

Microsoft 365 Veredelung mit Barracuda Email & Data Protection

Julian Schreier, Senior Sales Engineer



Teilweise geschützt

Less complex

Spam

geschützt

Data Exfiltration

Malware

URL Phishing

Scamming

Domain Impersonation

Spear Phishing

Brand Impersonation

Extortion

Business Email Compromise

Conversation Hijacking

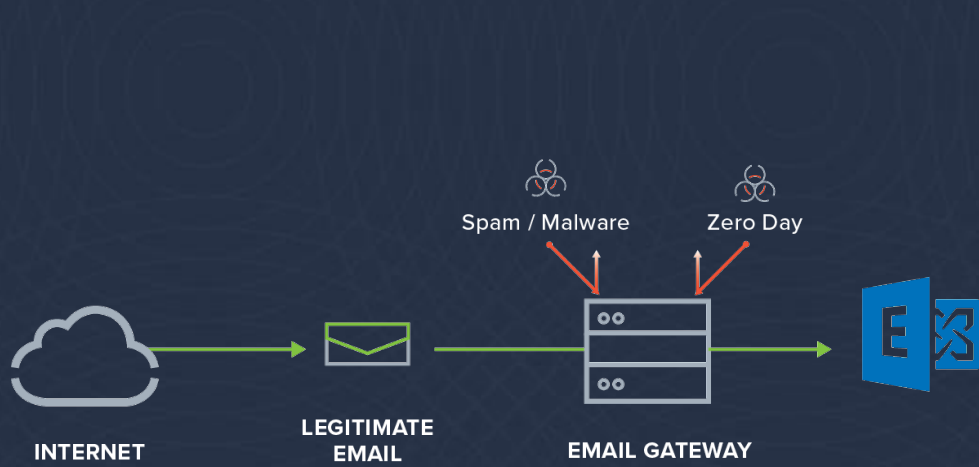
Lateral Phishing

Account Takeover

Oft ungeschützt

More complex





Inbox defense Technologie evaluiert unterschiedlichste Parameter



mehrere classifier



...und findet einzigartige Muster



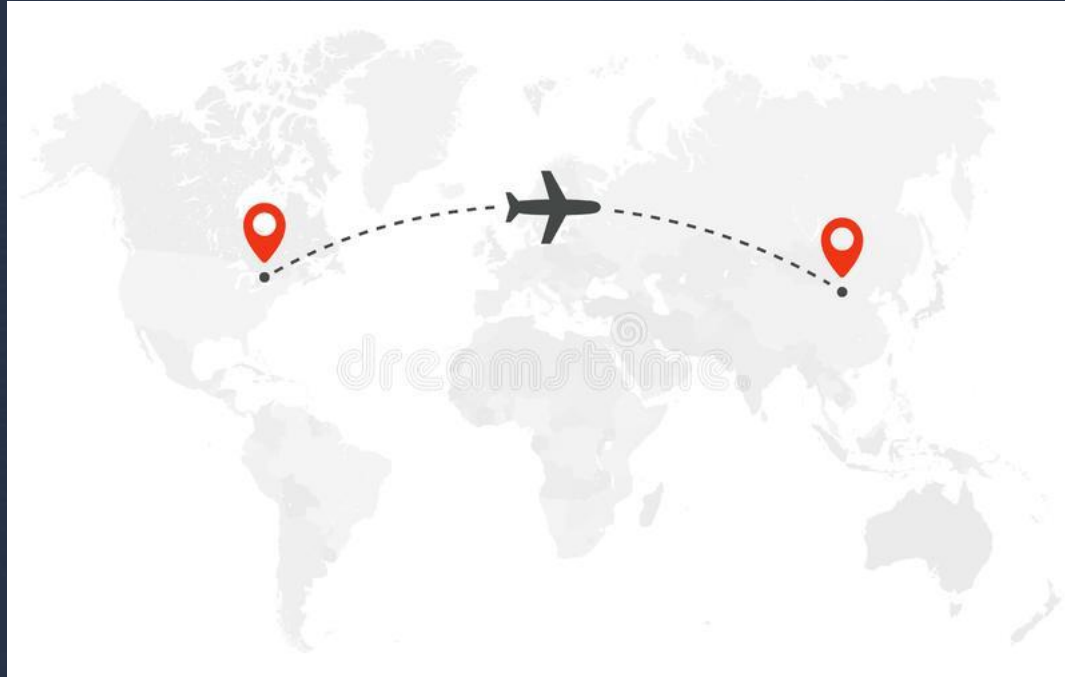
Versteht **abnormales Verhalten**

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

Message details

From: Peter Molnar <x123@132domain.org>
To: Marco Schweighauser <marco@sookasa.onmicrosoft.com>
Reply to:
Date: May 29, 2022 at 2:38 AM
Subject: Urgent

EMAIL HEADERS

Got a moment ?? Give me your personal phone number. I need you to complete a purchase, its needed urgently.

Thanks,
Peter Molnar
CEO

Analysis
Action Taken: Moved to Junk folder
Severity: High
Confidence: Very High
Determination: Impersonation

Key indicators

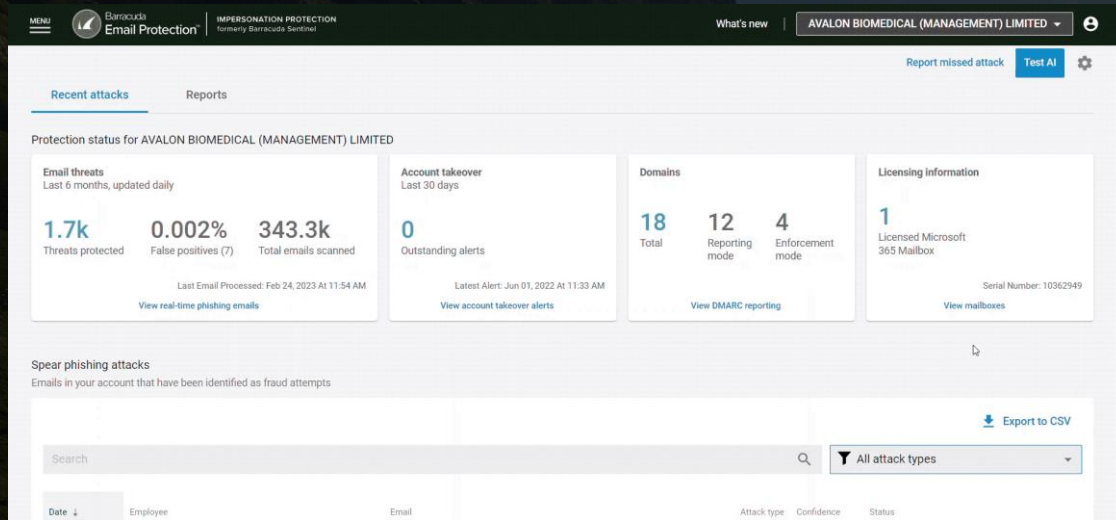
- 1 This email makes an unusual request to the recipient
- 1 The *from* address is not Peter Molnar's typical address

REPORT FALSE POSITIVE FIND SIMILAR MESSAGES CLOSE



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!

The screenshot shows the Outlook interface. The main email is from Adele Vance to Lily Nguyen, dated Wednesday, 3/8/2023 at 1:23 PM. The subject is "Rewards card order held up". A prominent orange warning banner is displayed at the top of the email body, stating: "Warning: Unusual sender <adelev@narracudabetworks.com> You don't usually receive emails from this address. Make sure you trust this sender before taking any actions." Below the banner are "Reply" and "Forward" buttons. The email content includes a greeting "Hi Demo," a question "Did you receive my last email?", and a message about a pending gift card order, with a link to confirm the order. The sender information at the bottom of the email reads: "From: Ben Argos <brian@wholesalegiftcardoffer.com> Sent: Friday, February 24, 2023 7:41 AM To: Adele Vance <AdeleV@narracudabetworks.com> Subject: Rewards card order held up".

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

Reported Email Tracker Status Update

Below are the emails you have reported for further review by the Barracuda team.

DANGEROUS

[EXTERNAL] Pls kindly check the space from China to U.S ---Tina
ho09@hongoceanusaa.com
SUBMITTED 12/16/2022 18:56 PM
REPORTED AS INCORRECTLY DELIVERED

BARRACUDA ANALYSIS
✔ **Confirmed:** Very confident this is Dangerous

SAFE

[EXTERNAL] Gravwell follow-up
corey.thues@gravwell-tech.com
12/23/22
REPORTED AS INCORRECTLY DELIVERED

BARRACUDA ANALYSIS
➤ **Correctly delivered:** Very confident this is Safe

[EXTERNAL] RE: RE: Intronis, LLC or move on?
ronnie@ConcreteFranco.com
12/15/22
REPORTED AS INCORRECTLY DELIVERED

BARRACUDA ANALYSIS
➤ **Correctly delivered:** Very confident this is Safe

What do the Reason Reported and Barracuda Analysis mean?
To learn more about this update and its content, refer to [Barracuda Campus](#).

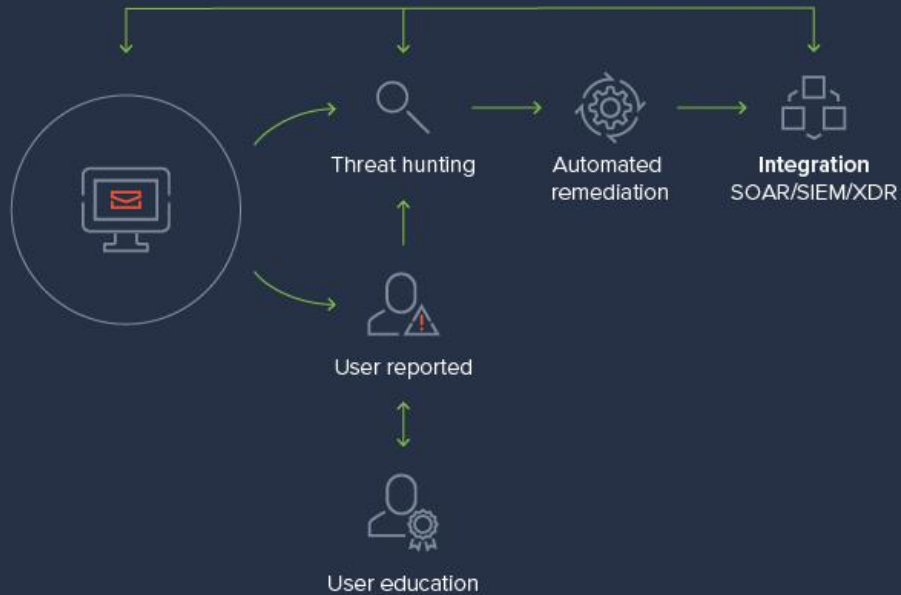
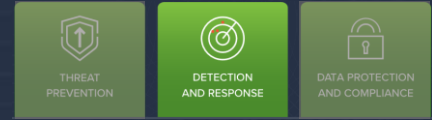
You received this update because you or your administrator reported emails for analysis. You will no longer receive these updates when your emails have all been analyzed.

DANGEROUS

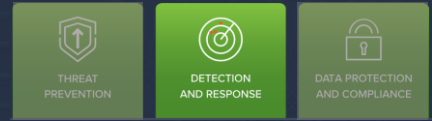
[EXTERNAL] Pls kindly check the space from China to U.S ---Tina
ho09@hongoceanusaa.com
SUBMITTED 12/16/2022 18:56 PM
REPORTED AS INCORRECTLY DELIVERED

BARRACUDA ANALYSIS
✔ **Confirmed:** Very confident this is Dangerous

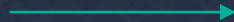
Detection and response



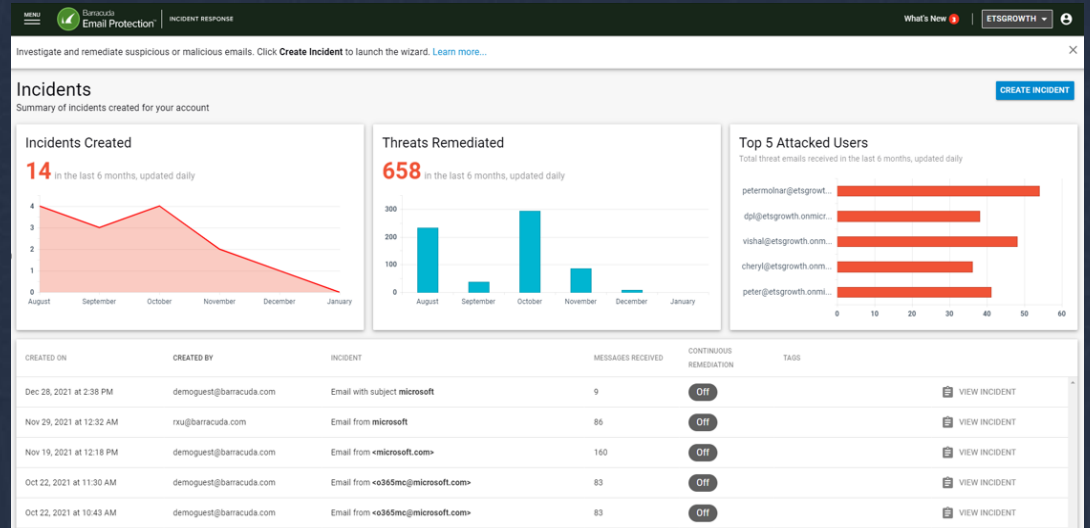
Better insights, faster remediation



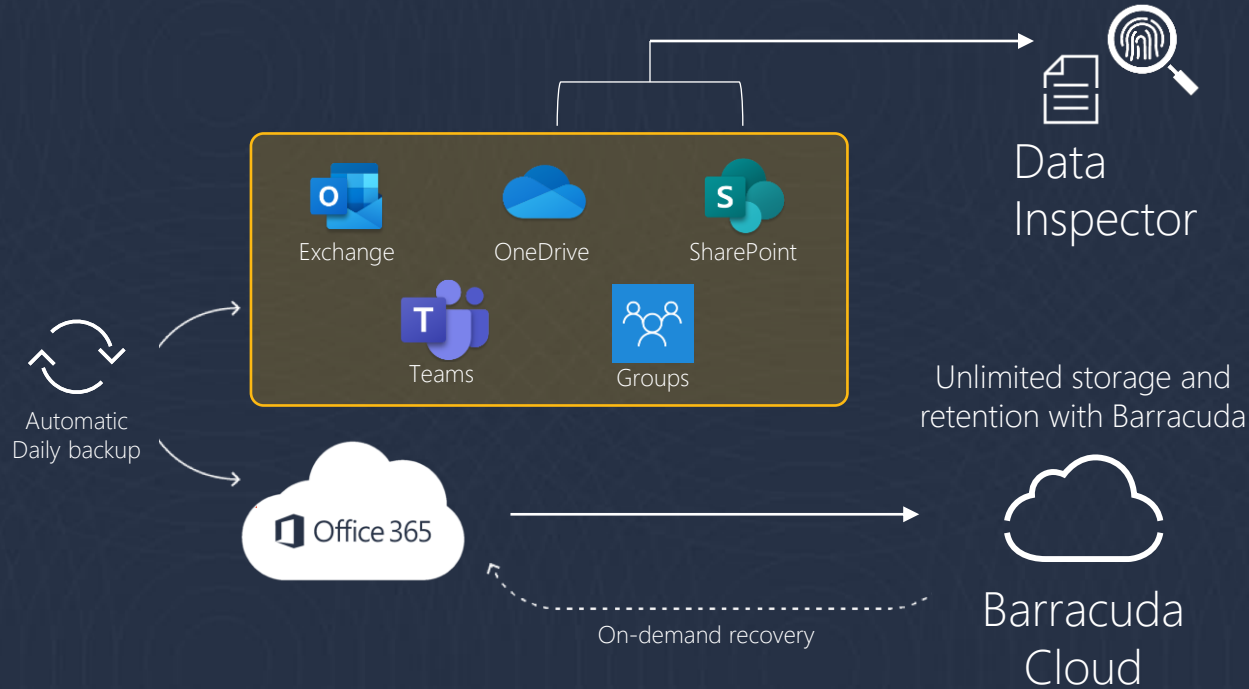
Community threat intelligence



Geographical Insights

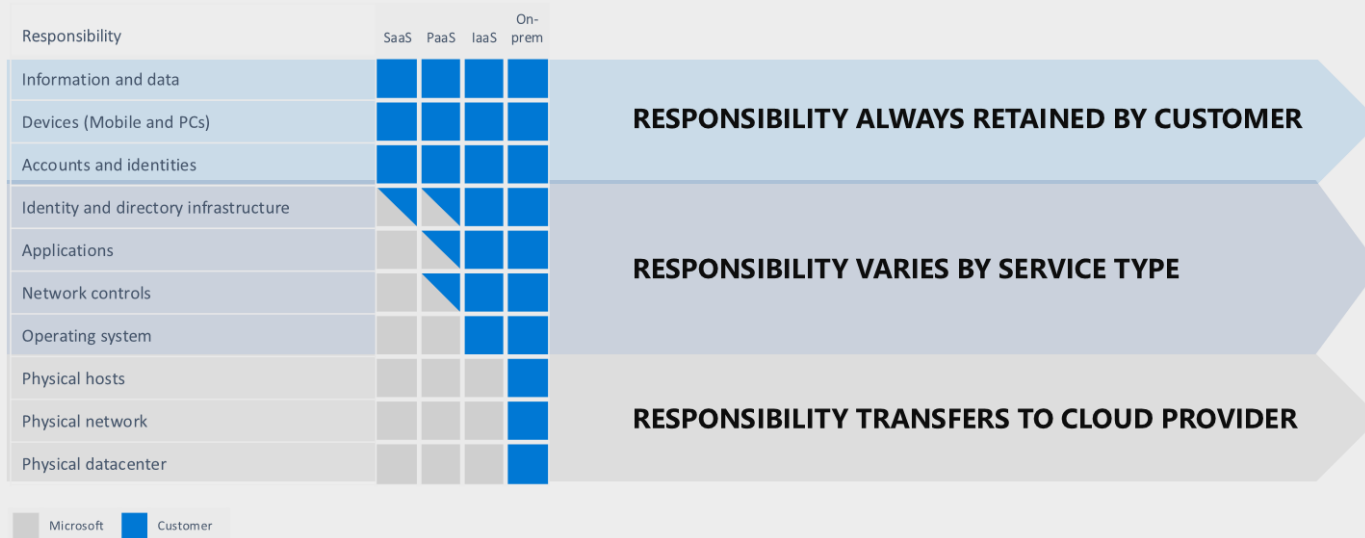


Data protection and compliance



Geteilte Zuständigkeit in der Cloud

Shared responsibility model





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

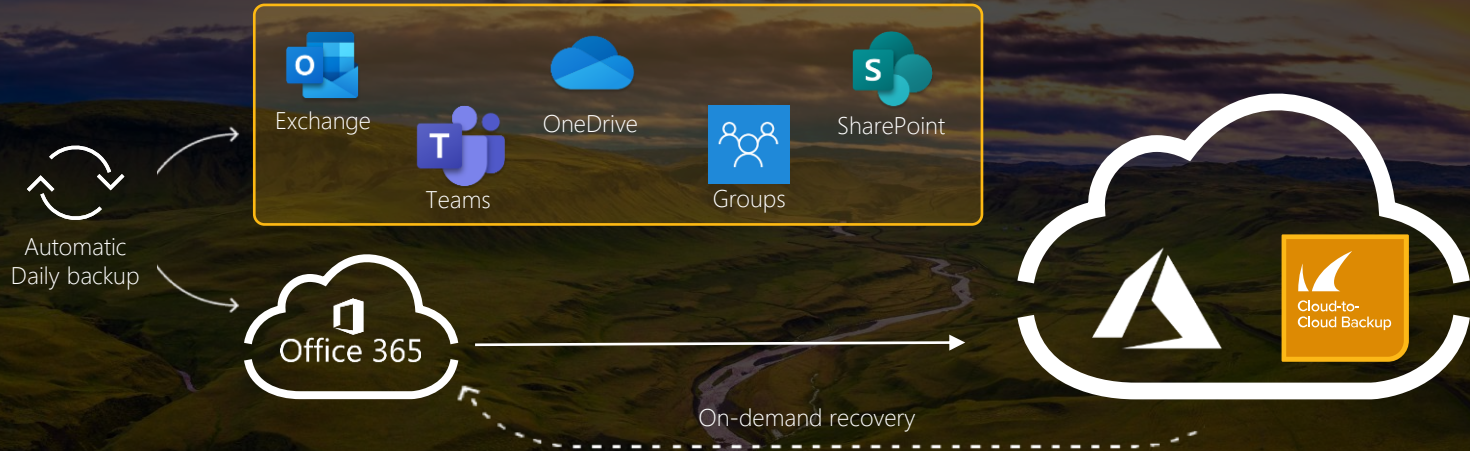


Accidental
Deletion



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:



Key findings

FINDING #1

Protecting data against attack and loss—both from outside actors and inside sources—is a key concern.

Data needs to be protected from outside attacks, such as [ransomware](#), and from internal loss, such as accidental or malicious deletion. Data protection and security for both scenarios is strongly desired by respondents.

Ransomware attacks may not occur every day, but they remain top of mind, which is no surprise based on the ransomware trends in the news. While most news reports describe the fallout, and often the means of attack, they don't describe what is targeted, lest this information be used for future attacks.

Despite not knowing what specifically may be attacked, those surveyed are well aware that Office 365 could be the target of ransomware; 72% of those polled were concerned about such an attack. Concern was highest in the U.S. (83%) and lowest in EMEA (67%), with APAC coming in at 73%.

This is perhaps not surprising, given that more than half of respondents have been a victim of ransomware. The geographic differences align here as well. Nearly two-thirds of U.S.

respondents (64%) have fallen victim to ransomware, while 55% of APAC respondents and only 43% of respondents in EMEA have been affected by these attacks. The pain associated with being shut out of email and other collaborative applications is clear, especially with the extent of remote work.

Another factor that ramps up the concern around ransomware is the current ransomware trend of data exfiltration, where the data is stolen before it is locked and the information is sold back to the owner, or in cases where the owner of the data will not pay. It is sold to the highest bidder on the dark web. Data breaches such as these are potentially embarrassing and often expensive.

When it comes to data protection, security against accidental or malicious deletion is a far more common issue and equally concerning. Nearly 80% of those surveyed want multiple layers of role-based access control to limit who has access to potentially harmful actions, such as data deletion and purging.

My organization has experienced a ransomware attack.

52% agree (n=124)



I am concerned with ransomware locking/attacking my O365 data.

72% agree (n=155)



Multiple layers of role-based access control for backup copies is important to me.

79% agree (n=163)



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

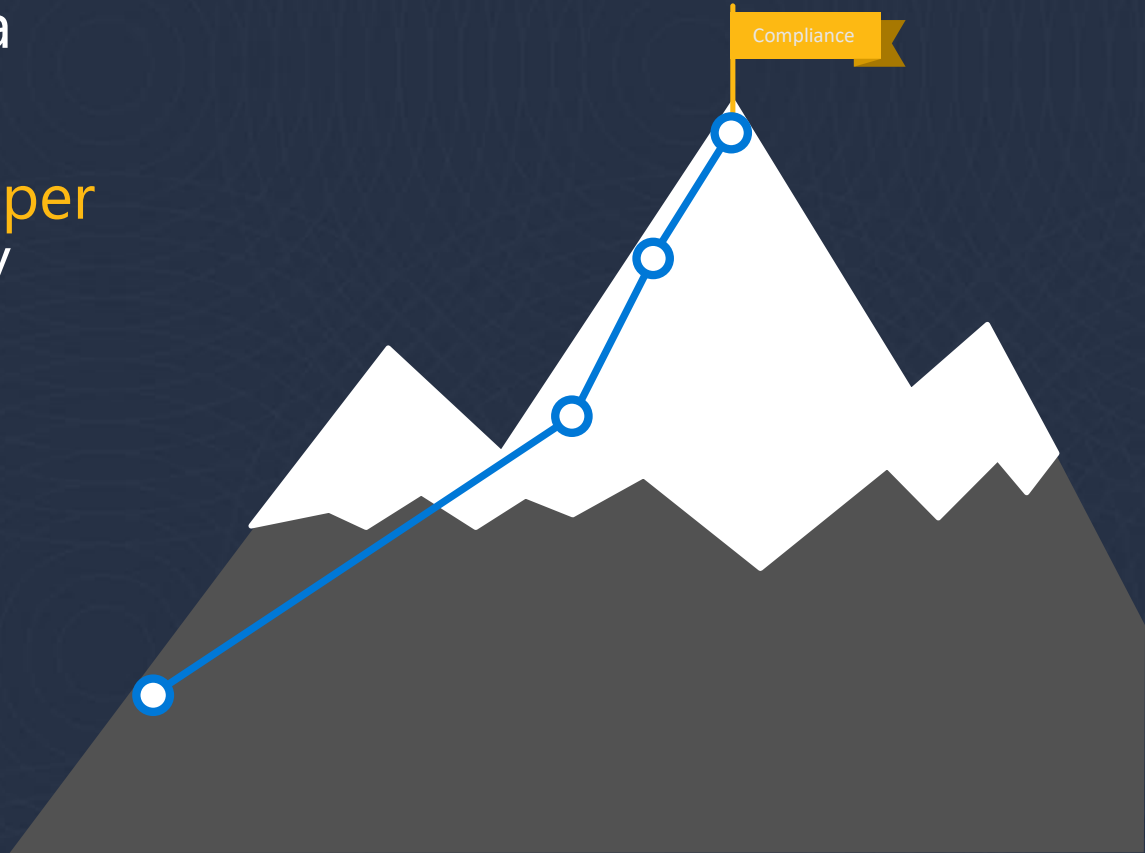


Maintaining compliance is challenging

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™





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

