrets aus der Software auf manipulationssichere Hardware-Geräte wie Smartcards, Hardware-Sicherheitsmodule (HSMs) und Trusted Platform Modules (TPMs).
- Verwenden Sie TPMs und erfasste Boot-Funktionen, um Hash-Messungen sicherer Boot-Prozesse und Runtime-Binärdateien kryptografisch zu berechnen und zu speichern.
- Überprüfen Sie die Boot-Daten mit Agenten für die Fernbestätigung, um festzustellen, ob Systeme kompromittiert sind, bevor Sie die entsprechenden Behebungsmaßnahmen einleiten.

Compliance Scanning

Die Non-Compliance mit Unternehmens- sowie Branchenstandards und -vorschriften kann für Ihr Unternehmen kostspielig und riskant sein. Red Hat Enterprise Linux enthält integrierte Scan Tools für Compliance und Schwachstellen wie Open Security Content Automation Protocol (OpenSCAP), mit denen Sie Audits automatisieren und vereinfachen, falsch konfigurierte Systeme finden und beheben sowie die Compliance mühelos aufrechterhalten können. Folgende Funktionen sind enthalten:

- Vordefinierte und anpassbare Compliance-Profile
- Funktionen zur Berichterstellung und Erstellung von Baselines
- Integration mit Red Hat Satellite und Red Hat Insights für umfangreiches Management
- Integrierte Basis-Sicherheitsstandards für den Payment Card Industry Data Security Standard (PCI-DSS), das Enhanced Operating System Protection Profile (OSPP), die Essential Eight des Australian Cyber Security Centre (ACSC), den Center for Internet Security (CIS) Benchmark, den Health Insurance Portability and Accountability Act (HIPAA) und die Security Technical Implementation Guides (DISA STIG) der Defense Information Systems Agency (DISA)

Verwendung von OpenSCAP für Sicherheits-Compliance und Schwachstellen-Scans

Zu den **interaktiven Labs**.

Erfahren Sie, wie Sie Schwachstellen mit Red Hat Insights beheben können.

Zu den **interaktiven Labs**.

Automatisiertes Konfigurationsmanagement

Automatisierung ist entscheidend für die Aufrechterhaltung konsistenter Sicherheitskonfigurationen und die Erfüllung von Governance- und Compliance-Anforderungen in großem Umfang. Mit den Systemrollen von Red Hat Enterprise Linux können Sie die Sicherheitskonfiguration und -verwaltung in Hybrid Cloud-Umgebungen automatisieren und die erforderliche Expertise für das Implementieren einer Zero Trust-Architektur reduzieren. Dieser vordefinierte Inhalt für die Automatisierung, der auf der Ansible® Automation Platform von Red Hat basiert, vereinfacht die Konfiguration sicherheitsbezogener Funktionen wie SELinux, NBDE, Secure Shell (SSH), kryptografische Richtlinien sowie Identitäts- und Zertifikatsverwaltung.

Testen Sie Red Hat Enterprise Linux Systemrollen.

Zu den **interaktiven Labs**.

Identitätsmanagement: Zugriffskontrolle für IT-Ressourcen

IdM-Lösungen (Identitätsmanagement) stellen sicher, dass autorisierte Nutzende – und nur autorisierte Nutzende – auf die benötigten Ressourcen zugreifen können. Durch Einbeziehen organisationsweiter Richtlinien und Technologien ermöglichen diese Lösungen die ordnungsgemäße Identifizierung, Authentifizierung und Autorisierung des Zugriffs auf Ressourcen über Identitäten, Attribute, Berechtigungen und Zertifikate.

Dieses Kapitel erläutert die zentralen Funktionen des Identitätsmanagement für die Einführung von Zero Trust.

Identitätsspeicher

Mit einem Domain Controller können Sie Identitäten, Zugriff und Richtlinien für Nutzende, Services und Hosts verwalten. Red Hat Identity Management ist Bestandteil von Red Hat Enterprise Linux und bietet einen zentralen Identitätsspeicher und Domain Controller, der den administrativen Aufwand reduziert, das Sicherheitsmanagement vereinfacht und für Konsistenz in Ihrer Umgebung sorgt. Damit können Sie sämtliche Identitäten an einem Ort speichern, Operationen konsolidieren und Richtlinien einheitlich auf die Ressourcen und Umgebungen anwenden. Dank der vereinfachten Domain-Registrierung können Sie eine vertrauenswürdige Sicherheitsgrenze schaffen und die optimierte Authentifizierung verbessert das allgemeine Benutzererlebnis.

Single Sign-On (SSO)

In Zero Trust-Architekturen erfordern die einzelnen Services, Geräte und Server eine separate Zugriffsauthentifizierung. Single-Sign-On-Systeme (SSO) vereinfachen den Zugang, indem sie einen zentralen Identitätsservice nutzen, mit dem Server nach verifizierten Nutzenden suchen können. Red Hat Enterprise Linux unterstützt OAuth 2.0 und Red Hat Identity Management, damit Nutzende sich nur einmal authentifizieren und auf mehrere Services zugreifen können und bietet so ein optimiertes IT-Erlebnis. Durch die Integration verschiedener Services, darunter die Single-Sign-On-Technologie von Red Hat, Microsoft AzureAD und GitHub, können Sie Ihre bestehenden ID-Services weiterhin nutzen und sind gleichzeitig flexibel für die Zukunft.

Integration mit anderen Systemen für das Identitätsmanagement

Die meisten Unternehmen verwenden bereits ein oder mehrere Identitätsmanagementsysteme für ihre Linux- und Windows-Umgebungen. Durch die Integration dieser Systeme in eine einzige Gesamtlösung können Sie Ihre Operationen zentralisieren, Konsistenz in Ihrer Organisation sicherstellen und die Verwaltungseffizienz verbessern. Red Hat Identity Management ist nativ in Microsoft Active Directory integriert, sodass Sie Identitäten in gemischten Umgebungen verwalten und gleichzeitig angepasste Zugangskontrollrichtlinien direkt auf Ihre Domain mit Red Hat Enterprise Linux anwenden können.

Richtlinienverwaltung

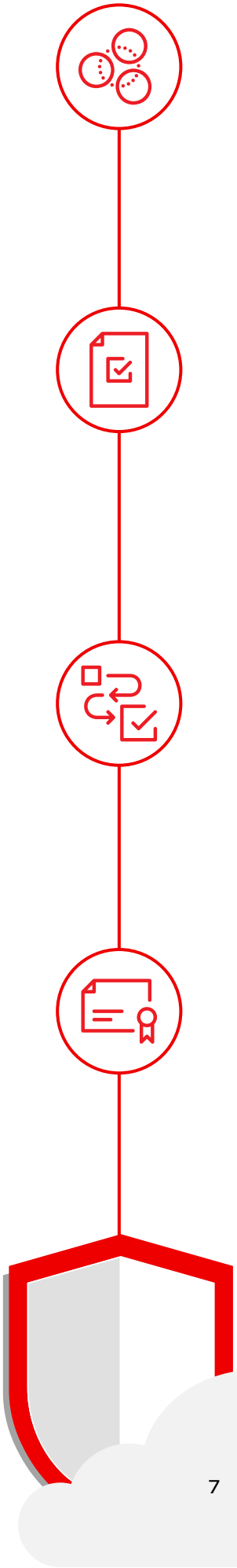
Mit einem richtlinienbasierten Ansatz für das Identitätsmanagement können Sie Konsistenz, Effizienz und Sicherheit verbessern. Mit Red Hat Identity Management können Sie richtlinienbasierte Kontrollen über eine zentralisierte Benutzeroberfläche festlegen und anwenden, um sicherzustellen, dass Identitäten, Zugriff und Ressourcen ordnungsgemäß konfiguriert sind. Anpassbare Richtlinien für Identität und Zugriff helfen dabei, Berechtigungseskalationen in Ihrer gesamten Umgebung zu begrenzen. Mithilfe von Role-based Access Controls (RBAC) können Sie dazu die Verwaltungsfunktionen des Identity Management Servers innerhalb Ihres Teams delegieren – einschließlich Authentifizierungs- und Autorisierungsverwaltung sowie Session-Aufzeichnung, -Prüfung und -Protokollierung.

Multi-Faktor-Authentifizierung

Mit der Multi-Faktor-Authentifizierung (MFA) wird eine zusätzliche Sicherheitsebene hinzugefügt, die eine mehrfache Überprüfung der Identität erfordert, bevor der Zugang gewährt wird. Red Hat Identity Management unterstützt MFA über kryptografische Geräte wie Hardware Token und Smartcards. Sie können auch mehrere Authentifizierungstypen auswählen und konfigurieren, darunter Kennwörter, Zertifikate, RADIUS (Remote Authentication Dial-In User Service), Einmalpasswörter (OTP) und PKINIT (Public Key Cryptography for initial authentication), und Standard-Authentifizierungsmethoden für sämtliche Nutzenden festlegen.

Verwaltung von Zertifikaten

Digitale Zertifikate enthalten Informationen, die zur Authentifizierung der Identität von Nutzenden, Anwendungen, Websites und anderen Subjekten benötigt werden. Sie sollten nach den Grundsätzen der geringsten Berechtigung erstellt, überwacht, erneuert und außer Kraft gesetzt werden. Red Hat Identity Management unterstützt das komplette Lifecycle Management für Zertifikate von Nutzenden, Hosts und Services. Sie können auch das Red Hat Certificate System einsetzen, eine Zertifizierungsstelle, die erweiterte Verwaltungsaktivitäten wie das Provisionieren von Smartcards, benutzerdefinierten Zertifikatstypen und geschützten Speichern für Secrets unterstützt. Durch die Unterstützung gängiger Protokolle und Standards – darunter X.509, ACME (Automatic Certificate Management Environment), SCEP (Simple Certificate Enrollment Protocol) und SSL (Secure Sockets Layer) sowie TLS – können Sie Zertifikate erstellen, die mit Ihrem IT-Ökosystem kompatibel sind. Das automatische Tracking des Ablaufdatums von Zertifikaten stellt sicher, dass rechtzeitig verlängert wird. Zudem lässt sich durch die Authentifizierung der Public Key Infrastructure (PKI) bestätigen, dass Identitäten vertrauenswürdig sind.



Einstieg in Zero Trust

Durch das Einführen einer Zero Trust-Architektur können Sie Ihre IT- und Geschäftsressourcen in einer sich schnell verändernden Welt schützen.

Red Hat bietet eine zuverlässige, integrierte und sicherheitsorientierte, fundierte Basis für Zero Trust-Architekturen. Tatsächlich verfügen Sie möglicherweise bereits über viele der Komponenten, die für das Implementieren eines Zero Trust-Modells erforderlich sind. Red Hat Enterprise Linux bietet Sicherheitstechnologien, Kontrollen, Zertifizierungen und Support für das Konzipieren, Entwickeln und Verwalten von Zero Trust-Architekturen. Darüber hinaus können Sie mit Red Hat Identity Management das Identitätsmanagement zentralisieren, Sicherheitskontrollen durchsetzen und Sicherheitsstandards in Ihrer gesamten Umgebung einhalten.

Testen Sie die Lösung noch heute mit unseren **kostenlosen, webbasierten interaktiven Labs**.

568051_0124_KVM

Red Hat