rubrik

“Daten sind das neue Gold”

Was bedeutet das für Ihre Cyber Resilienz?

Stefan Schmugge, 25.4.2024, Goldberg[werk]

Lernen von den Besten!

M - wir brauchen ein Briefing!

Begriffsdefinition

Resilienz

Resistenz

Lösegeld bezahlen ist noch nicht das Ende...

Rubrik Zero Labs

72%

der Organizsationen gaben an, Lösegeld gezahlt zu haben

NUR 16%

der befragten Organisationen haben alle ihre Daten nach einem Verschlüsselungs-Angriff wiederhergestellt

39%

zahlte Lösegeld, um die Offenlegung von Daten zu verhindern

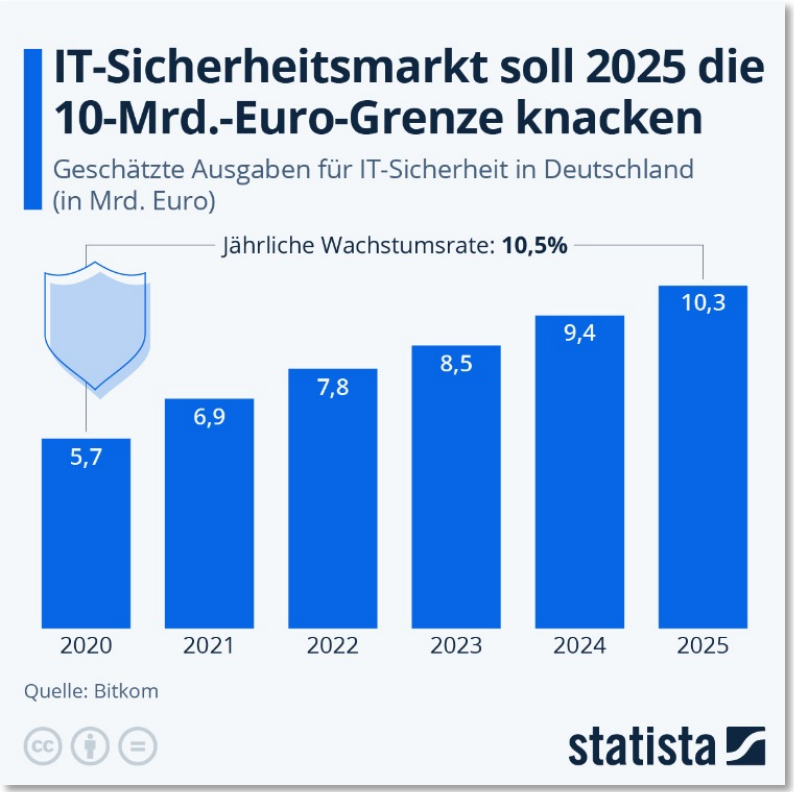
40%

zahlten Lösegeld, weil alle Daten verschlüsselt wurden

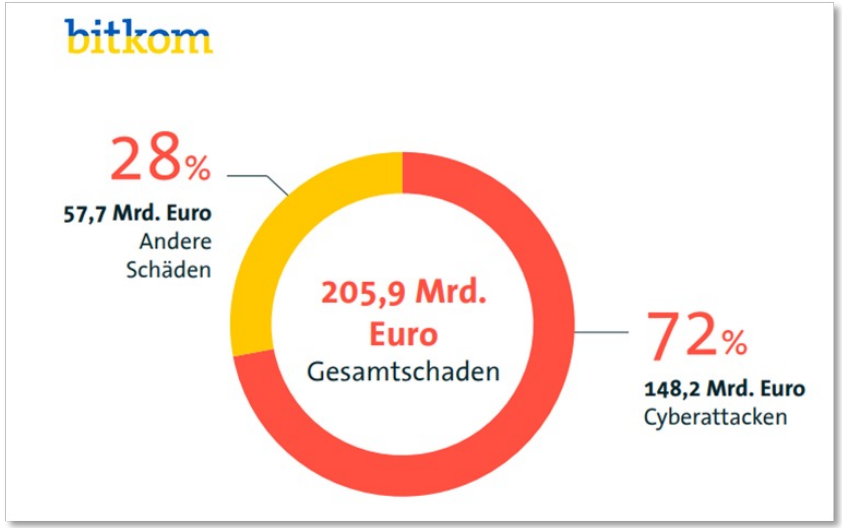
Auswirkung!

Wie hoch ist das 2024 Budget des deutschen IT-Sicherheitsmarktes?

Auswirkung Auflösung



Quelle: https://www.bitkom.org/Presse/Presseinformation/IT-Sicherheit-waechst-2022#



https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf

2021: 223 Mrd. / 132 Mrd.

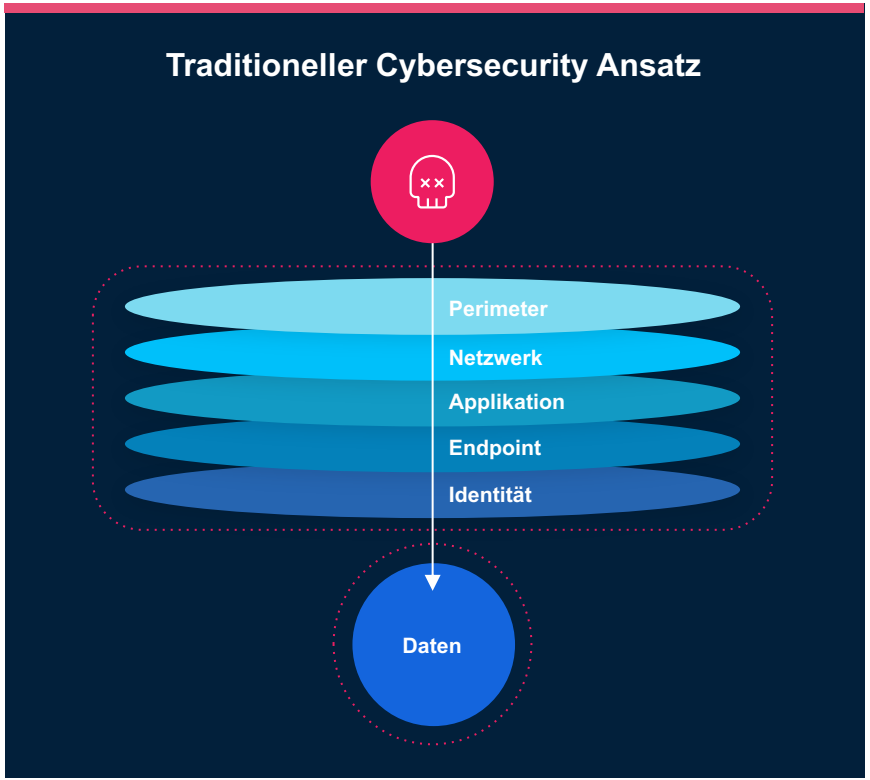
2022: 203 Mrd. / 128 Mrd.

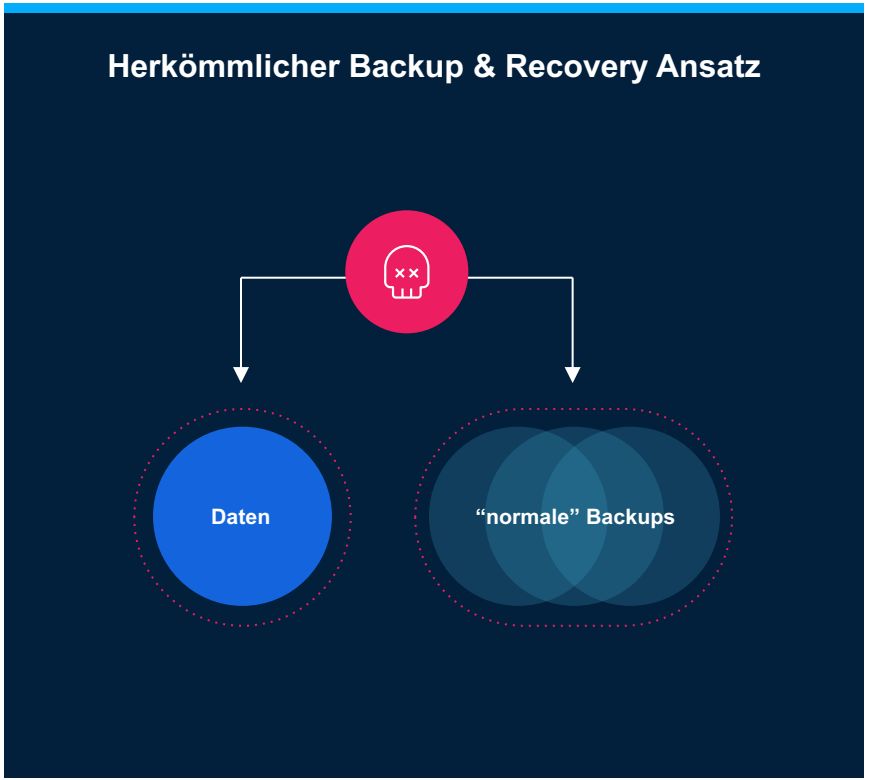
Auswirkung II

Schaden durch...	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)	Schadenssummen in Mrd. Euro (2021)
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	35,3	23,6	12,3
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	35,0	41,5	61,9
Kosten für Rechtsstreitigkeiten	29,8	16,2	12,4
Kosten für Ermittlungen und Ersatzmaßnahmen	25,2	10,1	13,3
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	21,5	41,5	29,0
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	16,1	10,7	24,3
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	15,3	21,1	22,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	12,4	18,3	17,1
Patentrechtsverletzungen (auch schon vor der Anmeldung)	10,4	18,8	30,5
Geldabfluss durch Betrugsversuche	3,9	-	-
Sonstige Schäden	1,1	0,9	0
Gesamtschaden pro Jahr	**205,9**	**202,7**	**223,5**

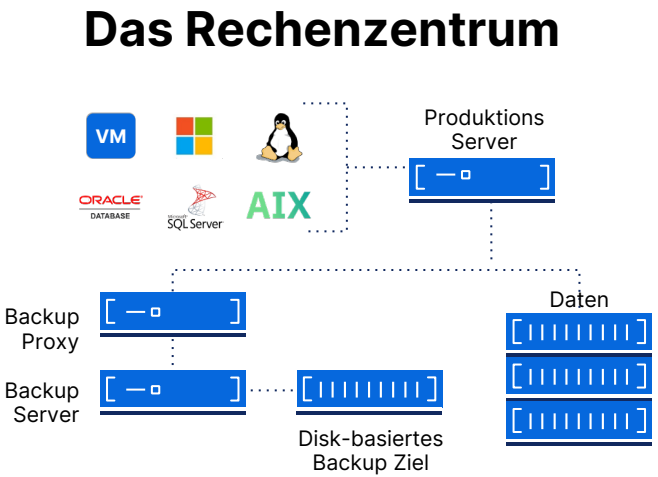
Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. |
Quelle: Bitkom Research 2023

IT Sicherheit scheitert am Sicherheitsgefühl





Warum hilft “klassisches” Backup nicht?



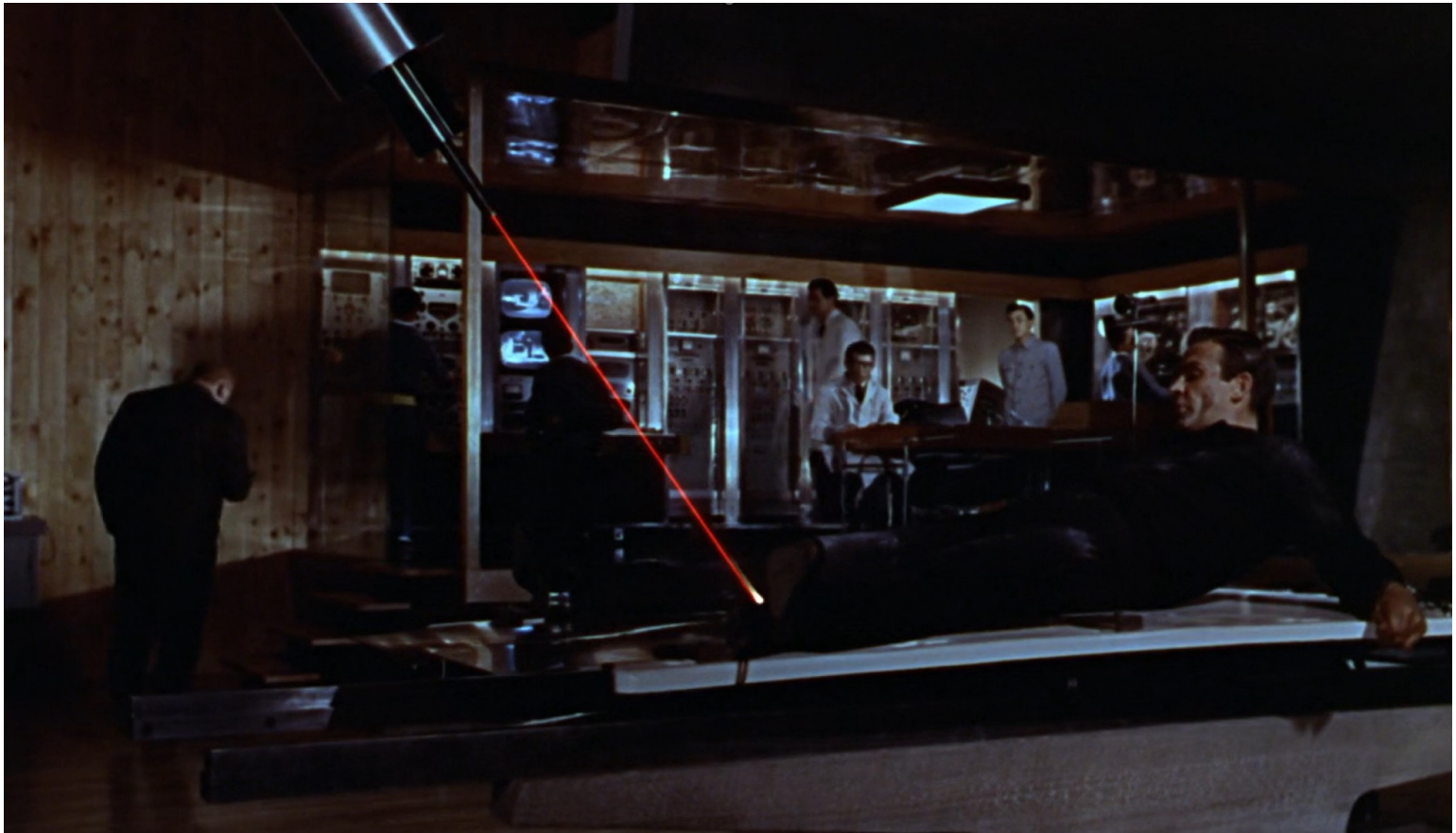
Nicht entwickelt für Angreifer hinter der Firewall

- Sind 100% Ihrer Backups immutable?
- Trennung von Produktion und Backup?
- Läuft die Backup Umgebung in einer VM?
- Läuft das etwa noch Windows?
- Wird MFA & Retention Lock erzwungen?

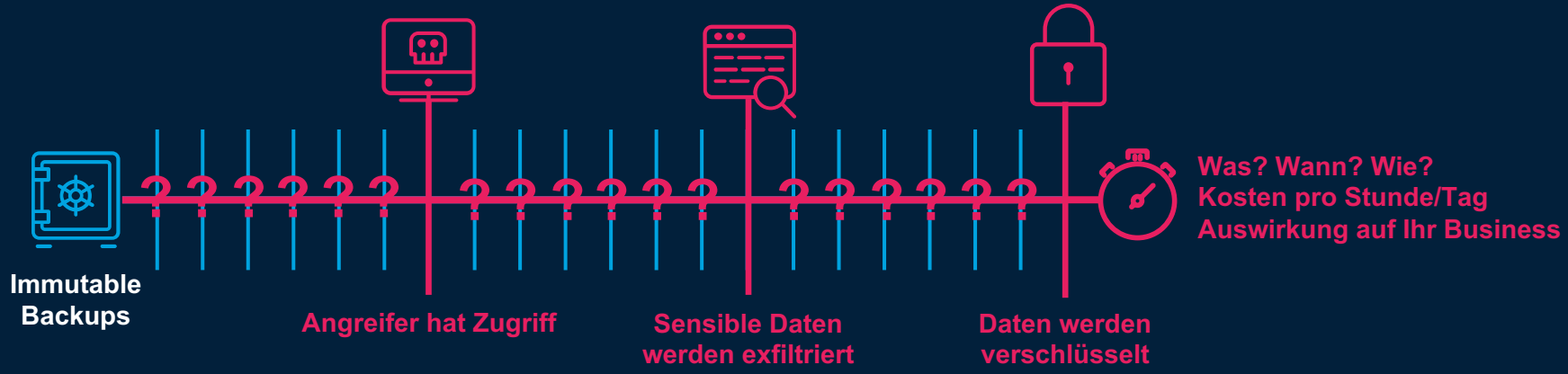
Falls nicht, gibt es ggf. nichts mehr zum Wiederherstellen..


NO SIGNAL

Es gibt immer eine dunkle Seite…



Warum ist Backup ≠ Cyber Resilienz



Können wir Recovern

1. 100% immutable Backup Infrastruktur ?

Was Recovern wir

2. Wissen, was verschüsselt wurde (ohne EDR)?

Was wurde gestohlen

3. Welche regulierten Daten waren “offen”?

Welchen Stand Recovern

4. Sauberen Recovery Punkt finden (ohne Reinfektion)?

Wie lange wird es dauern

5. Automatisiertes Recovery, auch getestet?

Cyber Resilienz

Was sollte das Gold Ihnen denn sagen?

Klassisches Backup

rubrik

Ein Blick auf den “Bösewicht”

Der beste Charakter für Tekkies?

Echte Cyber-Resilienz

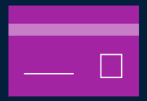
1. Rubrik Data Vaults

100% Immutable Backups
Logisch isoliert
Eingebaute Scanner
Scale-out Performance

2. Erkennung von Verschlüsselung

Erkennen von VM & In-Guest Verschlüsselungen
“Blast Radius” erkennen
Warnung <15Min

3. Finden von Sensitiven Daten



Scannen in den Backups
Incremental Forever
Risiko proaktiv minimieren

4. Threat Hunting + Monitoring

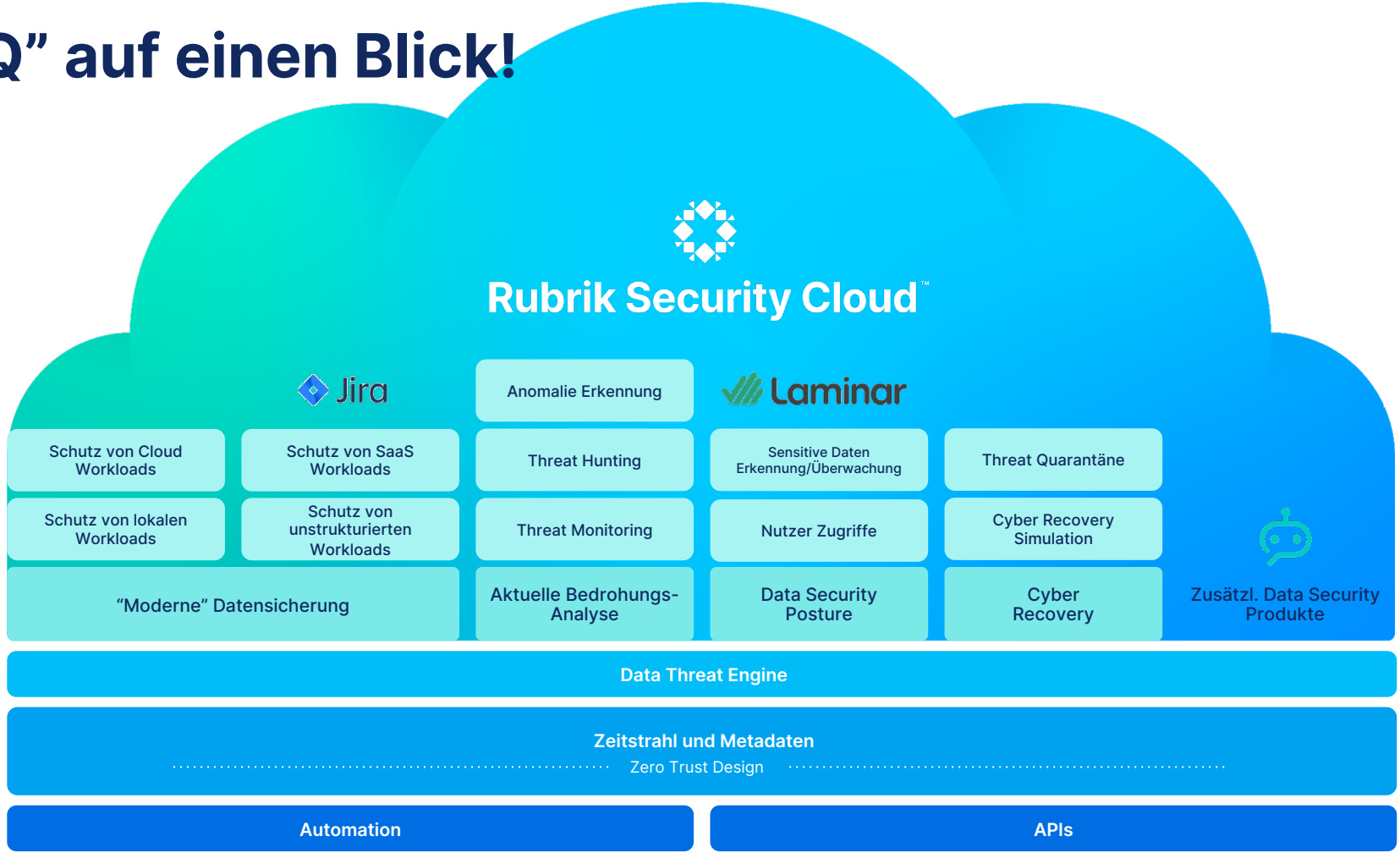
Scannen nach IOCs (Offline!)
Nutzung YARA/Hashes
Quarantäne

5. Cyber Recovery

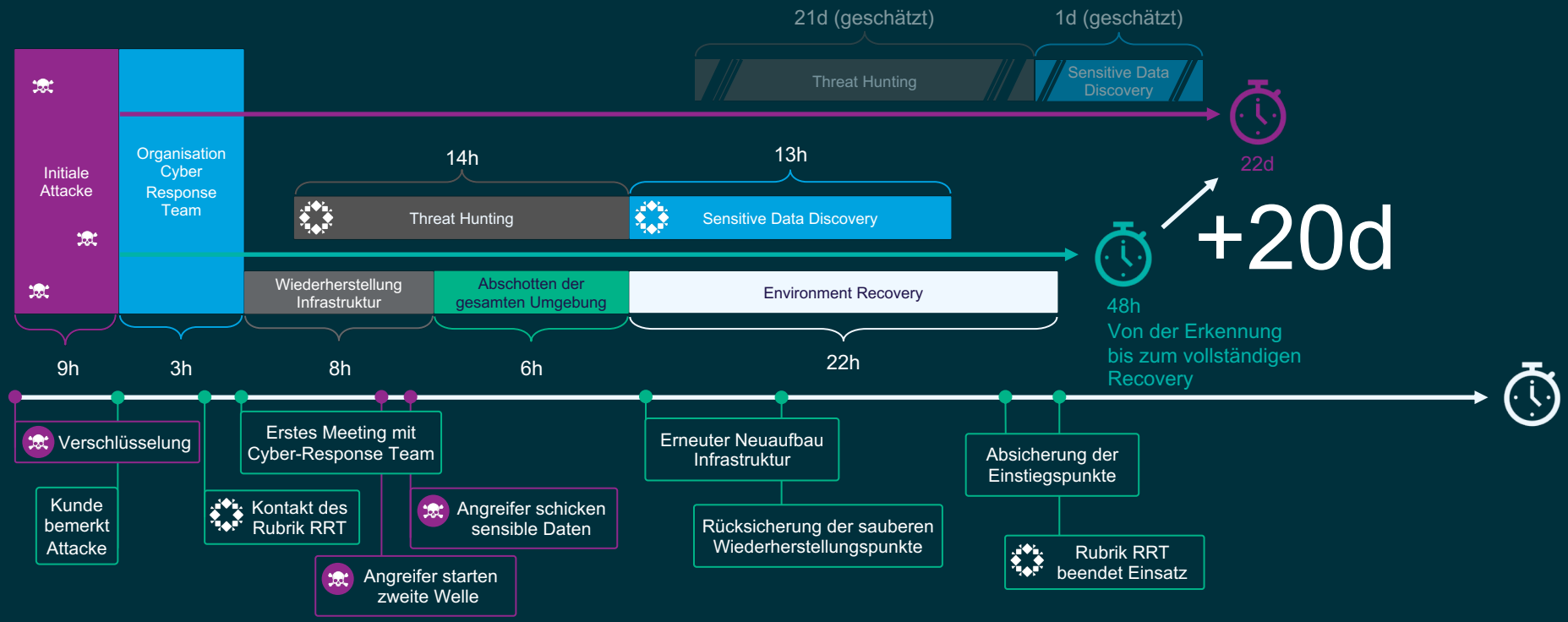
Recovery Automation
Letztes sauberes Backup
Testing & Reporting
Beweis der Wiederherstellung

paloalto NETWORKS
zscaler
CROWDSTRIKE
splunk>
Microsoft Sentinel

“Q” auf einen Blick!



Was ist Antwort auf alle Fragen?



Über 5.500 Kunden. 100% Wiederhergestellt.

FinServ	Manufacturing	Healthcare	Government	Security	Education	Media	Technology	Retail
Allstate	SIMPSON Manufacturing COMPANY	St Luke's UNIVERSITY HEALTH NETWORK	IRS	SONICWALL	HARVARD UNIVERSITY	GANNETT	Microsoft	THE HOME DEPOT
BARINGS	Driscoll's		CDC CENTERS FOR DISEASE CONTROL AND PREVENTION	Trellix	Duke UNIVERSITY	SESAME WORKSHOP	AMD	ESTĒE LAUDER
AMERICAN FAMILY INSURANCE	LUCID	GSK		Pulse Secure	UC San Diego	AMERICA'S TEST KITCHEN	ASML	petco
elements FINANCIAL	Alaska AIRLINES	Seattle Children's	Scottish Government Riaghaltas na h-Alba gov.scot	f5	NYU	NBC UNIVERSAL	Adobe	SEPHORA
mandiri	HONDA	DSH		proofpoint.	Penn	LAMAR	DocuSign	Domino's
CBRE	LAMBORGHINI	UCI Health	LA POSTE GROUPE	imperva	GW	HEARST	Lam RESEARCH	Krispy Kreme DOUGHNUTS
KeyCorp	dermalogica	LEE HEALTH		SECURITAS	UNIVERSITY OF THE PACIFIC	horizon media	World Wide Technology	PEPSICO

Nov. 2023

Zero Trust Architecture

Ransomware Response Team

Rubrik Zero Labs

Zusammenfassung!!!

- ✓ **SICHER (Garantiert und eingebaut)**
- ✓ **EASY**
- ✓ **SCHNELL (Fokus auf Restore)**
- ✓ **Rubrik „schenkt“ ihnen 20 Tage!**

Rubrik

DON'T BACKUP. GO FORWARD.

VIELEN DANK!

Fragen?