

Identity Resilience im Gesundheitswesen

Ausfallzeiten senken, Versorgungssicherheit stärken

Marius Booms

Account Executive Healthcare
Rubrik

Severin Oosterveld

Sr. Sales Engineer
Rubrik

AGENDA

1 | **Warum jetzt? Identity und Cyber Recovery im Fokus**

2 | **Identitäten als Einfallstor**

3 | **Wie Rubrik helfen kann**

4 | **Fragen & Antworten**



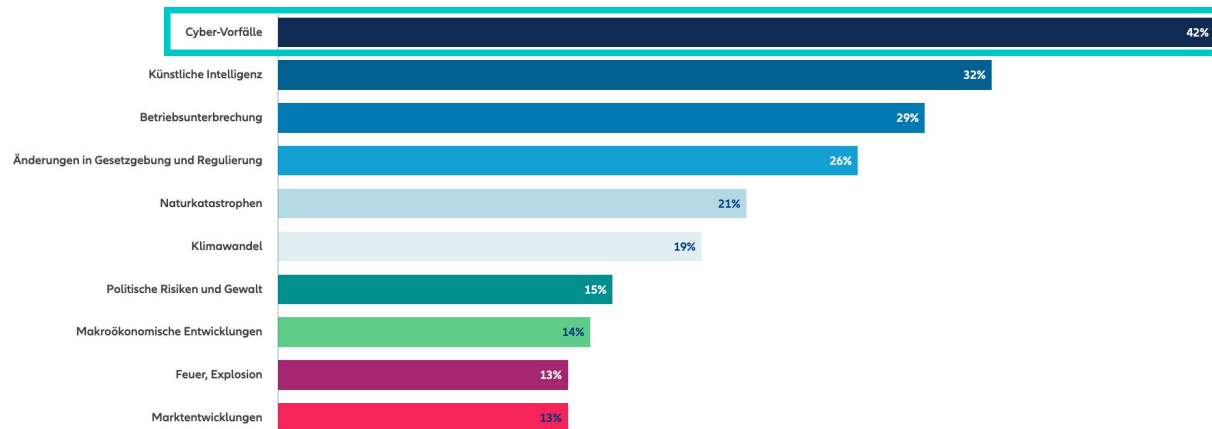
Warum jetzt? Identity und Cyber Recovery im Fokus



Top 10 Geschäftsrisiken weltweit im Jahr 2026

Allianz Risiko Barometer 2026

Basierend auf den Antworten von 3,338 Risikomanagement-Experten aus 97 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Allianz Commercial News & Insights

Quelle: Allianz Commercial

Vollständige Datenzerstörung

Erster KI-Agent führt autonomen Ransomware-Angriff durch

6. Juli, 2026 08:36



Quelle: <https://www.it-daily.net/it-sicherheit/cloud-security/ki-agent-ransomware-angriff>



Was andere Kliniken uns sagen



1 RZ Modernisierung → Kein garantierter, planbarer Wiederherstellungspunkt bei Cyberangriff

- Backups, die niemand nachträglich verändern oder löschen kann
- Automatische Warnung bei ungewöhnlichen Datenveränderungen
- Klarer letzter unversehrter Datenstand zum Zurückspringen

2 Cloud-Migration + Identity-Gap (AD/ EntraID) → Kein ausreichendes Backup für die Identität selbst

- Regelmäßige Sicherung von Konten, Gruppen und Zugriffsregeln
- Schnelle Rücksetzung nach Konto- oder Rechtemissbrauch
- Nachvollziehbarkeit des letzten unauffälligen Berechtigungsstands

3 KRITIS-Pflicht & NIS-2 → Manuelle Nachweisführung bindet knappes IT-Personal

- Prüfsichere Berichte auf Knopfdruck statt manueller Zusammenstellung
- Lückenlose Dokumentation aller Wiederherstellungstests als Nachweis
- KI-gestützte Erstellung der 72h-Meldung bei einem Sicherheitsvorfall

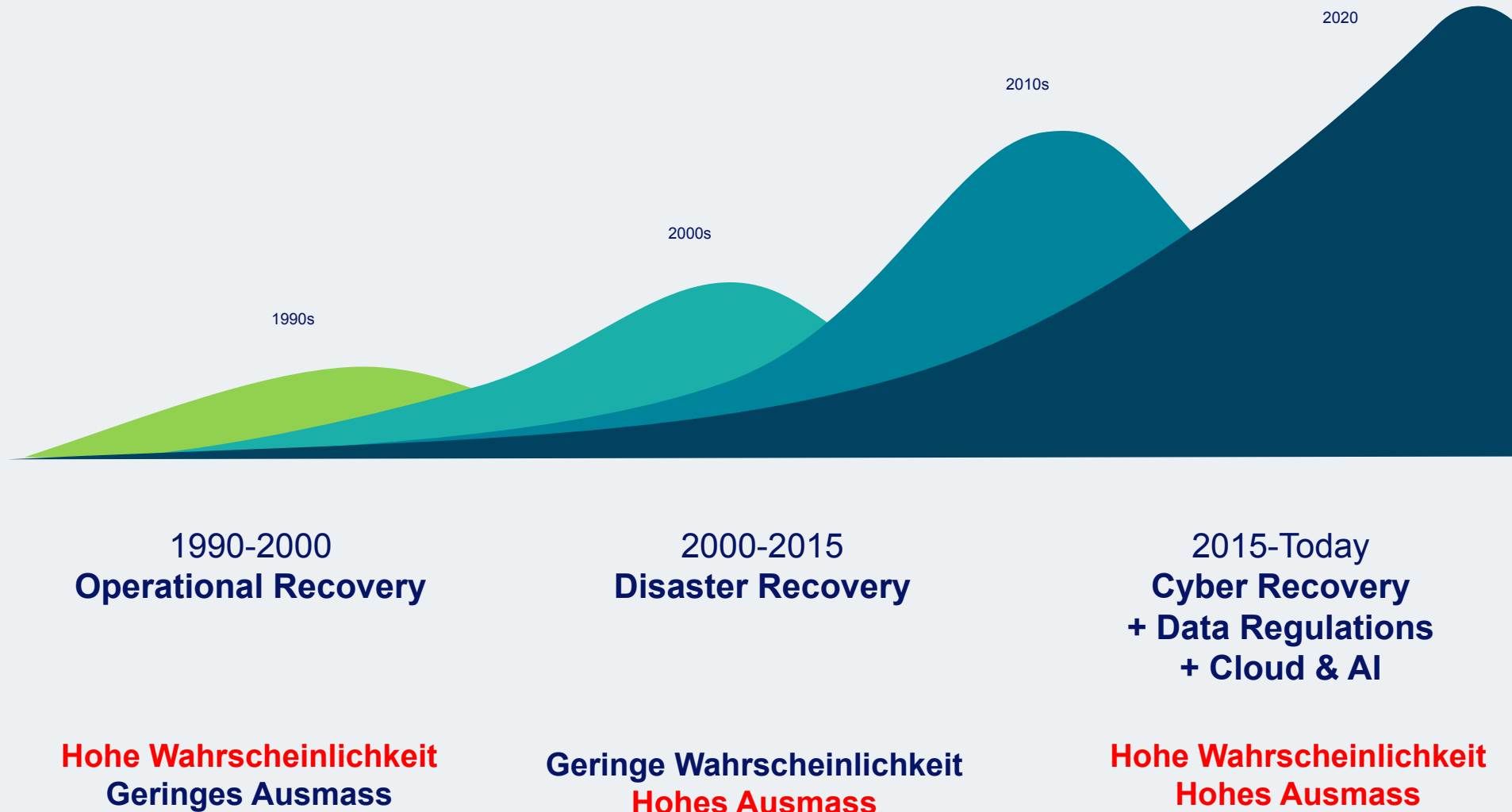


Frage #1

Aktuelle Identity-Umgebung: Welchen Identitätsprovider nutzen Sie primär?

Identitäten als Einfallstor

Evolution der IT-Resilienz



Mehr Ausgaben, dennoch mehr Ausfälle

Angriffsvektoren ändern sich

29 Min

durchschnittliche
breakout time
(kürzeste: 27
Sekunden) ¹

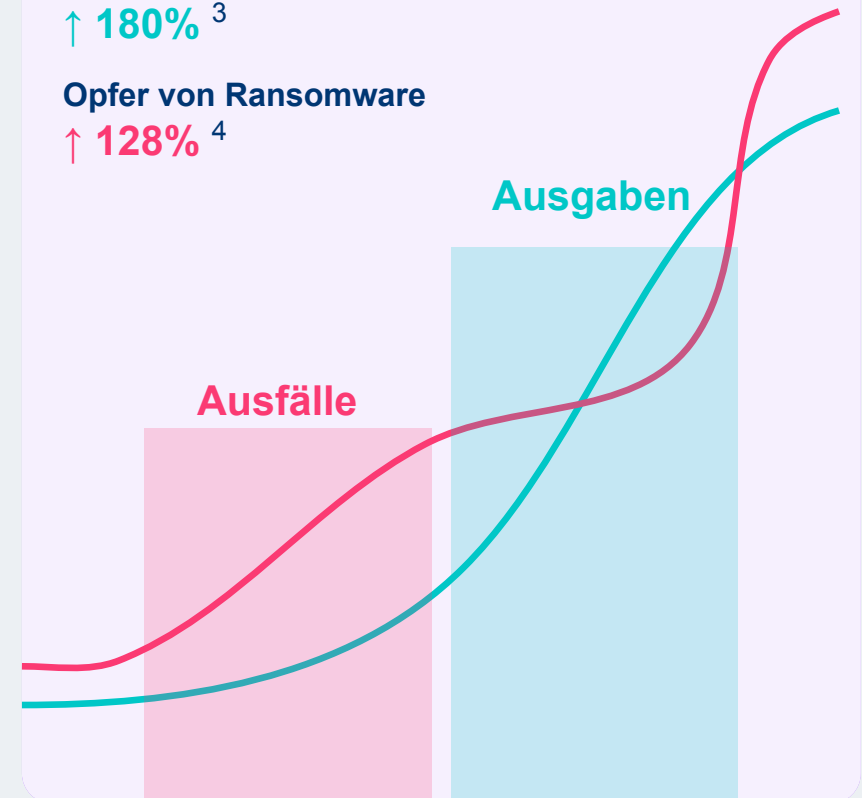
82%

von Erkennungen
sind **Malware-frei** ²

**Trotz erhöhten Cyber-Budgets
passieren mehr Ausfälle**

Global Ausgaben in Cyber Security
↑ **180%** ³

Opfer von Ransomware
↑ **128%** ⁴



¹ CrowdStrike 2026 GTR: <https://www.crowdstrike.com/en-us/global-threat-report/>

² CrowdStrike 2026 GTR: <https://www.crowdstrike.com/en-us/global-threat-report/>

³ <https://www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/>

⁴ <https://securityaffairs.com/157759/reports/ransomware-attacks-2023-report.html>



Moderne Identitätsangriffe

01



Initialer Zugriff

- Phished credential
- Übernommene Session
- Helpdesk MFA reset

Viel einfacher mit KI

02



Privilege Escalation

- Account zu account
- Mehr und mehr Rechte
- Bis hoch zum Admin

03



Laterale Bewegung

- Zw. Cloud und on-prem
- Weitere IdPs
- AD sync server

04



Persistenz

- Schatten-Admin
- Policy-Ausschluss
- IdP unter Kontrolle

05

Ausführung

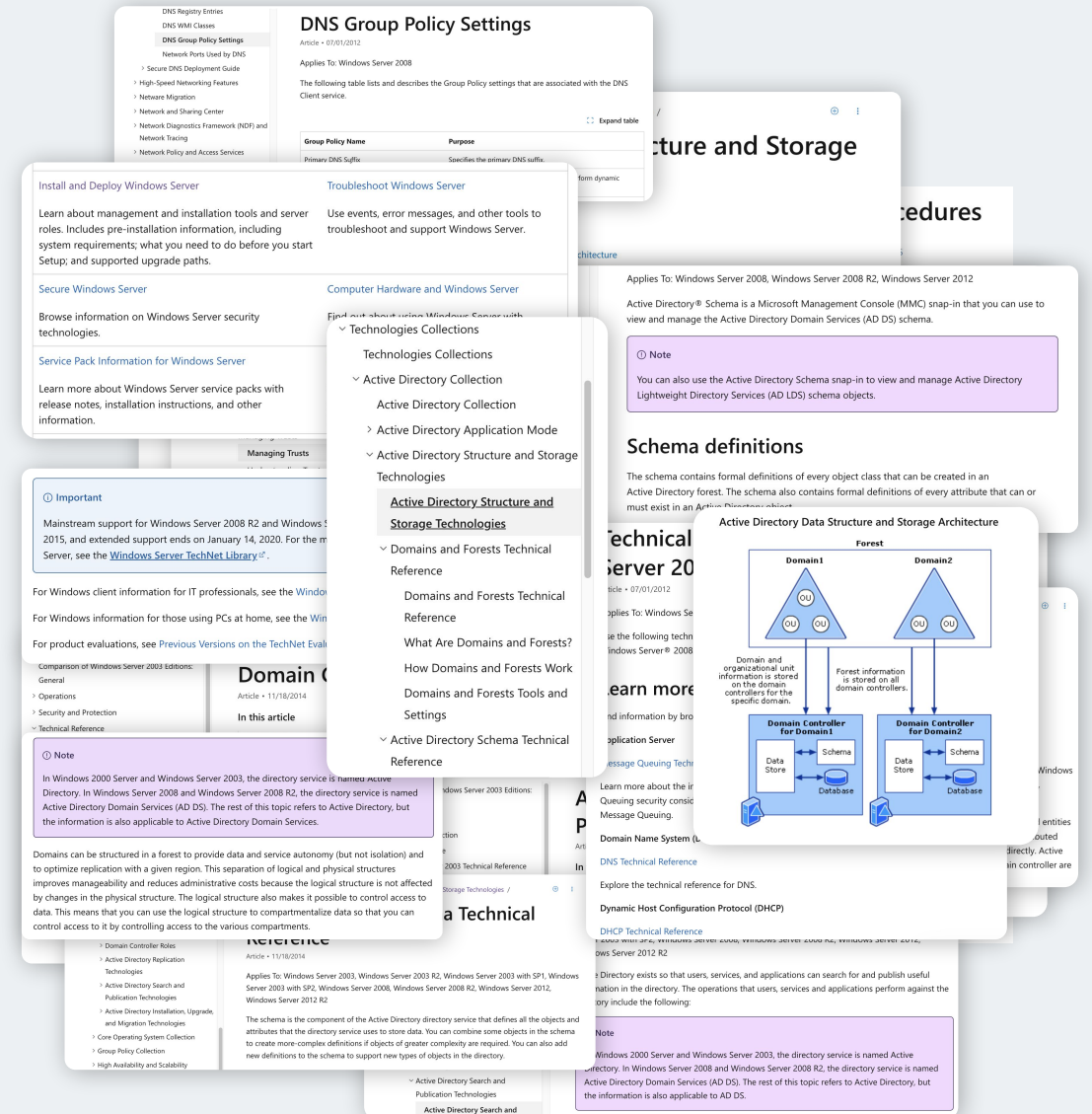
- Backups gelöscht
- Daten verschlüsselt
- Spionage, o.ä.



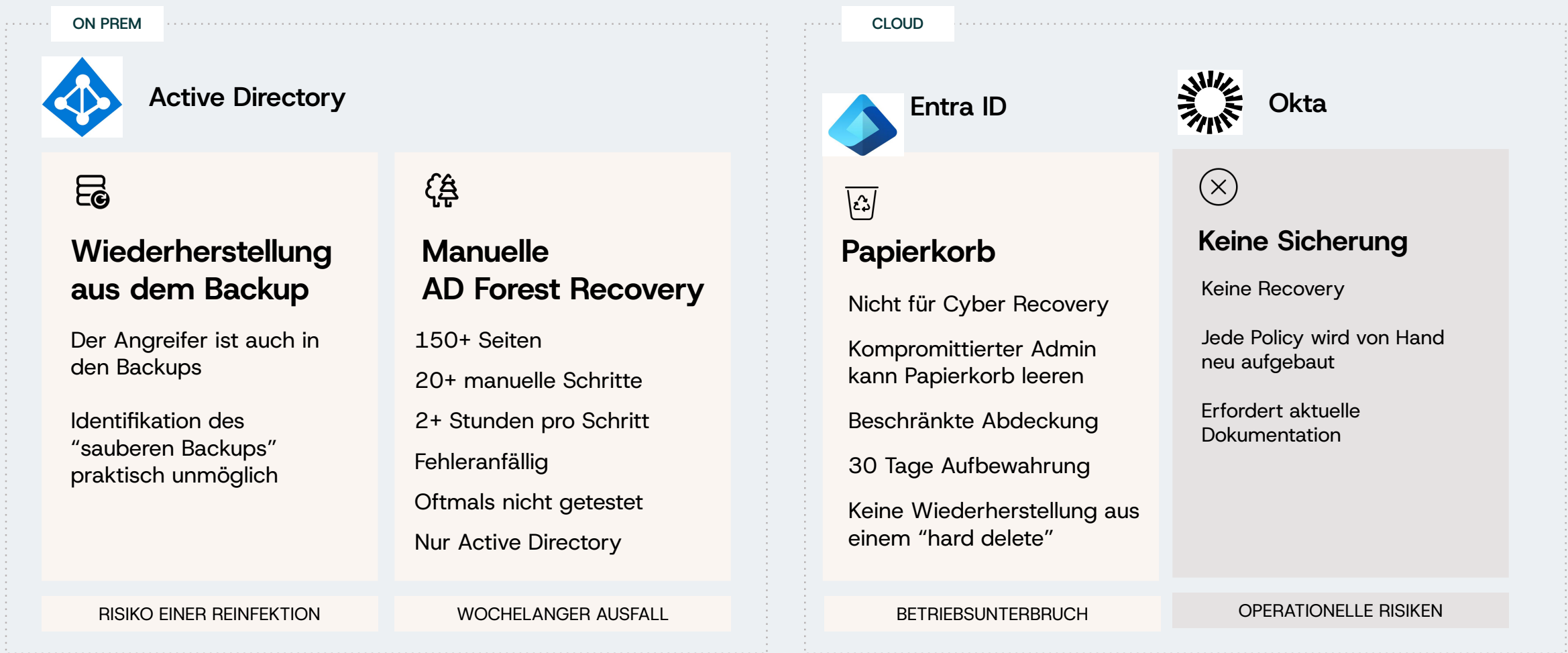
Identifikation des
"sauberen Backups"
praktisch unmöglich



WOCHELANGER AUSFALL



Langwierige Wiederherstellung



ALLE SYSTEME SIND VERBUNDEN - DIE RECOVERY SOLLTE ES AUCH SEIN

Sauber UND aktuell

ERSTE HÄLFTE

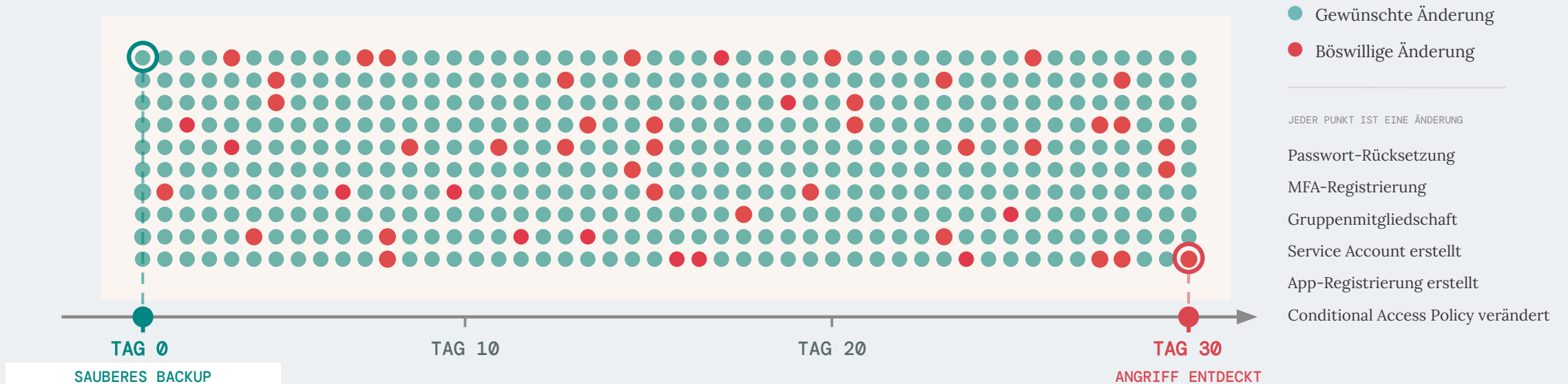
Das saubere Backup finden

Mit einer Wiederherstellung gehen auch alle
gewollten Änderungen verloren

ZWEITE HÄLFTE

Aktuellen Stand herstellen

Änderungen einspielen bedeutet wochenlange, manuelle Arbeit



Frage #2

Kritikalität für Patientenversorgung und Betrieb:

Wenn Ihre Identitätssysteme ausfallen, wie schnell hätte dies spürbare Auswirkungen auf die Patientenversorgung und andere kritische Abläufe?

Wie Rubrik helfen kann

Rubrik Identity Resilience

Saubere Wiederherstellung aller Identitäten in der Cloud und on-prem

- 01 **Angreifer aussperren**
Automatische Wiederherstellung des IdP auf einen sauberen Stand
- 02 **Wiederherstellung sauber und aktuell**
Einspielen der gewünschten Änderungen
- 03 **Vereinte Resilienz für alle Identitäten**
Konsistenz der on-prem und Cloud-IdPs



Gebaut um den Angriff zu überleben

Die Architektur geht von einem Angriff auf



Isolation

Überlebt den Angriff.
Keine Abhängigkeiten
an einen Hypervisor



Hardened Linux

Kein Windows, keine
Upgradefenster,
minimale Angriffsfläche



Air Gapped

OS, shell und Storage
nicht über das
Netzwerk erreichbar.
Kein NFS. Kein SMB.



Unveränderlich

100% der Backups
können nicht
modifiziert oder
gelöscht werden.
"Append-only"
Dateisystem



Unzerstörbar

Obligatorische MFA,
lokale User mit TOTP,
Retention Lock and
Schutz vor NTP
Poisoning



Alle Identitäten innert Stunden wiederherstellbar

Active Directory, Entra ID, und Okta



01

Verifiziertes sauberes Backup finden

Threat Hunting in den Backups findet rasch und zuverlässig das saubere Backup.

THREAT FEED

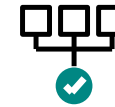


02

Orchestrate Forest Recovery

Rasche und orchestrierte Forest Recovery in fünf Schritten, automatisiert den manuellen Prozess basierend auf Microsoft Best Practices.

END-TO-END AUTOMATISIERUNG



03

Wiederherstellung aller IdPs

AD, Entra ID und Okta auf einer Plattform, inklusive der Abhängigkeiten und Beziehungen.

ZENTRALISIERTE WIEDERHERSTELLUNG

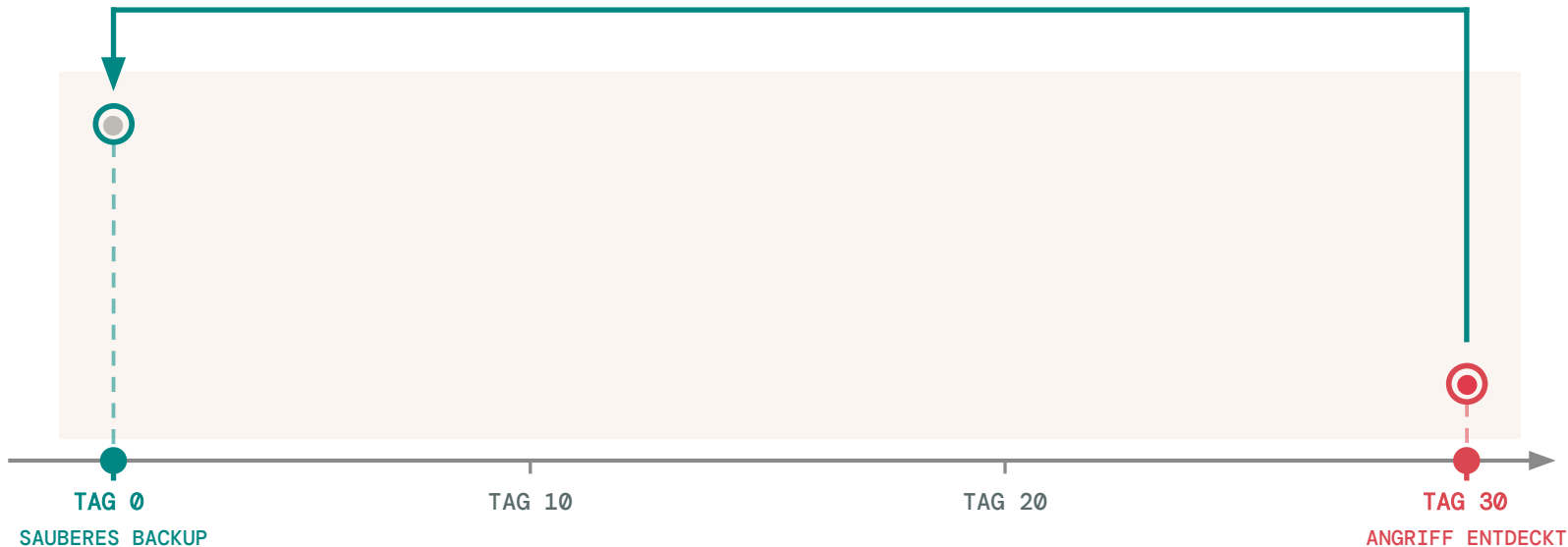
Saubere Recovery. Einspielen der Änderungen.

Nach dem Aussperren des Angreifers erfolgt das Einspielen der gewünschten Änderungen.

PHASE 01

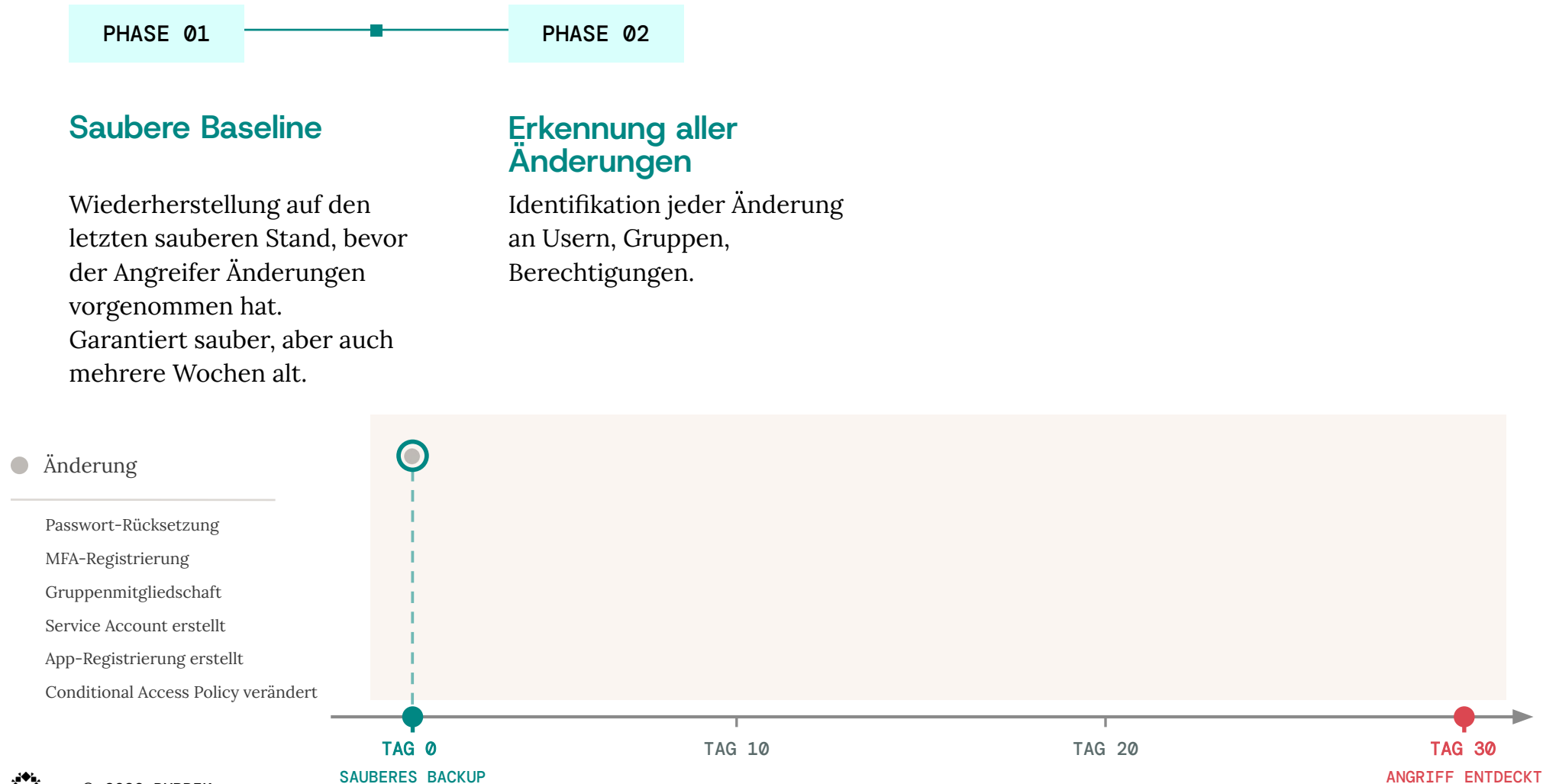
Saubere Baseline

Wiederherstellung auf den letzten sauberen Stand, bevor der Angreifer Änderungen vorgenommen hat.
Garantiert sauber, aber auch mehrere Wochen alt.



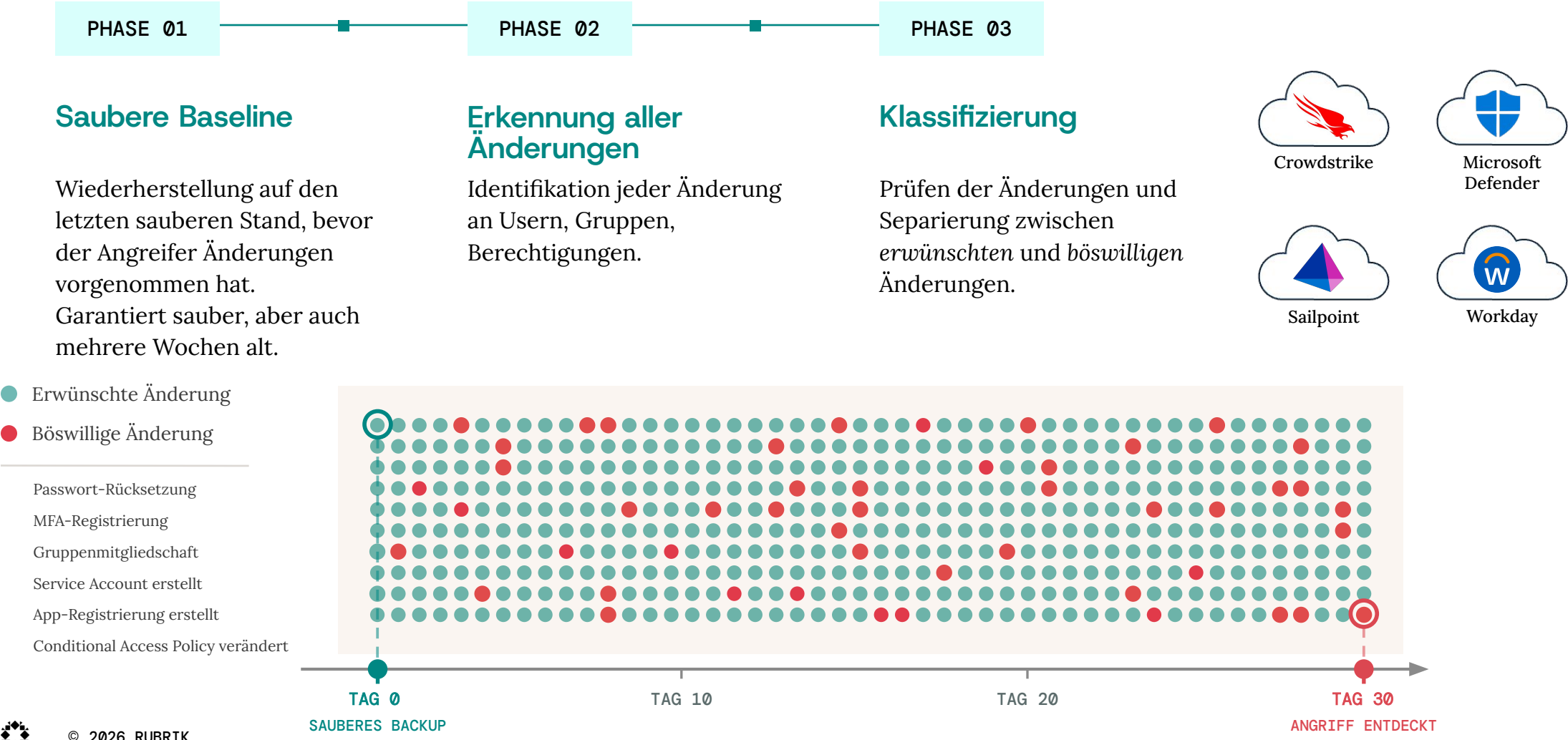
Saubere Recovery. Einspielen der Änderungen.

Nach dem Aussperren des Angreifers erfolgt das Einspielen der gewünschten Änderungen.



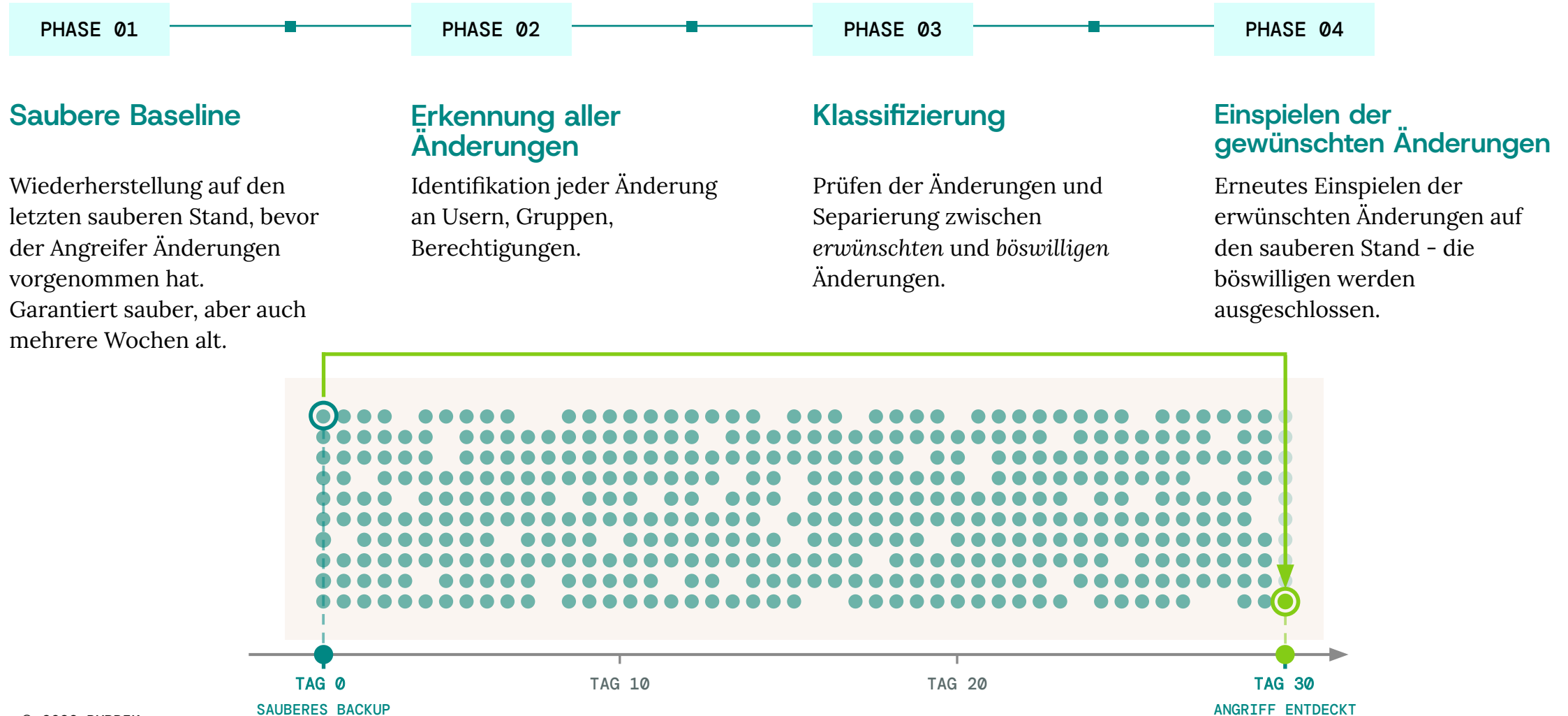
Saubere Recovery. Einspielen der Änderungen.

Nach dem Aussperren des Angreifers erfolgt das Einspielen der gewünschten Änderungen.



Saubere Recovery. Einspielen der Änderungen.

Nach dem Aussperren des Angreifers erfolgt das Einspielen der gewünschten Änderungen.



Frage #3

Einschätzung von Recovery und Resilienz: Wie würden Sie Ihre aktuellen Möglichkeiten zur Wiederherstellung der Identitätssysteme nach einem Cyber-Vorfall beschreiben?

Fragen & Antworten

**Vielen Dank
für die Teilnahme**