„Krypto-Agilität & Governance in hybriden Infrastrukturen“

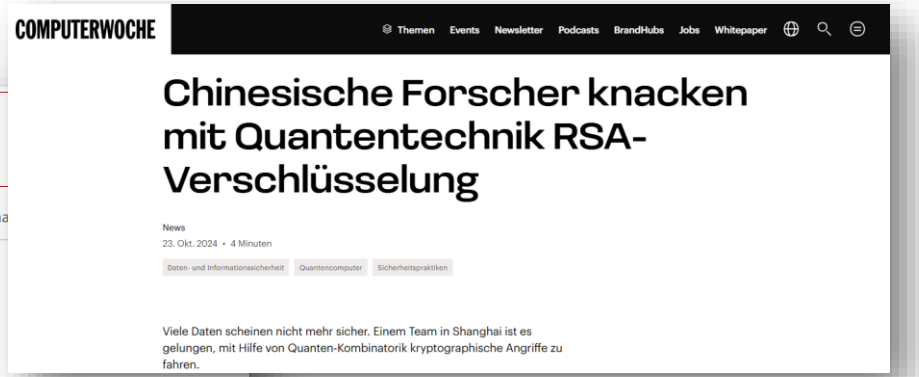
Ein Erfahrungsbericht aus der Praxis

Arthur Fischer, Senior Technical Consultant
Competence Center DevOps und Automation

17.09.2025, Congress Park Hanau

Quantentechnologie und die Folgen

Quantencomputing ermöglicht nicht nur viele wichtige Anwendungen, sondern ,
bedroht auch die kryptografischen Verfahren, die heute die Grundlage für Cybersicherheit bilden.
Quelle: BSI Impulspapier, https://www.forschung-it-sicherheit-kommunikationssysteme.de/dateien/forschung/2024-03-impulspapier-quanten-cybersicherheit.pdf



Quelle: https://www.computerwoche.de/article/3582353/chinesische-forscher-knacken-mit-quantentechnik-rsa-verschlusselung.html

Quelle: https://www.security-insider.de/risiken-quantencomputing-schutzmassnahmen-bsi-a-f447b0858fc05eb7d1cbd02b7cdb1472/

Krypto-Agilität

controlware

Warum Krypto-Agilität aktuell so präsent ist?

- Post-Quantum-Kryptografie: NIST-Standardisierungsprozess (z. B. Kyber, Dilithium)
- Regulatorik: Viele Standards (z. B. BSI TR-02102, NIST SP 800-131A, EU NIS2/DORA)
- Praxisprobleme: Viele Legacy-Systeme sind extrem „krypto-starr“ → hoher operativer Aufwand

Krypto-Agilität

controlware

Was ist Krypto-Agilität?

- Fähigkeit von Systemen, kryptographische Verfahren flexibel austauschbar
- ohne komplette Anwendungen oder Infrastrukturen neu zu bauen
- **Ziel**: schnell reagieren auf Bedrohungen, neue Standards oder regulatorische Anforderungen

Krypto-Agilität

controlware

Was ist Operational-Agilität?

- Die Fähigkeit Prozesse, Technologien und Betriebsabläufe schnell und flexibel anzupassen
- Durch flexible Strukturen, agile Teams, schnelle Entscheidungen
- **Ziel**: trotz ständigen Wandels handlungsfähig zu bleiben, Innovationen voranzutreiben und sich einen Wettbewerbsvorteil zu sichern

Der Weg zu Krypto-Agilität

controlware

Operational-Agilität

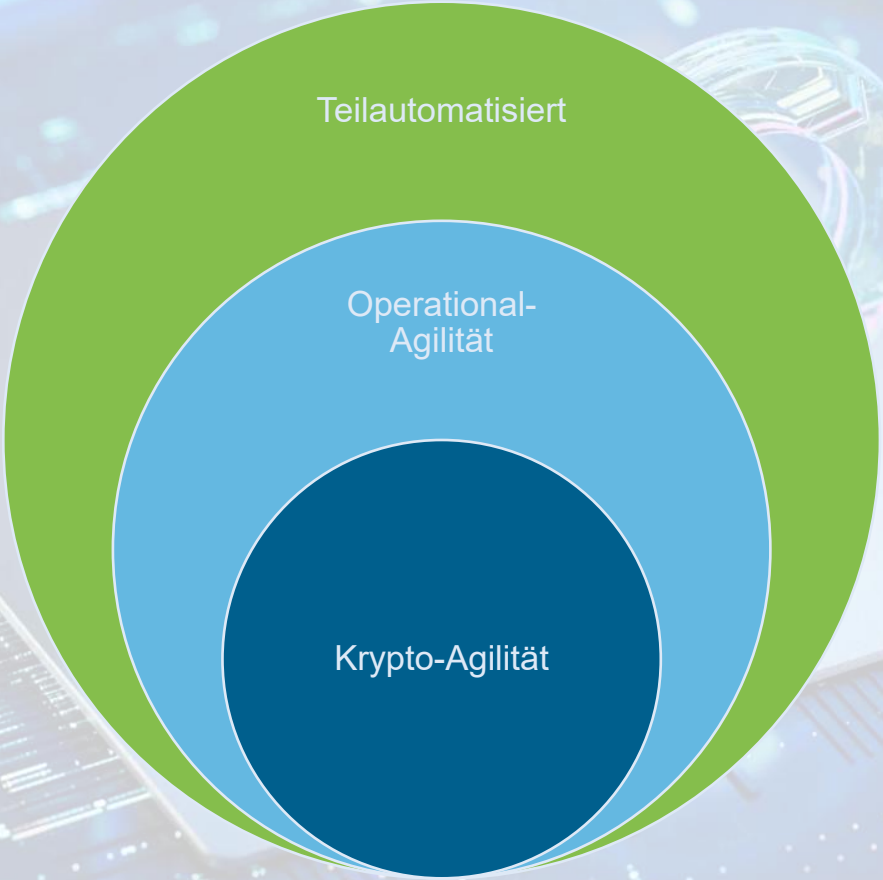
- Bereitstellung von Schlüsseln, Zertifikaten, Secrets
- Schnelle Rotation & Rollout in großem Maßstab
- Einheitliche Durchsetzung von Policies

Der Weg zu Krypto-Agilität

controlware

Operational-Agilität

- Operational Agility ist nicht selbst krypto-agil
- Aber: sie ist Grundvoraussetzung, um Verfahren und Algorithmen in der Praxis austauschbar zu machen
- Praxisbeispiel: dynamische, kurzlebige AWS-Credentials → kein Algorithmuswechsel, aber weniger Abhängigkeit von statischen Secrets → Organisation wird resilienter & anpassungsfähiger



https://postquantum.com/post-quantum/introduction-crypto-agility/

Krypto-Agilität

controlware

Beispiele

Krypto-agil

- TLS: Suites austauschen in Konfig
- Zertifikaten: PKI unterstützt wechselnde kryptographische Verfahren

Nicht krypto-agil

- TLS: Algorithmen in Code
- Zertifikaten: Legacy-Smartcards, Austausch nur per Hardware-Wechsel

Maschinen Identitäten wachsen schneller als menschliche – und die Absicherung wird komplexer

Machine Identities Growing Faster than Human Identities

Machine Identities Growing Faster than Human Identities

One of the reasons that machine identity vulnerabilities are becoming more commonplace is that there are simply more machine identities than ever — and that means more points of potential failure. The number of machine identities is growing exponentially, outpacing human identities and reshaping enterprise security priorities. It's not surprising that 79% of organizations expect the number of machine identities to grow over the next year, with 63% projecting increases of up to 50% and 16% anticipating more aggressive growth between 50-150% per year.

With machines already radically outnumbering humans in organizations, the growing disparity is clear. Cloud native technologies, AI and microservices drive this rapid growth, as workloads and containers spin up dynamically, often lasting minutes rather than years. Each instance demands unique identities to operate securely, adding to the growing complexity of machine identity security.

79% expect an increase in machine identities of up to 150% over the next 12 months

Machine Identity Security Becoming More Complex to Manage

Machine Identity Security Becoming More Complex to Manage

The expansion of digital ecosystems has dramatically expanded the complexity of managing machine identity security. Organizations now contend with a wide variety of machine identities, each requiring robust protection. Leading the list of the most challenging assets to secure are API keys (36%) and SSL/TLS certificates (34%), followed by IoT certificates, SSH keys, mobile certificates and secrets.

Security's Most Challenging Machine Identity Types

1. 36% API keys
2. 34% SSL/TLS certificates
3. 33% IoT certificates
4. 27% SSH keys and certificates
5. 26% Mobile certificates

Compounding this complexity is the sheer volume and velocity of machine identities, which are rapidly growing as organizations adopt cloud native technologies and IoT devices at scale. Protecting these machine identities is no small task. Key challenges are split pretty evenly, including the ability to quickly revoke and replace certificates, identifying who controls access to applications or devices using a machine identity, pinpointing the locations or applications where machine identities are in use, maintaining accurate inventories and determining who is authorized to access these identities.

Security's Machine Identity Challenges

1. 38% Quickly revoking and replacing machine identities
2. 38% Identifying the business group or administrator who controls access to the application or device using the machine identity
3. 37% Identifying the location or application where the machine identity is in use
4. 36% Gaining an accurate inventory of machine identities
5. 35% Understanding who is authorized to access and use the machine identity

Despite the rising stakes, automation remains underutilized. Given the nature of today's modern networks, an alarming 34% of organizations still use manual or non-automated methods to manage their machine identity lifecycles. This limits visibility, increases risks and slows response times to potential threats.

34% still use manual or non-automated methods to manage machine identity lifecycles

Quelle: https://www.cyberark.com/state-of-machine-identity-security-report/

Governance

controlware

Warum Governance?

- Governance = Regeln, Verantwortlichkeiten, Prozesse

- Anforderungen: Nachvollziehbarkeit, Zuständigkeiten, Auditierbarkeit und Policy Enforcement u.a.
  - Welche Algorithmen erlaubt/verboten?
  - Welche Schlüsselgrößen?
  - Rotationsintervalle

Governance, Krypto- und Operational-Agilität

controlware

Fazit

- Krypto-Agilität ≈ Algorithmus-Agilität + Operational-Agilität
  - Ohne Automatisierung → Agilität bleibt Theorie
  - Mit Automatisierung → Agilität wird Realität

- Krypto-Agilität = Fähigkeit zur Umsetzung (das „Wie & Wie schnell“)

Governance, Krypto- und Operational-Agilität

controlware

Fazit

- Governance = Steuerung & Kontrolle (das „Was & Warum“)
- Maschinen-Identitäten müssen sinnvoll berechtigt und geschützt werden

Beispiel: Zertifikatserneuerung

Dynamische Zertifikate

Google

BLOG POST | MAR 13, 2023

Google Announces Intentions to Limit TLS Certificates to 90 Days: Why Automated CLM is Crucial

Share this Subscribe

On March 3, Google announced in its "Moving Forward, Together" roadmap the intention to reduce the maximum possible validity for public TLS certificates from 398 days to 90 days, in a future policy update or a CA/B Forum Ballot Proposal. This drop to only 90 days maximum validity will mean major changes for the industry.

Contributor

Tim Callan
Chief Experience Officer

Quelle: https://securityboulevard.com/2023/03/google-announces-intentions-to-limit-tls-certificates-to-90-days-why-automated-clm-is-crucial/

Beschlossen: Lebensdauer für TLS-Serverzertifikate sinkt auf 47 Tage

Von derzeit maximal dreizehn Monaten sinkt die Gültigkeit auf anderthalb. Allerdings mit jahrelanger Übergangsfrist für Admins.

439

Die Web-PKI und das CA/Browser-Forum gefällig zu visualisieren, fällt selbst der KI recht schwer. (Bild: Erstellt mit Grok für heise security / Bearbeitung: cku)

16.04.2025, 08:42 Uhr Lesezeit: 3 Min. | Security

Quelle: https://www.heise.de/news/47-Tage-CAs-und-Browserhersteller-beschliessen-kuerzere-Laufzeit-fuer-Zertifikate-10352867.html

Krypto- und Operational-Agilität

controlware

ACME-Clients

365 / 47 = 7,7

7,7 * 2000 = 15.400

15.400 / 365 =

Krypto- und Operational-Agilität

ACME-Clients

Krypto- und Operational-Agilität

controlware

Automatisierte Zertifikatsbereitstellung (ACME, cert-manager, API-driven PKI)

- Zertifikate werden automatisch ausgestellt, verteilt und erneuert
- Kein manueller Aufwand bei Schlüsselwechseln, weniger Risiko durch abgelaufene Zertifikate
- Beitrag zu Krypto-Agilität: schafft die Grundlage für schnelle Algorithmus-Wechsel bei Signaturen oder Schlüssellängen

Krypto- und Operational-Agilität

controlware

Automatisierte Zertifikatsbereitstellung (ACME, cert-manager, API-driven PKI)

- Streng genommen Operational-Agil
- Statt reiner Zertifikatserneuerung auch Wechsel des Algorithmus oder Schlüssellänge möglich
- Applikation bekommt nichts

Wechsel der Schlüssellänge von 2048 auf 4096 Bit am Endpunkt quasi umgehend.

Krypto- und Operational-Agilität

controlware

CSC – Austausch Root CA

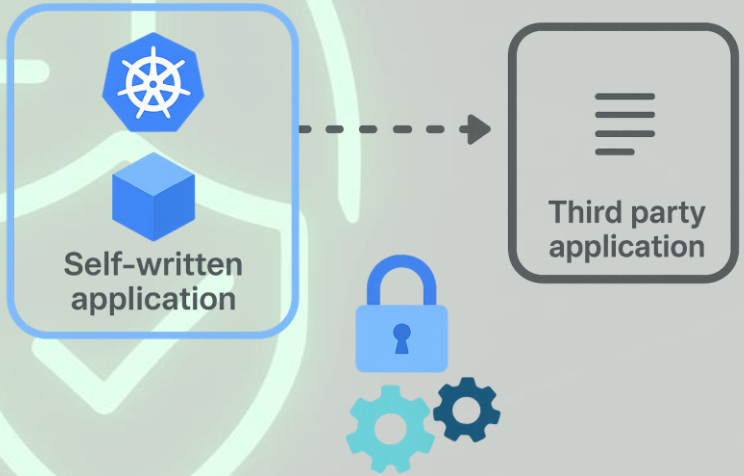
- CA Austausch erforderlich
- Einige hundert Maschinen betroffen
- Alle Maschinen mit RedHat Ansible provisioniert
- CA Austausch trivial: Eine Anpassung => innerhalb weniger Minuten Trust auf allen Maschinen

Umgesetzte Anwendungsfälle bei unseren Kunden

controlware

Nachrichten Signatur als Service

- Containerisierte **eigene Applikation** mit Kommunikation zu Third-Party-App
- Herausforderung: Signatur für Kommunikation (eigene Lösung oder über Service erledigen)
- Entscheidung: **Service Lösung**
  - Abstrakter Endpunkt
  - Algorithmen & Schlüssel flexibel in Sekunden änderbar
  - **Keine Code-Änderungen notwendig**



Umgesetzte Anwendungsfälle bei unseren Kunden

controlware

Programmatischer CISCO APIC Zugriff

- Requests aus GitLab Pipeline heraus
- Später Signatur durch Terraform, private Key wird programmatisch bezogen
- Algorithmus, Bits und Schlüssel nach Vault abstrahiert

HashiCorp Terraform

HashiCorp Vault

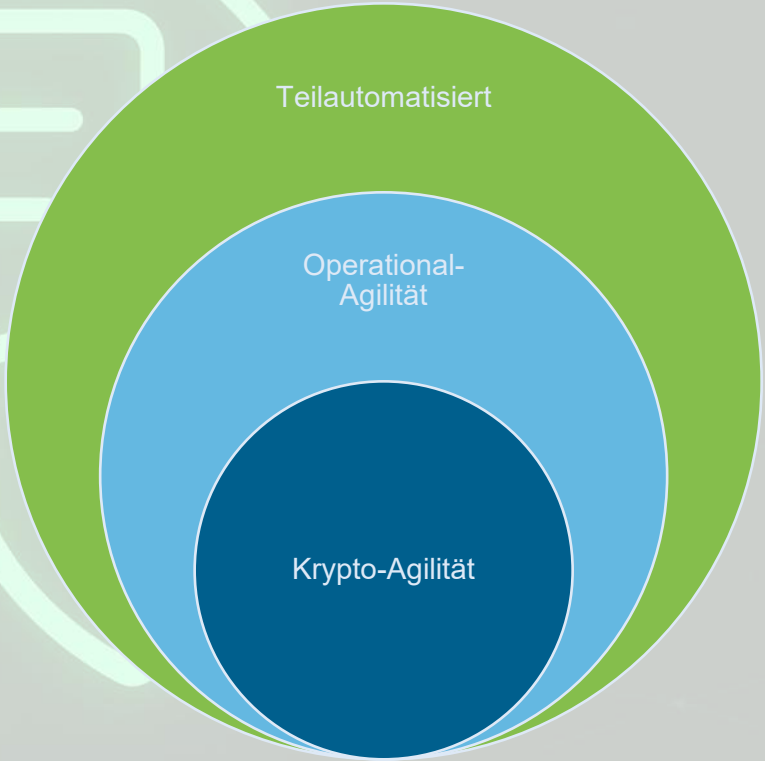
Umgesetzte Anwendungsfälle bei unseren Kunden

controlware

Dynamische Credentials + automatisierte Accounterstellung

- **Herausforderung**: Viele Product-Teams. Jedes Team braucht Accounts, Netzwerk-Konfigurationen u.a.

- Team kann Infrastruktur mit kurzlebigen, dynamischen Credentials ausrollen




KMIP

Umgesetzte Anwendungsfälle bei unseren Kunden

controlware

KMIP

- Compliance-Anforderung: Verschlüsselung von VMs in vSphere
- Krypto-Agil?
  - Data-Encryption-Key ✗
  - Key-Encryption-Key

Umgesetzte Anwendungsfälle bei unseren Kunden

KMIP

- Compli
- Krypto-
  - Data-E
  - Key-E

Umgesetzte Anwendungsfälle bei unseren Kunden

controlware

Statische/dynamische Schlüssel

Ein statisches Servicekonto für Deployments könnte in falschen Händen die gesamte Infrastruktur löschen.

Secret Management nutzt dynamische, kurzlebige Anmeldeinformationen für jedes Deployment.

Zertifikats Automatisierung

Ab Ende 2025 sind SSL-Zertifikate nur noch 90 Tage gültig. Automatisierung ist essenziell, da Hunderte Mandanten und Systeme integriert werden müssen.

Secret Mgmt. kann als Zertifikats-Proxy zur automatischen Verteilung von Zertifikaten genutzt werden.

KMIP Disk Verschlüsselung/vTPM

Festplattenverschlüsselung schützt Domain Controller vor Daten- und Passwort-diebstahl. vTPM bietet zusätzlichen Schutz.

Secret Mgmt. verwaltet sicher die Festplatten-verschlüsselung z.B. auf Domänencontrollern via KMIP und Cloud-Protokolle.

SSH CA für sicheren SSH Zugriff

SSH-Schlüssel auf Zielsystemen umgehen Passwortregeln und sind ein hohes Risiko. Private Schlüssel sind nicht sicher gespeichert.

Secret Mgmt. kann als SSH-CA genutzt werden und erlaubt nur kurzlebige, validierte SSH-Schlüssel mit MFA-Authentifizierung.

„Vermeidung von Klartext-Passwörtern in Konfigurationsdateien für die maschinelle Kommunikation“ wie Datenbankzugriff, Monitoring-Agent-Zugriff, API-Zugriff, Multicloud-DR...

HSM
HA
KMIP
Transit
Platformagnostisch
DB Credentials
Cloud Credentials
Machine Identity

Hashicorp Vault

controlware

Transit und PKI Secret Engines

Was wir gewinnen:

- Algorithmus-Abstraktion
- Schlüsselrotation & Versionierung
- API-Kapselung
- Governance & Compliance

Secret Management mit HashiCorp Vault

controlware

HashiCorp Vault ist eine Lösung zur **Verwaltung kryptografischer „Machine-to-Machine (M2M) Secrets“.**

HashiCorp Vault kümmert sich um deren **Generierung, Verteilung, Speicherung, Rotation und Löschung,** um Datensicherheit und Integrität zu gewährleisten.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen benutzerdefinierten Baustein veröffentlicht, der vom Bundesamt für Soziale Sicherung erstellt wurde.

Quelle:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Benutzerdefinierte_BS/BS_Secrets_Management_mit_Hashicorp_Vault.html

Bild-Quelle: Adobe Stock

Secret Management als Controlware Managed Service

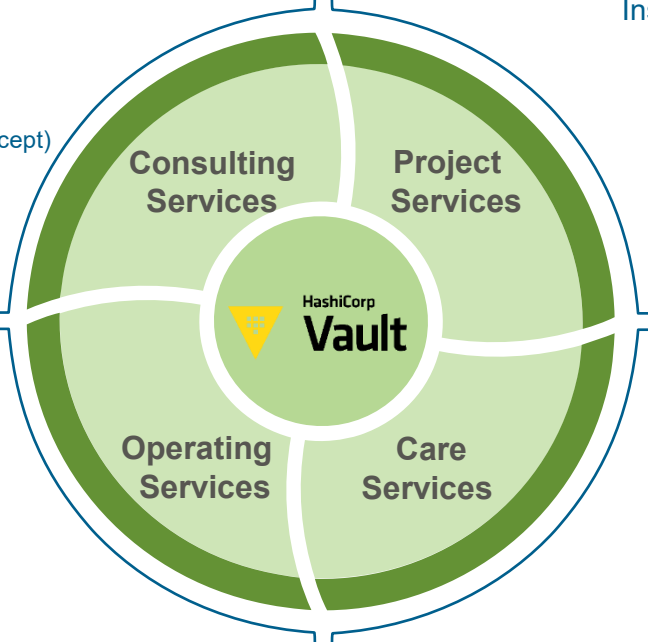
Controlware begleitet Kunden von der Idee bis zur erfolgreichen Umsetzung – und darüber hinaus.

Consulting

- Anforderungs- und Marktanalyse
- Strategieberatung und Konzeption
- Design- und Machbarkeitsstudien
- Machbarkeitsnachweis (Proof-of-Concept)
- Konzept- /Designreviews
- Entscheidungsvorlagen
- Innovationsworkshops

Projekte

- Installations- und Migrationskonzepte
- Projektmanagement / -controlling
- Remote- und On-Site-Installation
- Internationale Projekte
- Staging
- Produktivsetzung (Use-Cases)
- Schulungen



Managed Service (COS)

- 24/7 Managed Services
- Infrastructure Operating Services
- Cyber Defence Services
- Managed Cloud Services

Wartung (CCS)

- 24/7 Service-Organisation
- Service Desk
- Remote Diagnose
- Expertenhotline

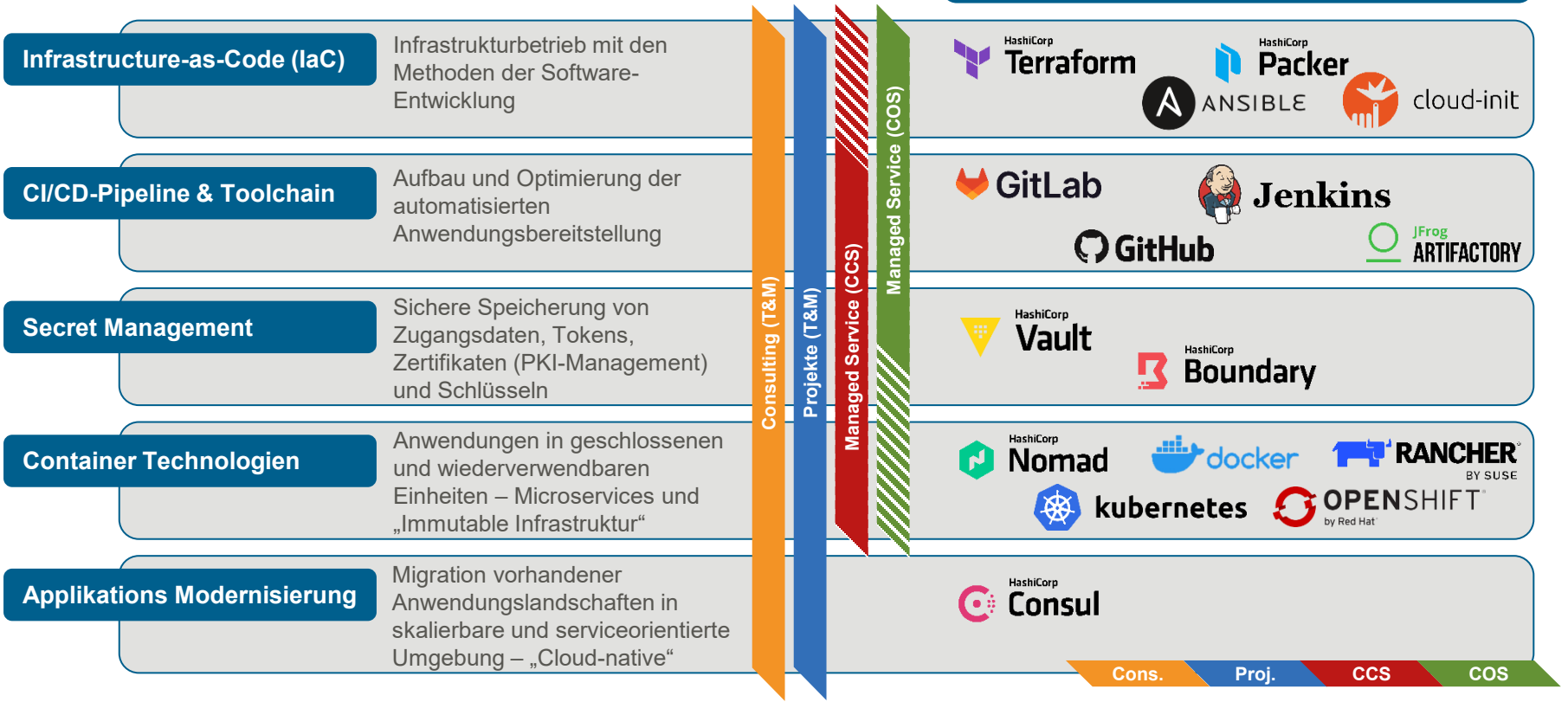
Bild-Quelle: https://www.it-daily.net/it-management/digitalisierung/fuenf-prioritaeten-fuer-einen-stoerungsfreien-it-betrieb

Competence Center DevOps & Automation

controlware

Themen, Lösungen und Leistungen

Technologie-Unabhängigkeit: Data Center & Cloud



Kundenstimmen

Das Controlware-Projektteam hat stets einen **proaktiven Ansatz** gezeigt, um den Status quo in Bezug auf **Lösungsdesign, Architektur und Governance** in Frage zu stellen.

Das Controlware-Team fördert ein **starkes Gefühl der Einigkeit und Zusammenarbeit und verkörpert den Geist eines Teams** anstelle einer Kunden-Lieferanten-Beziehung, die Synergien zwischen uns schafft.

Das Controlware-Team hat in Bezug auf seine Leistungen und Zusagen stets **Zuverlässigkeit** bewiesen und damit das **Vertrauen** in seine Fähigkeit gestärkt, Ergebnisse auf verlässliche Weise zu liefern.

Controlware hat durchweg ein **hohes Maß an Fachwissen** und Kenntnissen in ihrem Bereich bewiesen.

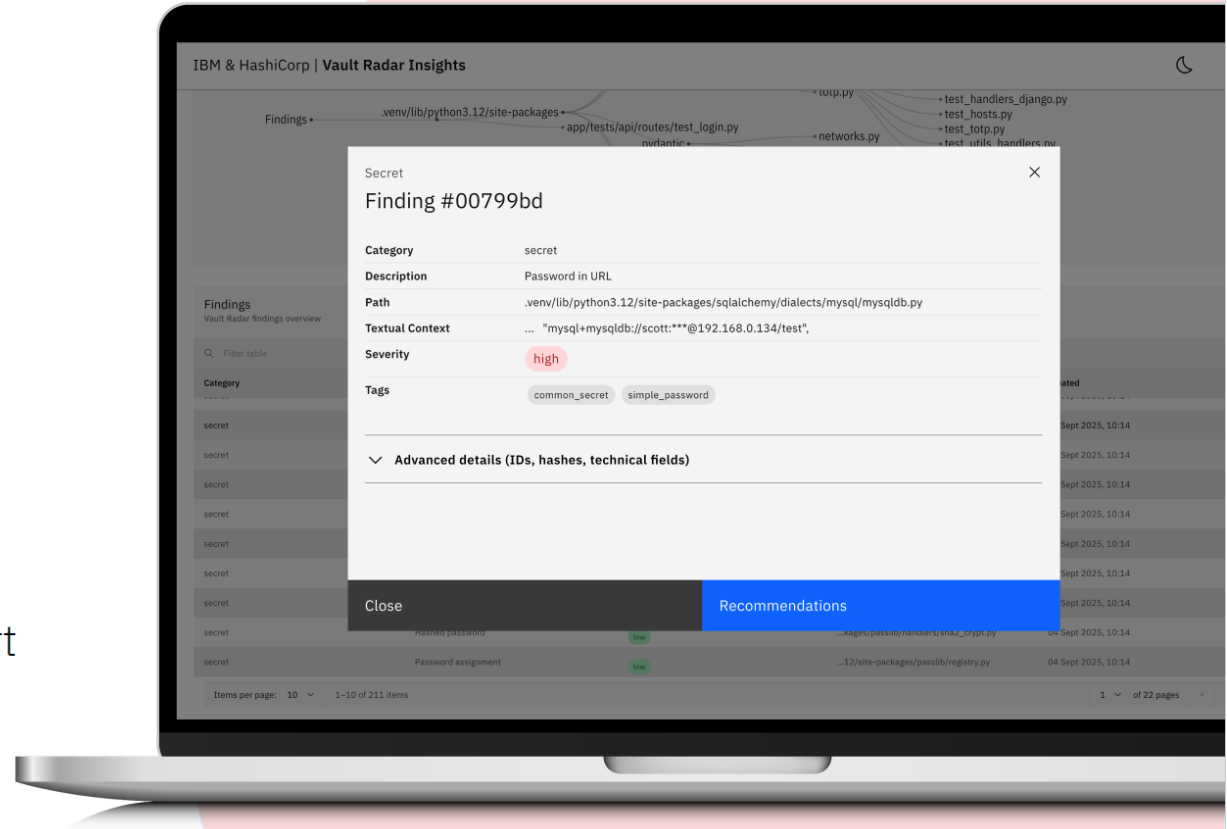
Wir schätzen es, dass sich das Controlware-Team weitgehend **an unsere etablierten Verfahren gehalten und unsere bevorzugten Tools eingesetzt hat**.

Bild-Quelle: Foto von Controlware Security Day 2024

IBM **Client Engineering**

Sind Ihre Secrets sicher?

- Kostenloses Workshop
- On-Prem-Scan der Anwendungslandschaft
- Detaillierter Findings-Report

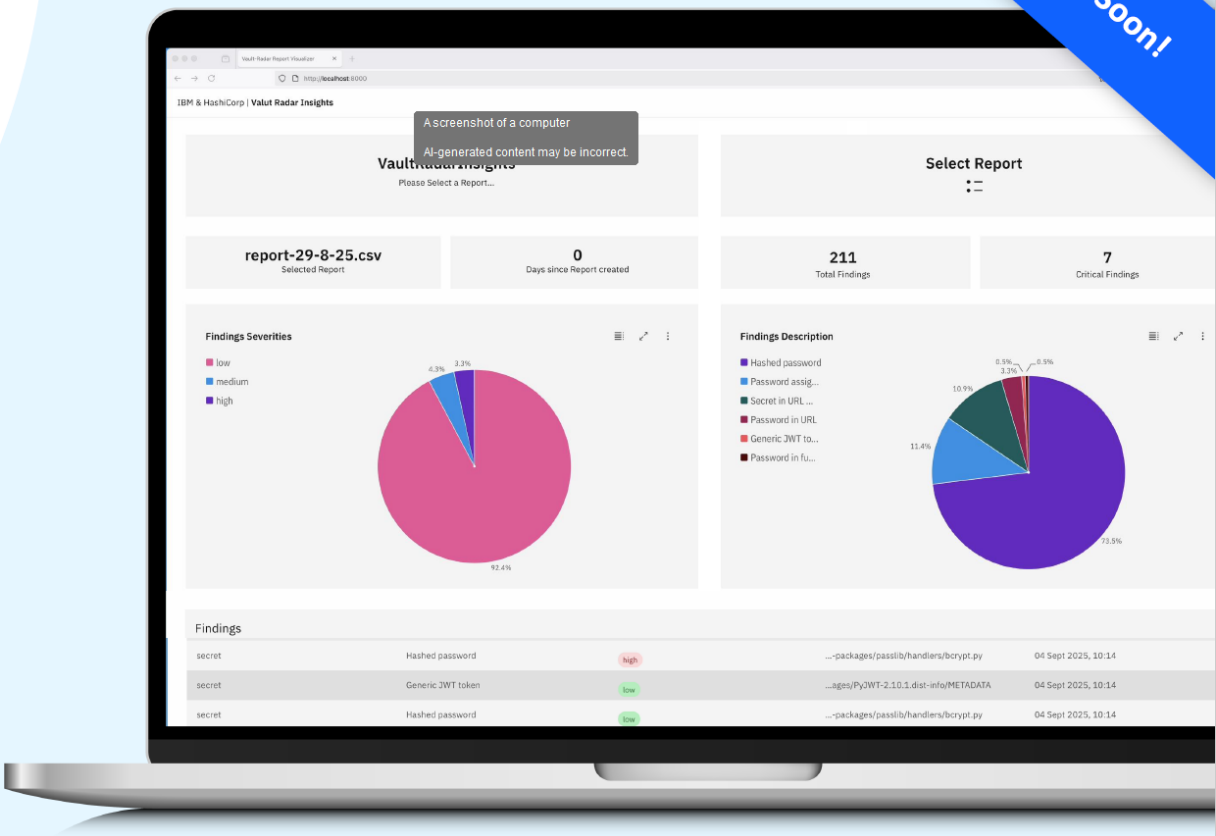


IBM HashiCorp an IBM Company

IBM **Client Engineering**

Vault Radar Assessment

100% On-Prem



IBM HashiCorp an IBM Company

Exklusives Angebot für Teilnehmer des Security Day

Beratungsgespräch:
One Hour of DevOps & Automation
One Hour of Krypto- & Operational-Agility
Vault Radar Assessment

Controlware Crypto-Workshop zum Schutz kritischer Daten durch zukunftssichere Kryptographie

Bild-Quelle: https://www.linkedin.com/pulse/pre-sales-call-planning-heres-what-you-need-know-joe-arioto/

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön eine kleines Präsent.