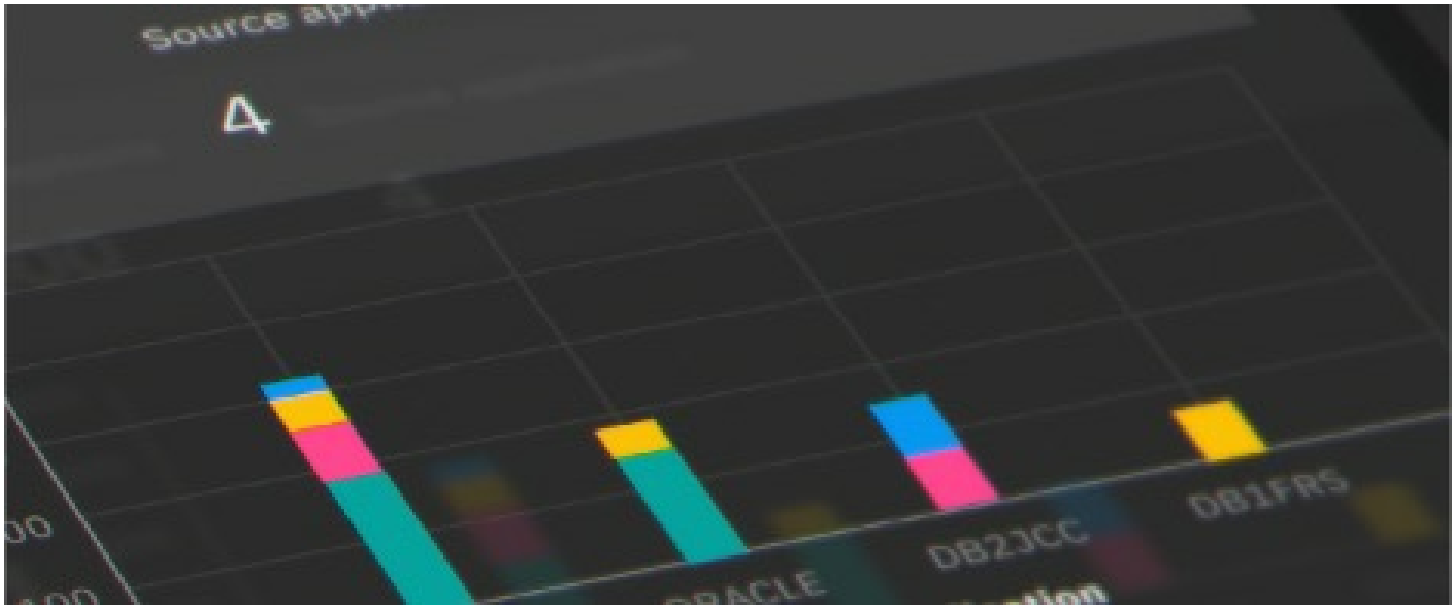
IBM DACH Newsroom

IBM entwickelt sichere KI und quantensichere Technologie weiter mit IBM Guardium Data Security Center

IBM Guardium Data Security Center bietet einheitliche, SaaS-first-Datensicherheitsfunktionen inmitten von Hybrid Cloud, KI und Quanten-Transformation

Neue Software ist Teil des umfassenden Ansatzes von IBM zum Schutz von Hybrid-Cloud und KI



ARMONK, N.Y., 22. Oktober 2024. Da Hybrid-Cloud-, KI- und Quantenrisiken das traditionelle Datensicherheitsparadigma auf den Kopf stellen, bringt IBM (NYSE: IBM) das **IBM Guardium Data Security Center** auf den Markt, das es Unternehmen ermöglicht, Daten in jeder Umgebung, während ihres gesamten Lebenszyklus und mit einheitlichen Kontrollen zu schützen.

IBM Guardium Data Security Center bietet eine einheitliche Sicht auf die Datenbestände von Unternehmen und ermöglicht es Sicherheitsteams, Arbeitsabläufe zu integrieren und Datenüberwachung und Data Governance, Datenerkennung und -reaktion, Daten- und KI-Sicherheitsmanagement sowie Kryptografiemanagement in einem einzigen Dashboard zusammenzufassen. IBM Guardium Data Security Center enthält generative KI-Funktionen, mit denen Risikozusammenfassungen erstellt und die Produktivität von Sicherheitsexperten gesteigert werden kann.

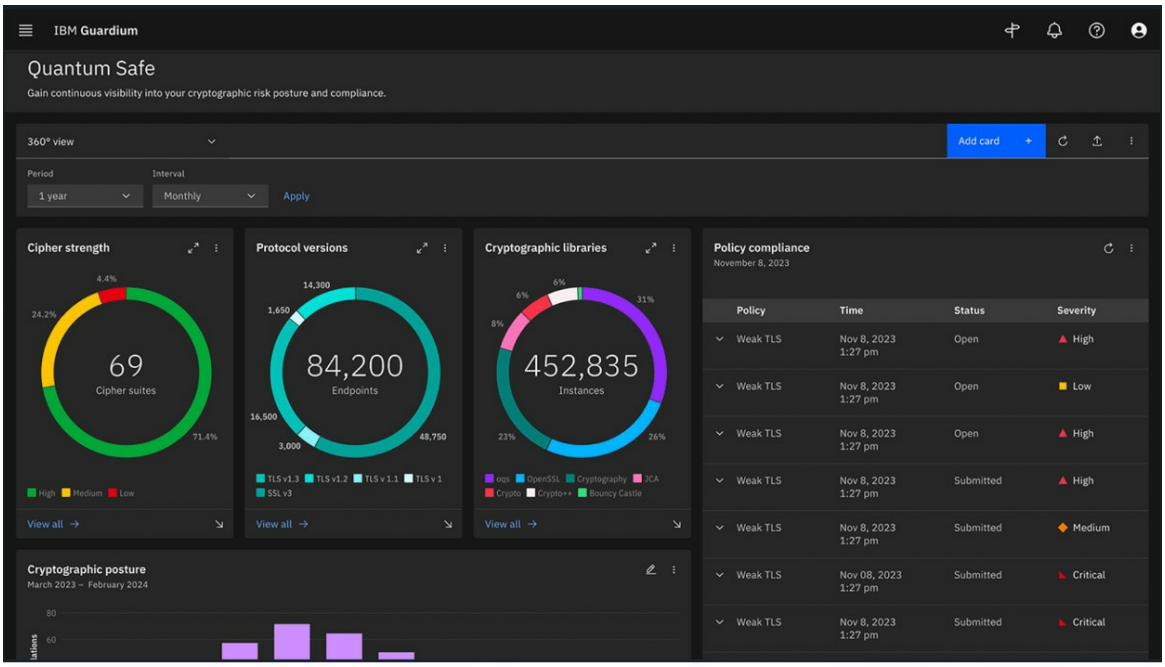
Das Center verfügt über **IBM Guardium AI Security**, eine Lösung, die Unternehmen dabei hilft, ihre KI-Implementierungen vor Sicherheitsschwachstellen und Verstößen gegen Data-Governance-Richtlinien zu schützen – und das in einer Zeit, in der die Akzeptanz generativer KI und das Risiko von „Schatten-KI“, also nicht genehmigten Modellen, stark zunimmt.

IBM Guardium Data Security Center enthält auch **IBM Guardium Quantum Safe**, eine Lösung, die Kunden dabei unterstützt, verschlüsselte Daten vor dem potenziellen Risiko künftiger Cyberangriffe zu schützen, die von böswilligen Akteuren ausgehen, die sich Zugang zu kryptografisch relevanten Quantencomputern verschaffen. IBM Guardium Quantum Safe stützt sich auf das Know-how von IBM Research – einschließlich der Post-Quantum-Kryptographie-Algorithmen von IBM – und IBM Consulting.

„Generative KI und Quantencomputing bieten enorme Chancen, aber sie bringen auch neue Risiken mit sich“, so Akiba Saeedi, Vice President, IBM Security Produkt Management. „In dieser Zeit des Umbruchs müssen Unternehmen ihre Krypto-Agilität

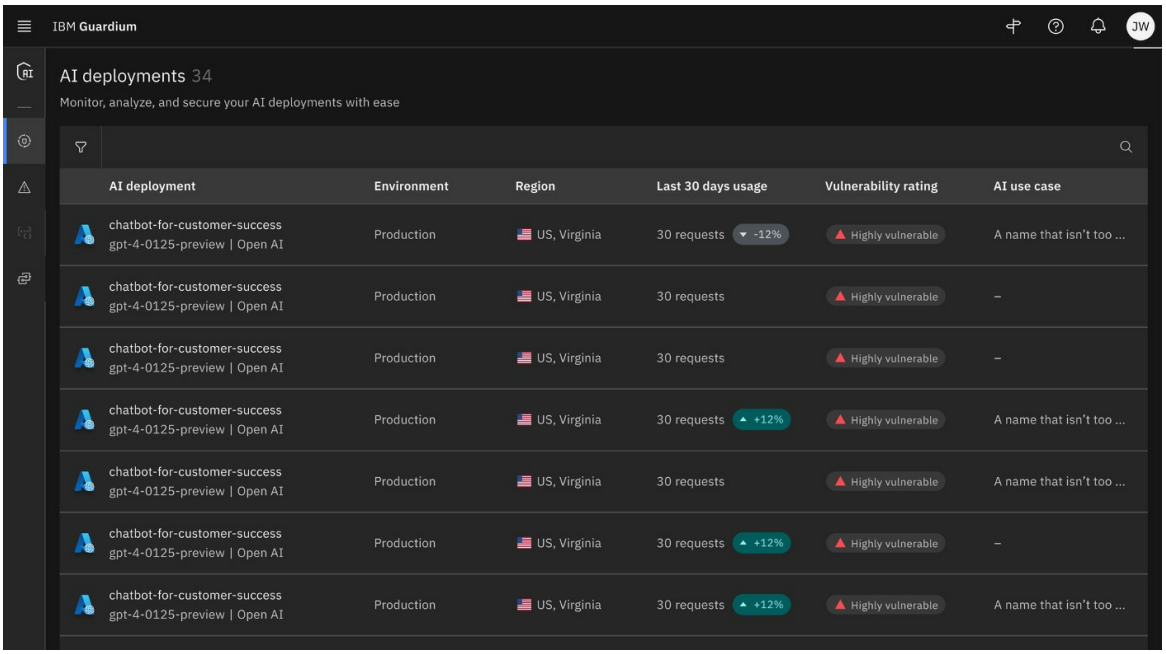
verbessern und ihre KI-Modelle, Trainingsdaten und Nutzung sorgfältig überwachen. IBM Guardium Data Security Center – mit AI Security, Quantum Safe und anderen integrierten Funktionen – bietet eine umfassende Risikotransparenz.“

IBM Guardium Quantum Safe hilft Unternehmen dabei, die kryptografische Sicherheitslage in ihrem Unternehmen transparent zu machen und zu verwalten, um Schwachstellen zu beheben und Maßnahmen zu empfehlen. Es ermöglicht Unternehmen die Durchsetzung von Richtlinien auf der Grundlage externer, interner und behördlicher Vorschriften, indem es die im Code verwendeten Kryptoalgorithmen, die im Code entdeckten Schwachstellen und die Netzwerknutzung in einem einzigen Dashboard zusammenfasst, damit Sicherheitsanalysten Richtlinienverstöße überwachen und den Fortschritt verfolgen können – ohne dass sie die über verschiedene Systeme, Tools und Abteilungen verteilten Informationen zusammenstellen müssen. Guardium Quantum Safe bietet anpassbare Metadaten und flexible Berichterstellung, so dass kritische Schwachstellen für die Behebung priorisiert werden können.



Erfahren Sie mehr über IBM Guardium Quantum Safe

IBM Guardium AI Security verwaltet Sicherheitsrisiken und Data Governance-Anforderungen für sensible KI-Daten und KI-Modelle. Die Lösung hilft dabei, KI-Implementierungen zu erkennen, die Einhaltung von Vorschriften sicherzustellen, Schwachstellen zu minimieren und sensible Daten in KI-Modellen durch eine gemeinsame Ansicht der Datenbestände zu schützen. IBM Guardium AI Security lässt sich mit IBM watsonx und anderen Anbietern generativer KI-SaaS integrieren. IBM Guardium AI Security hilft beispielsweise bei der Erkennung von „Schatten-KI“-Modellen und gibt sie dann an IBM watsonx.governance weiter, damit sie sich der Governance nicht mehr entziehen.



Erfahren Sie mehr über IBM Guardium AI Security

Ein integrierter Ansatz für eine Zeit des Umbruchs

Hybrid-Cloud-, KI- und Quantenrisiken bedeuten, dass wichtige Daten – von medizinischen Daten und Finanztransaktionen bis hin zu geistigem Eigentum und kritischer Infrastruktur – neue Formen des Schutzes erfordern. In dieser Zeit des Umbruchs brauchen Unternehmen dringend einen vertrauenswürdigen Partner und einen integrierten Ansatz für die Datensicherheit – und keinen Flickenteppich von Einzellösungen. IBM ist Vorreiter bei diesem integrierten Ansatz.

IBM Guardium Quantum Safe fügt sich in das breitereQuantum Safe-Angebot von IBM Consulting and Research ein. Die Lösung basiert auf Technologien und Forschungsergebnissen von IBM Research. Mehrere der Post-Quantum-Kryptographie-Algorithmen von IBM Research wurden inden USA kürzlich standardisiert. Das National Institute of Standards and Technology (NIST) hat damit einen entscheidenden Meilenstein gesetzt, um die verschlüsselten Daten der Welt vor dem Risiko böswilliger Akteure zu schützen, die sich Zugang zu kryptografisch relevanten Quantencomputern verschaffen könnten, um in Zukunft Cyberangriffe durchzuführen.

Die Quantum Safe Transformation Services von IBM Consulting nutzen diese Technologien, um Unternehmen dabei zu helfen, Risiken zu definieren, sie zu inventarisieren und zu priorisieren, ihnen zu begegnen – und dann den Prozess zu skalieren. In der Cybersecurity-Abteilung von IBM Consulting arbeiten zahlreiche Fachleute mit Erfahrung in den Bereichen Kryptografie und Quantensicherheitstechnologie. Dutzende von Kunden aus den Bereichen Telekommunikation, Finanzen, Behörden und anderen Branchen nutzen die IBM Quantum Safe Transformation Services, um ihre Unternehmen gegen künftige und gegenwärtige Risiken abzusichern (z. B. „harvest now, decrypt later“).

IBM erweitert heute auch sein Verify-Portfolio um dezentrale Identitätsfunktionen:**IBM Verify Digital Credentials** ermöglicht es Benutzern, ihre eigenen Berechtigungsnachweise zu speichern und zu verwalten. Die Funktion digitalisiert physische Berechtigungsnachweise wie Führerscheine, Versicherungskarten, Kundenkarten und Mitarbeiterausweise, die dann mit umfassender Sicherheit, Datenschutz und Kontrolle standardisiert, gespeichert und gemeinsam genutzt werden können. IBM

Verify ist eine IAM-Lösung (Identity Access Management), die Identitäten in der Hybrid-Cloud schützt.

Aussagen über die künftige Ausrichtung und Absicht von IBM können ohne Vorankündigung geändert oder zurückgezogen werden und stellen lediglich Ziele und Absichten dar.

Über IBM

IBM ist einer der führenden Anbieter in den Bereichen globale Hybrid-Cloud und KI sowie Consulting. Wir helfen Kunden in mehr als 175 Ländern, Erkenntnisse aus ihren Daten zu vermarkten, Geschäftsprozesse zu optimieren, Kosten zu senken und in ihrer Branche führend zu bleiben. Mehrere Tausend Behörden und Unternehmen in Bereichen der kritischen Infrastruktur, wie Finanzdienstleistungen, Telekommunikation und Gesundheitswesen vertrauen bei der schnellen, effizienten und sicheren digitalen Transformation auf die Hybrid-Cloud-Plattform von IBM und Red Hat OpenShift. Die bahnbrechenden Innovationen von IBM in den Bereichen KI, Quantencomputing, branchenspezifische Cloudlösungen und Consulting eröffnen offene und flexible Optionen für unseren Kunden. Gestützt wird das Ganze durch das langjährige Bekenntnis von IBM zu Vertrauen, Transparenz, Verantwortung, Inklusion und Service.

Besuchen Sie www.ibm.com für weitere Informationen.

Kontakt für Journalisten:

Barbara Jax

IBM Unternehmenskommunikation

barbara.jax@at.ibm.com
