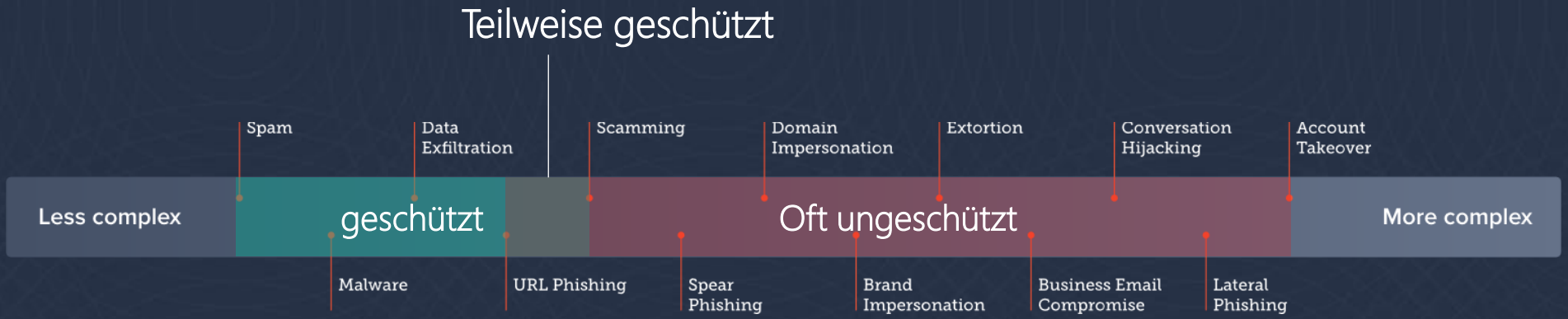
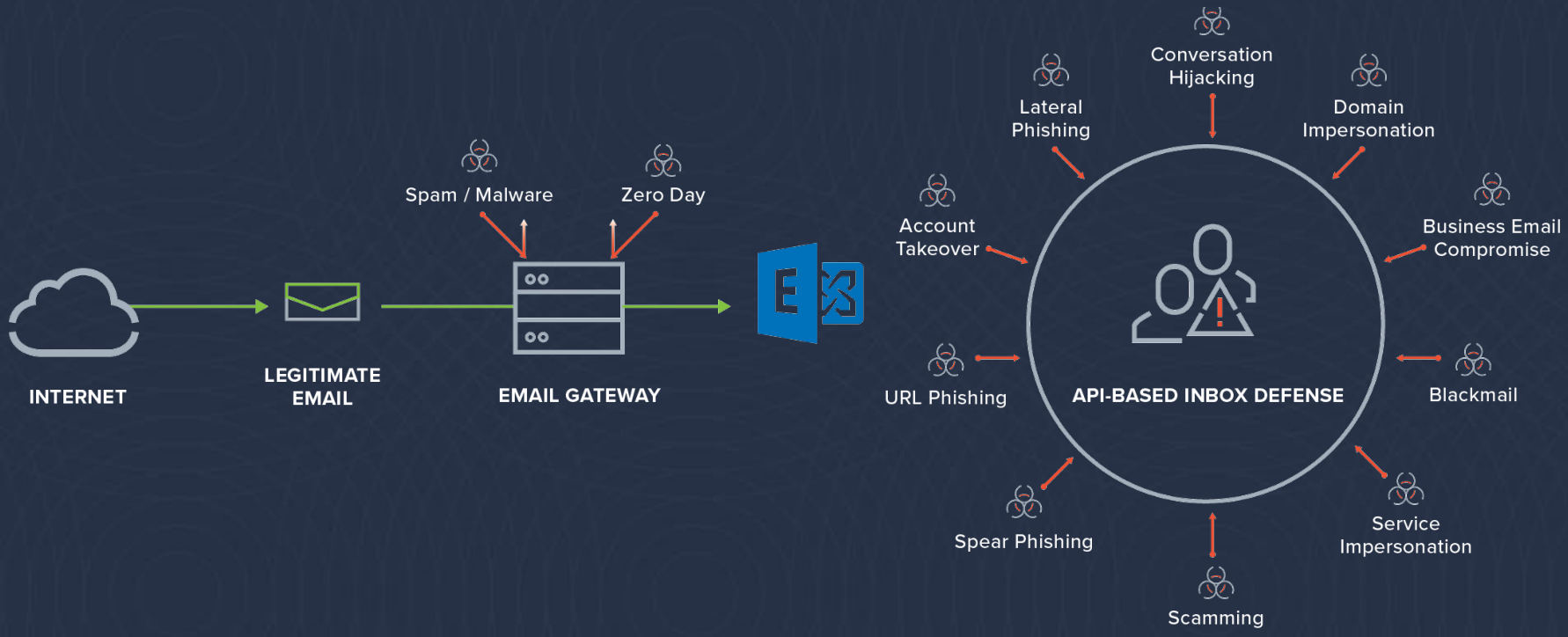
Microsoft 365 Veredelung mit Barracuda Email & Data Protection

Julian Schreier, Senior Sales Engineer

Barracuda
Your journey, secured.


Teilweise geschützt
Spam
Data Exfiltration
Scamming
Domain Impersonation
Extortion
Conversation Hijacking
Account Takeover
Less complex
geschützt
Oft ungeschützt
More complex
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Lateral Phishing


Spam / Malware
Zero Day
INTERNET
LEGITIMATE EMAIL
EMAIL GATEWAY
Conversation Hijacking
Lateral Phishing
Domain Impersonation
Account Takeover
Business Email Compromise
URL Phishing
API-BASED INBOX DEFENSE
Blackmail
Spear Phishing
Service Impersonation
Scamming

Inbox defense Technologie evaluiert unterschiedlichste Parameter

mehrere classifier

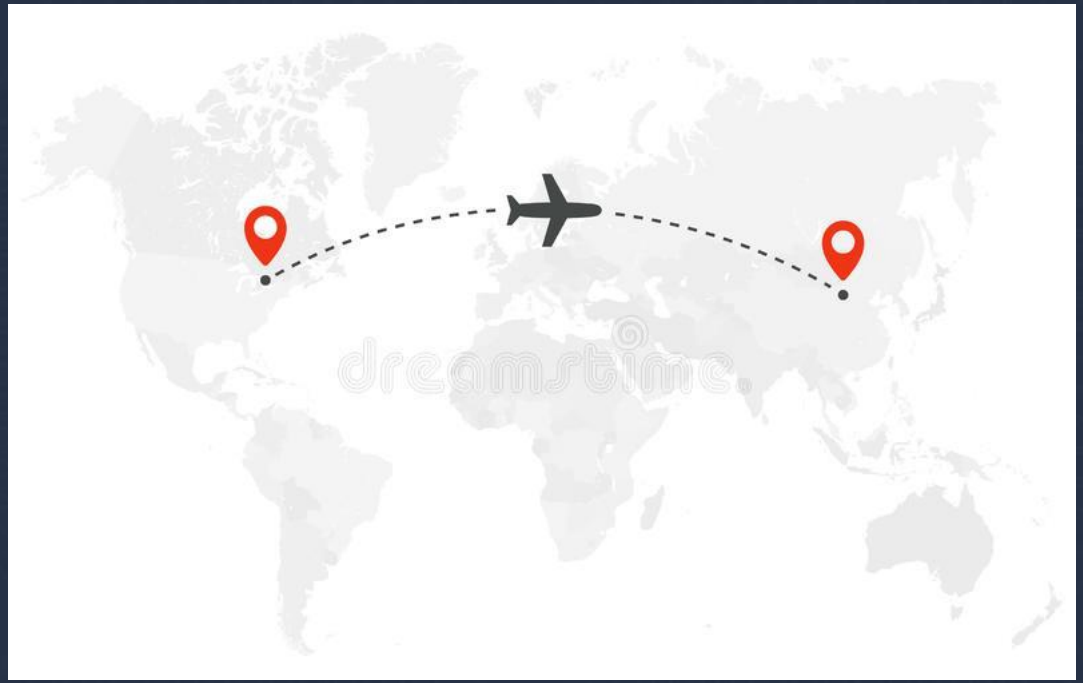
…und findet einzigartige Muster

Versteht abnormales Verhalten

Gateways = hunderte Regeln für zig individuelle Benutzer = nicht skalierbar

Beispiel: Impossible travel

Von Klagenfurt nach Moskau in 15 Minuten



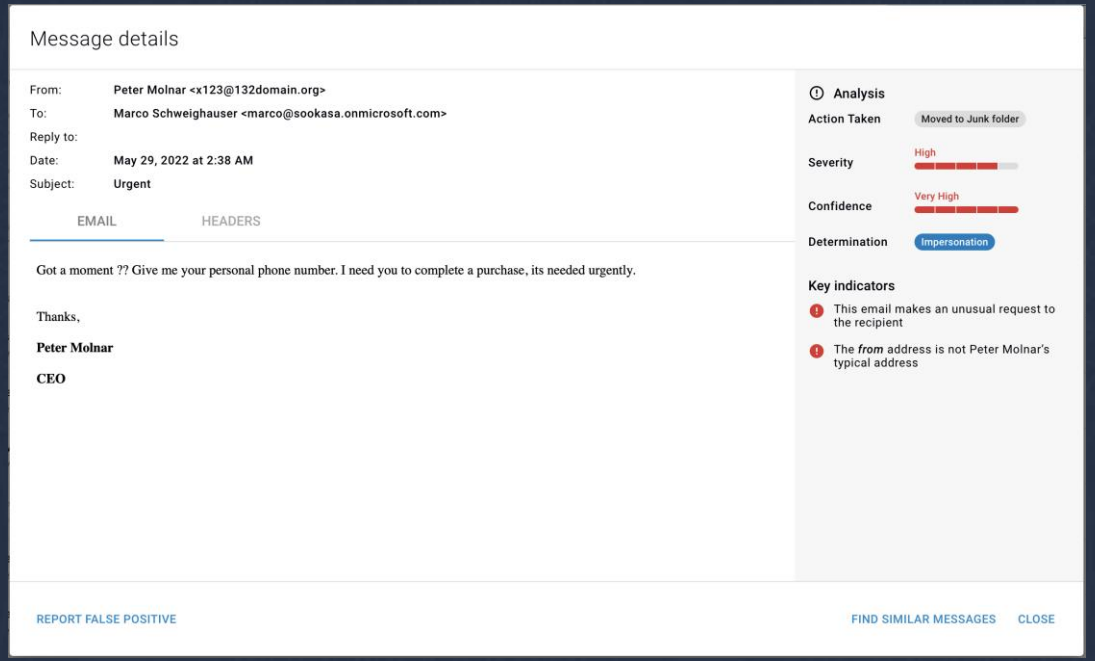
BEC: Impersonation model

Based on company sender stats model

Peter Molnar	
Absender	1421

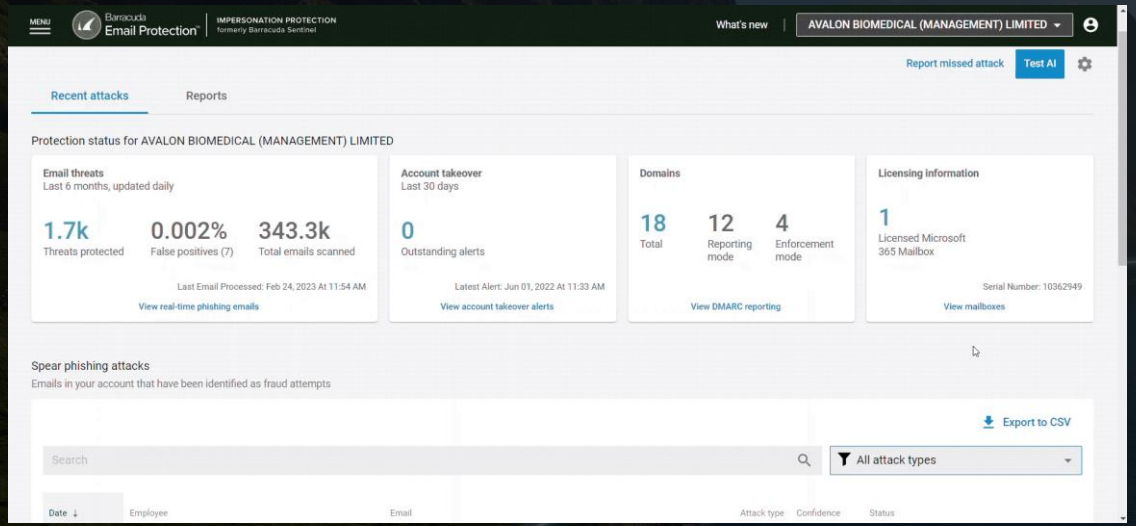
Peter Molnar x123@123domain.org	
Sender name + Email Address	0

x123@123domain.org	
Sender Email Address	0



Explainable AI/ML creates trust

IMPROVED!



What

- Inline highlighting of threats
- New: Key phrases and statistics highlighting

Benefit to customer

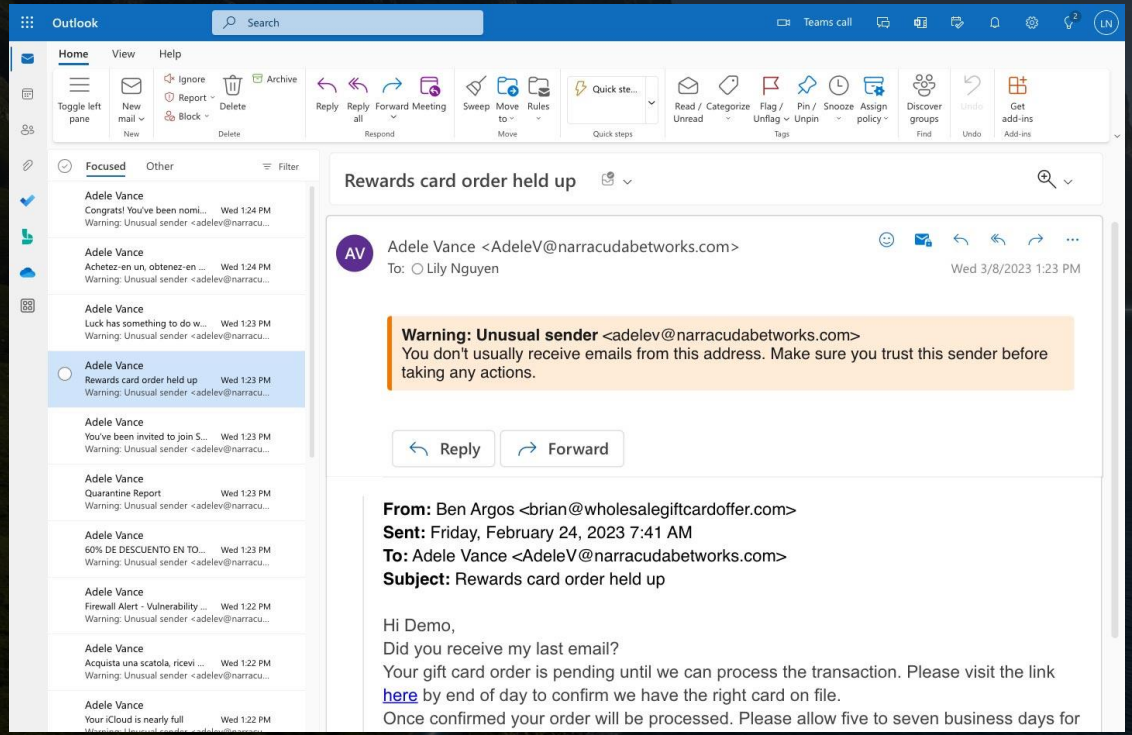
- Easy to understand threat detections

Benefit to you

- Competitor advantage

Email banners to guide end users

NEW!



What

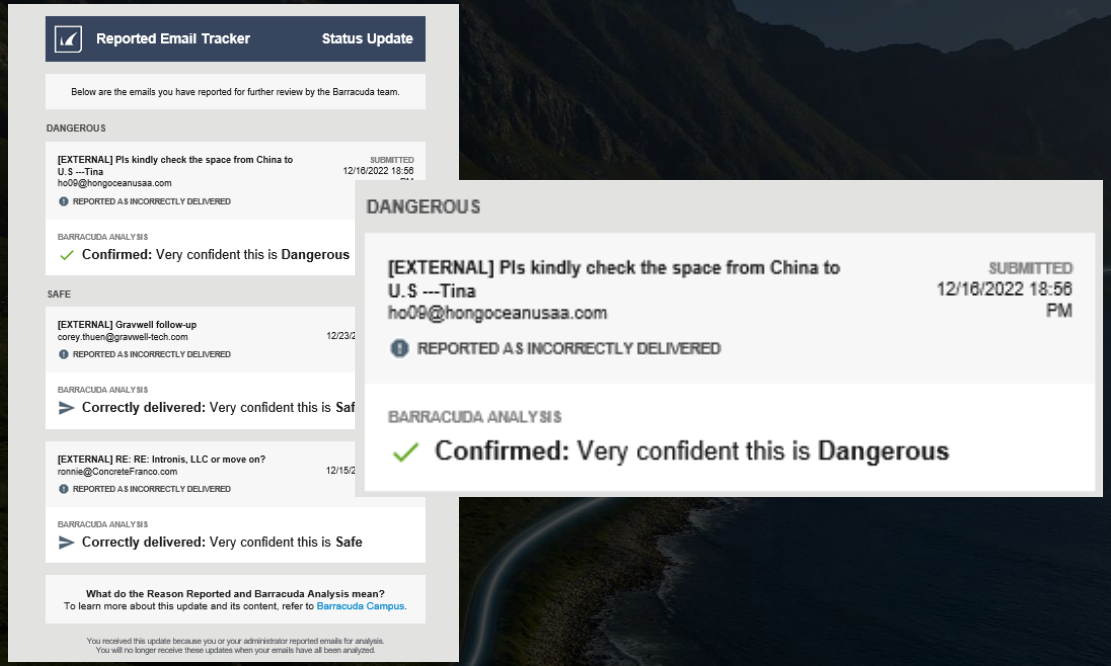
- Banners to educate end users

Benefit to customer

- Reduces risk and improves security awareness

Customer feedback is essential

NEW!



What

- Reported Email Tracker, providing Barracuda analysis to end users

Benefit to customer

- Visibility into efficacy feedback loop

Benefit to you

- Competitive advantage

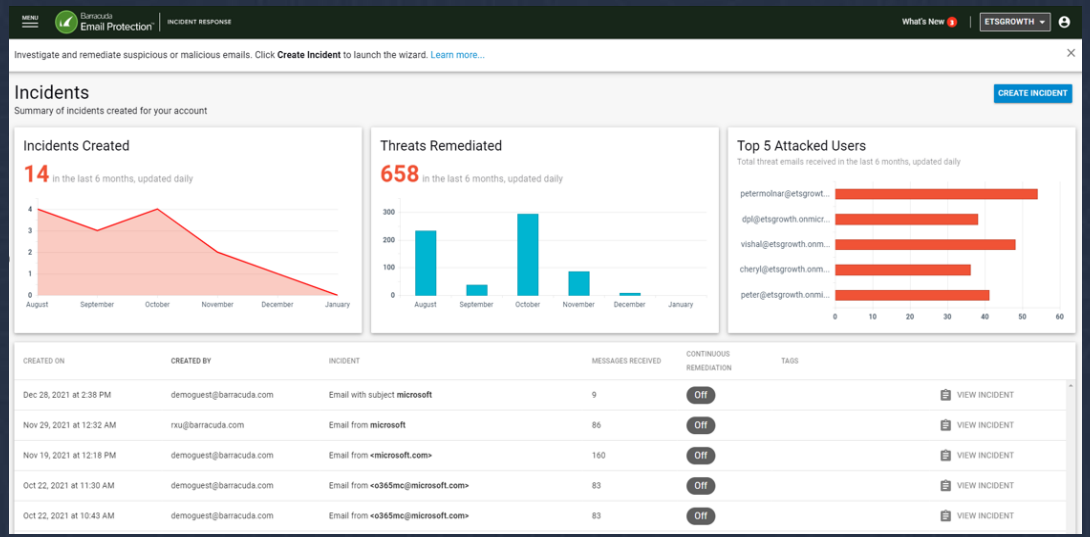
Detection and response

Better insights, faster remediation

THREAT PREVENTION | DETECTION AND RESPONSE | DATA PROTECTION AND COMPLIANCE

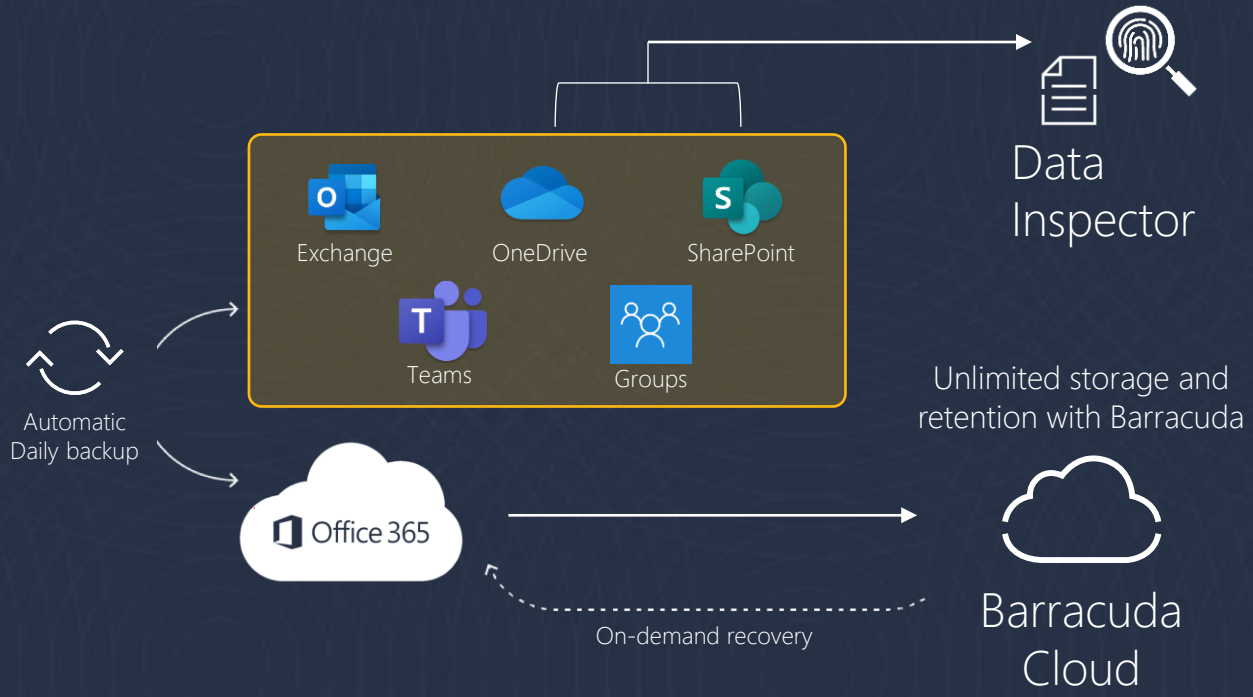
Community threat intelligence

Geographical Insights



Data protection and compliance

THREAT PREVENTION | DETECTION AND RESPONSE | DATA PROTECTION AND COMPLIANCE



Geteilte Zuständigkeit in der Cloud

Graphics by Microsoft

Microsoft

Files are permanently removed from the online recycle bin 93 days after they're deleted

Hi Julian Schreier,

We noticed that you recently deleted a large number of files from your OneDrive.

When files are deleted, they're stored in your recycle bin and can be restored within 93 days. After 93 days, deleted files are gone forever.

If you want to restore these files, go to the recycle bin. Select what you want to restore, and click the Restore button.

Ignore this mail if you meant to get rid of these files.

Learn more about deleting and restoring files.

Recycle bin

An underlying theme

Intentional Deletion

- Mobile Mitarbeiter
- ‘Mailbox voll’ Benachrichtigung
- Löscht versehentlich Inhalt
- IT stellt wieder her

An underlying theme

Intentional Deletion

- Travelling executive
- ‘Mailbox full’ message
- Deleted all inbox content
- Requested IT restore all deleted messages

Encryption

- Konversation mit externem Kontakt
- Externer Kontakt uploaded ein infiziertes File
- Mitarbeiter öffnet es
- Ransomware lokal verschlüsselt OneDrive

An underlying theme

Intentional Deletion

- Travelling executive
- ‘Mailbox full’ message
- Deleted all inbox content
- Requested IT restore all deleted messages

Encryption

- Conversation between employee and external contact
- External contact uploaded malicious file
- Employee opened attachment
- Ransomware against OneDrive

Ransomware

- Ransomware verteilt sich
- Malware wurde über Cobalt Strike zugestellt
- OneDrive am Endpoint verschlüsselt und nach MS365 repliziert

An underlying theme

Intentional Deletion

- Travelling executive
- ‘Mailbox full’ message
- Deleted all inbox content
- Requested IT restore all deleted messages

Encryption

- Conversation between employee and external contact
- External contact uploaded malicious file
- Employee opened attachment
- Ransomware against OneDrive

Ransomware

- Ransomware spreads across the network
- Malware was delivered via Cobalt Strike
- OneDrive encrypted on the endpoint and replicated to Microsoft 365

Accidental Deletion

- Verwendet native Retention
- Storage Limit erreicht, Kunde möchte nicht mehr benötigte Kopien löschen. Verwendet die PowerShell dafür
- Löscht versehentlich zu viel

An underlying theme

Intentional Deletion

- Travelling executive
- ‘Mailbox full’ message
- Deleted all inbox content
- Requested IT restore all deleted messages

Encryption

- Conversation between employee and external contact
- External contact uploaded malicious file
- Employee opened attachment
- Ransomware against OneDrive

Ransomware

- Ransomware spreads across the network
- Malware was delivered via Cobalt Strike
- OneDrive encrypted on the endpoint and replicated to Microsoft 365

Accidental Deletion

- Implemented native retention
- Hit storage limit allocations and had to remove copies of data via PowerShell
- During deletion accidentally removed many items

Accidental Deletion

- User hatte mehr Zugriff als notwendig
- Löschte versehentlich eine SharePoint Site
- Möchte es wiederherstellen
- Native Tools nicht leicht zu bedienen

An underlying theme

Intentional Deletion

Encryption

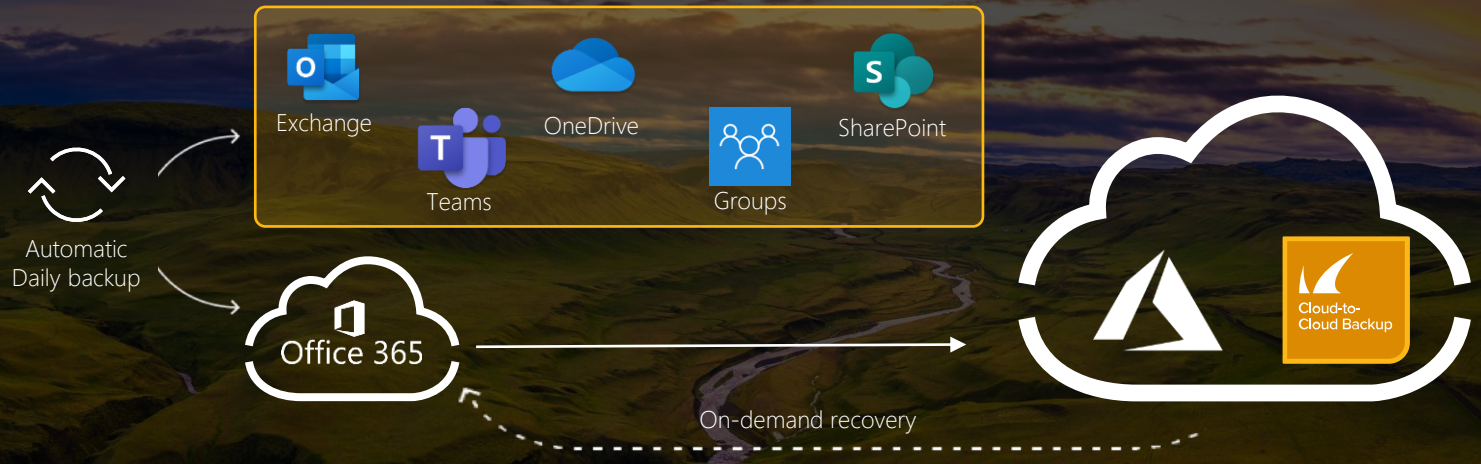
Ransomware

Accidental Deletion

Accidental Deletion

Barracuda

Cloud-to-Cloud Backup™



Schnelles deployment in unter 10 Minuten

Granulare Wiederherstellung von Office 365 data sources

Keine Software or **Hardware** die installiert oder gemanaged werden muss. SaaS Service managed von Barracuda

Unlimitierter storage und retention

Barracuda Office 365 survey:

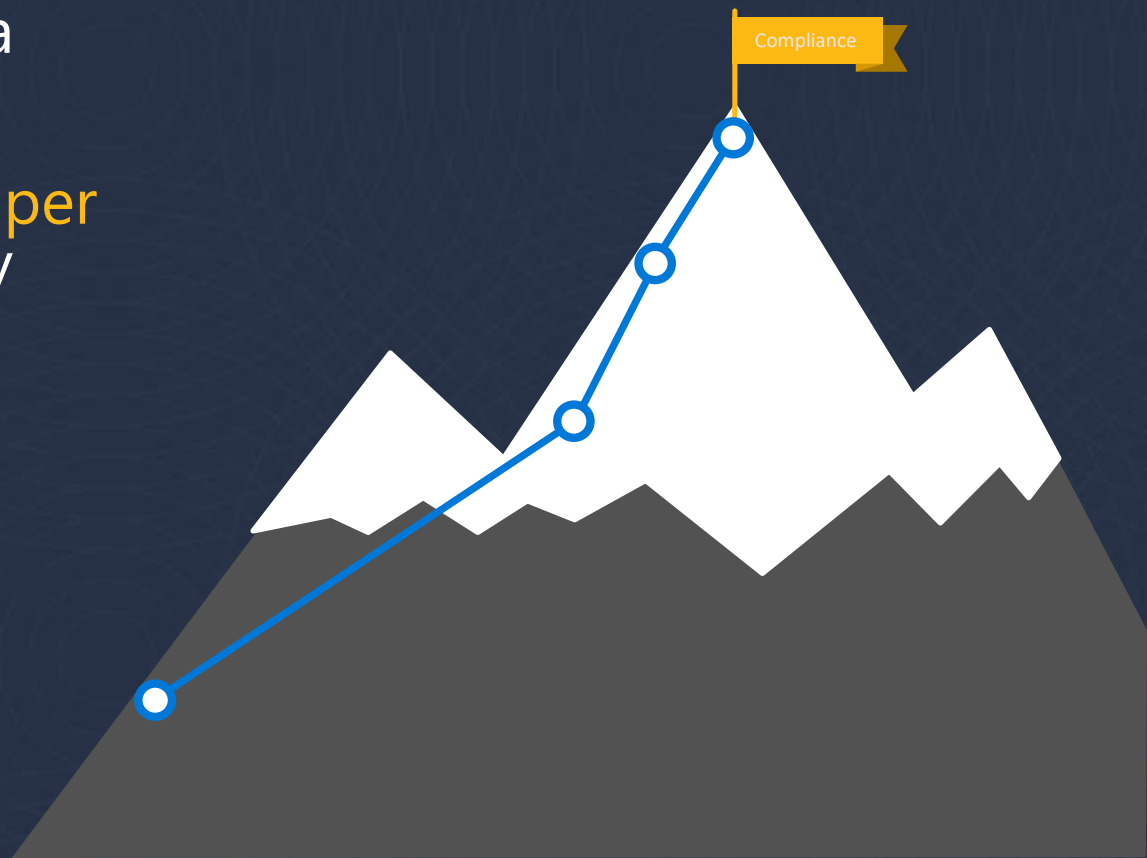
73% - I am concerned around complying with data privacy requirements

Maintaining compliance is challenging

50% YoY, electronic data growing exponentially

200 regulatory updates per day from 750 regulatory bodies

47% of executives were unsure what data compliance standards applied to their organization



Was ist falsch daran, sensible Daten auf OneDrive und SharePoint zu speichern?

- Sie können schwer kontrollieren, was Benutzer in SharePoint und OneDrive ablegen
- Es kann herausfordernd sein die Freigabe dieser Daten zu kontrollieren
- Es ist schwierig, sensible Daten zu finden, die ein Risiko für Ihr Unternehmen darstellen.
- Es erfüllt möglicherweise nicht die Compliance-Anforderungen für die Speicherung sensibler Daten

Barracuda
Data Inspector™

Automatisierte Erkennung von sensiblen Daten und Malware in OneDrive und SharePoint.

- Einfache Überprüfung der Ergebnisse mit Hilfe von geschwärzten Vorschaubildern
- Über 130 integrierte Klassifikatoren + Unterstützung für benutzerdefinierte Klassifikatoren
- Automatische Benachrichtigungen an Administratoren und Endbenutzer
- Kontrolle der Datenresidenz
- 100% SaaS, keine Einrichtung, schnelle Anmeldung

Lets walk through –

Barracuda
Data Inspector™

- Überblick über PII (personally identifiable information)
- Erkennen Sie Risiken auf einen Blick.
- Erkennen von latent threats in SharePoint und OneDrive ohne dem Risiko einer versehentlichen Aktivierung.
- Durch das Aufspüren vorhandener und neuer sensibler Daten gewährleisten Sie die Einhaltung von Vorschriften und reduzieren Risiko


Thank You
Barracuda
Your journey, secured.