Sichere E-Mails – nur ein Mythos?

Thomas Thaler

thomas.thaler@itelio.com

mimecast | managed service provider

Warum überhaupt E-Mail-Security?

Über 90% aller Hackerangriffe über E-Mail

Cyber-Kriminalität wird immer lukrativer

Kleine Lücken betreffen die ganze Organisation

Was ist die Gefahr?

Identitätsdiebstahl

Diebstahl von Zugangsdaten von Benutzern

Betrügerische Zahlungen

Über „CEO-Fraud“ werden nicht autorisierte Zahlungen angewiesen

Installation von Trojanern

Trojaner installieren weitere Malware nach oder öffnen Backdoors

Installation von Ransomware

Verschlüsselung von Unternehmensdaten

Was ist eigentlich dieses „Phishing“?

Phishing

Spear-Phishing

Whaling

Meeting wegen Technologie-Updates

Di, 05.07.2022 13:00 – 13:30

Microsof

Andreas

Nachrich

[EXTERNA

Hallo Tor

ich habe
Unten fir

Sollte de

Viele Grü
Andreas

Micro

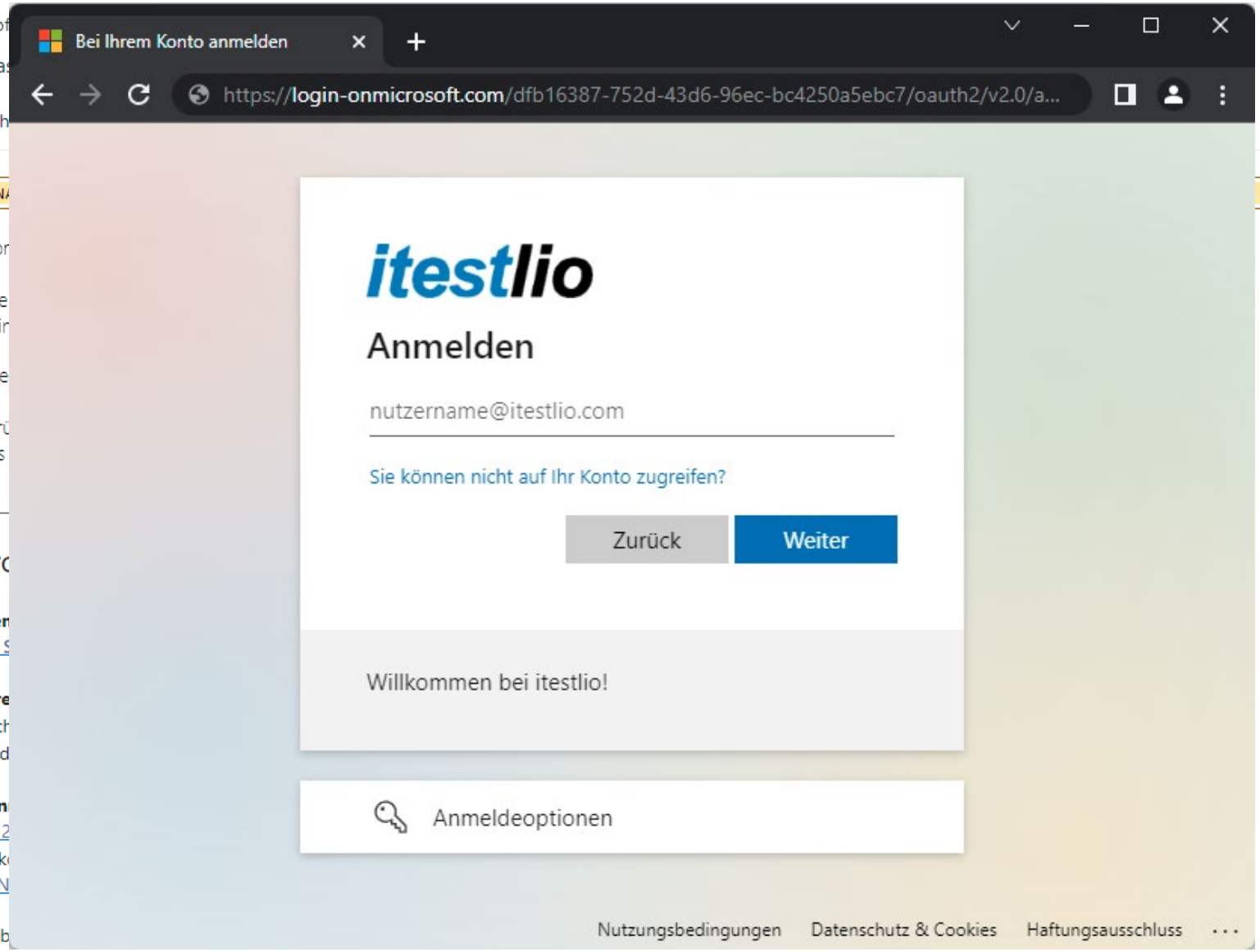
Nehmer
Klicken S

Oder tre
Besprech
Kenncod

Oder an
+49 89 2
Telefonk
Lokale N

Für die b

Weitere Infos | Besprechungsoptionen



Was gegen E-Mail-Angriffe hilft

Technische Barrieren

- E-Mail Gateway
- Virenscanner
- EDR-Tools
- Multifaktor-Authentifizierung

Menschliche Barrieren

- Schulung
- User Awareness Training
- Passwort-Hygiene

Was ist ein E-Mail-Gateway?

Blockiert unerwünschte E-Mails

- Spam
- Phishing-Angriffe
- Malware
- Betrügerische Inhalte

Stellt unbedenkliche E-Mails zu

Überprüft ausgehende Nachrichten

- Spam von intern erkennen
- Datenabfluss vermeiden

Was wollen Anwender

E-Mails bekommen

Keinen Spam bekommen

Intuitive Verwaltung von Absendern

Transparenz warum E-Mails nicht zugestellt wurden

Verwalten und freigeben aller sie betreffenden E-Mails

DEMO

Was wollen Admins

Gefühlte und tatsächliche Sicherheit

Transparente Verwaltung von E-Mails

Granulare Kontrolle über Einstellungen

Technologie auf dem aktuellsten Stand der Technik

Reporting und Nachvollziehbarkeit

Vorteile in der Cloud

- Keine Downtime durch Updates
- Extrem schnelle Updatezyklen
- Hohe Skalierbarkeit
- Kalkulierbare Kosten auf Benutzerbasis
- Geringer Betriebsaufwand

Wer ist Mimecast

Anbieter von E-Mail-Sicherheits-Lösungen

Cloud-Only seit 2003

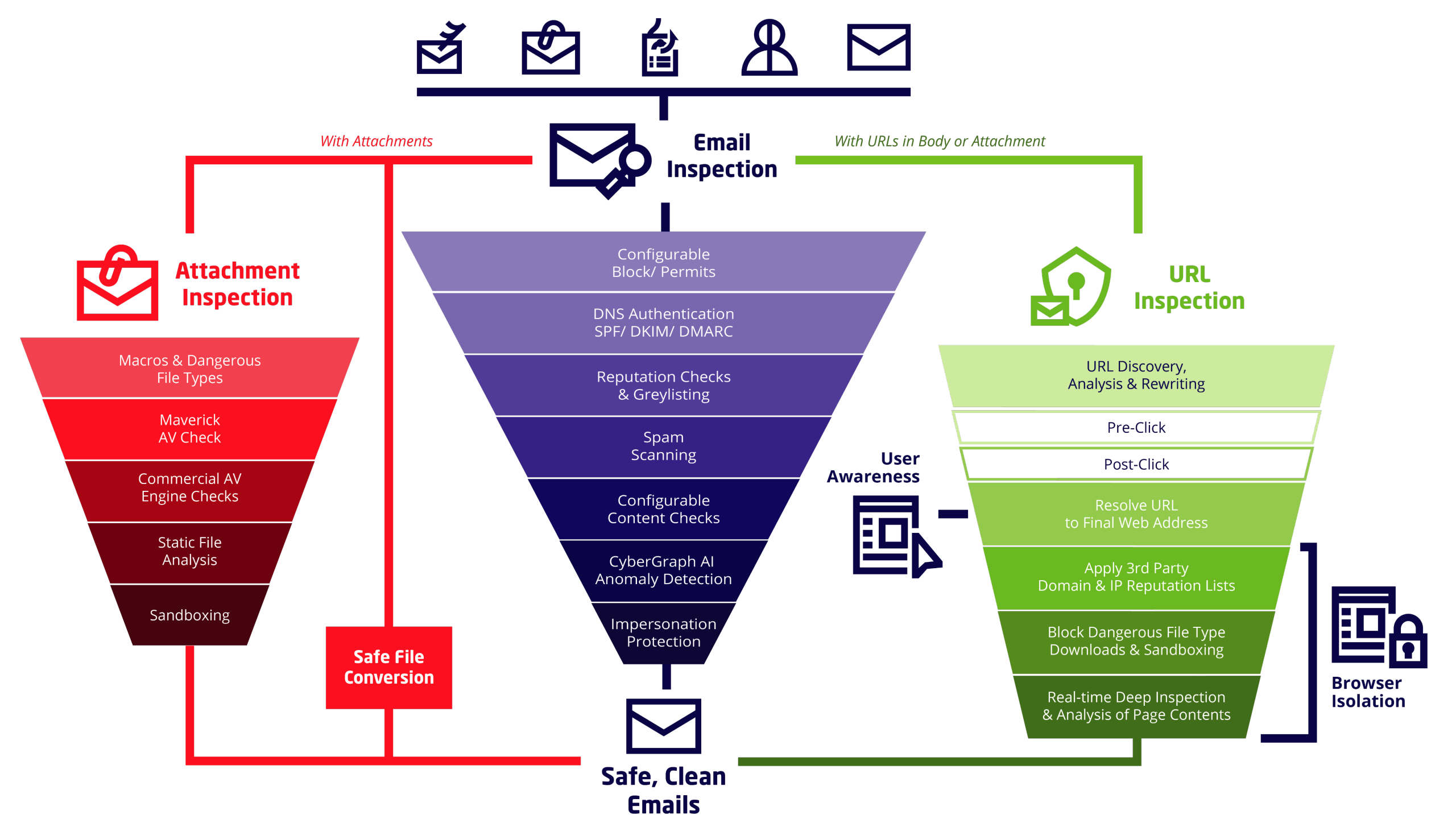
Hauptsitze in Südafrika und UK

2000+ Mitarbeiter weltweit

mimecast®

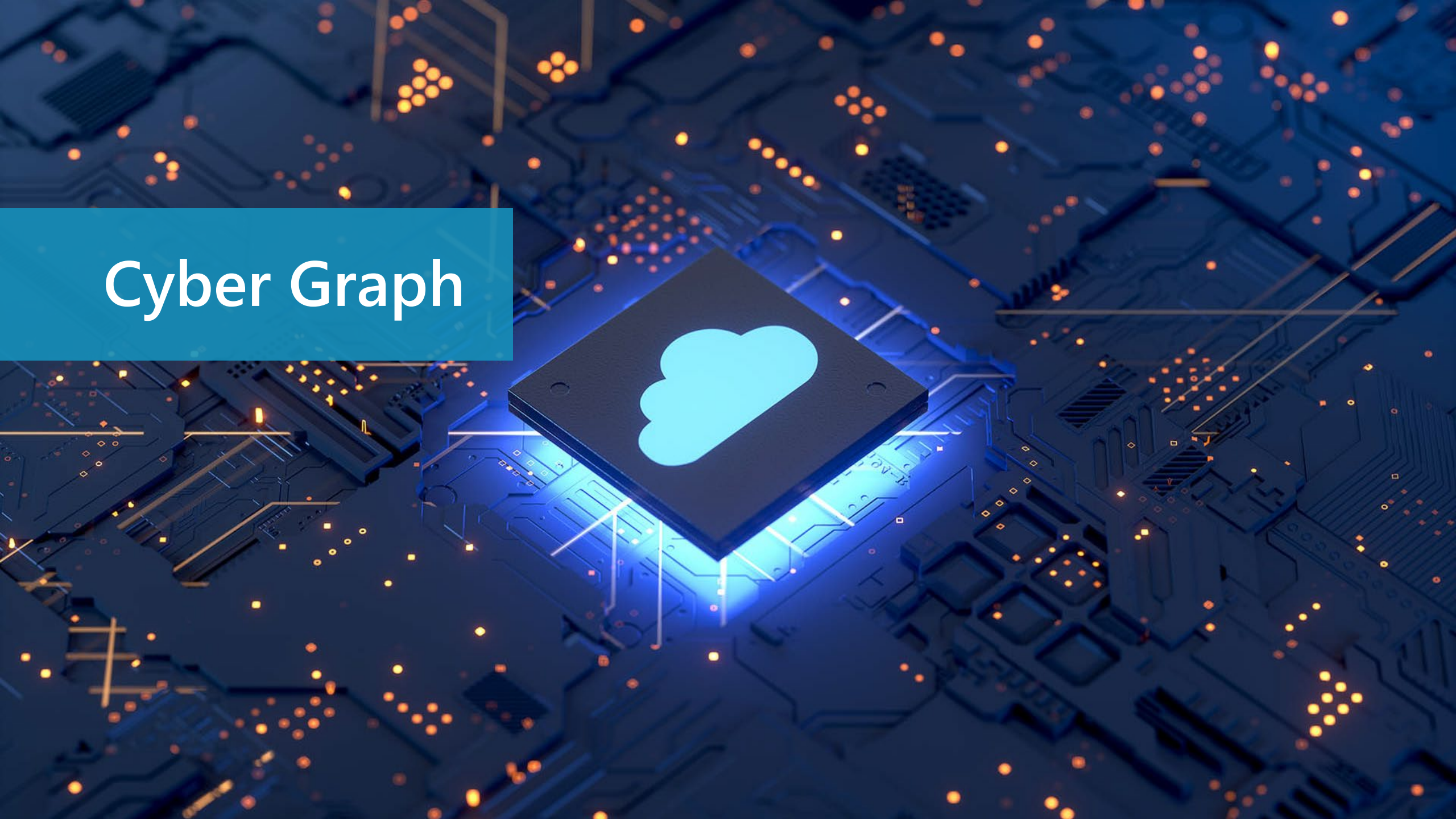
Warum Mimecast E-Mail Security?

- Schutz vor ausgefeilten Angriffen
- Innovative Ansätze und ausgereifte Technologien
- Eine zentrale Verwaltungskonsole
- Hohe Transparenz über Funktionalität
- Unterstützung für eine Vielzahl von E-Mail-Umgebungen
- Intuitiver Self-Service für Benutzer
- Umfangreiches Reporting und Auditing


With Attachments
Email Inspection
With URLs in Body or Attachment
Attachment Inspection
Macros & Dangerous File Types
Maverick AV Check
Commercial AV Engine Checks
Static File Analysis
Sandboxing
Safe File Conversion
Configurable Block/ Permits
DNS Authentication SPF/ DKIM/ DMARC
Reputation Checks & Greylisting
Spam Scanning
Configurable Content Checks
CyberGraph AI Anomaly Detection
Impersonation Protection
Safe, Clean Emails
URL Inspection
URL Discovery, Analysis & Rewriting
Pre-Click
Post-Click
Resolve URL to Final Web Address
Apply 3rd Party Domain & IP Reputation Lists
Block Dangerous File Type Downloads & Sandboxing
Real-time Deep Inspection & Analysis of Page Contents
User Awareness
Browser Isolation

DEMO

Cyber Graph

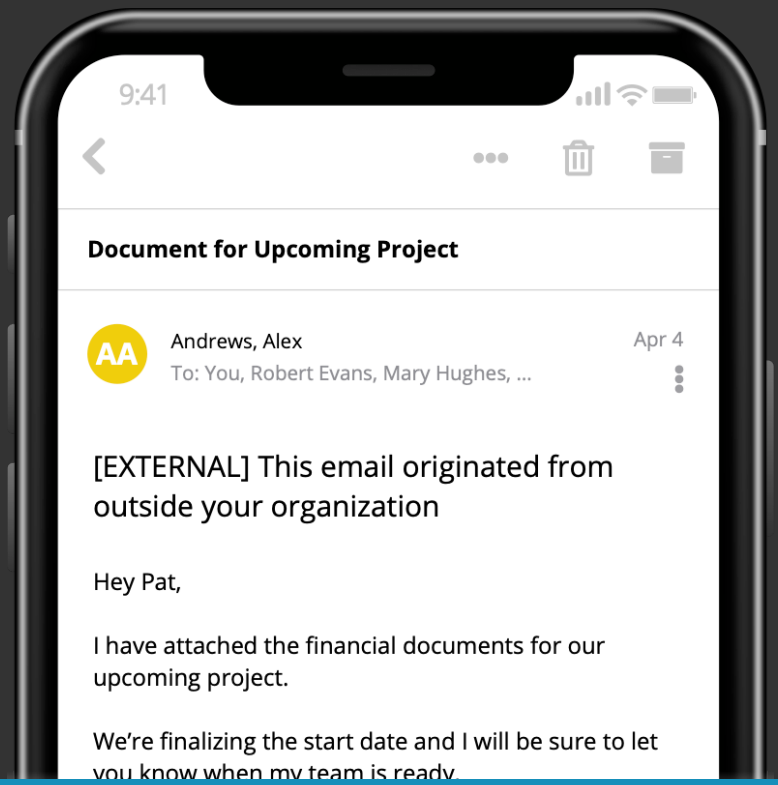


Contextual warnings

Real-time learning

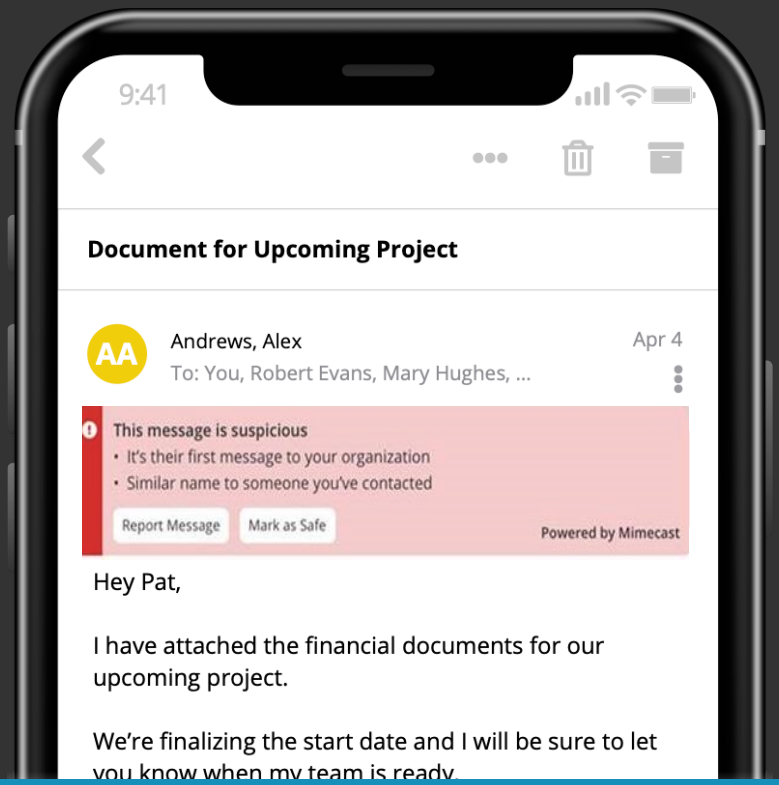
Retroactive warnings

Generic Email Warning



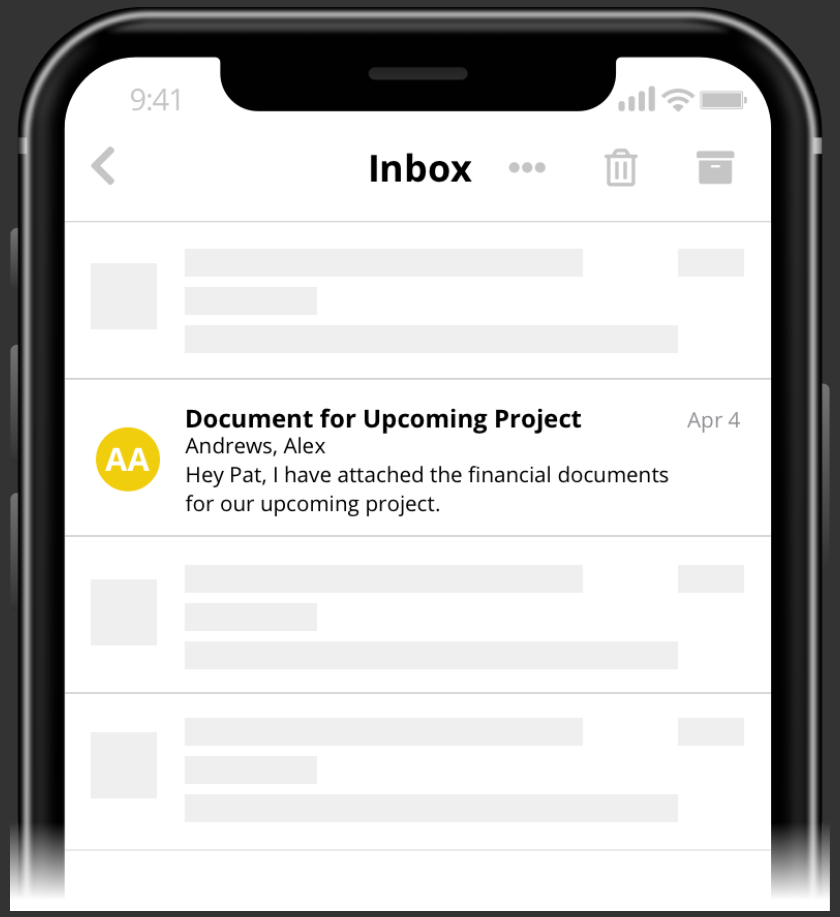
Regardless if it's a real or fake Alex, external warning always shows

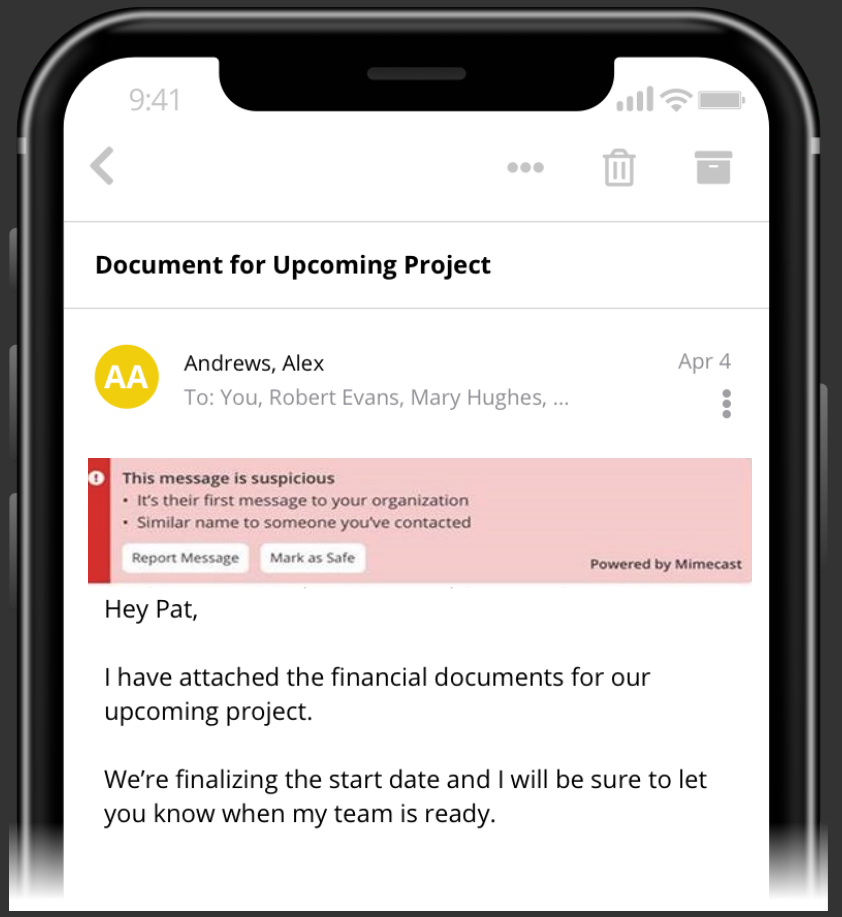
Mimecast Email Warning



Contextual warning only shows on the fake Alex

Clear message preview in native IOS mail

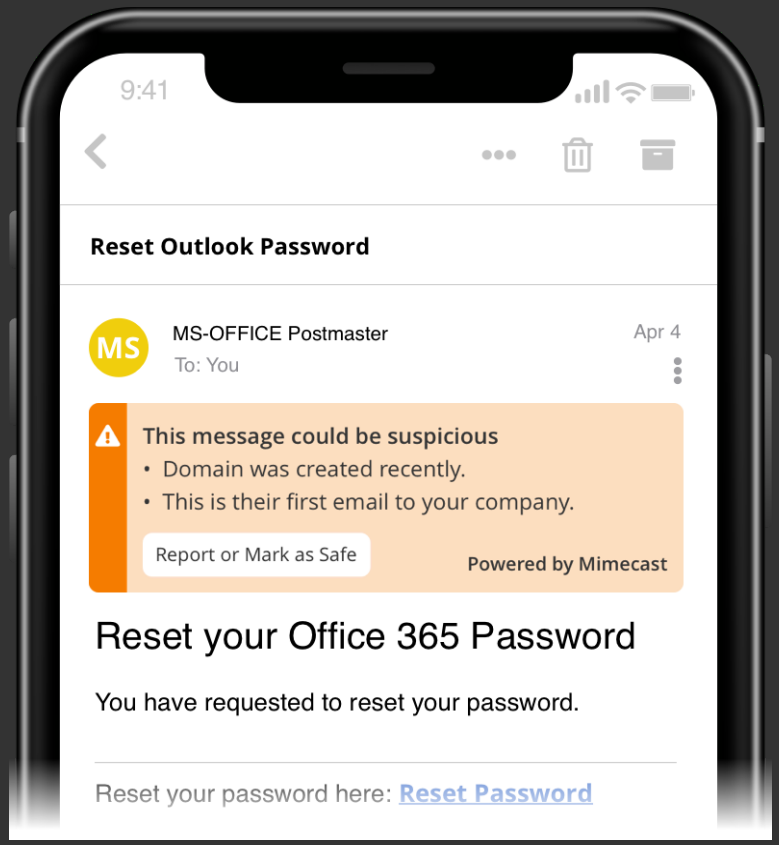


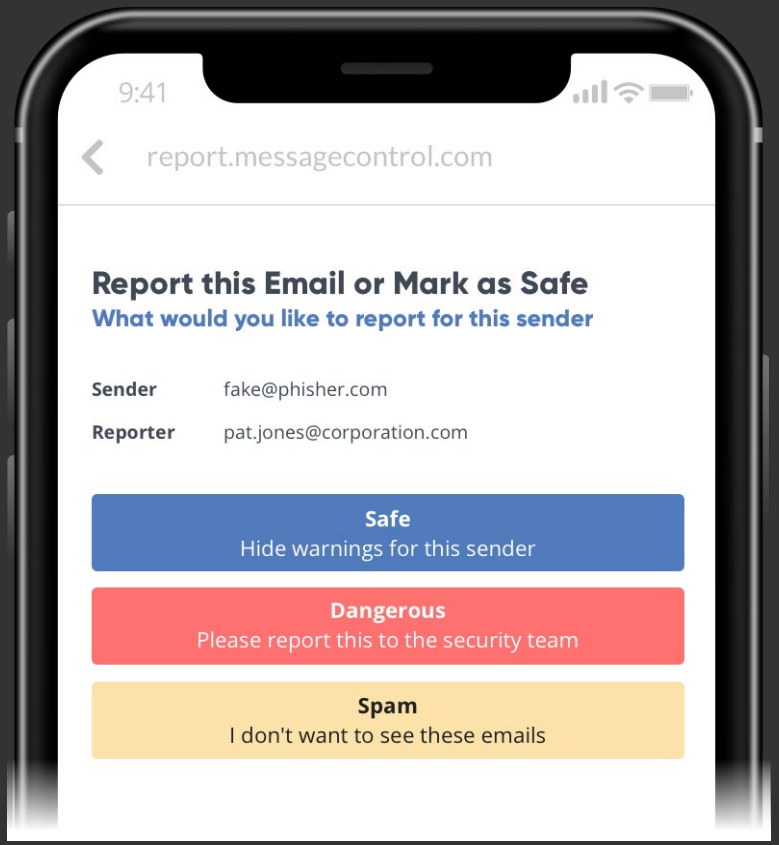


Contextual warnings

Real-time learning

Retroactive warnings

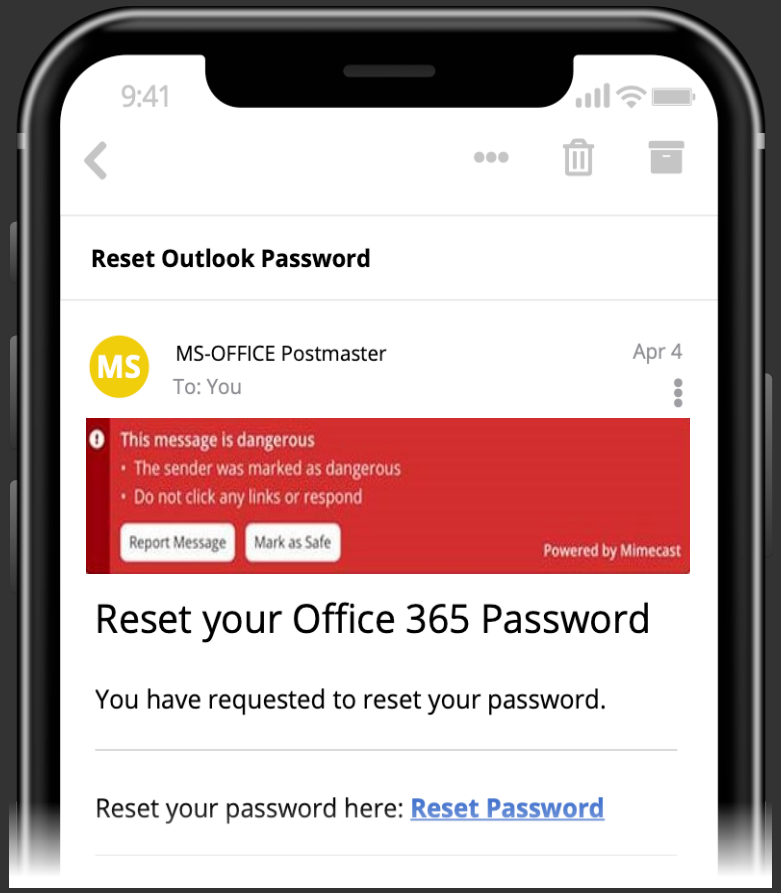




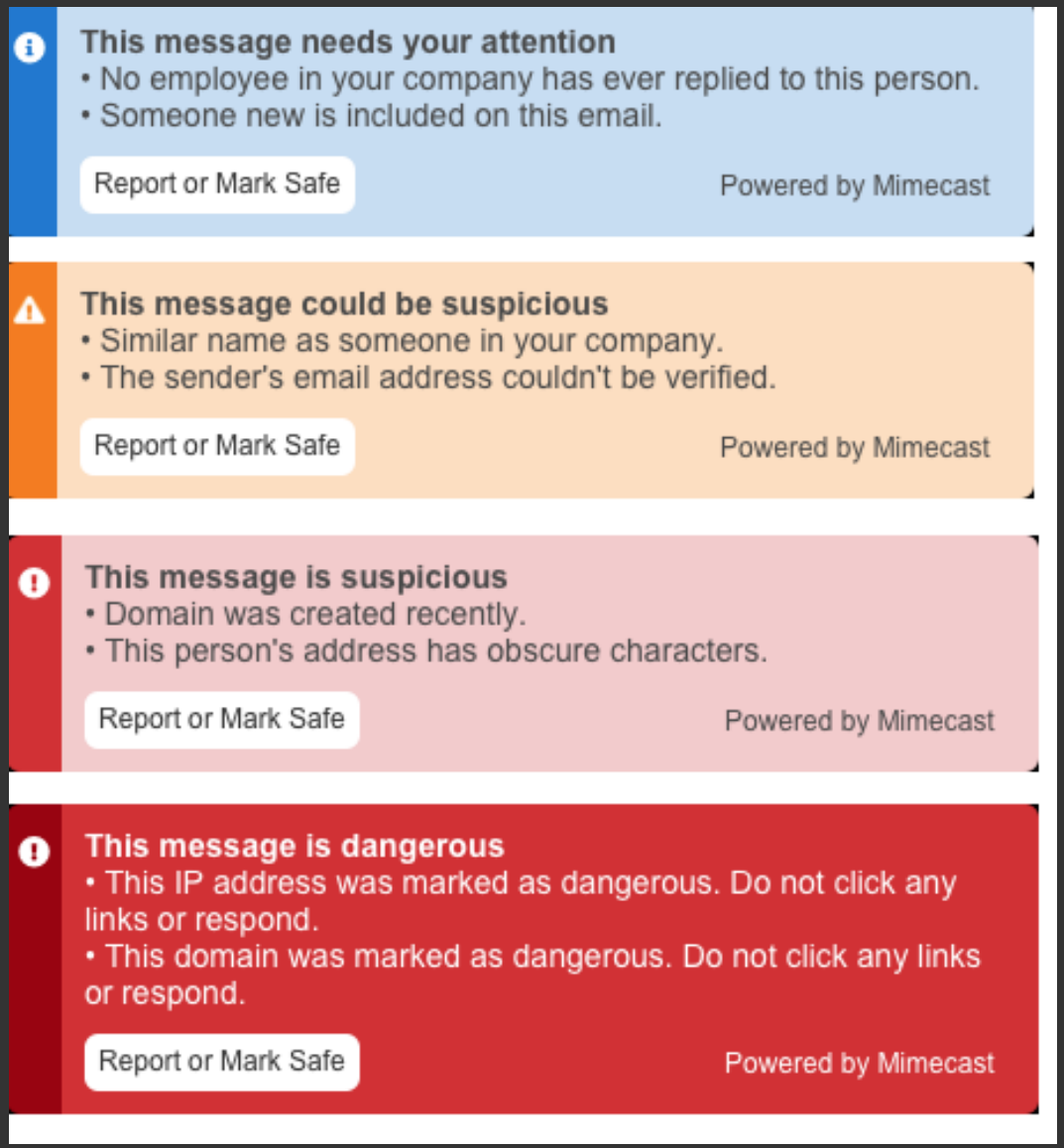
Contextual warnings

Real-time learning

Retroactive warnings

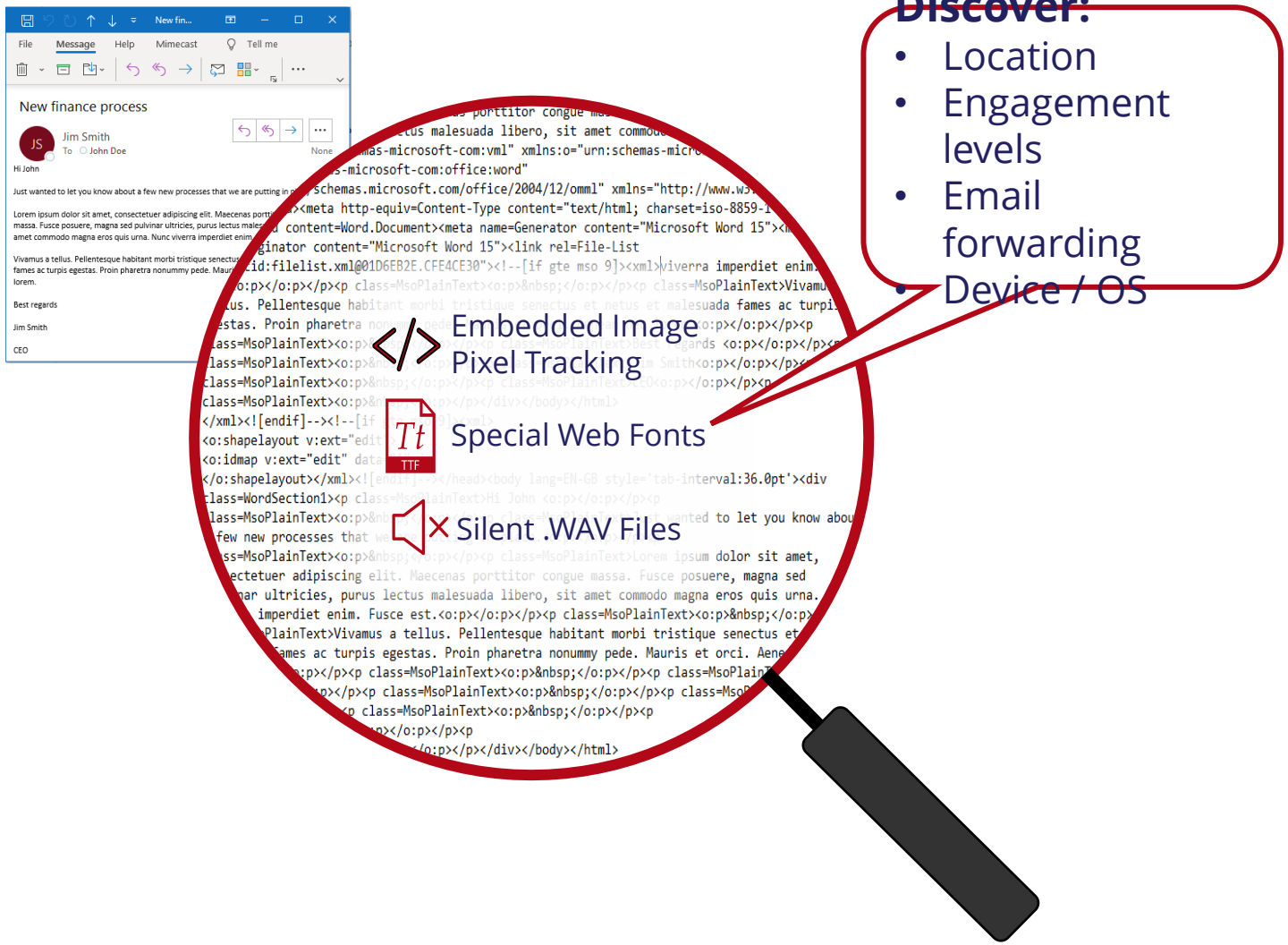


Empower employees to thwart spear-phishing and identity attacks



Preventing sophisticated, targeted phishing attacks is a significant challenge

Trackers are embedded in emails



What is revealed…from just opening an email?

TRACKING DETAILS

Opened

Shown	4-Feb-05 at 16:18:28pm (CST +11:00) - 2min5secs after sending
Location	Washington, District of Columbia, United States (86% likelihood)
Opened on	relay2.cia.gov (198.81.129.194.58140), (203.217.18.9:9033)
Device fingerprint	used by recipient: Moz/4.0 (MSIE 7.0; WinNT 6.1; WOW64; Trident/7.0; SLCC2; NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E; InfoPath.3; wbx1.0.0; Microsoft Outlook 14.0.7194; ms office; MSOffice 14)
Accepts	Files browser can open: i/png, */*,q=0.5

Forwarded/opened on different computer

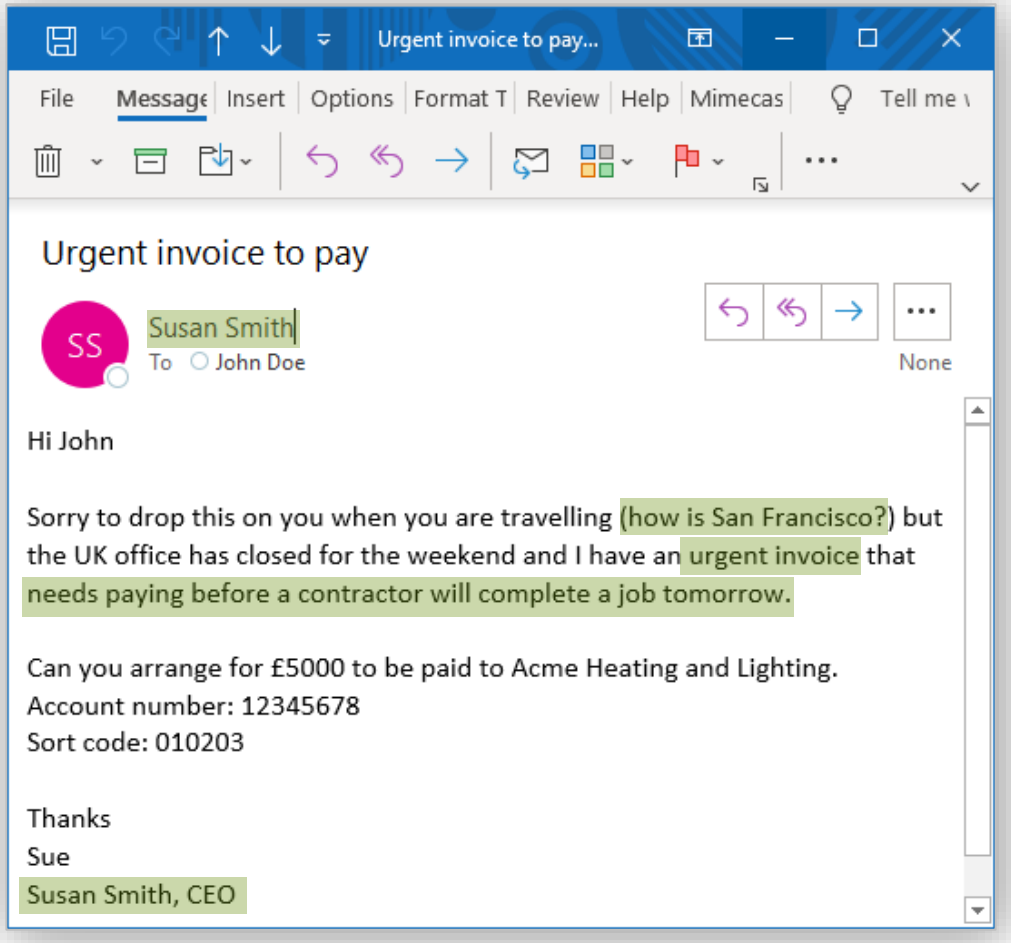
Shown	4-Feb-05 at 16:21:09pm (CST +11:00) - 4min46secs after sending
Location	Sydney, Australia (86% likelihood)

To:	webmaster@example.gov
From:	drakecn@yahoo.com
Subject:	Great tracking service!
Sent on:	4-Feb-05 at 16;16;23pm'Central US time
1st open:	4-Feb-05 at 16:18:28pm +11:00

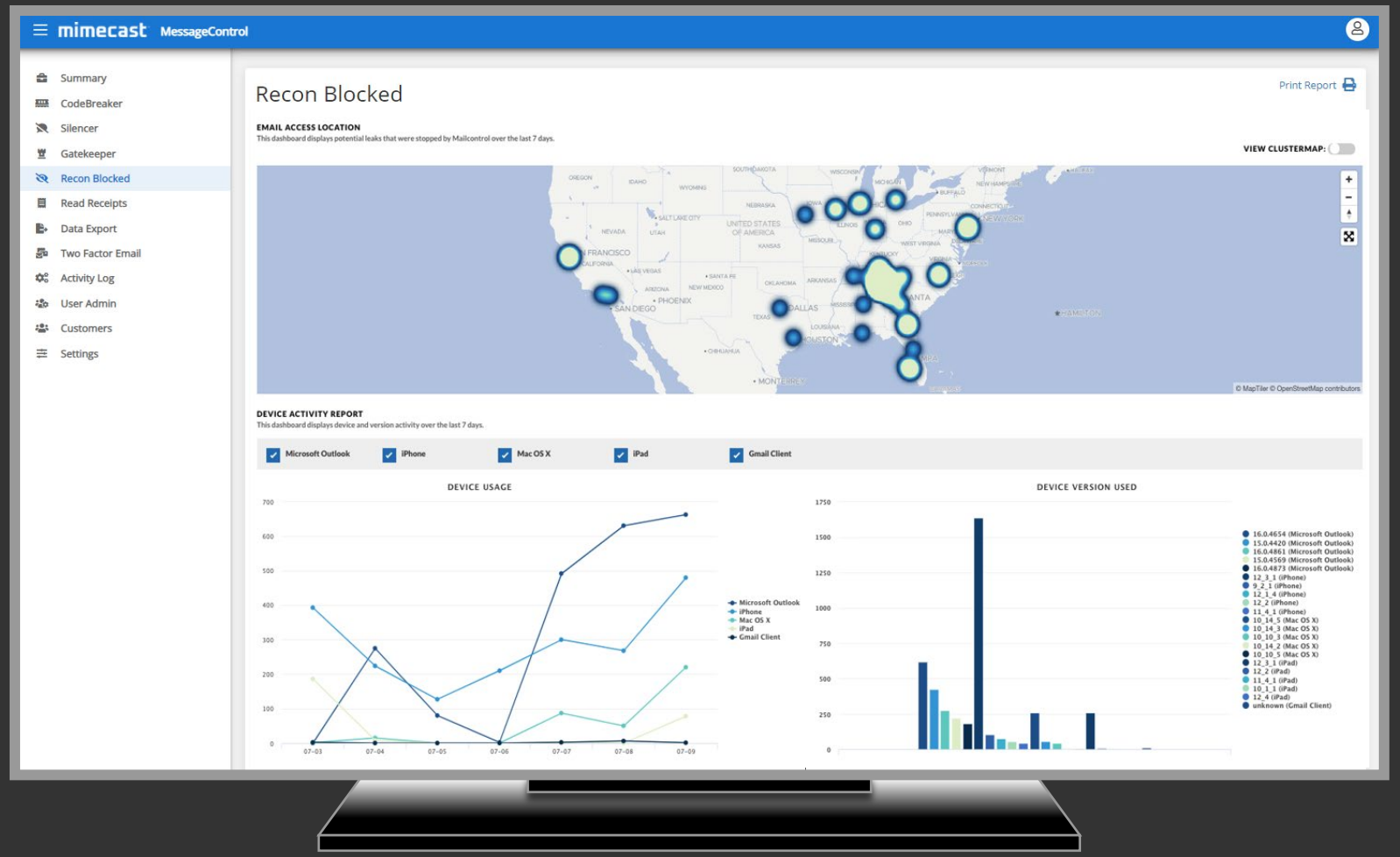
(86%) Washington, District of Columbia, United States

Preventing sophisticated, targeted phishing attacks is a significant challenge

A social engineering attack is crafted

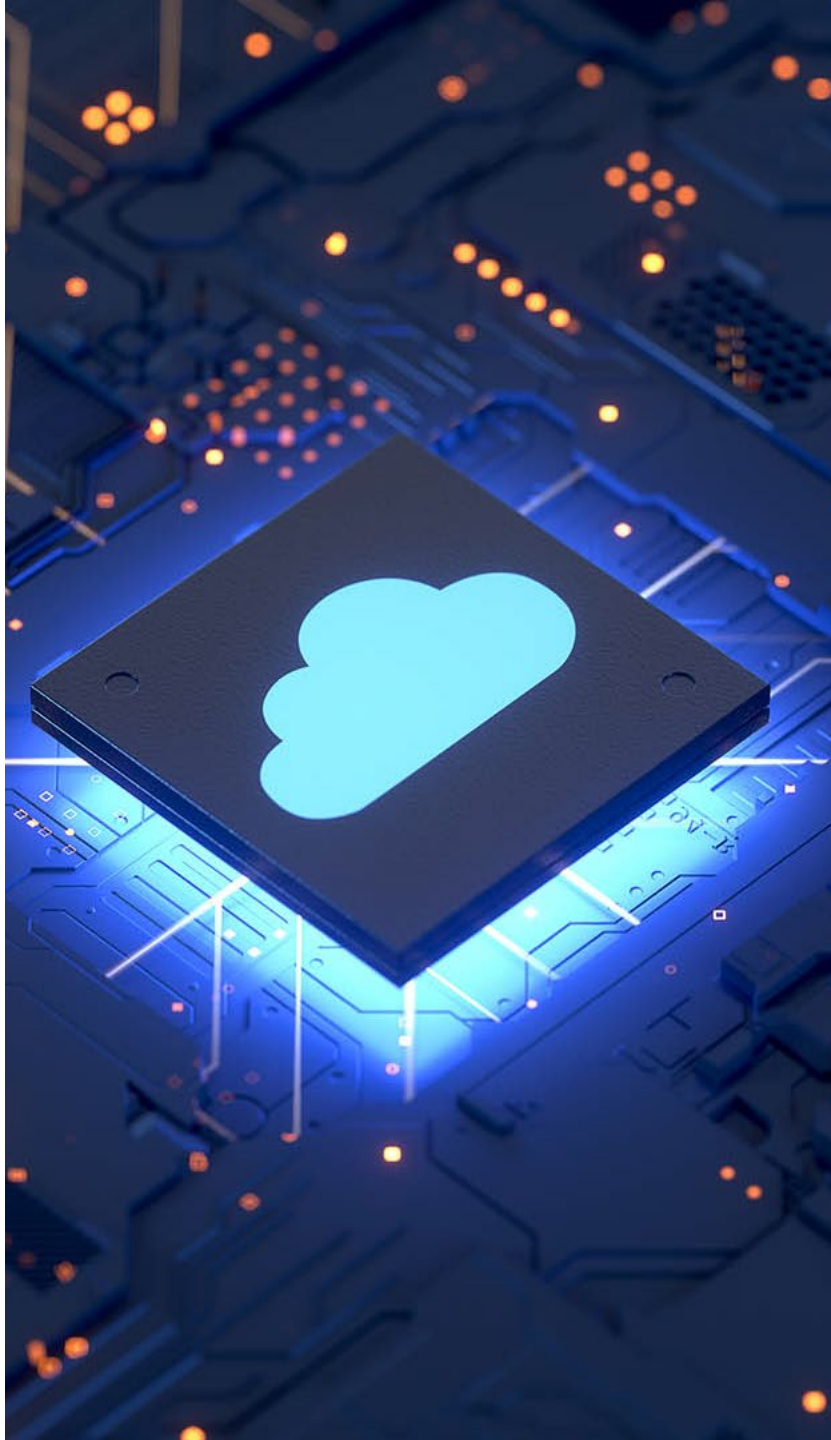


Provides visibility of targeted users



Cyber Graph

- Kontaktwarnungen bei Emails
- User-Awareness durch ständige Präsenz
- Ersatz für statische Disclaimer
- Interaktion durch Benutzer
- Infos über bösartige Mails kommen schnell in die breite Masse
- Dynamisches Entfernen von Trackern z.B. (Tracking-Pixel)
- Misaddressed Email Protection



Kommunikation? Aber sicher!

We understand IT.