Datenschutz neu gedacht

Commvault Überblick

14. Juni 2023

Heute führt durch das Programm:

Dominik Steinmann

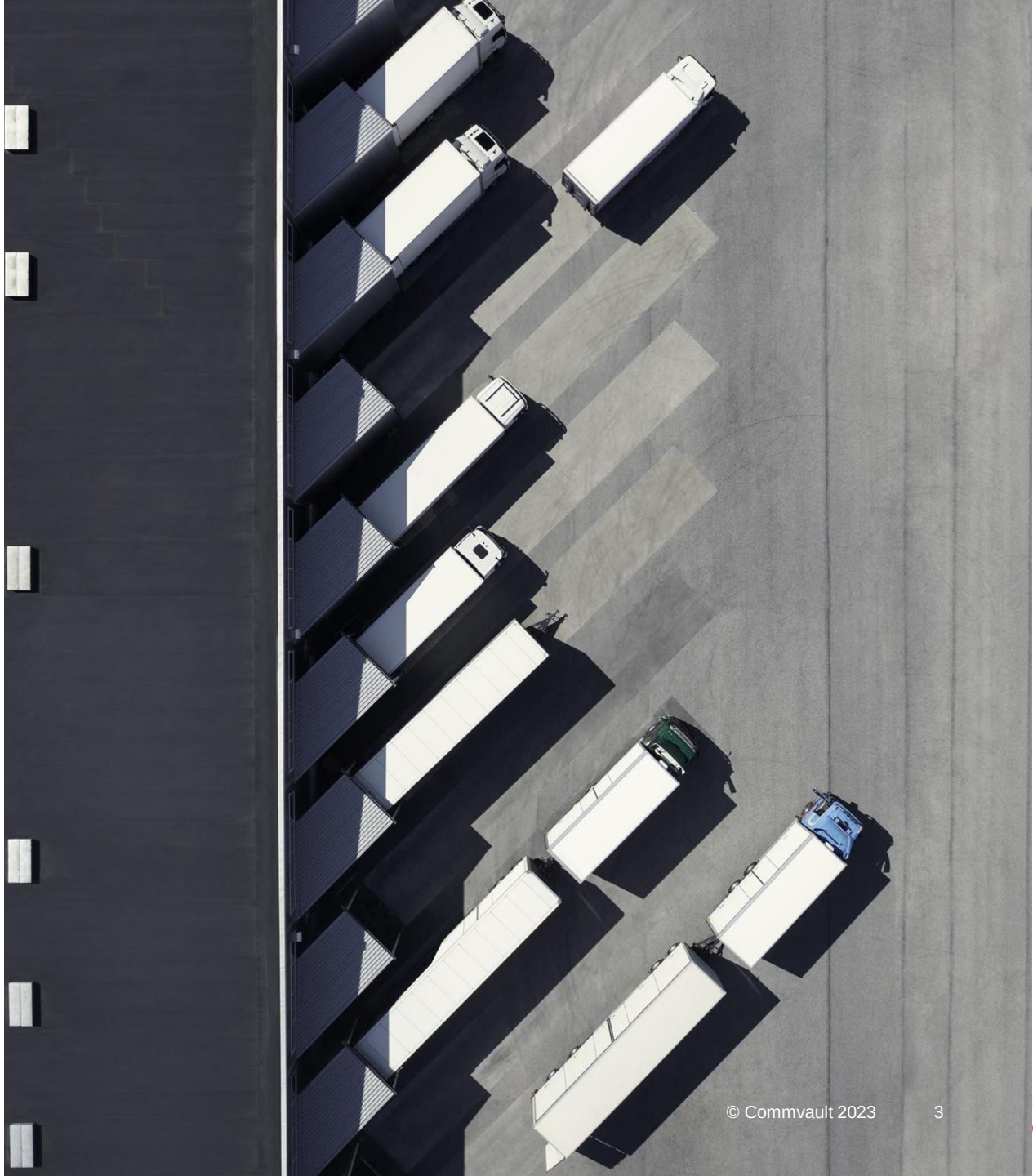
Commvault Evangelist
✉: dsteinmann@commvault.com
✆ : +41 79 207 3293

Agenda

01 Commvault?

02 Cyber-Attacken-Früherkennung

03 Q&A



Wir sind führend beim Schutz von Daten.

Mehr als 100’000 der führenden Firmen weltweit

vertrauen auf Commvault um mehr als
3.8 Exabytes Daten in der Cloud zu schützen

Wir helfen ihnen:

- Ihr Geschäft am Laufen zu halten
- Daten zu schützen, zu verteidigen und wieder herzustellen
- Neue Geschäftsfelder zu erschliessen

Adobe
SONY
BARON
DOW JONES
Telefónica
NTT DATA
adidas
AstraZeneca
HarperCollinsPublishers
orange Business Services

Daten sind überall

(...und schwieriger zu schützen als je zuvor)

89% der Fimen haben eine MultiCloud Strategie[1]

50% der Unternehmens-kritischen Daten befinden sich ausserhalb der eigenen Cloud[2]

60% der Firmen können nicht genau sagen, wo sich ihre Daten befinden[3]

1. 1. Flexera State of the Cloud Report 2023
2. 2. Gartner 12 Data and Analytics Trends to Keep on Your Radar
   3. 5th Annual Nutanix Enterprise Cloud Index

2021:
ein Schweizer Logistikunternehmen verzeichnet 340’000 Cyberangriffe
– alle ~90 Sekunden ein Angriff!!!

Raketenhaft ansteigende Cyber-Kriminalität befeuert das Thema noch weiter.

Attacken laufen schneller ab als je zuvor.

Was früher Monate dauerte, passiert heute innert Minuten.

Attacken sind breiter aufgestellt als je zuvor.

Backup & Recovery Umgebungen sind heute mehr gefährdet.

Zutritt

Einbrechen und Fuss fassen

Schaden

Angriffe unterhalb des Radars, Daten stehlen, filtern und verschlüsseln

Deaktivieren

Unterbrechen der Betriebsprozesse, um die Wiederherstellung zu verhindern

ACROSS HYBRID MULTI-CLOUD ENVIRONMENTS

Neu durchschnittlich bis zum Durchbruch noch » **84 MINUTEN**

Eine initial erkannte Kompromittierung muss schnellstmöglich eingedämmt werden

Ziel sind nicht mehr länger nur die Kronjuwelen » **83% MEHR RANSOMWARE ATTACKEN**

mit Doppel- oder Dreifach-Erpressung

Backup & Recovery Umgebungen werden dabei immer häufiger direkt attackiert.

Source: CrowdStrike 2023 Global Threat Report

Recovery als letzte Verteidungungslinie ist notwendig, aber unzureichend.

Zutritt

Einbrechen und Fuss fassen

Schaden

Angriffe unterhalb des Radars, Daten stehlen, filtern und verschlüsseln

Deaktivieren

Unterbrechen der Betriebsprozesse, um die Wiederherstellung zu verhindern

Schlüsselaspekte des NIST Sicherheits-Framework sind nicht abgedeckt.

Genau hier benötigen sie in den Umgebungen effektiven Datenschutz. Ohne sind sie Angriffen schutzlos ausgeliefert.

Wiederherstellen

Schnelle Wiederherstellung

Dies ist ihre letzte Verteidigungslinie. Wenn sie hierauf zurückgreifen müssen, ist es wohl zu spät...

Commvault – der einzige Hersteller

der Datenschutz mit aktiver Verteidigung und Automatisierung über den gesamten Datenschutz-Lifecycle bietet.

Früh-Erkennung

Scannen nach Bedrohungen

Risiko-Analyse

Backup & Recovery

eDiscovery & Compliance

Unveränderliche Speicherablage

COMMVAULT'S EINHEITLICHE PLATFORM

Sichern

Breiteste Abdeckung, um alle Workloads schützen und wiederherstellen zu können

Reduzieren sie das Datendiebstahl- und Compliance-Risiko um 60%[1]

Verteidigen

Aktive Verteidigung des Backups UND der Produktion, um effektiv Auswirkungen von Cyberattacken einzugrenzen.

Erkennen von Bedrohungen innert 5 Minuten statt 24 Stunden[2]

Wiederherstellen

Einzigartige Fähigkeiten zur schnellen Wiederherstellung mit den niedrigsten Betriebskosten in der Branche.

Bietet führenden Datenschutz zu 1/3 des TCOs[2]

1. IDC: Quantifying the Business Value of Commvault Software: Worldwide Customer Survey Analysis
2. Commvault Customer Value Research

Zusammenfassend

01 Datenschutz in einer Hybrid/Multi-Cloud Welt ist herausfordernd.

02 Cyber-Attacken machen es nur noch schwieriger.

03 Klassische Ansätze zum (reaktiven) Datenschutz greifen zu kurz...

04 Commvault bietet einen neuen, proaktiven, einzigartigen Ansatz!

So, die Marketing-Slides haben wir überlebt ☺

Jetzt – wie sieht das im richtigen Leben aus?

Security & Ransomware

COMMVAULT

Commvault's Ransomware Ansatz

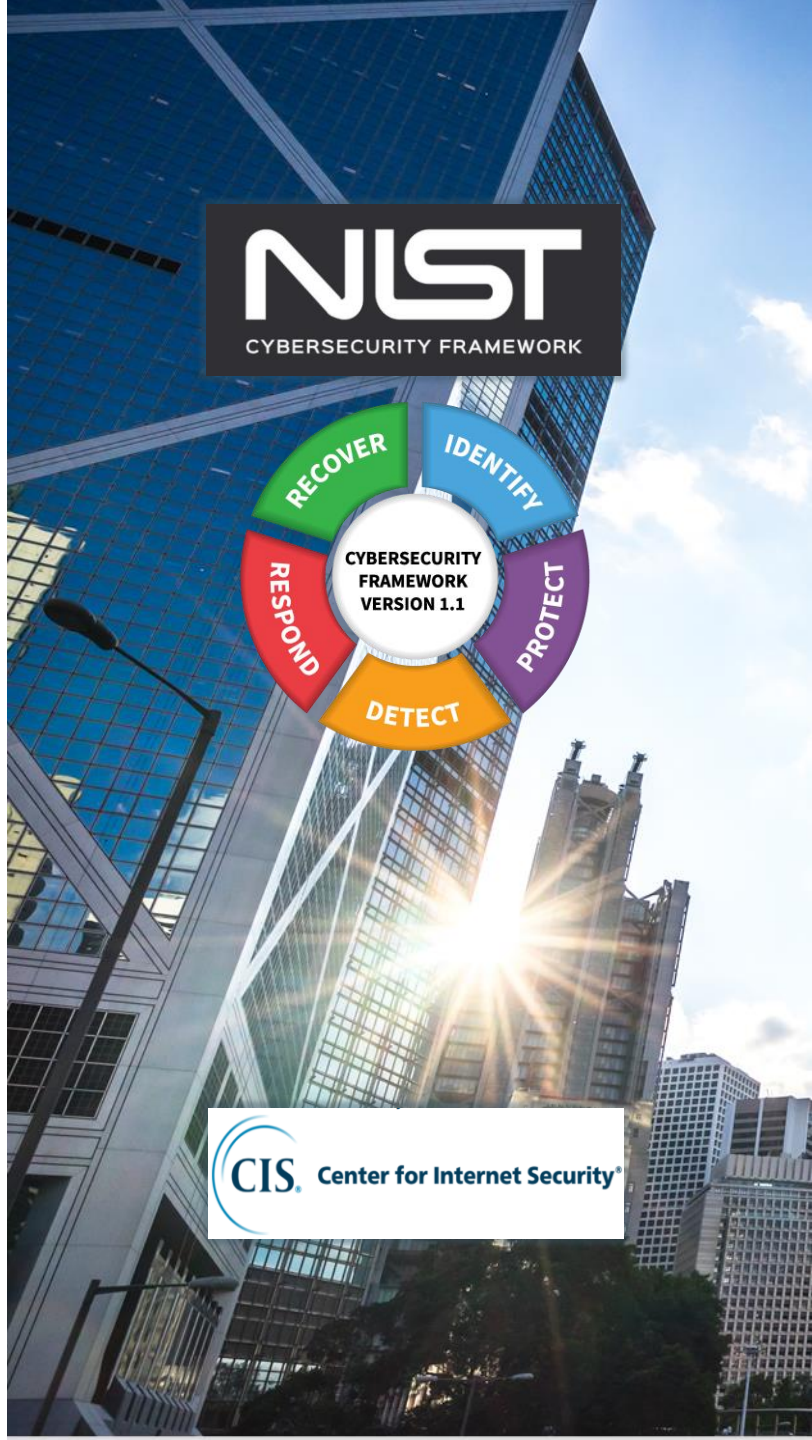
Umfassendster Ransomware-Schutz und breiteste Workload-Abdeckung

Beste Sichtbarkeit Ihrer Daten zur Verwaltung und Identifizierung von Risiken.

Konsistente, wiederholbare Prozesse und die meisten Wiederherstellungs-Optionen

Sichern	Risiken bewerten und mindern
	Isolieren, "Lock", und Daten vor Änderungen schützen
Verteidigen	Überwachen und Finden von Änderungen/Angriffen
	Daten analysieren und Aktionen automatisieren
Wiederherstellen	Schnellstmögliche Wiederherstellung von Daten

COMMVAULT



Wie schützen wir ihre Umgebung von A-Z?

Commvault Proaktive Erkennung

Reaktiv…. **Post Process**

Ein böser Bube verschafft sich Zugang zur Um-gebung und legt sie sich für spätere Aktionen zurecht

✓ Bedrohungs-Früherkennung

Hacker bewegen sich durch die Umgebung, suchen Schwachstellen und kritische Systeme/Daten

✓ Verdächtige Aktivitäten
✓ Honeypots
✓ Entropy | MIME Mismatch

Nach z.T. monatelanger Arbeit im Verborgenen (z.B. Datenklau), wird endlich eine Attacke ausgeführt und ein Lösegeld eingefordert

✓ Malware Scans
✓ “Moderne” Bedrohungen

Reguläre Backups um Daten unveränderlich abzulegen

Anomalie Erkennung gegen die gesicherten Daten. Alarme und Warnungen werden generiert – **die Fehlerbehebung beginnt**

Sekundäre Kopien der Daten werden auf Air-Gap Cloud/Objekt-Speicher geschrieben für zusätzlichen Schutz

6+ Monate früher | Lateral Movement | ATTACKE! | Tägl. Backups | Anomalie Erkennung | DR | Air-Gap | Vault Kopie

Zero Loss Strategy

Früherkennung & Orchestrierte Wiederherstellung…

COMMVAULT

Globales Daten-Management

- Dashboard zur Sicherheitslage
- Lifecycle - Deduplikation, Encryption, Verifikation
- Multi-Authorization Approvals

Zero-Trust

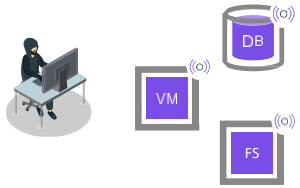
- Unveränderlicher Speicher
- Air Gap Netzwerk-Topologie Einstellungen
- Umfassende SAML | MFA | RBAC Einstellungen & Audit

COMMVAULT

Early WARNING

ThreatWise™ Cyber Deception

- ✓ Vorspielen realer Assets
- ✓ Täuschen böser Buben
- ✓ Bedrohungen früh zeigen
- ✓ Attacken abwehren



Köder, die richtige Assets vortäuschen und sich wie solche verhalten

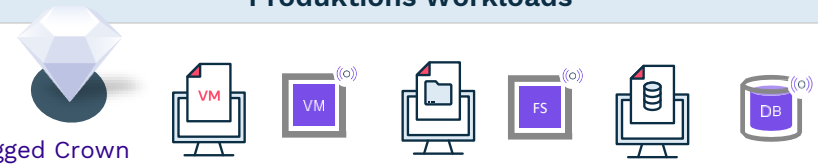
Ausrollen gefälschter Produktions-ressourcen, basierend auf Crown-Jewel-Tags

1 MFA | MPA | SAML | PAM | RBAC

SIEM | SOAR | XDR

paloalto | RAPID7 | splunk> | LogRhythm | Microsoft Sentinel | CROWDSTRIKE | TANIUM | servicenow

Produktions Workloads



Tagged Crown Jewels

2 Anomalie Erkennung

Aktive Erkennung	Verdächtige Datei-Aktivitäten	Bedrohungsanalyse
✓ Datei Aktivitäten	✓ Verdächtige Dateien	✓ Malware Scans
✓ Backup Aktivitäten	✓ Beschädigte Dateien	✓ Versionenvergleich
✓ Root Size Änderungen	✓ Verschlüsselte Dateien	✓ Malware Quarantäne
✓ Honeypot Files		

3a Scan auf Aktivitäten von dem Backup

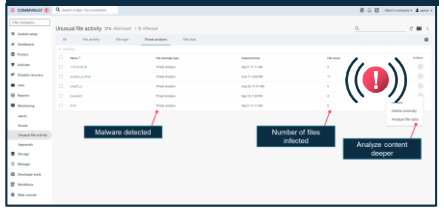
3b Markieren beim Schreiben

3c Malware Scan & Quarantäne

Alarm zum SEIM

Anomalien im Dashboard markieren

Unusual Activity Dashboard



Alarme | Events | Logs

- ✓ Syslog
- ✓ Webhook's
- ✓ SDKs
- ✓ API

Secure Immutable Storage

MA MA

Mimic Real Backup Servers

HyperScale | SAN | NAS | Object | Tape | Cloud

Airgap

5 Clean Recovery & Investigation

Cybervault + Clean Room

Recovery Site, isolierte Wiederherstellung zur unabhängigen Analyse

Sensitive Data Governance

Legal Dept

Inhalte auf Leakage- oder Offenlegungsrisiken zu PII und anderen DSGVO-relevanten Bereichen überprüfen

FSO – Identifiziren, Breiningen Quarantäne

Data Owner

Verdächtige Inhalte zur IRT Analyse exportiern, und beschädigte Dateien aus allen Sicherungskopien löschen

4 Cybervault / Clean Room

443 OUT-bound only

HyperScale | Metallic MRR™ | S3 Cloud oder HW Object Time Locks

NIST National Institute of Standards and Technology

COMMVAULT ZERO TRUST FOUNDATION

Commvault definiert modernen Datenschutz für die Cloud-getriebene Welt neu.

Data – protected!

That’s it.

✉: dsteinmann@commvault.com
✆: +41 79 207 3293