itsa 365

No Backup, No Mercy

Clemens von Baum

27.10.2022

Microsoft Partner

Microsoft

Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Collaborate with Confidence

Accessible content is available upon request.

Die Herausforderung

Was wir
nutzen...

Was wir
behalten müssen...

Was
sonst noch alles da ist...

No Backup, No Mercy

Ransomware ist nicht neu, jedoch nehmen Angriffe in Qualität und Anzahl zu und entwickeln sich zu einer der größten Sicherheitsbedrohungen. Letztes Jahr war alle 11 Sekunden ein Unternehmen von Ransomware betroffen.

Ein Backup Ihrer Daten und eine frühzeitige Erkennung einer Infektion sind die besten Schutzmaßnahmen gegen einen Angriff. AvePoint Cloud Backup mit integrierter Ransomware Erkennung unterstützt Sie dabei!

485%

mehr Ransomware-Angriffe
im Jahr 2020 im Vergleich zu 2019

Source: https://www.infosecurity-magazine.com/news/ransomware-attacks-grow-2020/

$283k

durchschnittliche Kosten für
Ausfallzeiten durch Ransomware

$178k

durchschnittliche Zahlungsforderung für
die Rückgabe von Daten

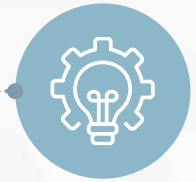
Source: https://www.cloudwards.net/ransomware-statistics/

Warum sollten Sie die Cloud sichern?

Ist das nicht der Grund, warum ich mich für einen Cloud-Dienst entschieden habe?

Ist mein Cloud-Anbieter nicht dafür zuständig?

Brauche ich das wirklich?



Wie würde ich das überhaupt machen?

Besteht die Gefahr, dass Sie Daten verlieren?

Haben Sie die Service-Level-Agreements (SLAs) Ihres Cloud-Anbieters gelesen und wissen Sie, was diese in Bezug auf Backup-Abdeckung und Datenschutz bietet?

Kennen Sie Ihre eigenen Backup-Anforderungen für den Fall, dass Ihr Cloud-Anbieter ausfällt oder Ihre Daten durch einen Ransomware-Angriff verschlüsselt werden?

Verantwortung für den Schutz Ihrer Daten

Schutz durch Cloud-Anbieter

- Service-Ausfall aufgrund eines Fehlers in der Hardware oder in der Infrastruktur
- Service-Ausfall aufgrund einer Naturkatastrophe oder eines Ausfalls des Rechenzentrums
- Kurzzeitiger Datenverlust durch Nutzerfehler mit Papierkorb/Versionsverlauf (einschließlich neuer „Datenwiederherstellung“ von OneDrive)
- Kurzzeitiger Datenverlust durch administrative Fehler mit Soft-Delete für Gruppen und Postfächer oder servicegeführtem Rollback

Kunden-Verantwortung

- Datenverlust aufgrund von ausscheidenden Mitarbeitern, deaktivierten Konten und "Human Error"
- Datenverlust aufgrund von böswilligen Insidern/Hackern, die Inhalte löschen
- Datenverlust aufgrund von Schadsoftware/Ransomware
- Wiederherstellung nach längeren Ausfällen
- Abdeckung langfristiger versehentlicher Löschungen mit selektivem Rollback

*Forrester: “Backup Your SaaS Data – Because Most SaaS Providers Don’t”, Naveen Chhabra, December 2017

Cloud Backup: Ransomware erkennen

Wir sitzen in der ersten Reihe,
wenn sich ungewöhnliche Änderungen in Ihren Daten ergeben!

#1: Ransomware muss den Zugriff auf so viele Dateien wie möglich unterbinden, um die Chance auf eine Auszahlung zu erhöhen.

Erkennung von Anomalien:
unsere KI untersucht und lernt die Standardmuster im Verlauf von 12 Tagen inkrementeller Backups (neue Dateien, Änderungen, Löschungen)

Beispiel: Kopieren > Verschlüsseln > Löschen führt zu ungewöhnlich hohen Änderungsraten

#2: Die gebräuchlichste Methode, jemandem den Zugriff auf seine Datei zu verwehren, ist die Verschlüsselung.

Erkennung von Verschlüsselung:
Jeder Versuch, Dateien zu verschlüsseln, erhöht automatisch die "Entropie" (Zufälligkeit) einer Datei. Wir verfolgen die Heuristik im Laufe der Zeit für OneDrive und Sharepoint.

Beispiel: Ein Versuch, viele Dateien zu verschlüsseln, erzeugt ein verdächtiges Ereignis

Cloud Backup

Menu

Home

Microsoft 365 Backup

- Restore
- Data Management
- Job Monitor
- Reporting
  - License Consumption Report
  - System Auditor
  - Job Analytics
  - Microsoft 365 Unusual Activities Analysis Report
  - AVA Report
- Settings

Microsoft 365 Unusual Activities Analysis Report

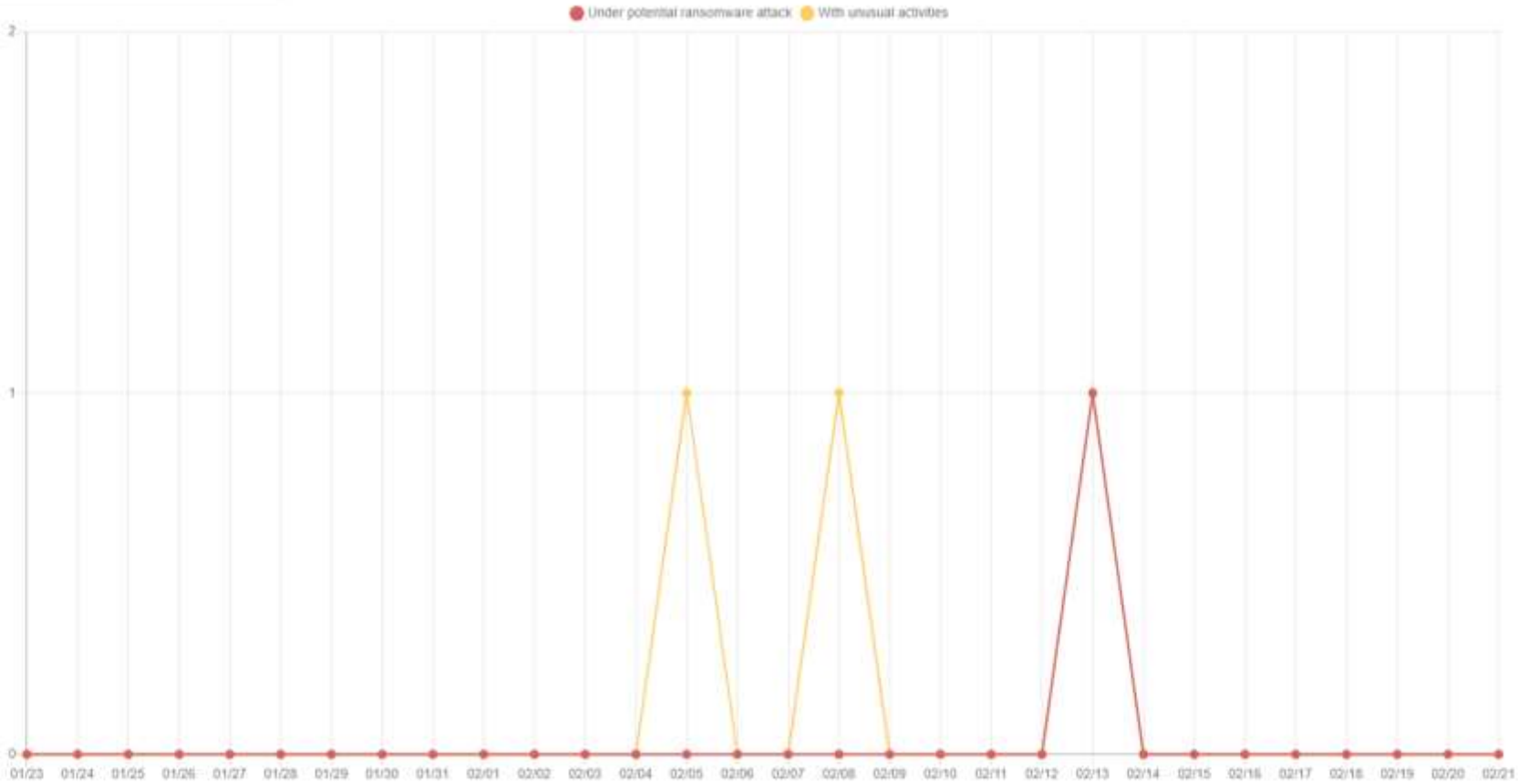
OneDrive for Business | SharePoint Online

Displays an overview of the unusual activities detected in your OneDrive for Business backup data in the last 30 days.

Protected OneDrive Accounts **45**

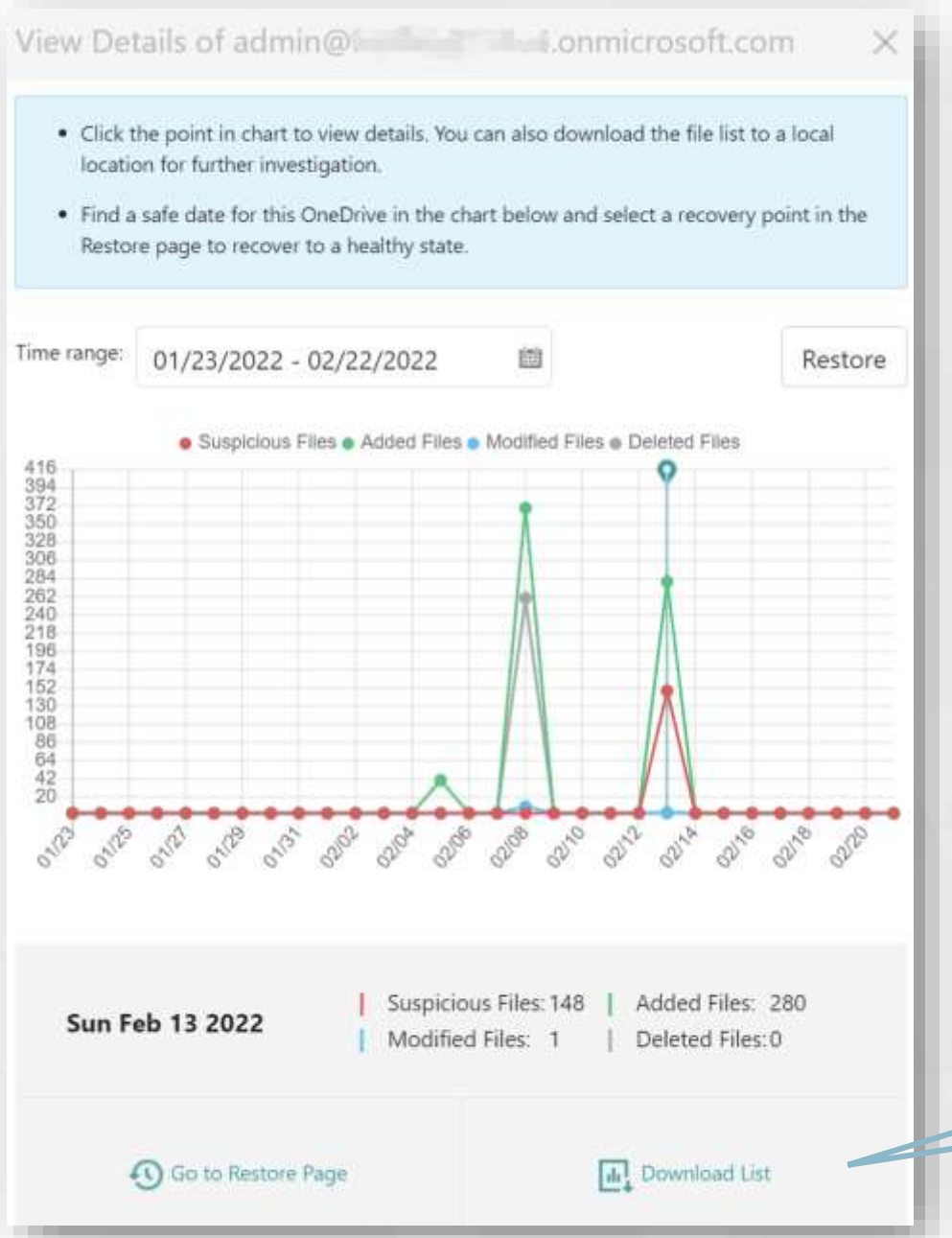
Suspicious OneDrive Accounts **1**

Time range: 01/23/2022 - 02/22/2022



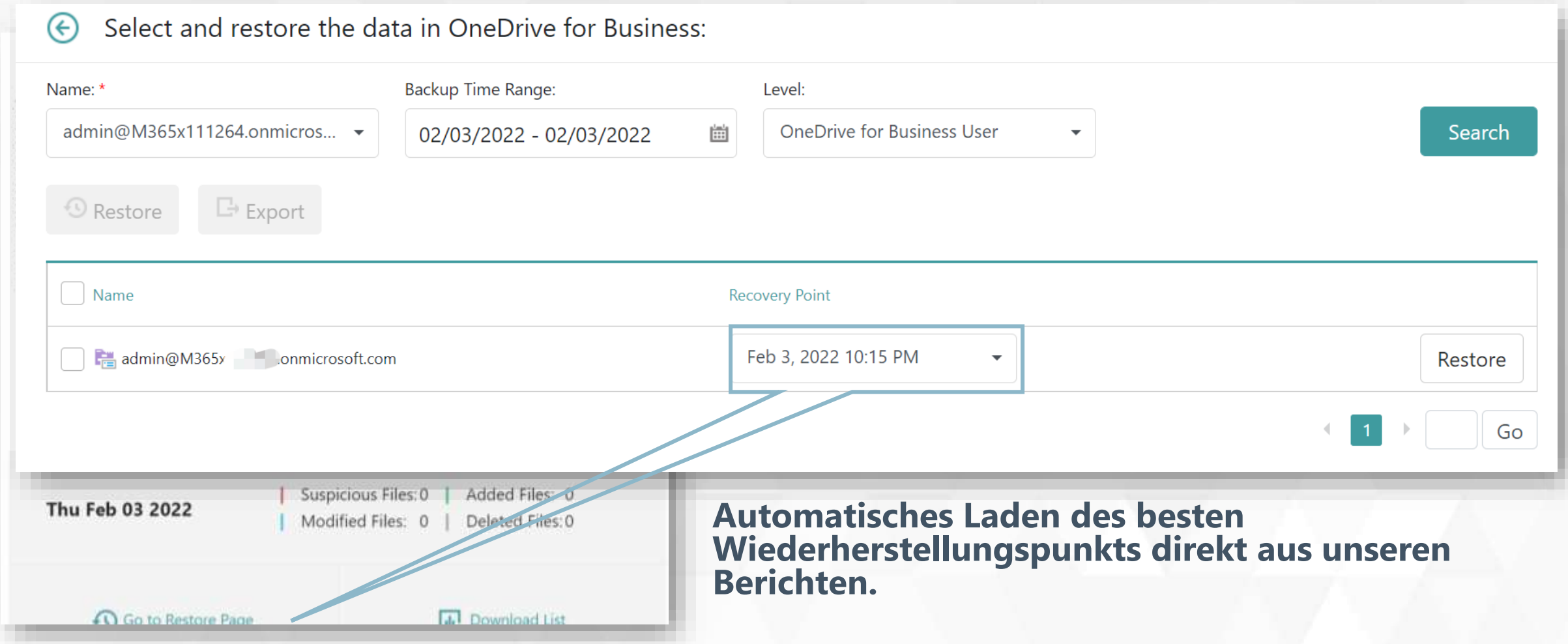
Schnelle Untersuchung

- Detaillierter Einblick in wichtige Aktivitäten
- Verdächtige Dateien (Verschlüsselungsverdacht)
- Erkennen von Ereignissen (Hinzufügen/Löschen/Ändern)
- Auf Fakten basierende Berichte für die Untersuchung



	A	B	C	D
1	File Name	Location	File Status	Unusual Activity Detected Time
2	Contoso Purchasing Data - Q1.xlsx	https://m365x[redacted]-my.sharepoint.com/personal/admin_m365x[redacted]_onmicrosoft_com/Documents/Contoso Purchasing Data - Q1.xlsx	Suspicious, Modified	08/10/2021 9:00 AM (UTC)
3	Contoso Purchasing Data - Q2.xlsx	https://m365x[redacted]-my.sharepoint.com/personal/admin_m365x[redacted]_onmicrosoft_com/Documents/Contoso Purchasing Data - Q2.xlsx	Added	08/10/2021 9:00 AM (UTC)

Sicherheit für Ihre Daten– Quick Restore



Automatisches Laden des besten Wiederherstellungspunkts direkt aus unseren Berichten.

Proaktive Erkennung von Ransomware-Angriffen

1 2 3

PROBLEM

DATA PROTECTION

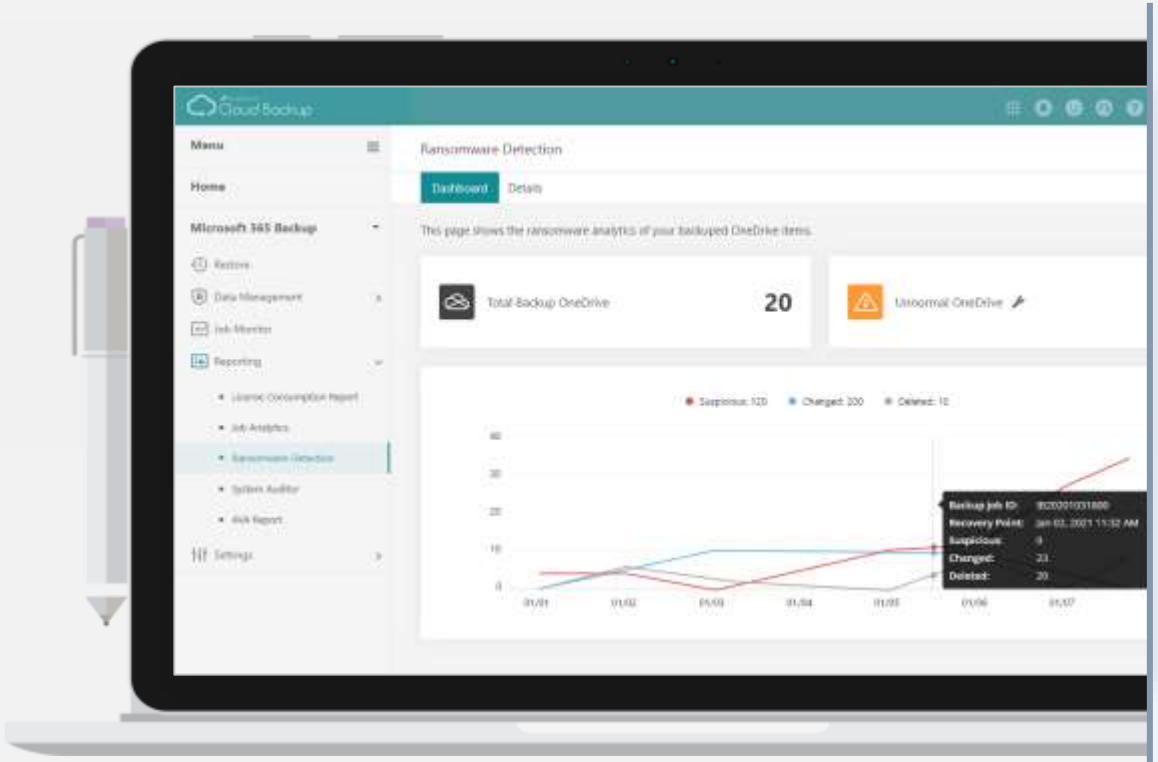
Ein einzelner Benutzer lud versehentlich einen Anhang herunter, wodurch eine seiner persönlichen Dateien verschlüsselt wurde. Eine One-Drive-Synchronisierung brachte sie in die Cloud.

LÖSUNG

- Warnung bei verdächtigen Aktivitäten
- Schnelles Identifizieren der Quelldatei
- Vermeiden von Lösegeld-kosten und Ausfallzeiten
- Risikominimierung und “Brandschutzübung”
- IT-Belastung minimieren

WIE KÖNNEN WIR HELFEN?

- ✓ Frühzeitige Erkennung von Ereignissen
- ✓ Einblicke und Anleitungen in Echtzeit
- ✓ Wiederherstellung auf granularer Ebene



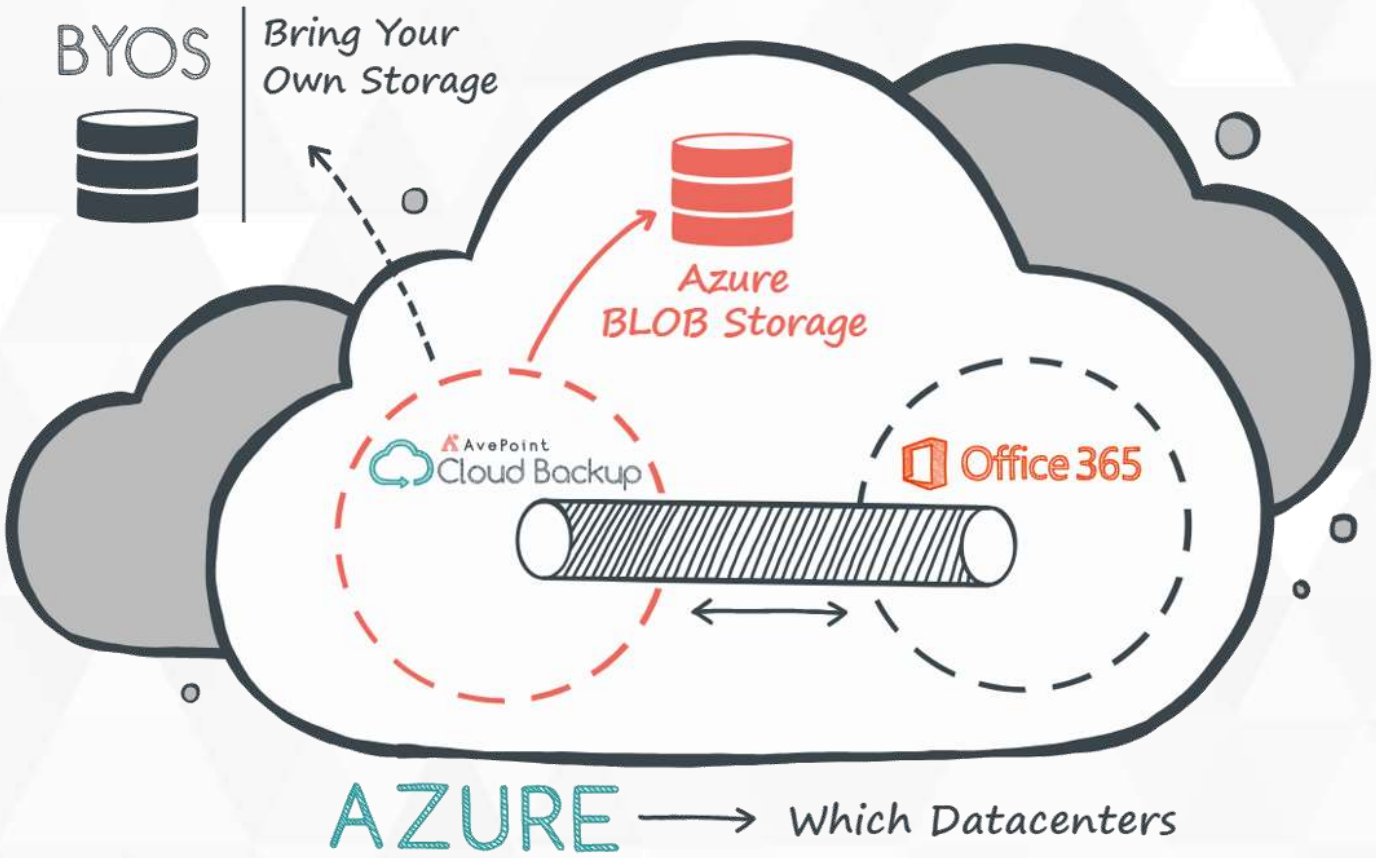
AvePoint Cloud Backup

RESULTS*

* MCI Inc.

"We had a ransomware issue with a user's OneDrive and we discovered that Microsoft could only restore the full OneDrive at a specific date and only in the last 14 days....we compared AvePoint to another provider and Cloud Backup gave us the insurance that our data is secured and always available."

Edouard Duverger
Global Vice President Information Technology, MCI



- ✓ SaaS
- ✓ Auto-Scale
- ✓ High-Performance

- ✗ VMs
- ✗ Storage
- ✗ Complex Config

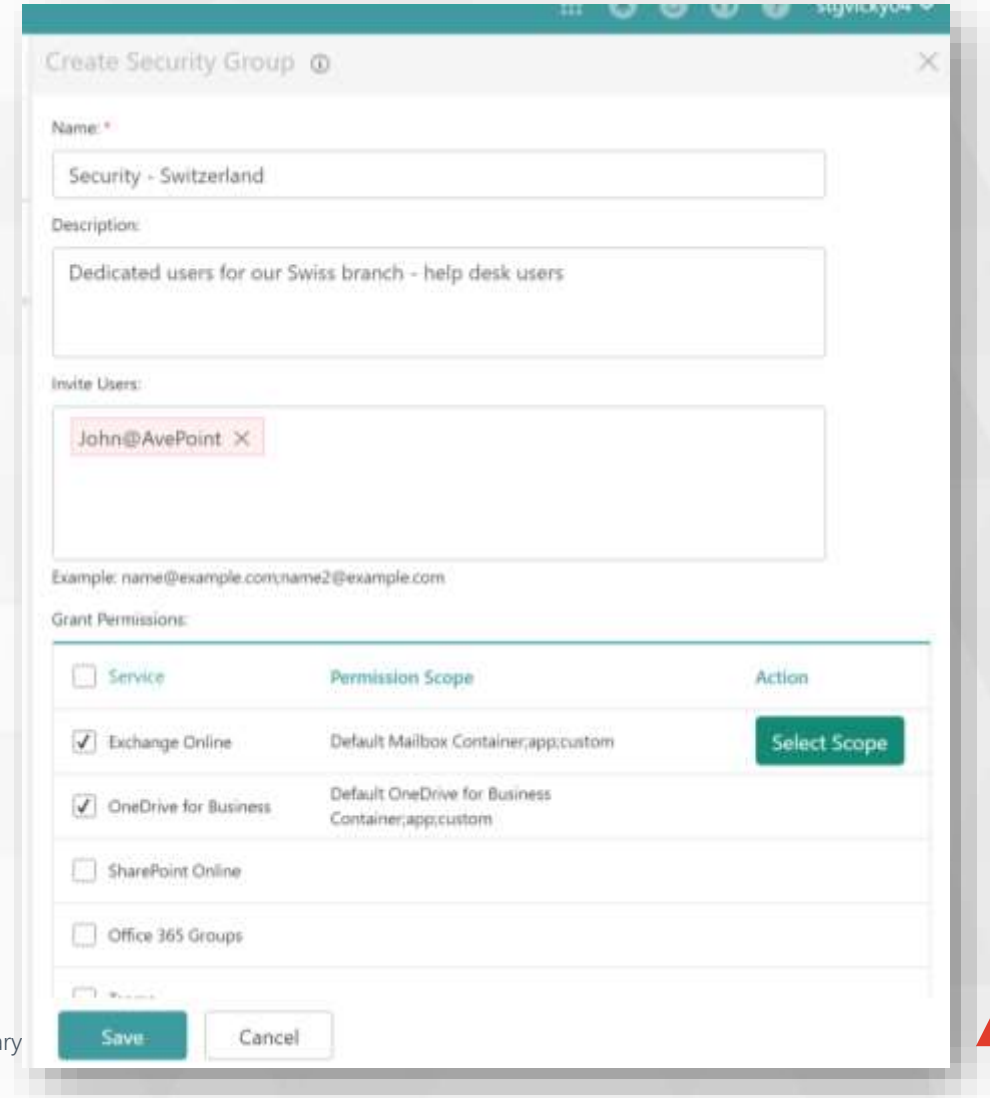
Teams | Exchange | Public Folder | SharePoint | M365 Groups | OneDrive | Planner | Project | Yammer

Einen Moment… da ist noch mehr

- AVA (AvePoint Virtual Assistant) – Einfache End-User Restores
- GDPR – Löschen von Backup-Daten bei Bedarf
- Ransomware Detection – Benachrichtigung, wenn Ungewöhnliches auftritt
- Encryption – Verwenden Sie Ihren eigenen Azure KeyVault
- Account Management – Wer kann was wiederherstellen?
- AzureAD Authentication – Voll integriert mit Sicherheitsfunktionen
- Scan Profiles – Sichern Sie nur, was sie wollen

Delegierte Kontrolle und Zugriff

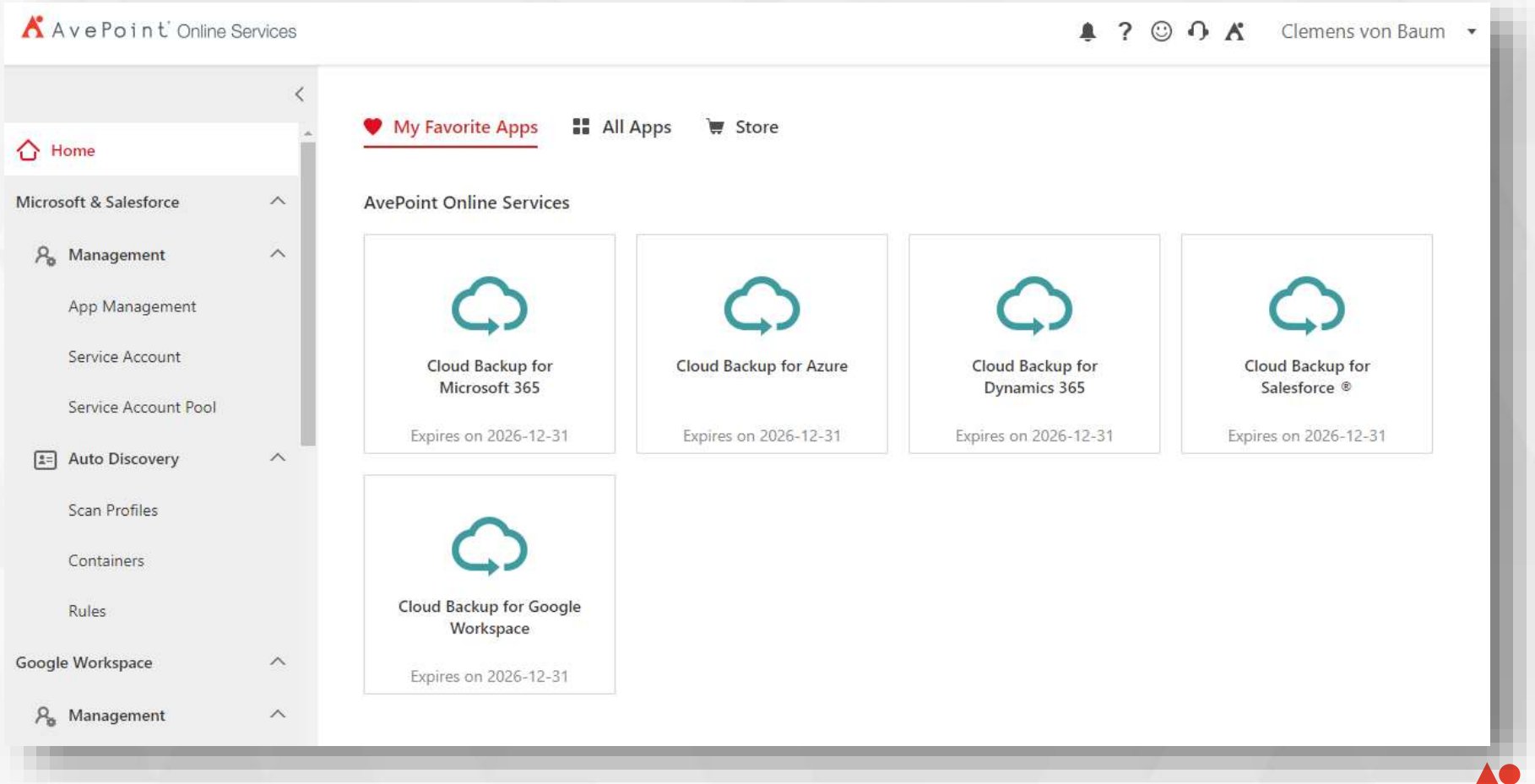
- Zusammenarbeit mit Security
  - Ein Backup-SLA, aber viele Wege zur Wiederherstellung
  - Aufteilung nach Land, Abteilung, Titel, Bereich, etc..
- Identifizierung von Admins
  - Exchange-Teams Zugriff auf E-Mails geben
  - SharePoint-Teams Zugang zu Gruppen/Teams geben
- Helpdesk-Anrufe delegieren
  - OneDrive- und Mailbox-Anfragen können an untergeordnete Helpdesk-Administratoren weitergeleitet werden



Data Security – nur M365?

Backup für

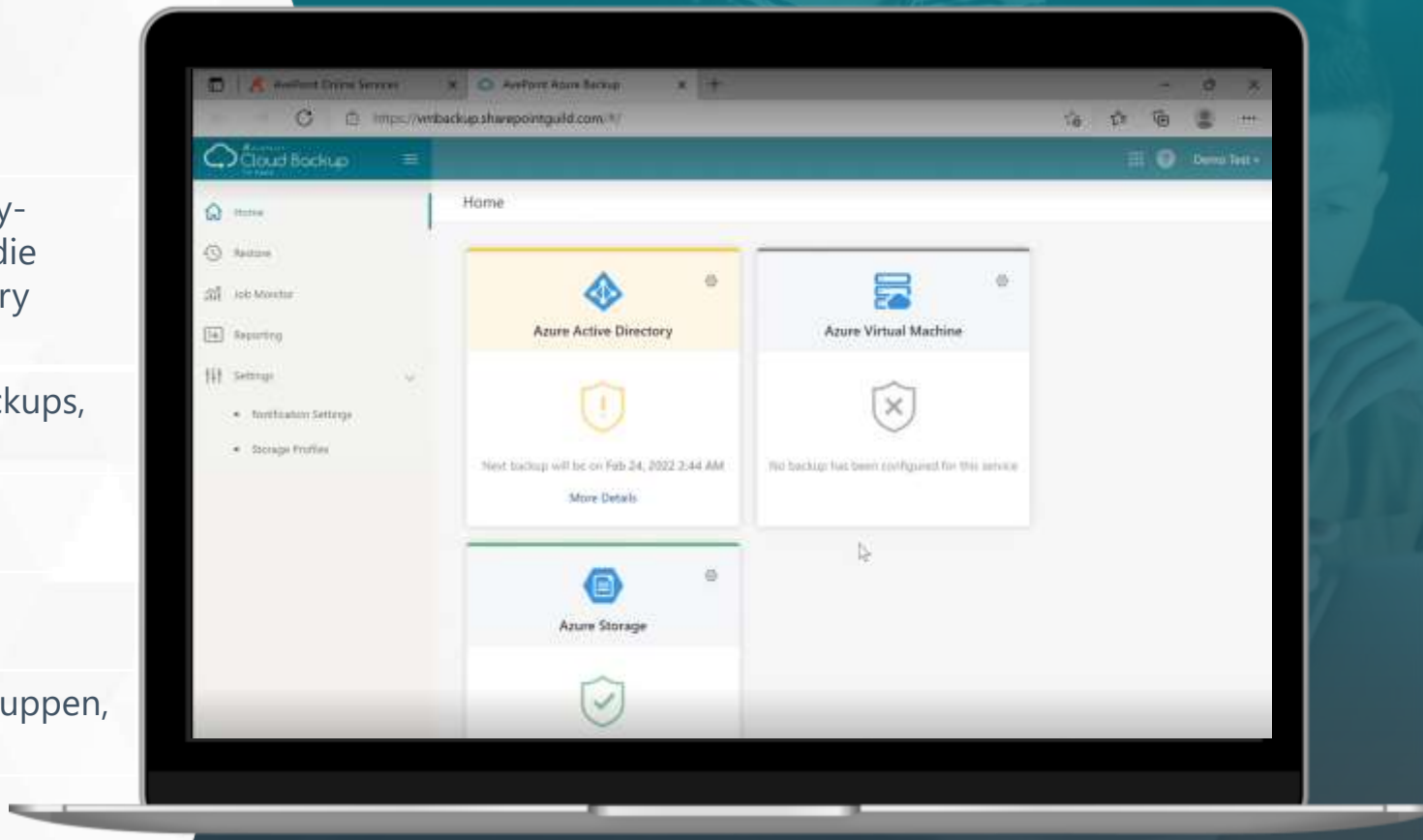
- M365
- Azure
- Dynamics 365
- Salesforce
- Google Workspace



Backup für Azure > Spotlights

Azure AD, Azure VM, Azure Blobs/Files storage

- Hybride Active-Directory-Umgebung oder Cloud-only-Kennungen, die nicht synchronisiert sind. Stellen Sie die Verfügbarkeit und Integrität von Azure Active Directory sicher.
- Regelmäßige vollständige Backups, inkrementelle Backups, flexible Backup-Aufbewahrung.
- Cloud-to-cloud backup (BYOS + AP Storage).
- Point-in-Time und granulare Wiederherstellung.
- Originalgetreue Wiederherstellung von Benutzern, Gruppen, Gruppenmitgliedschaften und Anwendungen.



Warum ist Dynamics Backup wichtig?

Business Critical Application

Microsoft View

- Nur Organisations-Backups
- Wiederherstellung zur Sandbox
- 28 Tage Retention

AvePoint View

- Granulare Wiederherstellung
- Related Entity Wiederherstellung
- Wiederherstellung zu Production
- Unbegrenzte Retention
- Compare Feature

The Leader in Multi-SaaS Backup Solutions

AvePoint named a Leader in The Forrester New Wave™: SaaS Application Data Protection, Q4 2021. AvePoint received the highest current offering score of all 10 vendors for Cloud Backup

Differentiated ratings – highest possible! – in M365, Google Workspace and Salesforce criteria

Differentiated ratings in security and privacy, usability, storage options criteria

Differentiated ratings in planned enhancements and innovation roadmap criteria

Data Security mit AvePoint

Clemens von Baum

Solution Engineer

AvePoint Deutschland GmbH

Munich, DE

No Backup, No Mercy

Dank AvePoint selbst bei Ransomware-Attacken schnell wieder im Geschäft

thank you

AvePoint®

SalesDE@AvePoint.com | +49 89 2190 98 900

www.AvePoint.com/DE