



Barracuda Email Protection

Securing your email, users, data, and access



WOUTER HOEFFNAGEL - 08 MEI 2024

Deel dit artikel



Aantal cyberaanvallen in Nederland bovengemiddeld hard gegroeid

Het aantal wekelijkse cyberaanvallen is in het eerste kwartaal van 2024 in Nederland harder gestegen dan de wereldwijde trend. De onderwijs- en onderzoekssector is daarbij de meest geviseerde sector met gemiddeld 1301 aanvallen per week.

Security

Data protection

Hardware



Impact

Hackers vragen vaak 2% van de jaaromzet als losgeld, terwijl het IT budget over het algemeen 3-5% van de jaaromzet is. De boete van de ransomware aanval (enkele tonnen) zijn daarnaast niet de enige kosten die hiermee gemoeid gaan.

Kosten zitten met name ook in:

- **Reputatie schade**
- **Het niet kunnen geven van onderwijs voor 3 weken**
- Inschakelen van IT bedrijven voor incident response
- Verlies van gegevens
- Herstelkosten

Bron: Dutch IT Channel

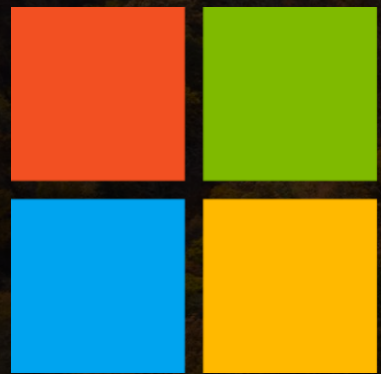
Normenkader

Eerste prioriteit zou uit moeten gaan naar:

- Bescherming van de medewerker op technisch vlak (betere detectie tooling)
- Bescherming van de medewerker door trainen bewustwording (security awareness)
- Identity and Access Management (zero trust ontsluiten van toegang tot M365 om account take-overs tegen te gaan)
- Incident Beheer: incident reponse
- Back-up en herstel (cloud to cloud backup en archivering zijn onderdeel van het pakket)

Mitigeren hoge risico's

Voor de mitigatie van de hoge risico's zijn de volgende onderdelen van belang: Risicomanagement, Personeelsbeheer (het veiligheidsbewustwording bij medewerkers en technisch veilige omgeving voor wijzingen), Identity en Access Management, Security Management (het beheer fysieke toegangsrechten), IT-operatie (back-up en herstel), Bedrijfscontinuïteitsmanagement en Leveranciersmanagement. In Tabel 17 is een selectie gemaakt van de percentages van schoolbesturen dat op deze domeinen de norm haalt. De tabel toont aan dat zelfs bij de domeinen met de hoogste scores hooguit een kwart van de besturen voldoet aan de norm. Hiermee heeft slechts een klein deel van de besturen de maatregelen genomen om de hoge risico's op het vlak van informatiebeveiliging te mitigeren.



Microsoft



Email attacks in 2024: what's the risk?



75%

Organizations experienced a successful email attack in 2023



\$1M

Serious attacks are expensive:

- Downtime
- Data loss
- Reputation
- Ransoms

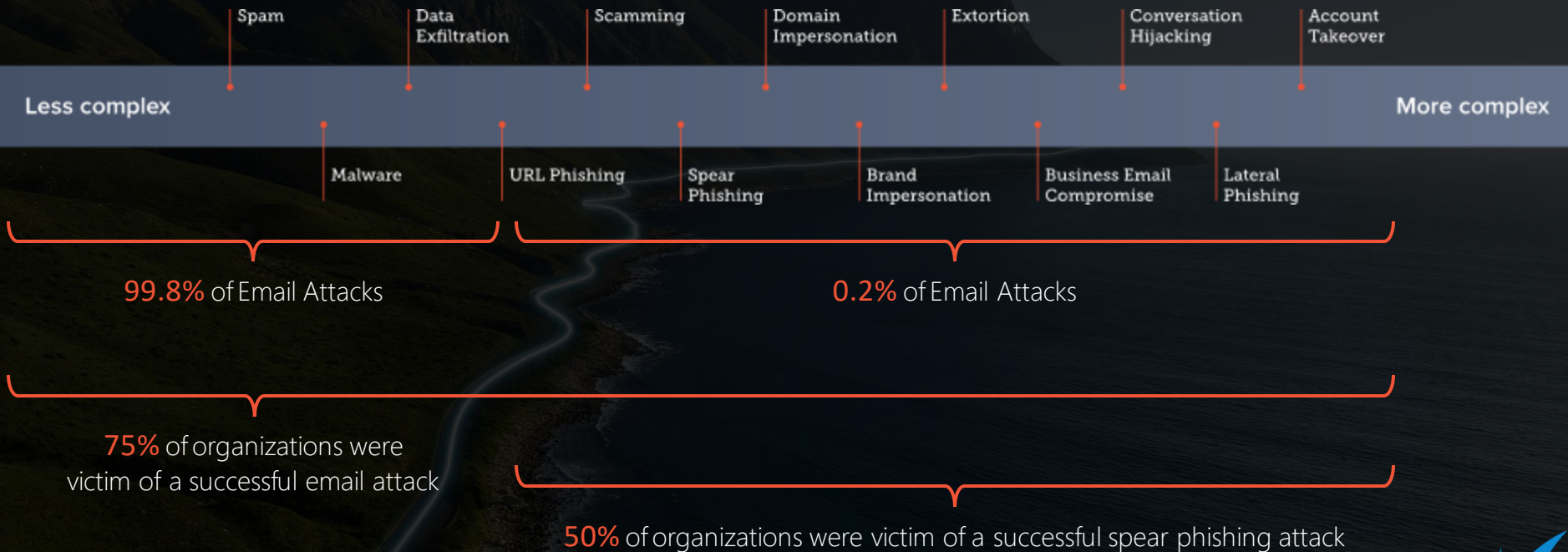


98%

Organizations are not fully prepared to deal with email security risks

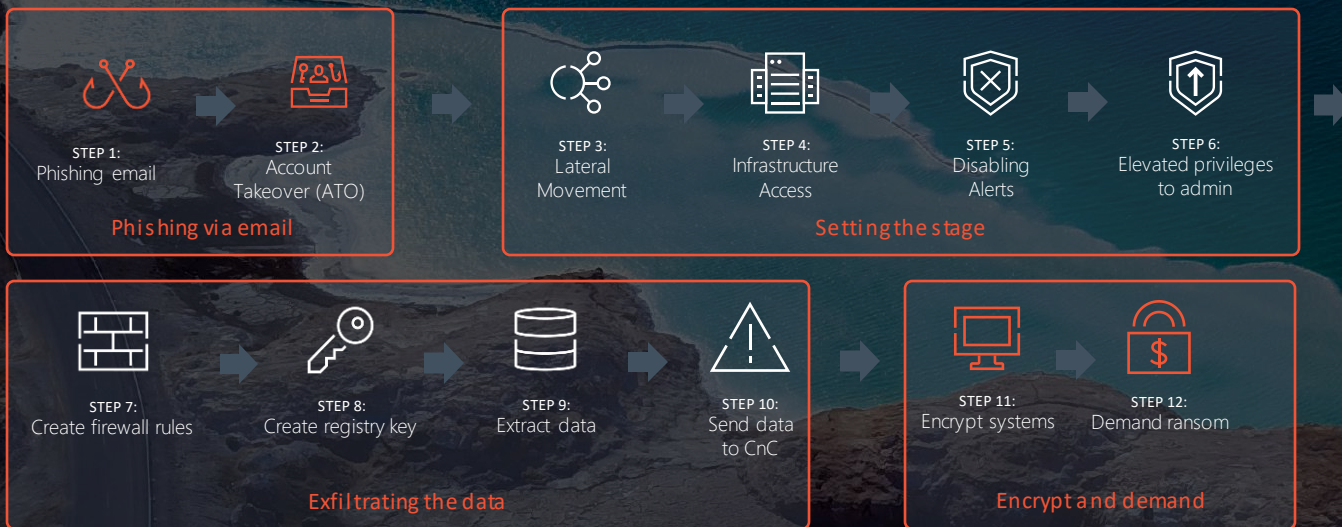


Phishing is **STILL** the primary risk surface



Today, Ransomware is the most prevalent attack type

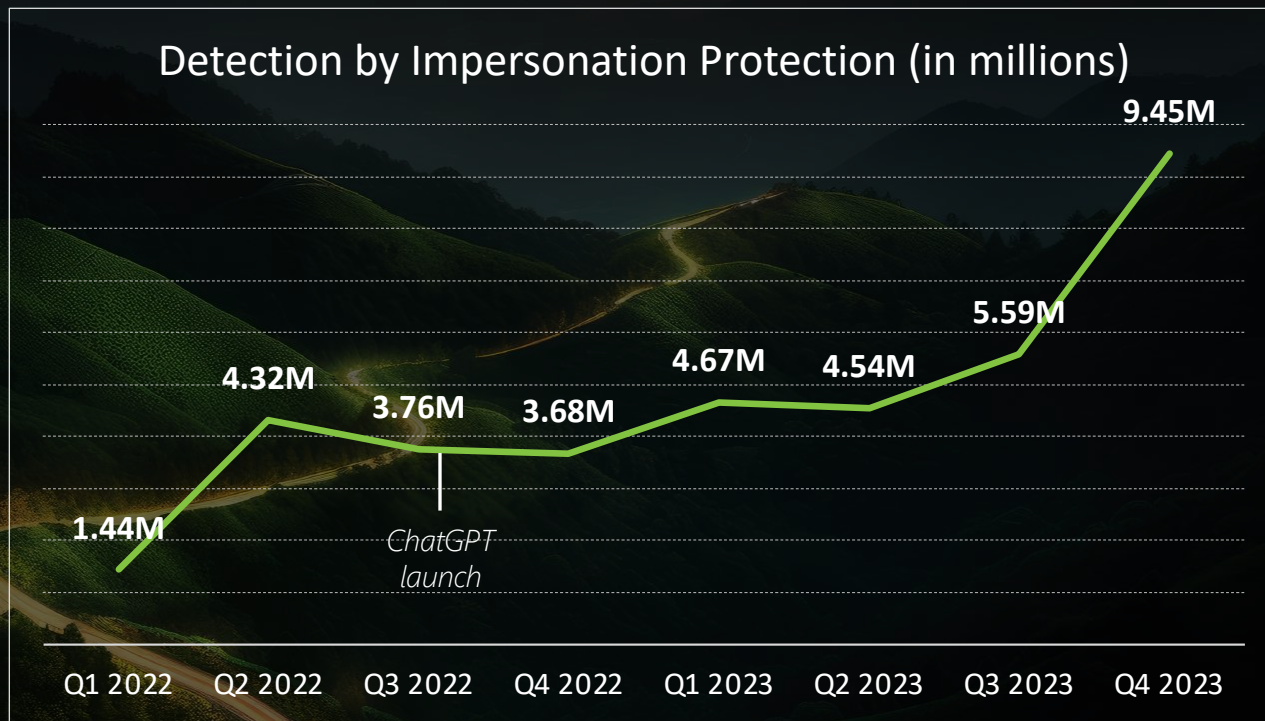
Example ransomware attack chain



Surge in phishing with GenAI-based attacks

Phishing detections significantly increased in the past 18 months

- ChatGPT enables hackers to scale up attacks
- Solution: continuous improvement in detection efficacy



Secure your email, users, data, and access

THREAT PREVENTION

Spam, Malware, and ATP
Phishing and Impersonation Protection
Account Takeover Protection
Domain Fraud Protection
Web Security
Zero Trust Access for Microsoft 365

DETECTION AND RESPONSE

Incident Response
Security Awareness Training

DATA PROTECTION AND COMPLIANCE

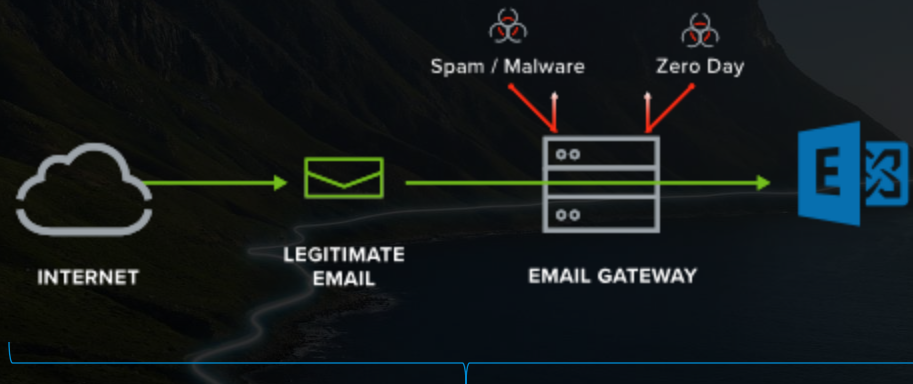
Email Encryption and DLP
Cloud-to-Cloud Backup
Cloud Archiving Service
Data Inspector™



Barracuda
Email Protection™



Gateway defense: stop volumetric attacks



- Blocks spam and malware
- Protects against bad links and attachments
- Intercepts sensitive data leaving your organization
- Encrypts outbound email



Detecting Image-based phishing using ML

Your Order Has Been Placed!

MZ

o

To: o

Tuesday, January 10, 2023 at 8:21 AM

Order Summary

Description	Quantity	Unit Price	Total
Geek Squad Best Buy Service	1 Year Subscription	\$389.99	\$389.99
		\$0.00	\$0.00
		Total:	\$389.99

Receipt Id:
Any issue with this transaction?

Important Information About Your Order:

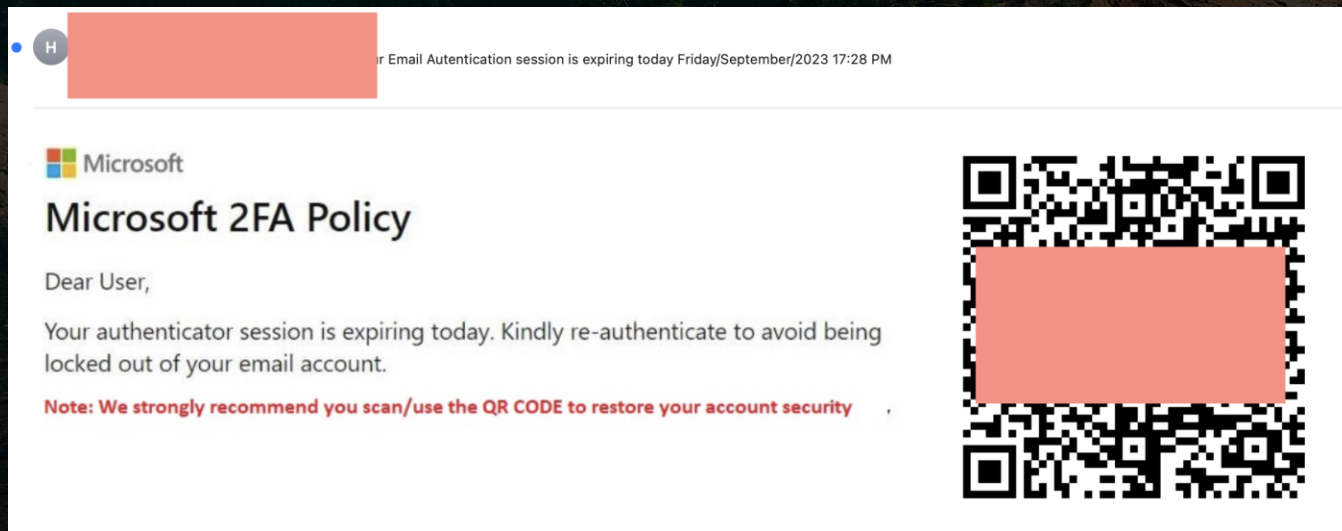
If you didn't authorize this Charge, you have 24 Hrs. To cancel & get an instant refund of your annual subscription, please contact our customer care at

Sincerely,
GEEK-SQUAD™ Best Buy Customer Care

Customer Support

Copyright © 2023 Support Inc. All rights reserved

Detecting QR Code attacks using ML



Employee Impersonation

Message details

From: Sheila Tracy <mail4152803@gmail.com>
To: Rhonda Larson <rlarson@...>
Reply to:
Date: Mar 21, 2022 at 1:04 PM
Subject: PAYROLL ACCOUNT UPDATE

Impersonation
techniques

Analysis

Determination

Impersonation

Key indicators

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

EMAIL

HEADERS

[External]

Good Afternoon
ASAP - I want to update my paycheck account information. Will the change be effective for the next pay date

Thanks
Sheila Tracy

No malicious payload (i.e., link or attachment) Making a simple request from a known contact

[FIND SIMILAR MESSAGES](#) [DISMISS](#)

High reputation senders | No links | No attachments

Conversation Hijacking

Message details

From: JoAnn Dase <joann.dase@dynamicquests.com>
To: Yolanda Childs <ychilds@dynamicquest.com>
Reply to:
Date: Jul 13, 2021 at 10:14 AM
Subject: ACH Payment Method

EMAIL

HEADERS

CAUTION: This email originated from outside the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

We had a change in payment procedures, and we are switching to ACH method of receiving payment only. Also we have a 3.5% discount on payment made via ACH this week.
Please advise when is our next scheduled payment date and what is the total amount? So we can forward our updated ACH instructions.

Thanks.

JoAnn Dase // Manager of Revenue & Billing
joann.dase@dynamicquest.com



Direct: 336-389-0911

IT Services // Service Desk // Data Center // Security // Backups // Phone Systems // Software Development

Analysis

Determination

Conversation Hijacking

Key indicators

- ❗ This email is potentially part of a conversation hijacking attack
- ❗ This email has a sender domain **dynamicquests.com** that appears to be impersonating the domain **dynamicquest.com**

One extra letter "s" in the email address
dynamicquest.com vs. dynamicquests.com

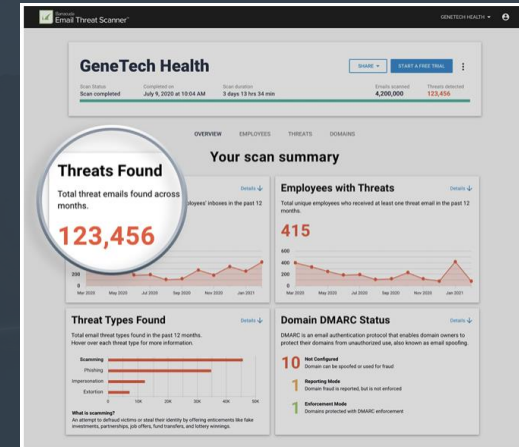
Asking to make/update
payment via ACH

See for yourself with a free Email Threat Scan



Barracuda
Email Threat Scanner™

- Identify gaps in email security
- Find threats inside Microsoft 365 inboxes
- See threats visualized in multiple ways
- Get a shareable report about threats
- Start a free trial directly from the results!



21,000

Organizations already run the scan

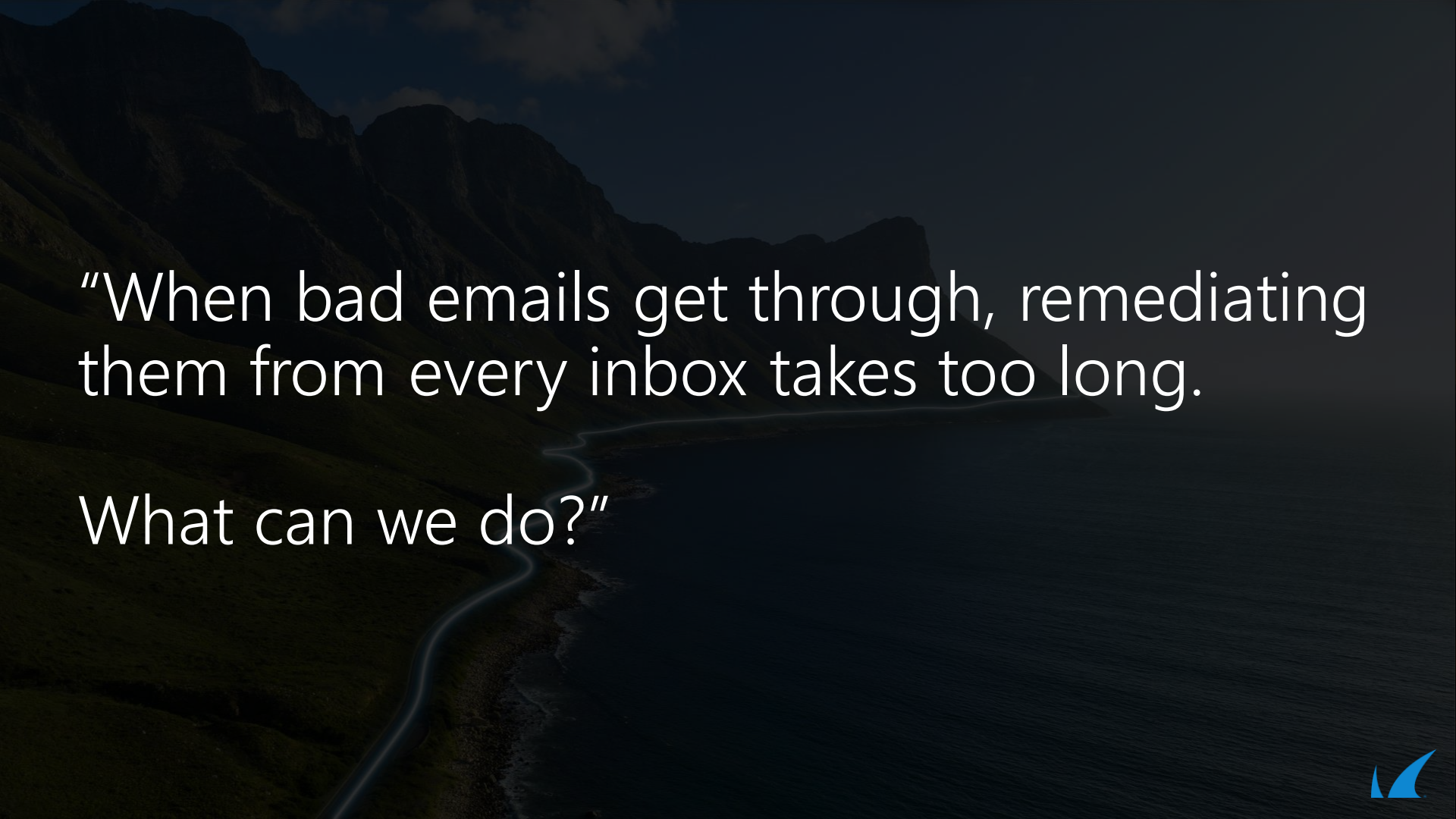
20M

Mailboxes scanned
for threats

21M

Spear-phishing
attacks identified





"When bad emails get through, remediating them from every inbox takes too long.

What can we do?"



Post-delivery response: a key bottleneck

3.5 days



Average amount of time an attack spends in a user's inbox until it is discovered and remediated



The answer: Incident Response with M-SOAR



Threat Intelligence



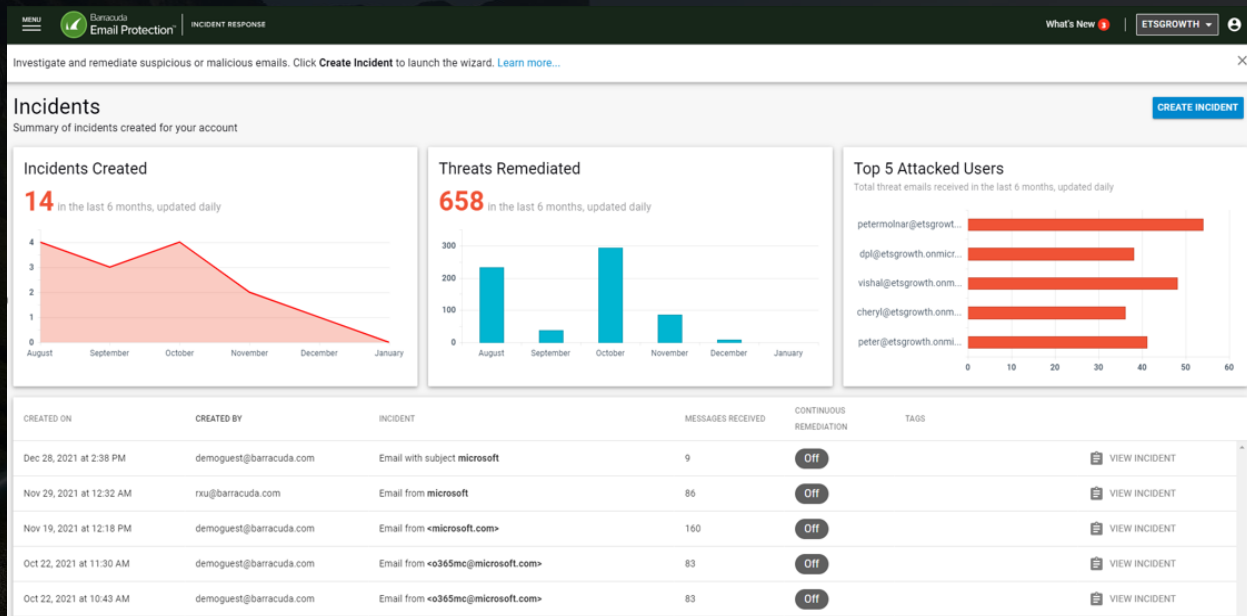
Automation



Response



Orchestration



M-SOAR: reduce workload by up to 90%



Threat Intelligence



Automation



Response



Orchestration



Community Intel



Geo Insights



User Reported



Admin Reported



Incident
Response



M-SOAR: reduce workload by up to 90%



Threat Intelligence



Automation

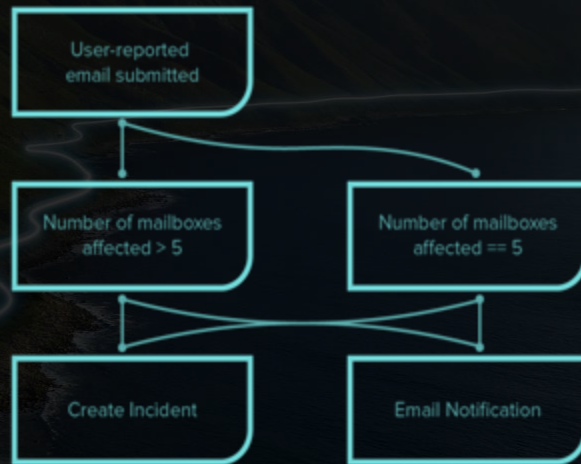


Response



Orchestration

Automates repetitive manual processes:



M-SOAR: reduce workload by up to 90%



Threat Intelligence



Automation

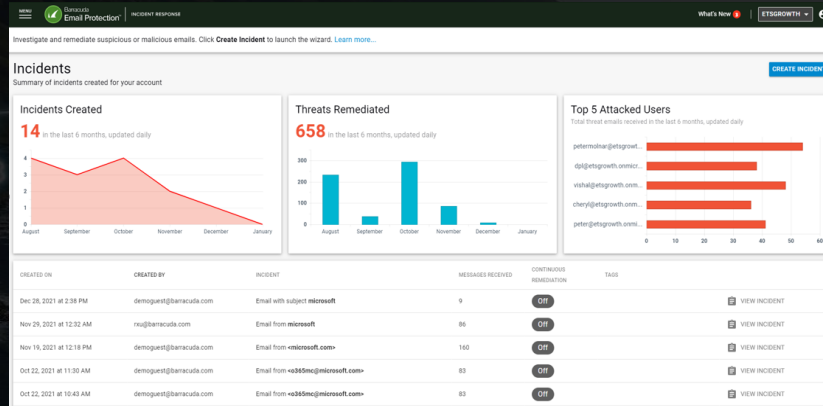


Response



Orchestration

Single dashboard to monitor, report and execute incident response



"It's more automated now, with the AI doing a lot of the heavy lifting." – Head of IT @ UK Car Dealer



M-SOAR: reduce workload by up to 90%



Threat Intelligence



Automation



Response



Orchestration

Supports integrations between email security applications



Incident Response

Email
Gateway
Defense

Impersonation
Protection

Security Awareness Training™



"We use Microsoft 365 extensively – email, SharePoint, OneDrive, and Teams.

We have in-office and remote employees.

If there's an account takeover, how do we protect our Microsoft applications?"



Zero Trust Access for M365: secure access



In the office or Remote



Zero Trust Access

- Identity-Based User Authentication
- Device Authentication
- Device Health Checks (ongoing)
- Per-Application Permissions
- Central Management and Logging
- On-Demand Autoscaling
- Simple Always-On Connectivity



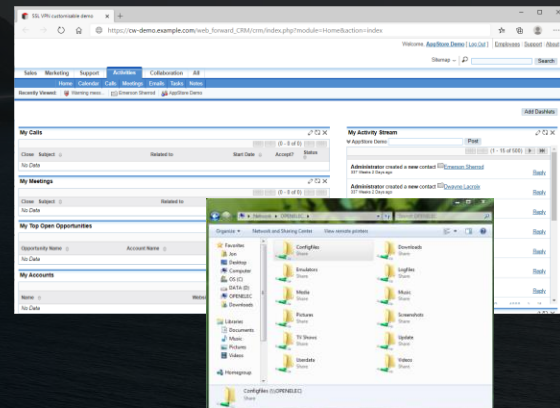
Compromised Accounts



Insecure or Untrusted
Devices



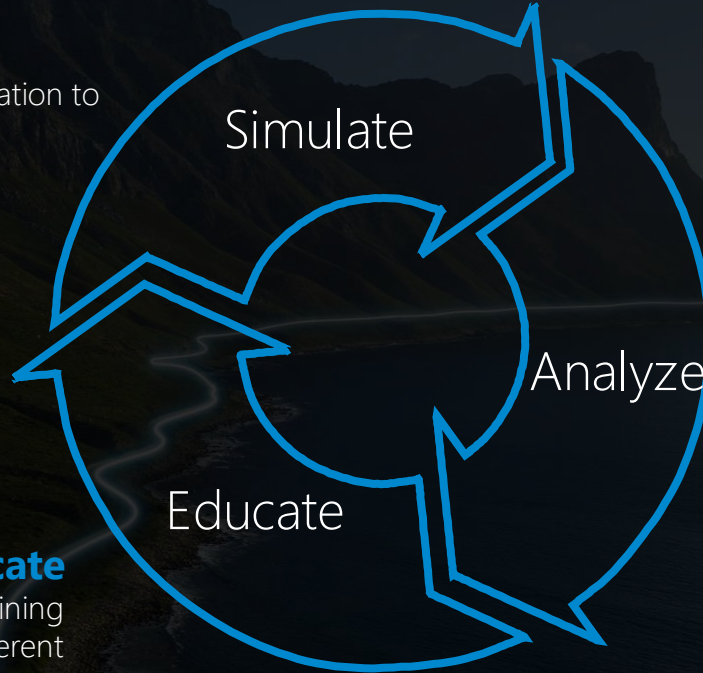
Microsoft 365 Applications



Security Awareness Training: the process

Simulate

Real-world threat simulation to assess user awareness



Analyze

Detailed reporting metrics to determine threat risk and inform the next campaign

Educate

Extensive library of training content tailored for different learning styles and abilities

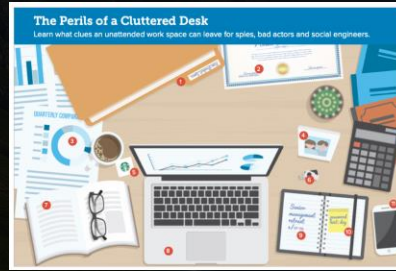


Multi-modal, multi-country content

Animated videos (3-5 mins)



Infographics



Threat spotting guides



Curriculums



"With the advanced anti-phishing protection and security awareness training, we have built the best security against ransomware getting in. " – Superintendent of Technology @ Texas-based Independent School District



Integrated with Incident Response

View incident
Incidents > Email from <adelev@narracadabetworks.com> with subject Testing Shared Mailboxes

Incident details
Information about the incident

Reported: Jul 20, 2023 at 3:51 AM
By: nguyenv@bostonbrew.gq
Impact: 1 messages affected 1 internal and 0 external users
Continuous remediation: ☐

Search criteria

Sender: <adelev@narracadabetworks.com>
Subject: Testing Shared Mailboxes
Message body text:
Message body URL:
Attachment:

Actions taken for remediation
Remediation actions you chose to take on the emails below

- Deleted email in 1 internal users' mailboxes
 - 1 emails deleted, 0 through continuous remediation
- Sent email alert to 1 internal recipients

Tags: test test3 test4

[Additional recommended actions to recover from the incident](#)

Users involved
The following users were affected by emails in this incident

	Email	User type	Clicked on links	Opened email	Replied to email	Forwarded email
<input type="checkbox"/>	bostonshared@bostonbrew.dev	Internal	Off	No	No	No

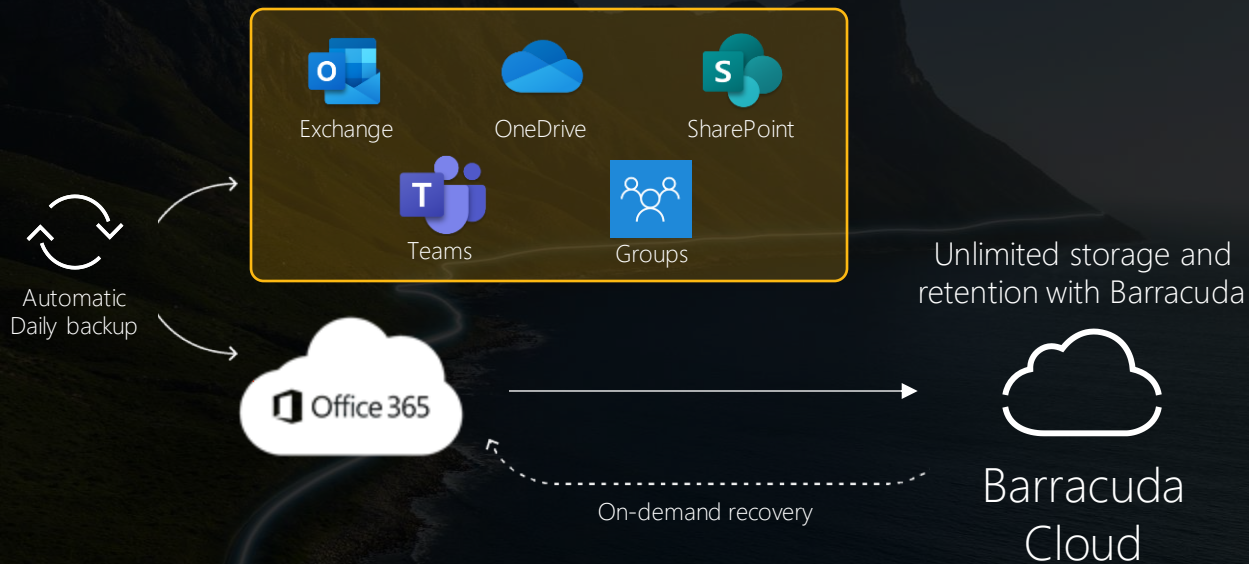
1 - 1 of 1 items

[Create training group](#) [Export to CSV](#)

Send users affected by an incident into an awareness training group without having to leave Incident Response



Cloud-to-Cloud Backup: set and forget



SharePoint and OneDrive risks

Preventing PII leakage

- Sensitive data like credit card, passport, password, medical info, etc.

Preventing Intellectual Property (IP) leakage

- Trade secrets, source code, general IP

Protection against stored malware

- Dormant ransomware files

Data Compliance

- GDPR, CCPA, HIPAA, PCI-DSS...



Data Inspector: protect Microsoft 365 data

Scan: Automatic and real-time

Classify: Automatic classification of data and malware, including custom classifiers

Notify: Notify admins and end users

Remediate: Protect data with remediation and blocking

Compliance: Reporting to meet regulatory requirements



Barracuda

Data Inspector™

Account: Barracuda Demo Account

Detections

Unresolved

In Progress

Resolved

Date Range

02/08/2024 - 05/08/2024

Search by file or owner

X

🔍

📄

🔄

Reset

<input type="checkbox"/>	File	Last Detected	Owner/Creator	Violations	Sharing	Classifiers	
<input type="checkbox"/>	british-passport.jpg OneDrive - Business > 2024-04-17 19:42:11	Apr 17 7:44 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:32 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:26 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:23 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:19 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:13 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:03 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:01 PM	SharePoint App	+1 more	2	Private	Passport 2
<input type="checkbox"/>	british-passport.jpg OneDrive - Personal	Apr 05 11:00 PM	SharePoint App	+1 more	2	Private	Passport 2

1 - 25 of 27 items



Deep international support



Local classifications for 27 countries

7 data centers worldwide

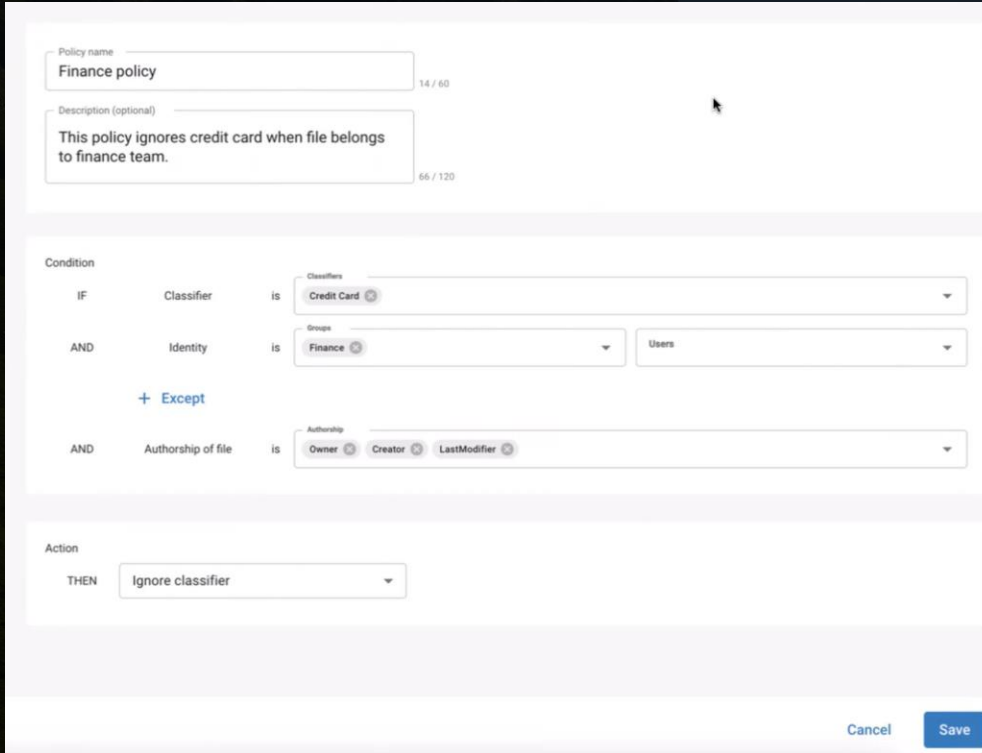
150 built-in classifications

- And counting

Up to 10 custom classifications



Easy, flexible, and automated remediation



The screenshot shows a web-based interface for configuring a remediation policy. It includes fields for a policy name and description, a condition builder with logical operators (IF, AND), classifiers (Credit Card, Finance), groups (Users), and authorship (Owner, Creator, LastModifier), and an action section with a dropdown for 'Ignore classifier'. The interface is clean and modern, with a light gray background and white form elements.

Policy name: Finance policy 14 / 60

Description (optional): This policy ignores credit card when file belongs to finance team. 66 / 120

Condition

IF Classifier is Credit Card

AND Identity is Finance Users

+ Except

AND Authorship of file is Owner Creator LastModifier

Action

THEN Ignore classifier

Cancel Save

Set up remediation policies per user-group and directory

- Different departments have different needs
- Can be as granular as you want
- Flexible remediation (Unshare, Quarantine, Delete, Ignore)



See for yourself with a free Data Inspector scan

1. Go to <http://datainspector.barracuda.com>
2. Login with a Microsoft 365 Global Admin account
3. Follow the onboarding wizard:
 - a) Agree to T&Cs
 - b) Select data location
 - c) Provide consent for read-only access to OneDrive and SharePoint

Less than 5 minutes to start your first scan!





Managed XDR



Email Protection

Defend your company with the world's most comprehensive email protection, made radically easy.

- ✓ Spam, malware, threats
- ✓ Phishing & impersonation
- ✓ Account takeover
- ✓ Incident response
- ✓ Security awareness



Application Protection

Protect all your web apps and APIs with one comprehensive platform.

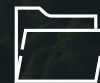
- ✓ OWASP Top 10
- ✓ Bot protection
- ✓ DDoS protection
- ✓ Client-side protection
- ✓ API security



Network Protection

Secure and connect your infrastructure with the power of Barracuda Network Protection.

- ✓ Secure Access Service Edge
- ✓ Zero Trust security
- ✓ Secure SD-WAN
- ✓ Network firewalls
- ✓ IoT/OT security



Data Protection

Safeguard your critical data wherever it resides to minimize downtime and prevent data loss.

- ✓ Backup
- ✓ Archiving
- ✓ Data classification

Start je Normenkader reis met SLB & Barracuda



+31 6 4229 3513

frank.wijmans@slbdiensten.nl



+31 6 219 23 911

mmartens@barracuda.com





Thank You

