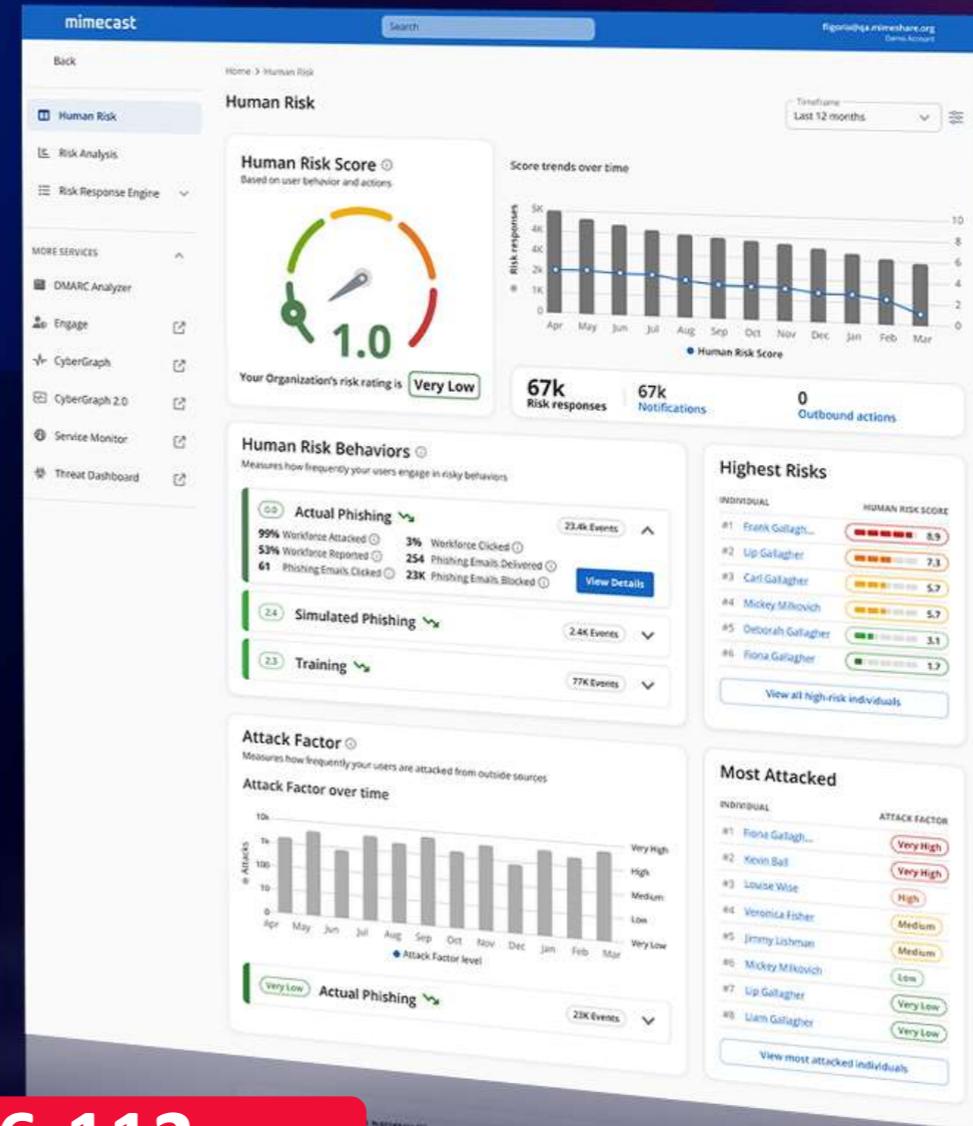


Human Risk Management: der Faktor Mensch in der Risikostrategie

Das menschliche Risiko ist die größte Lücke in der Cybersicherheit, da 8% der Mitarbeiter 80% der Vorfälle verursachen

Kommen Sie zu unserem Stand: 6-112



Wer ist Mimecast?

Unser Stand: 6-112



42,000+

Kunden in mehr als
100 Ländern



26Mio

Endnutzer geschützt



3.2Mio

Anfragen nach E-Mail-
Archiv-Suchen pro Woche



2,000+

Mitarbeiter weltweit



16

Int. Rechenzentren (2 in DE)



Unsere Chance – Absicherung von Human Risk



Das Human Risk Problem



90%

der Angriffe
beginnen mit
Email¹

1 von 17

von Nachrichten durch
Collaboration-Tools
enthalten sensible Daten²

8%

der Mitarbeiter sind an
80% der Vorfälle
beteiligt³

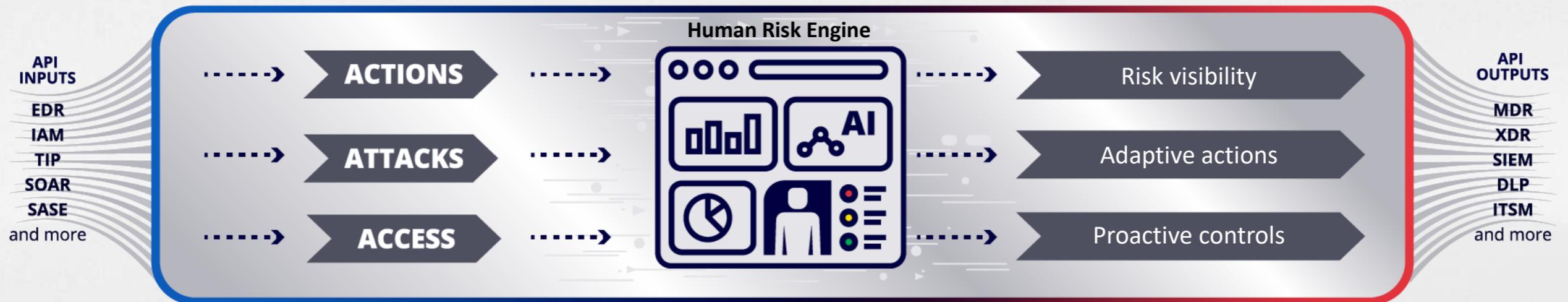
\$15M

Durchschnittliche Kosten eines
Insider-Datenlecks⁴

Sichere Zusammenarbeit mit einer einheitlichen Plattform



Die vernetzte Human Risk Management-Plattform



Anwendungsfälle

PROTECT COLLABORATION

Nutzlast-basierte Angriffe

Credential Harvesting

Business Email Compromise

Brand & Domain Impersonation

Data Retention & E-Discovery

Data Recovery

EXTERNAL RISKS

EMPOWER USERS

Targeted Awareness Training

Phishing Simulation

Sentiment

Insider Bedrohungen

Kontoübernahme



DETECT INSIDER RISK

Sensitive Data Loss

Exfiltration von Daten

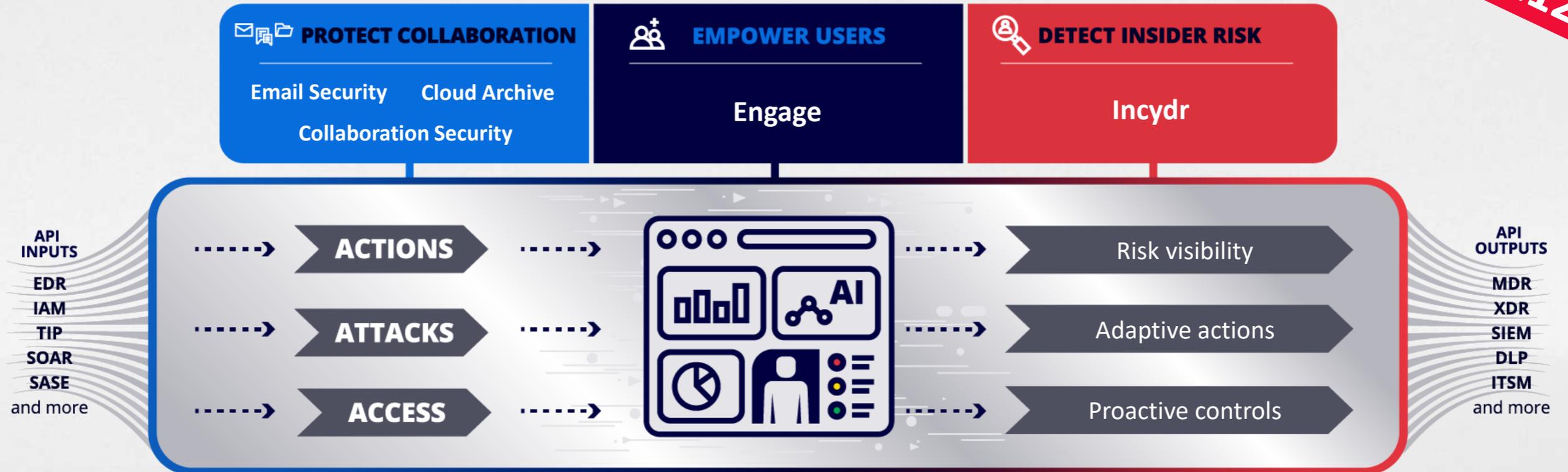
Laterale Phishing-Angriffe

Erkennung
kompromittierter Benutzer

INTERNAL RISKS

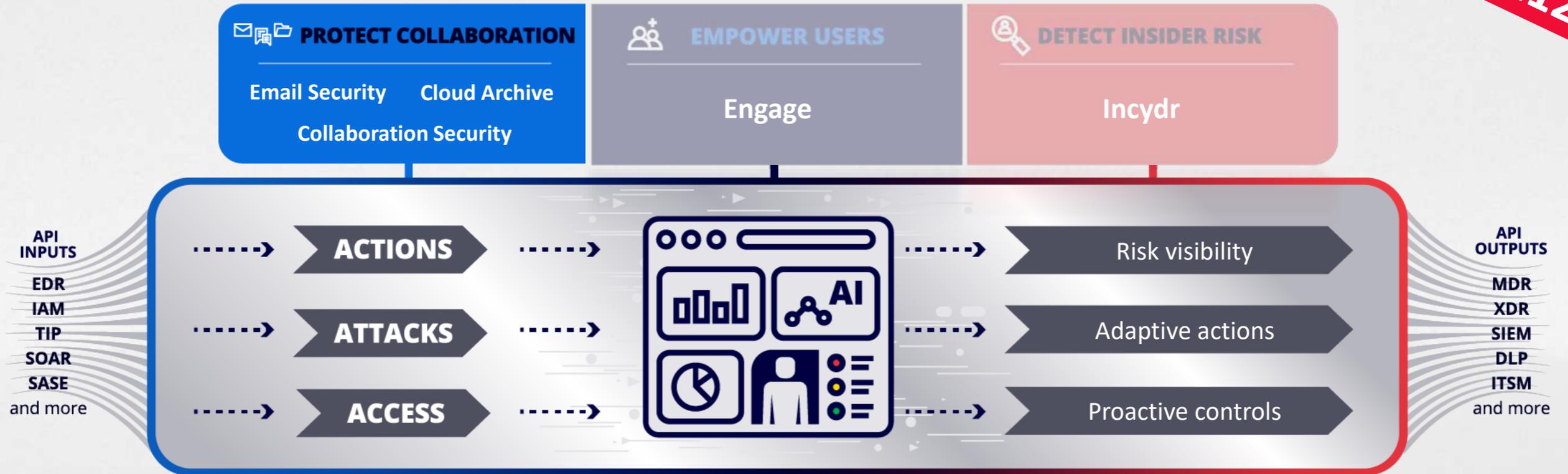
Unsere Produkte

Unser Stand: 6-112

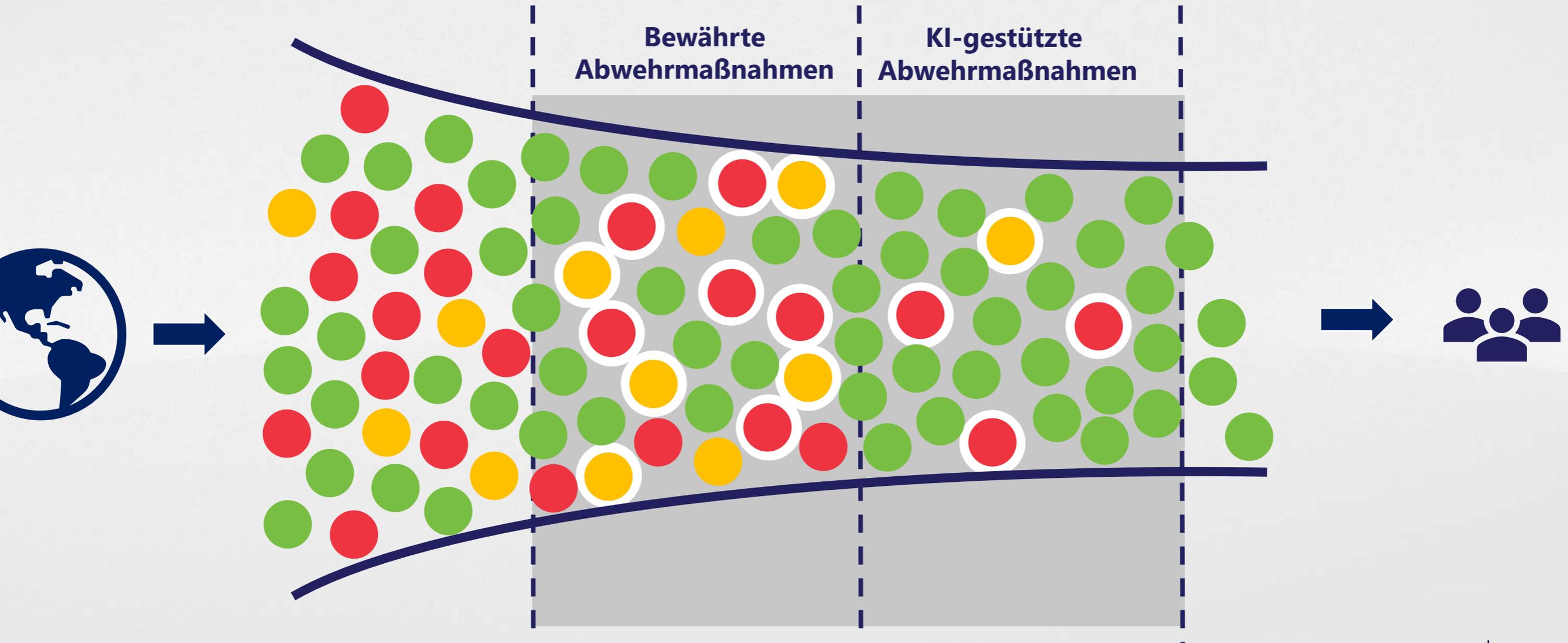


Human Risk Management Platform

Unser Stand: 6-112



Blockieren Sie E-Mail-basierte Bedrohungen



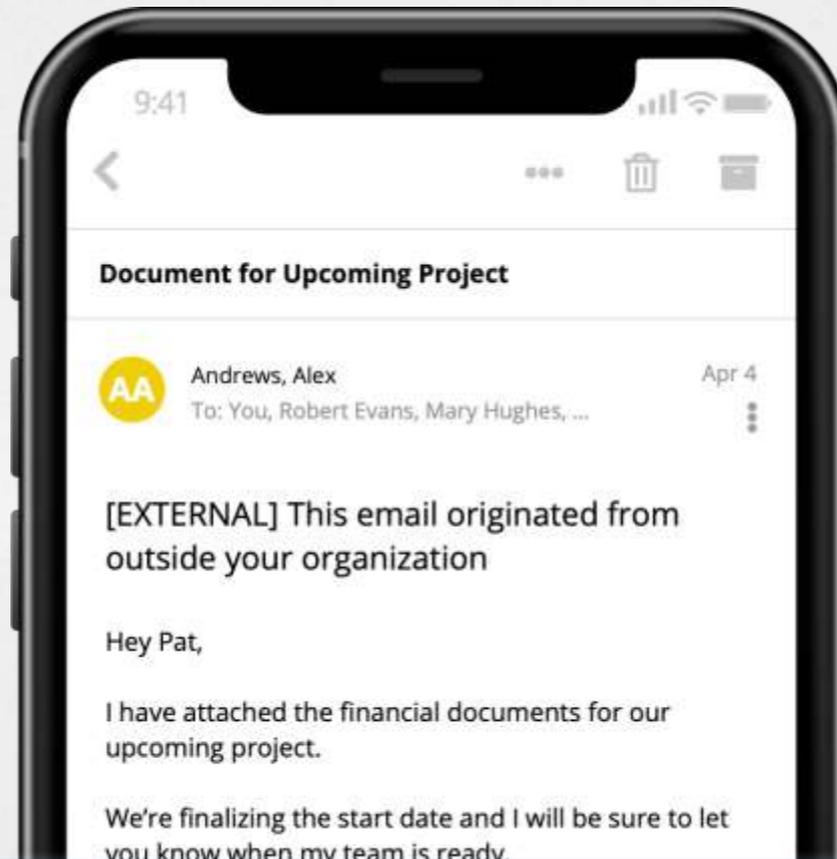
Mimecast KI Nutzung



Friday 2nd August 2024

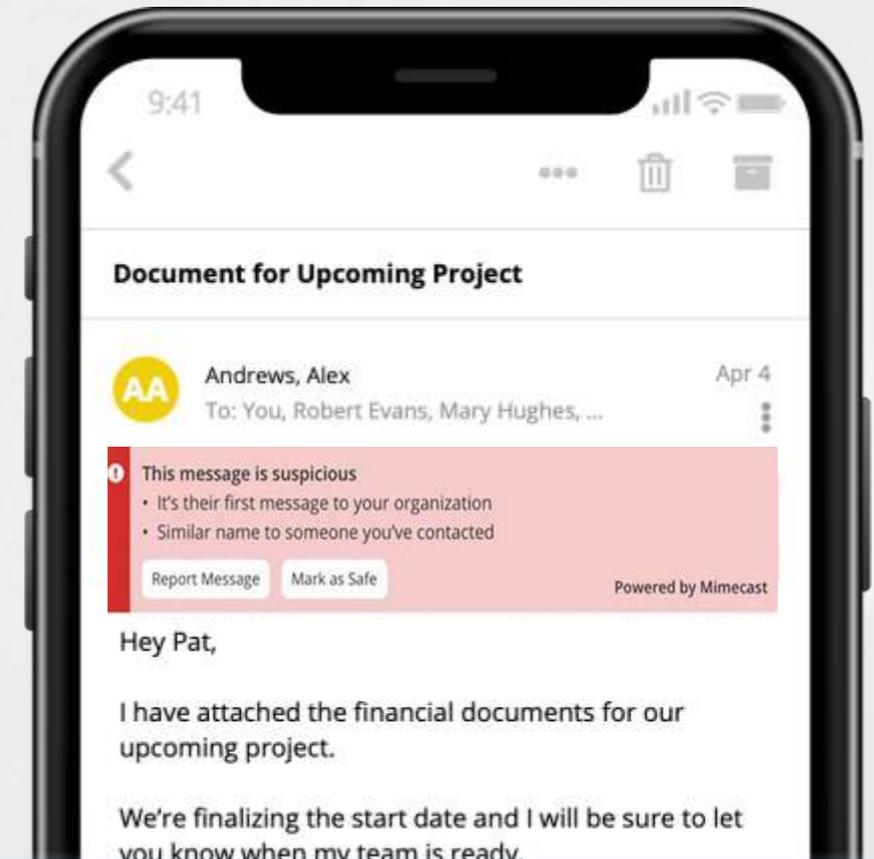
CyberGraph – Warnmeldungen

Allgemeine E-Mail-Warnung



Unabhängig davon, ob es sich um einen echten oder gefälschten Absender handelt, es wird immer eine externe Warnung angezeigt

Mimecast E-mail Warnung



Die kontextbezogene Warnung erscheint nur bei dem gefälschten Absender

Kontextbezogene
Warnungen

Lernen in Echtzeit

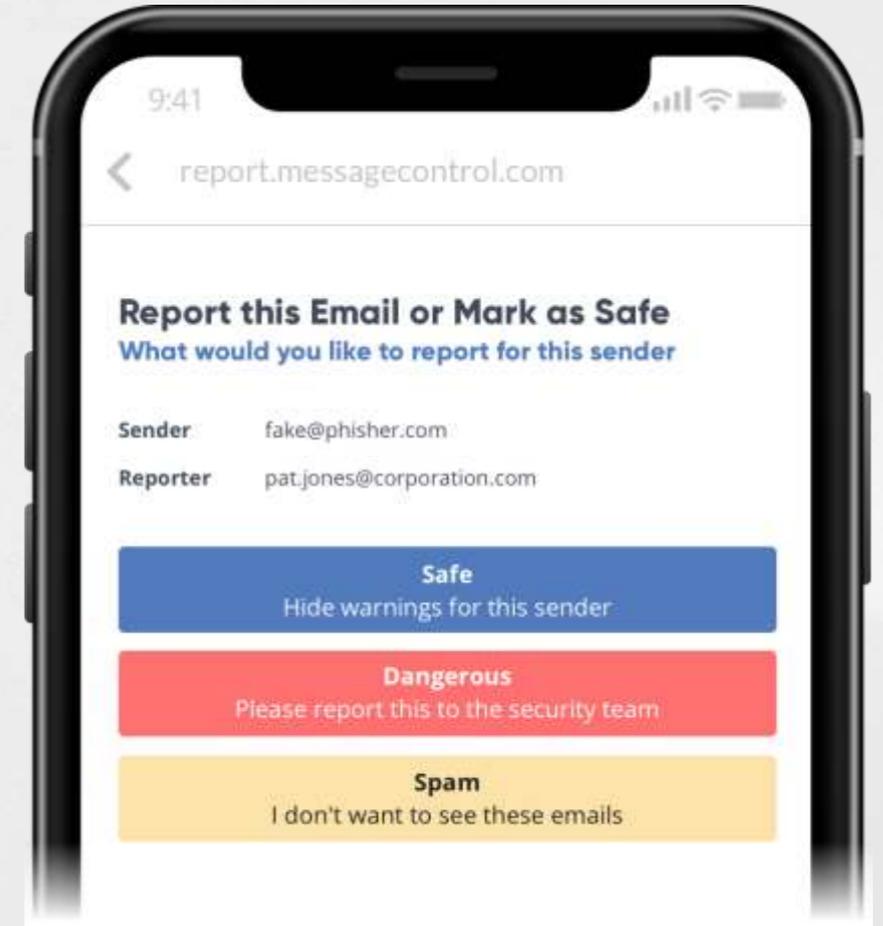
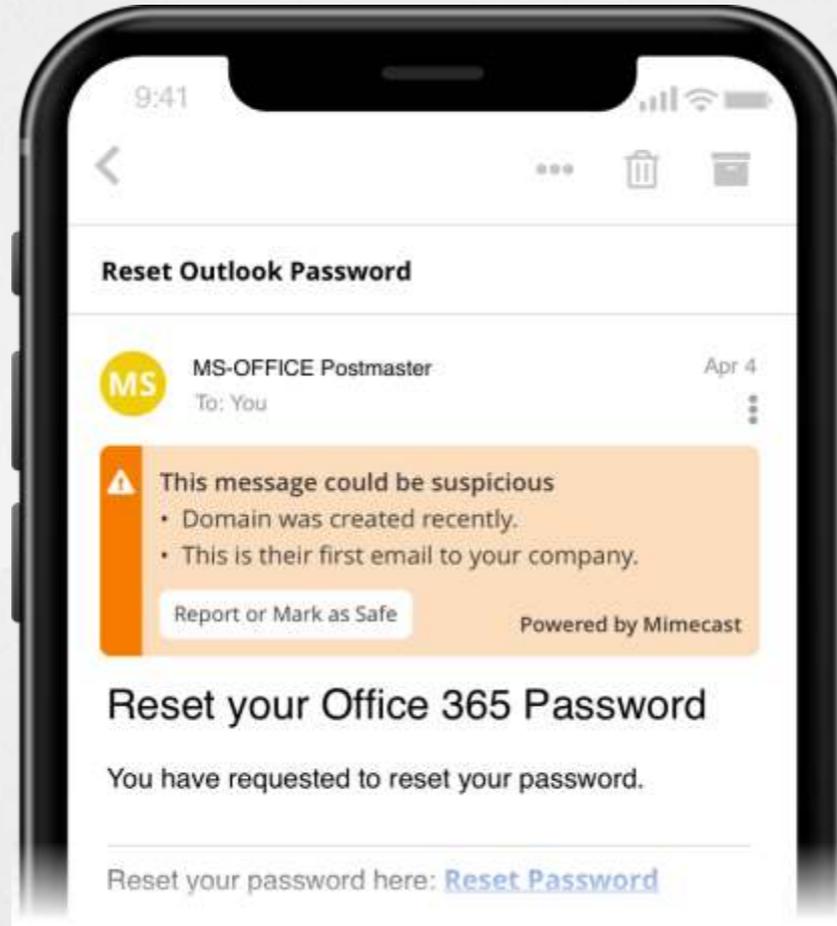
Rückwirkende
Warnungen

CyberGraph – Warnmeldungen

Kontextbezogene
Warnungen

Lernen in Echtzeit

Rückwirkende
Warnungen



CyberGraph – Warnmeldungen

Kontextbezogene
Warnungen

Lernen in Echtzeit

Rückwirkende
Warnungen



Business Email Compromise (BEC)-Angriffe abwehren

1

Persönliche Reputation

Beziehung zwischen Absender und Empfänger

2

Social Graph

Kommunikationsmuster und von Nutzern gemeldete Nachrichten

3

Domain-Verifizierung

Freemail, neu registriert, Tippfehler-Domains bekannter Marken

4

Betreffzeilenüberwachung

Riskante Phrasen in Betreffzeilen identifizieren

The screenshot shows an email analysis interface. The 'Analysis' section has a 'Floating' status and a 'Quarantined' status. The 'Policy' section shows a table with columns for Name, Mode, and Action. The table contains one row: 'Default OMS Mail policy', 'Protect', and 'Quarantine'. Below this is a 'Detailed Analysis' section with the heading 'Business Email Compromise Scan (BEC)'.

The screenshot shows two sliders. The 'Relationship Strength' slider is positioned at the 'Weak' end of a scale from 'Weak' to 'Strong'. The 'Reputation Strength' slider is positioned at the 'Weak' end of a scale from 'No History' to 'Strong'.

A partial screenshot of a 'Reputation Strength' slider, showing the 'Weak' end of the scale.

The screenshot shows an email header with several fields: 'Subject' (Change Direct Deposit Information, Change of Payroll), 'From Display' (Ragupathi Ravi, rravi.mc@aol.com, Personal Email), 'From Envelope' (rravi.mc@aol.com), 'To' ('sadmin@citeamsqa2.onmicrosoft.com', <sadmin@citeamsqa2.onmicrosoft.com>), 'Direction' (Inbound), 'Date/Time' (02 May 2024 - 19:55:47), and 'Message ID' (<541196339.6444460.1714676142901@mail.yahoo.com>). Annotations 2, 3, and 4 are placed over the 'From Display', 'From Envelope', and 'Subject' fields respectively.

The screenshot shows an email body with the text: 'Hello Jake, I want to change my direct deposit information before the next payroll is completed. What details do you need? Your response will be appreciated. Thanks, Miles Morales'. Annotations are placed over the text 'change my direct deposit information' and 'before the next payroll is completed'.

Business Email Compromise (BEC)-Angriffe abwehren

5

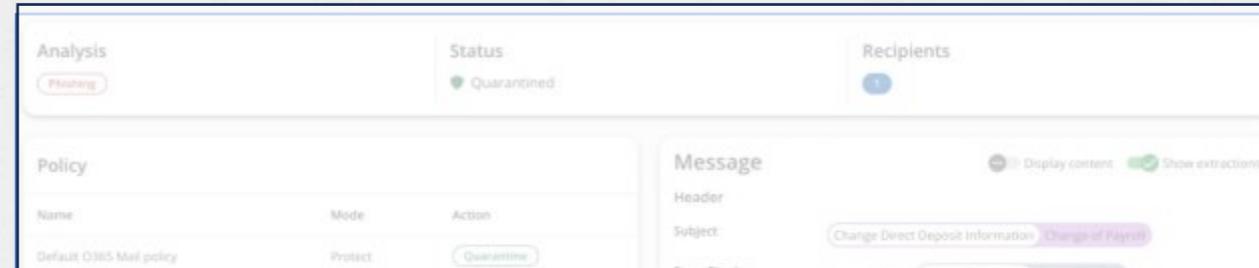
Bedrohungsspezifische Sprache

Modelle, die darauf trainiert sind, bedrohungsspezifische Sprache zu erkennen.

6

Nachrichtenintention

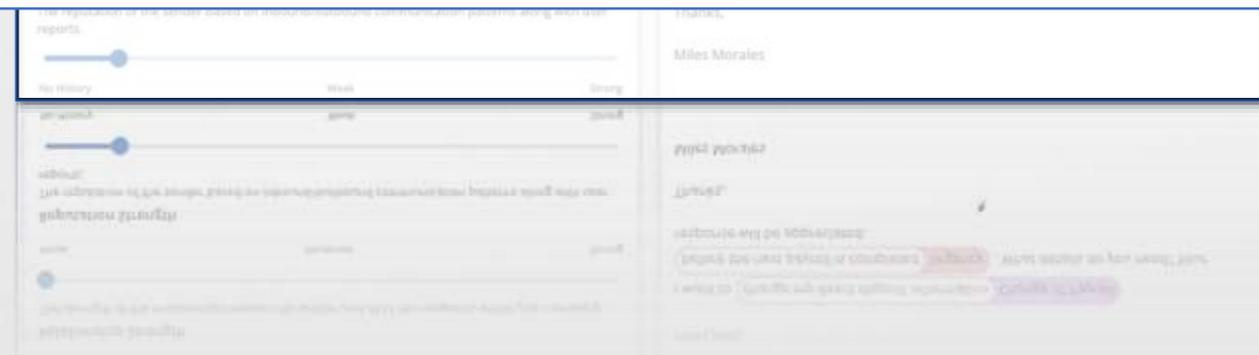
Fokus auf die zugrundeliegende Bedeutung und Absicht



Hello Jake,

I want to **change my direct deposit information** **Change of Payroll** **5**
before the next payroll is completed **Urgency** . What details do you need? Your
response will be appreciated. **6**

Thanks,



Eine Zentrale Plattform



Advanced Threat Analytics

Bekommen Sie einen besseren Eindruck in die Bedrohungen Ihrer Organisation

Inhaltliche Intelligenz

Verschaffen Sie sich einen umfassenden 360-Grad-Blick auf jede E-Mail-Interaktion.

Dringlichkeit & Awareness

Ermitteln Sie häufig angegriffene Benutzer und häufige böswillige Absender.

Granular Einstellungen

Flexible Richtlinien für Maßnahmen zur Bekämpfung von Bedrohungen.

Unser Stand: 6-112

Kostenloser Check Ihrer M365 Postfächer

Mimecast Threat Scan jetzt starten!

- 30 Tage Live-Check
- 30 Tage historischer Check
- Abschlussbericht mit Auswertung
 - Nicht erkannte Phishing-Mails
 - Zugestellter SPAM
 - Malware in E-Mail-Anhängen

Die Bereitstellung dauert nur zwei Minuten.



mimecast

Kostenloser 30-Tage M365 Threat Scan
Scannen Sie Ihre Inbox und identifizieren Sie potenziell gefährliche E-Mails!

Die E-Mail bleibt nicht nur das Einfallstor Nr.1 für Cyberattacken - Phishing-Angriffe werden dank generativer KI noch raffinierter und glaubwürdiger. Unternehmen sollten für den Schutz Ihrer E-Mail und Collaboration-Landschaft gleiche Mittel wie KI und ML einsetzen, um potenziellen Angreifern auf Augenhöhe Paroli bieten zu können.

Mimecast Cloud Integrated bietet eine einfache Verwaltung und sofort einsatzbereite Schutzfunktionen. Bedrohungen werden in Echtzeit abgewehrt, während historische Bedrohungen effektiv beseitigt werden. Zudem erhöhen Warnmeldungen die Sicherheit und schützen Sie proaktiv vor potenziellen Risiken.

Voraussetzungen
Einfacher Start: Nur ein M365-Tenant/ Exchange Online erforderlich.

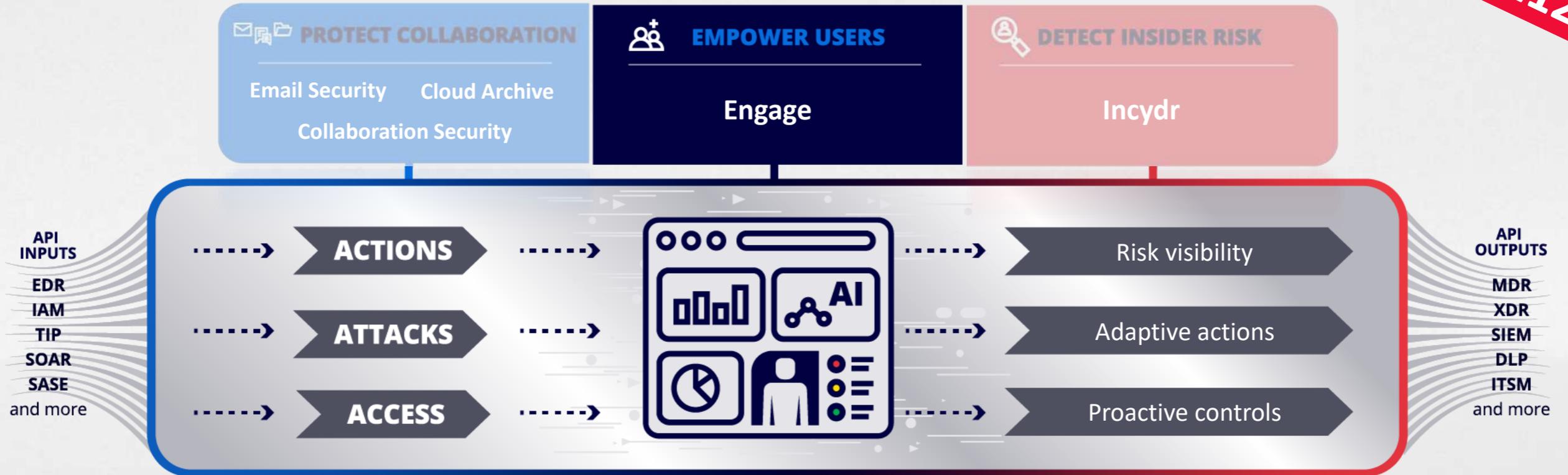
Erkennung
Entdecken Sie potenzielle Bedrohungen wie Phishing, Malware, verdächtige Absender, Spam und weitere Sicherheitsrisiken.

Detaillierte Analyse
Erhalten Sie umfassende Berichte inklusive Handlungsempfehlungen. Zusätzlich erhalten Sie eine prägnante Zusammenfassung per E-Mail und auf Wunsch einen ausführlichen Bericht.



Human Risk Management Platform

Unser Stand: 6-112



Es braucht mehr als Schulungen und Simulationsmetriken, um Human Risk wirklich zu verstehen

-  Schulungen und Simulationen allein zeigen nicht das Gesamtbild.
-  Simuliertes Risiko entspricht nicht dem realen Risiko.
-  Verhaltensanalysen sind der Schlüssel zur effektiven Verwaltung des Human Risk.

Wer stellt das *reale* Risiko dar?



Mitarbeiter A



Mitarbeiter B

Traditionelle Kennzahlen

Training Modul	✓ Erledigt	✗ Unvollständig
Training Modul	✓ Erledigt	✓ Erledigt
Phishing Simulation #1	✓ Bestanden	✗ Nicht Bestanden
Phishing Simulation #2	✓ Bestanden	✗ Nicht Bestanden
Phishing Simulation #3	✓ Bestanden	✓ Bestanden

Echte Risikosignale

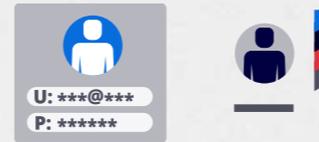
Verdächtiger Anhang	✗ Heruntergeladen	✓ Kein Download
Dringende Anfrage von jmd. Unbekanntem	✗ Geantwortet	✓ Ignoriert
Phishing Angriff	✗ Geklickt	✓ Nicht geklickt
Phishing Angriff	✗ Geklickt	✓ Gemeldet

Nutzen Sie echte Sicherheitssignale und Verhaltensanalysen

MONITOR

ACTIONS

Teilt Login-Daten



Sendet Unternehmensdaten an persönlichen Datei-Speicher



VERSTEHEN

ATTACKS

Erhält böser Anhang



Ziel von Phishing-Angriffen



BERÜCKSICHTIGEN

ACCESS

Zugriff auf Finanzdaten



Senior Leadership Rolle

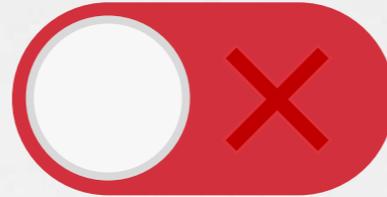


Security Awareness, Re-Envisioned

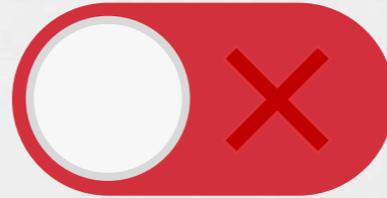


Traditionelle Lösungen

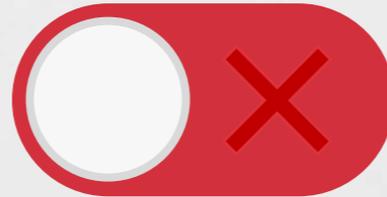
One-size-fits-all Ansatz.



Output orientiert.



Misst nur simuliertes Risiko



Security Awareness, Re-Envisioned



Traditionelle Lösungen

One-size-fits-all Ansatz.



Output orientiert.



Misst nur simuliertes Risiko.



Powered by a Human Risk Management Platform

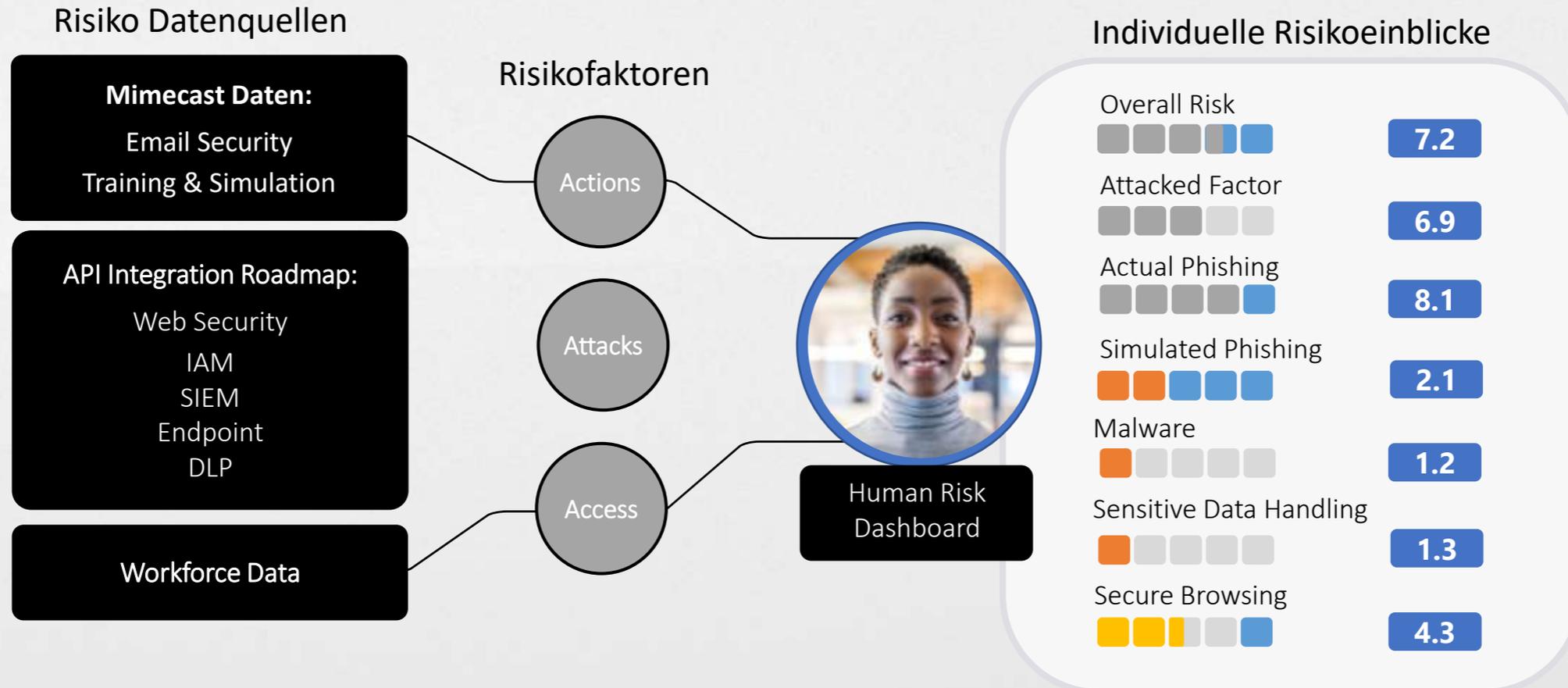
Personalisiert.

An echten Sicherheitsergebnissen ausgerichtet.

Gestützt auf echte Risikoeinblicke.

Identifizieren Sie Ihre risikobehaftetsten Mitarbeiter

Human Risk Dashboard: Ungeahnte Risiko-Sichtbarkeit



Identifizieren Sie Ihre risikobehaftetsten Mitarbeiter

Human Risk Dashboard | Features & Fähigkeiten

Human Risk Dashboard

- Unternehmensweites Risikoscoring
- Angriffsfaktor
- Hebt die risikobehaftetsten Mitarbeiter hervor

Individuelles Risikoprofil

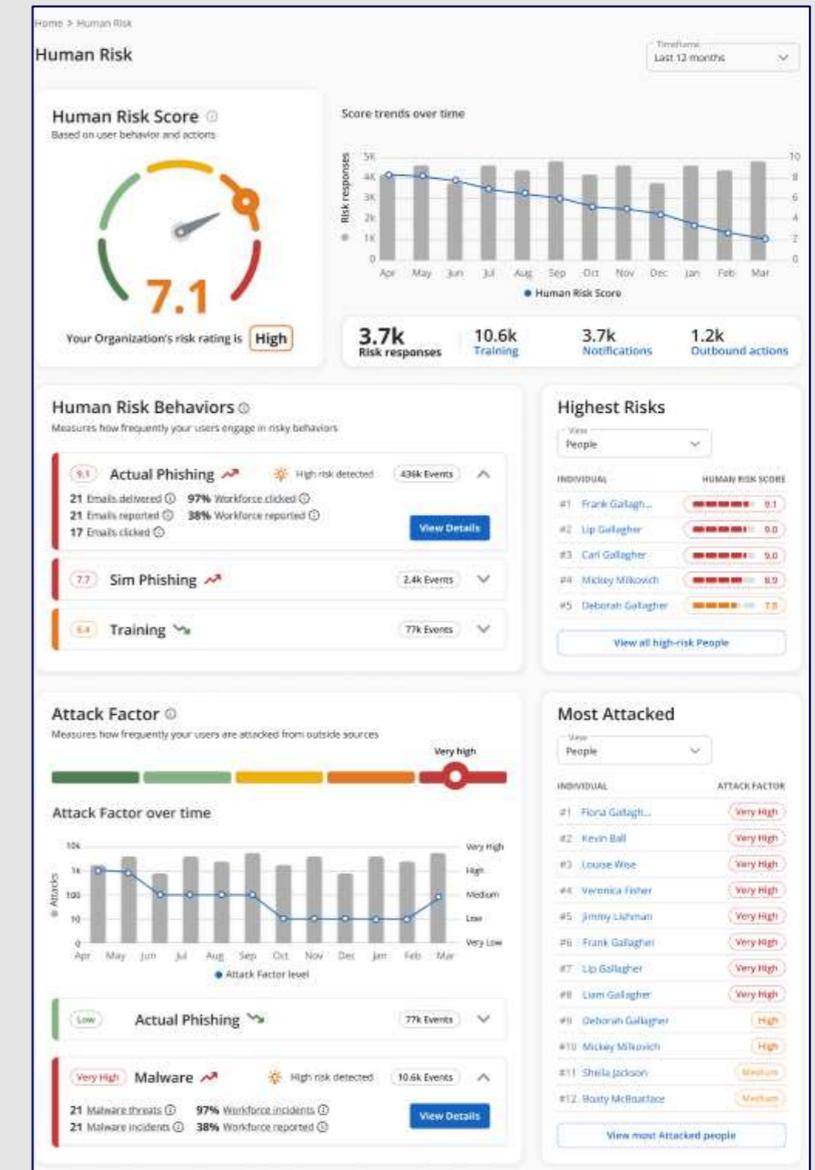
- Individualisiertes Risikoscoring
- Dokumentiert individuelle Risikoreaktionen
- Erfasst Risikoereignisse

Risiko Response Engine

- Organisationales Protokoll der Risikoreaktionen
- Regelbasierte Berichterstattung und Analyse

Risiko Analyse Seite

- Tabellarische Ansicht aller Mitarbeiter-Risiken
- Risikobasierte Suche und Filter



Veranlassen Sie echte Verhaltensänderungen

Schneiden Sie Schulungen und Maßnahmen auf die tatsächlichen Verhaltensweisen jedes Mitarbeiters zu.

Der Mitarbeiter führt eine Sicherheitsmaßnahme durch.



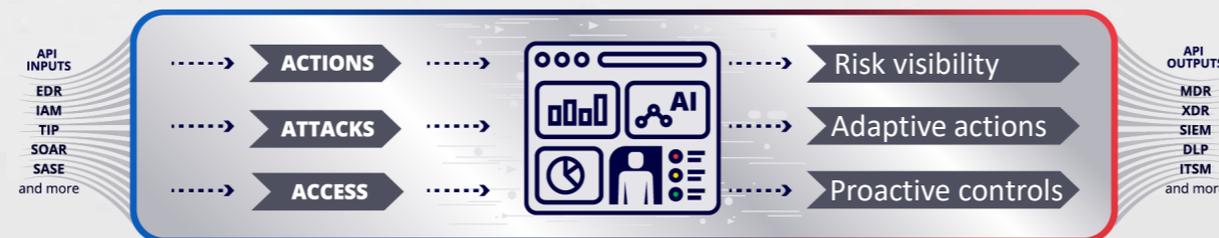
Human Risk Management Platform analysiert die Aktion.



Die Risiko-Response-Engine löst einen Verhaltensimpuls in Mimecast Engage aus.

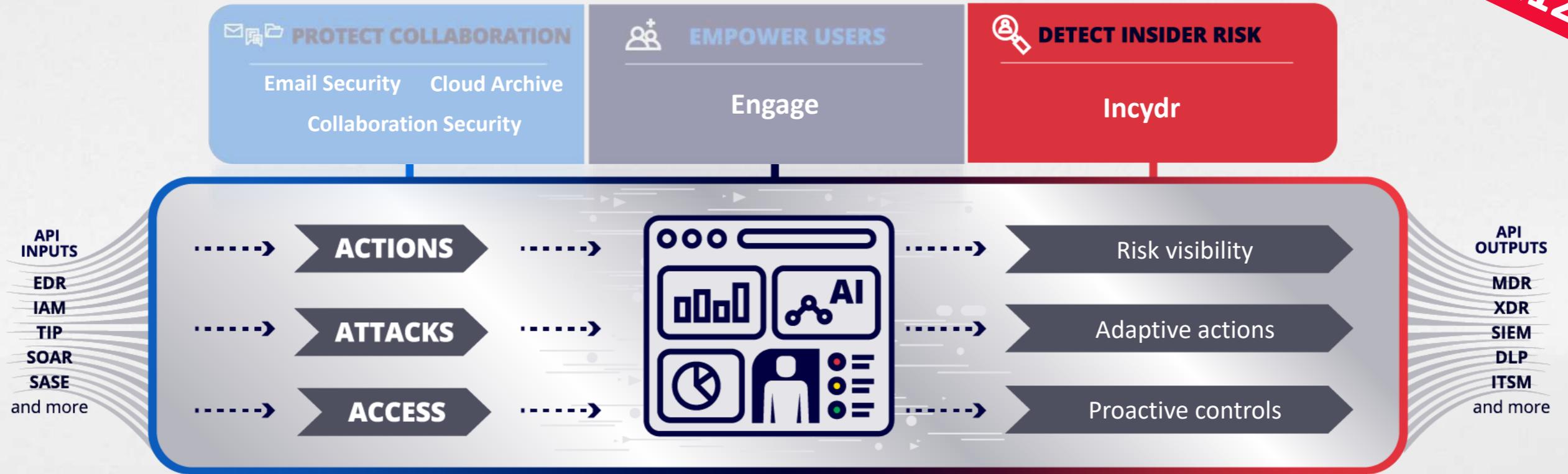


Impuls wird an Mitarbeiter geschickt.



Human Risk Management Platform

Unser Stand: 6-112



Erkennen und verhindern Sie Datenverlust



IP Theft



Departing Employee
Exfiltration



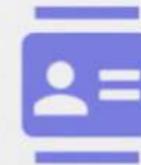
Security Awareness &
Culture Change



Cloud Visibility



Source Code
Protection



Customer Data
Protection

Traditionelle Lösungen **verursachen Arbeit** und erledigen sie nicht.

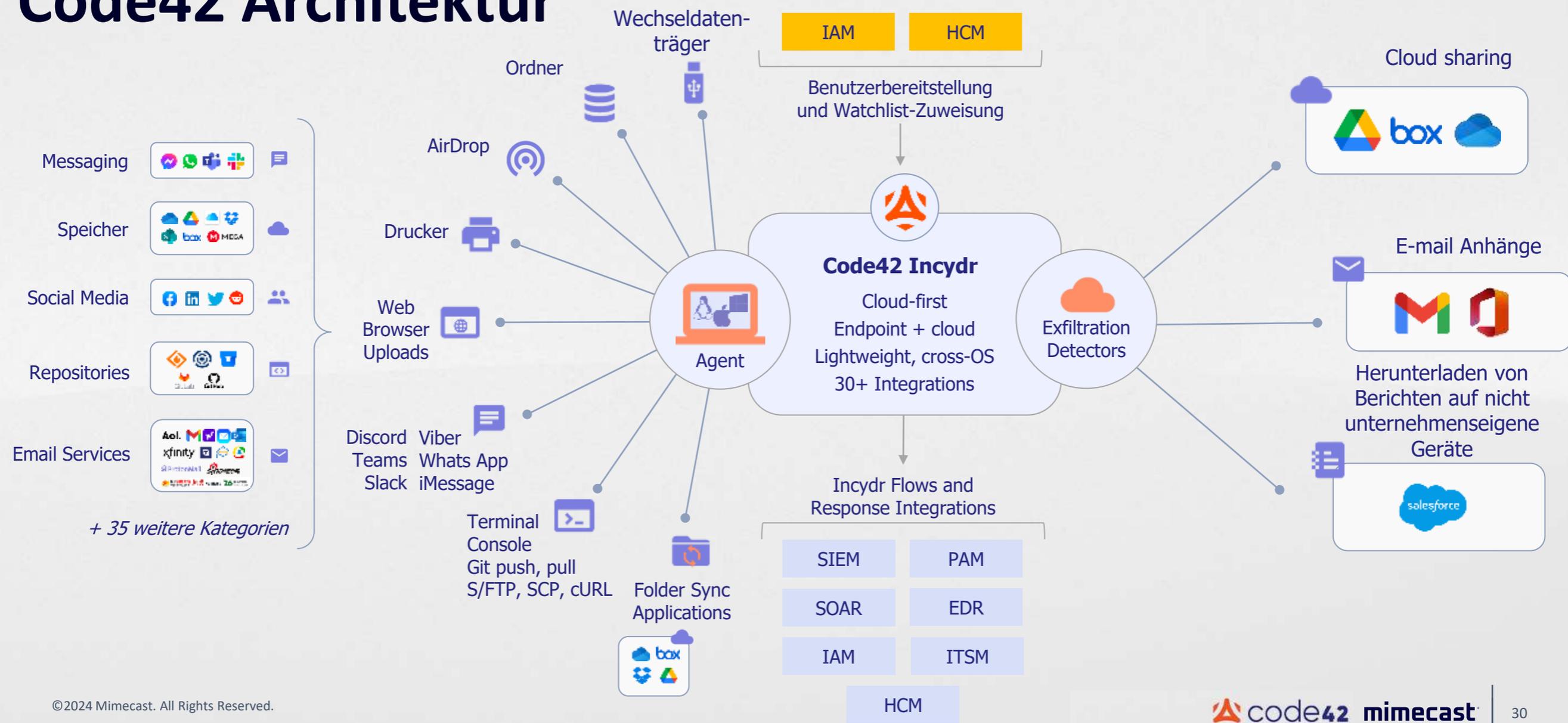


DLP + CASB + UEBA

- ⊘ **Eingeschränkte Sichtbarkeit:** Erkennung ist an Regelwerke gebunden, unzureichender IP-Schutz, fehlt an Kontext und Integrationen.
- ⊘ **Komplexe Verwaltung:** 6-12-monatige Implementierungen, erfordert ständige Anpassungen, führt zu Alarmmüdigkeit.
- ⊘ **Benutzerbeschwerden:** verlangsamt Geräte, führt zu Umgehungen und Ausnahmen, wirkt sich negativ auf die Unternehmenskultur aus.

UNSERE LÖSUNG

Code42 Architektur



State of Data Loss

Häufig

60 % der Endbenutzer in mittelständischen Unternehmen geben zu, regelmäßig Arbeitsdateien auf ihre privaten Konten zu übertragen. (Gartner)

Teuer

Die durchschnittlichen Kosten eines Insider-Bedrohungsvorfalles belaufen sich auf **\$16Mio.** (Code42 DER 2023)

Eindrucksvoll

Mindestens **1 von 3** Datenschutzverletzungen betrifft Insider (Code42 DER 2021)

Unkontrolliert

90% der Sicherheitsteams setzen mehr als 3 Lösungen ein, um Datenverluste zu verhindern. Dennoch gehen Unternehmen von bis zu 300 durch Insider verursachten Datenverlusten pro Jahr aus (Anstieg um 32 % im Vergleich zum Vorjahr) (Code42 DER 2023)

Datenrisiken
steigen an



Source code
exfiltration via Git



Airdrop-Ereignisse
steigen um 1.000%
QoQ



Salesforce exfiltration
auf persönliche Geräte



Öffentliche Links von
Firmenkonten wie OneDrive

**Data Protection
+ Insider
Bedrohungen**



**Förderung einer
risikobewussten
Kultur**



Customer experience:

- Bereitstellung von Agent, Cloud und Identität in 1 Stunde
- Mehr als 30 Integrationen
- Launchpad-Vorlagen und Tipps zum Aufbau eines erfolgreichen Programms; Rollout mit bewährten Datenschutzverfahren Ihnen zugewiesener CSM und Customer Success Engineer
- Ausführliche Dokumentation und US-Support

Unsere Produkte



PROTECT COLLABORATION

Email Security

BEC, Phishing, Malware
Incident Remediation
Brand Protection

Cloud Archive

Case Review
Legal Holds
Supervision
Sync and Recover

Collaboration Security

Microsoft Teams, SharePoint, and OneDrive
Protection against Phishing and Malware



EMPOWER USERS

Engage

Human Risk Dashboard
Adaptive Training
Nudges
User Scorecards
Phishing Simulations
Entertaining Content



DETECT INSIDER RISK

Incydr

Monitor Corporate Applications

- Cloud: OneDrive, Google Drive, Box
- Email: O365, Gmail
- Apps: Salesforce, Git

Cloud Visibility

- Windows, Mac, Linux

Unser Stand: 6-112

Kostenloser Check Ihrer M365 Postfächer

Mimecast Threat Scan jetzt starten!

- 30 Tage Live-Check
- 30 Tage historischer Check
- Abschlussbericht mit Auswertung
 - Nicht erkannte Phishing-Mails
 - Zugestellter SPAM
 - Malware in E-Mail-Anhängen

Die Bereitstellung dauert nur zwei Minuten.



mimecast

Kostenloser 30-Tage M365 Threat Scan
Scannen Sie Ihre Inbox und identifizieren Sie potenziell gefährliche E-Mails!

Die E-Mail bleibt nicht nur das Einfallstor Nr.1 für Cyberattacken - Phishing-Angriffe werden dank generativer KI noch raffinierter und glaubwürdiger. Unternehmen sollten für den Schutz Ihrer E-Mail und Collaboration-Landschaft gleiche Mittel wie KI und ML einsetzen, um potenziellen Angreifern auf Augenhöhe Paroli bieten zu können.

Mimecast Cloud Integrated bietet eine einfache Verwaltung und sofort einsatzbereite Schutzfunktionen. Bedrohungen werden in Echtzeit abgewehrt, während historische Bedrohungen effektiv beseitigt werden. Zudem erhöhen Warnmeldungen die Sicherheit und schützen Sie proaktiv vor potenziellen Risiken.

Voraussetzungen
Einfacher Start: Nur ein M365-Tenant/ Exchange Online erforderlich.

Erkennung
Entdecken Sie potenzielle Bedrohungen wie Phishing, Malware, verdächtige Absender, Spam und weitere Sicherheitsrisiken.

Detaillierte Analyse
Erhalten Sie umfassende Berichte inklusive Handlungsempfehlungen. Zusätzlich erhalten Sie eine prägnante Zusammenfassung per E-Mail und auf Wunsch einen ausführlichen Bericht.





mimecast[®]

The Connected Human Risk Management Platform

Kommen Sie zu unserem Stand: 6-112