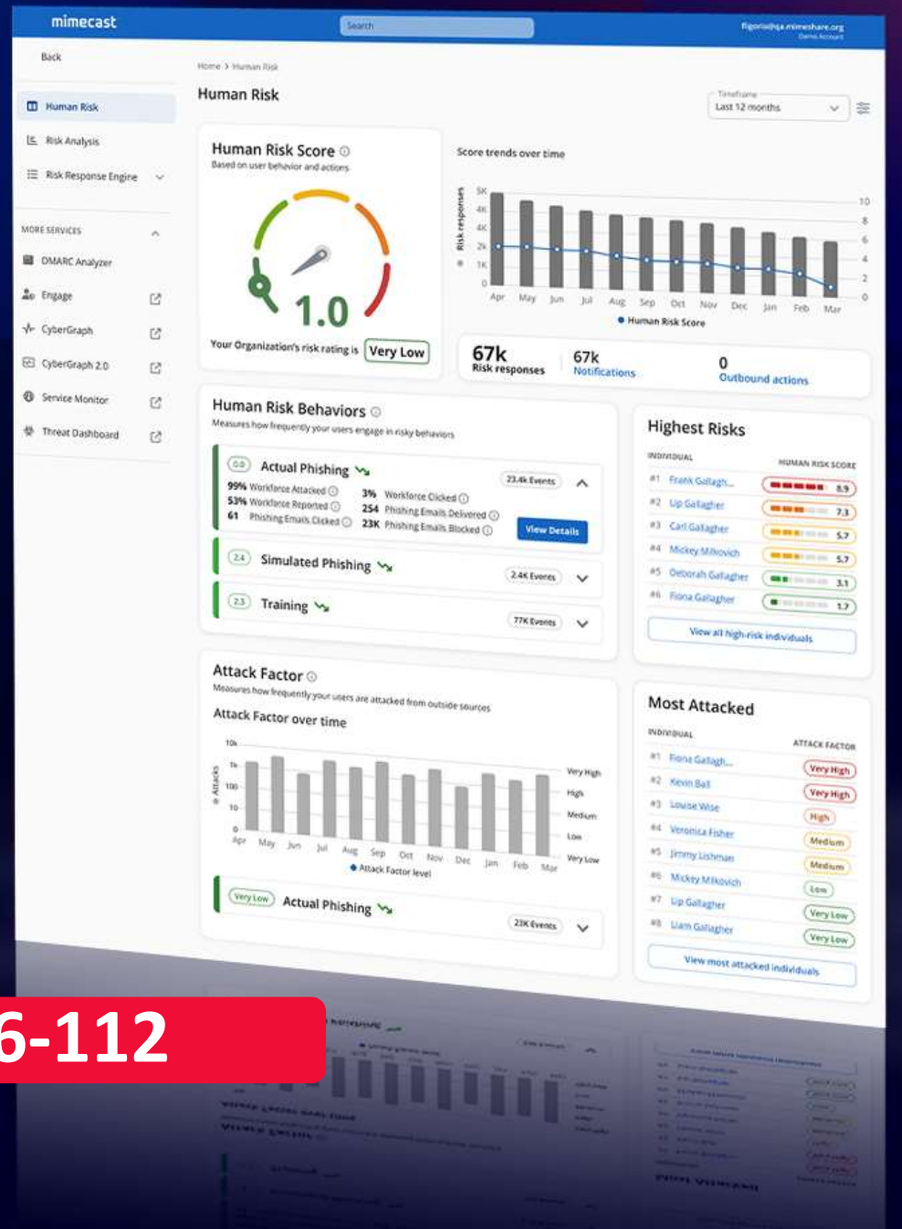
mimecast

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

ACTIONS

Teilt Anmeldeinformationen
Sendet Unternehmensdaten an persönlichen Dateifreigabedienst
Klickt auf eine betrügerische URL

ATTACKS

Mit bösartigem Anhang angegriffen
Gezielt für Social-Engineering-Angriffe

ACCESS

Zugriff auf Finanzanwendungen
Höhere technische Rolle
Privilegierter Zugriff

Das Human Risk Problem

90%

der Angriffe beginnen mit Email[1]

1 von 17

von Nachrichten durch Collaboration-Tools enthalten sensible Daten[2]

8%

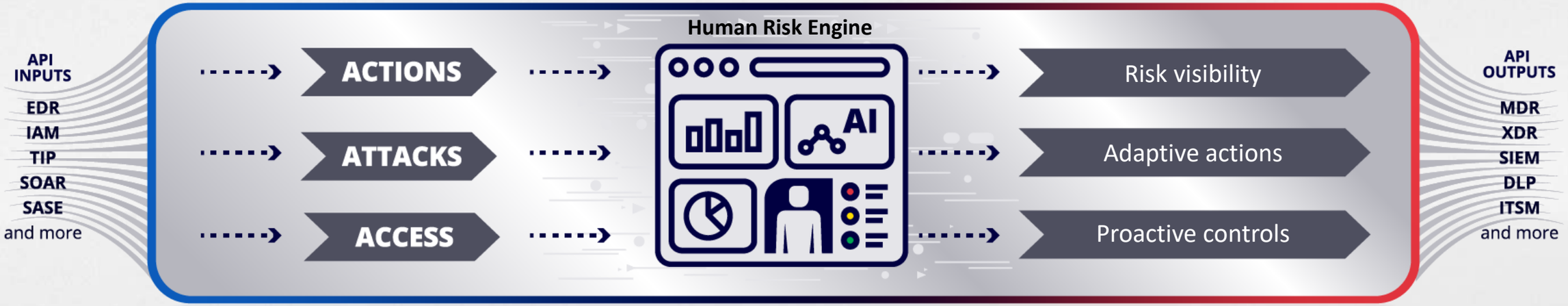
der Mitarbeiter sind an **80%** der Vorfälle beteiligt[3]

$15M

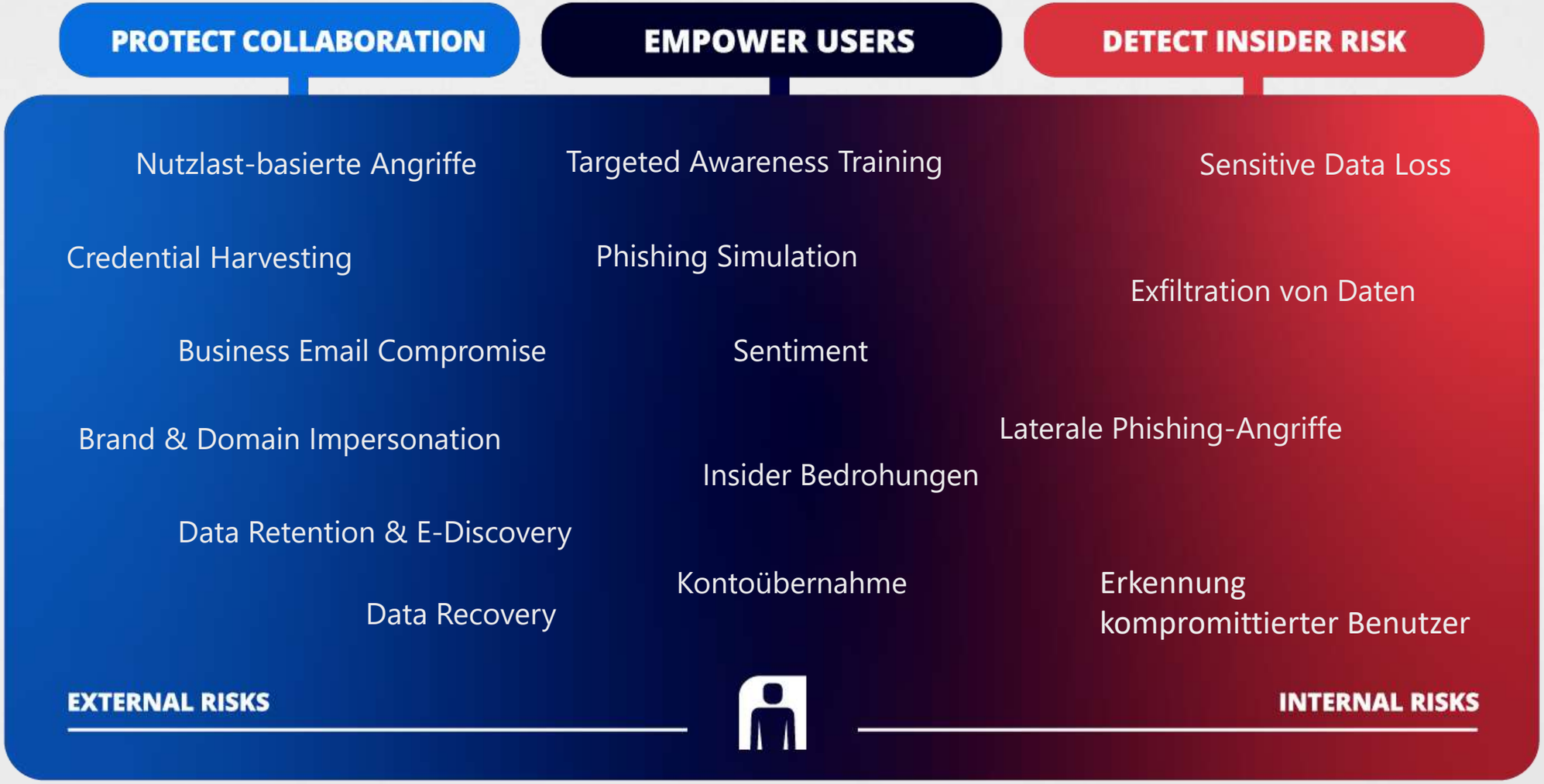
Durchschnittliche Kosten eines Insider-Datenlecks[4]

Sichere Zusammenarbeit mit einer einheitlichen Plattform

Die vernetzte Human Risk Management-Plattform

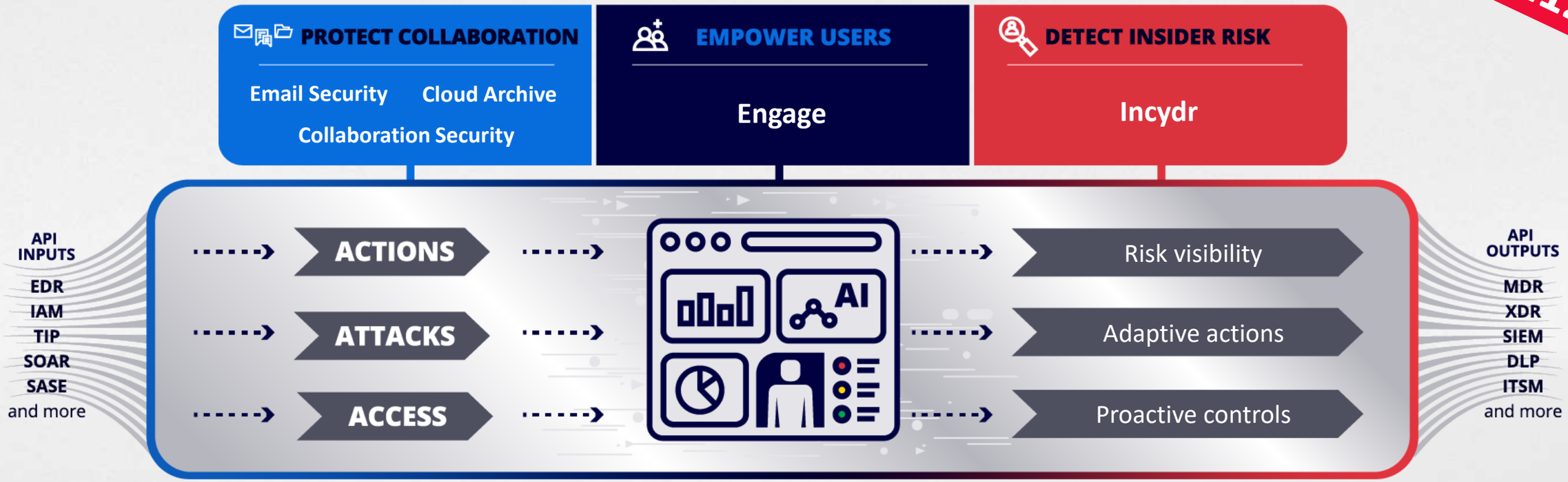


Anwendungsfälle



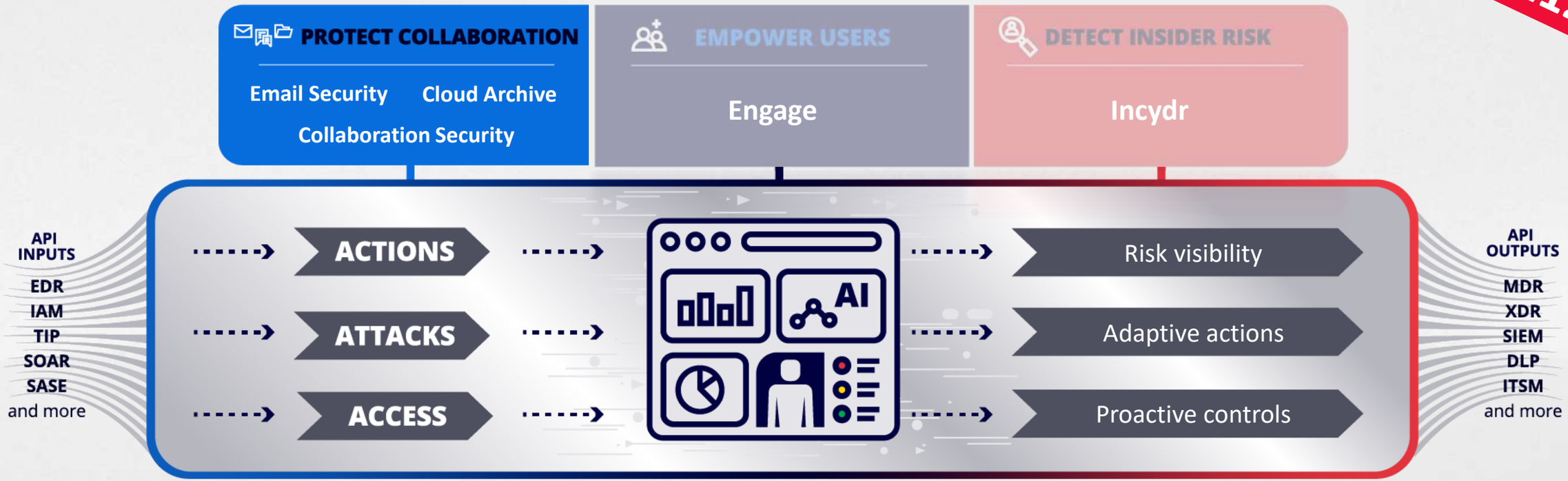
Unsere Produkte

Unser Stand: 6-112

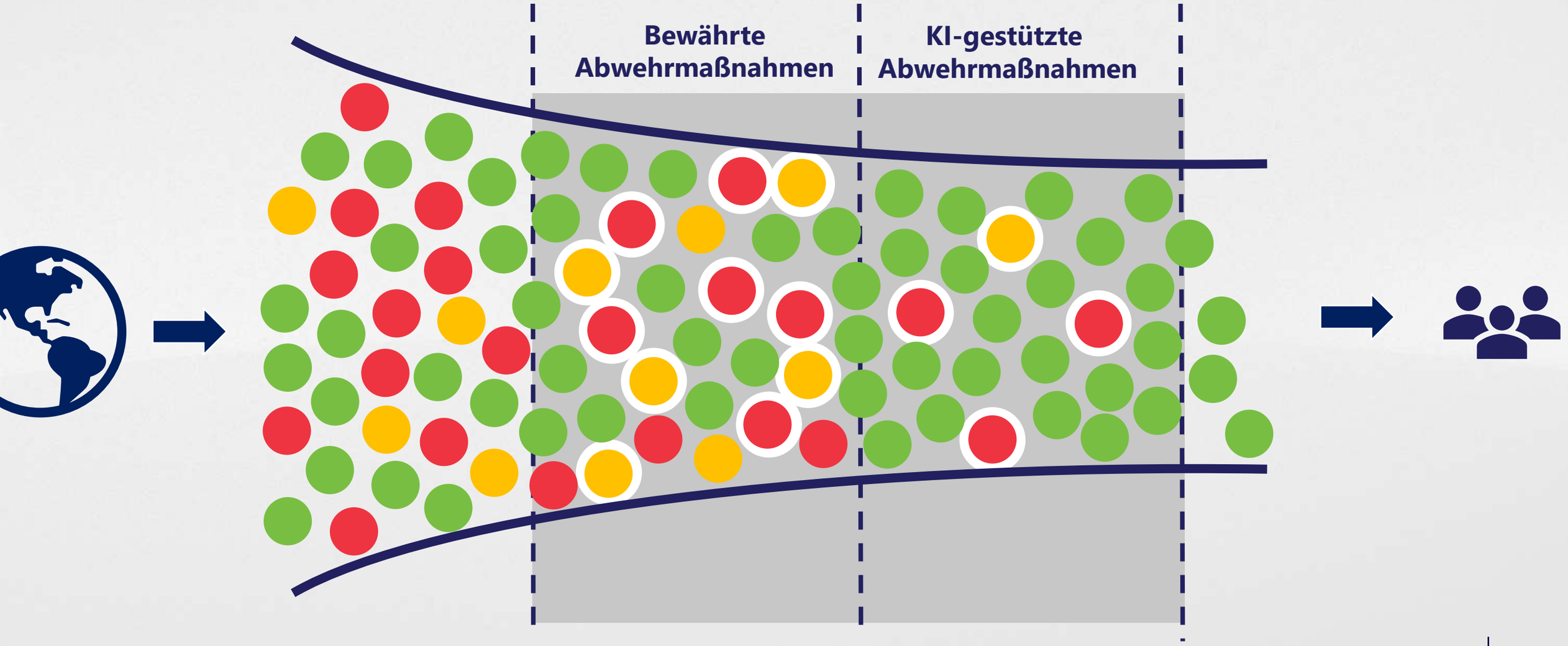


Human Risk Management Platform

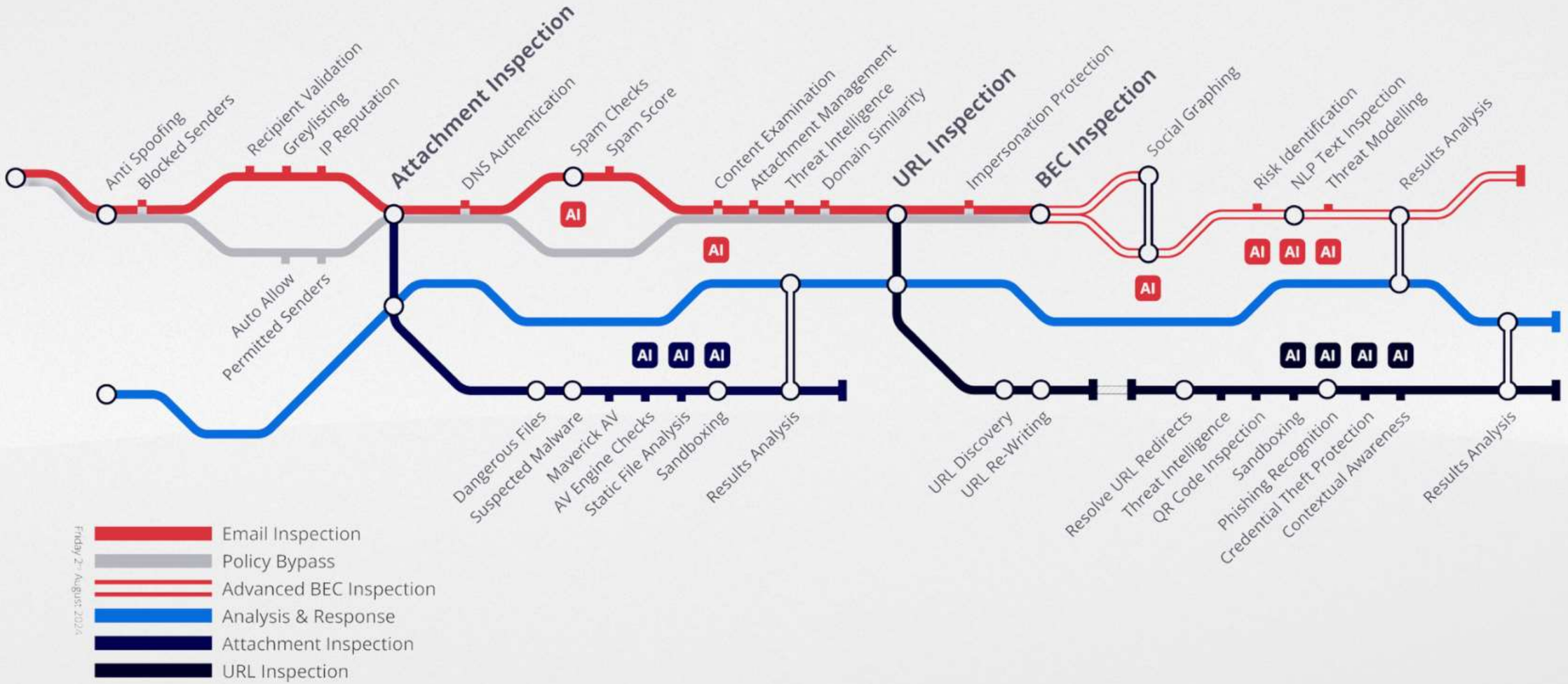
Unser Stand: 6-112



Blockieren Sie E-Mail-basierte Bedrohungen



Mimecast KI Nutzung



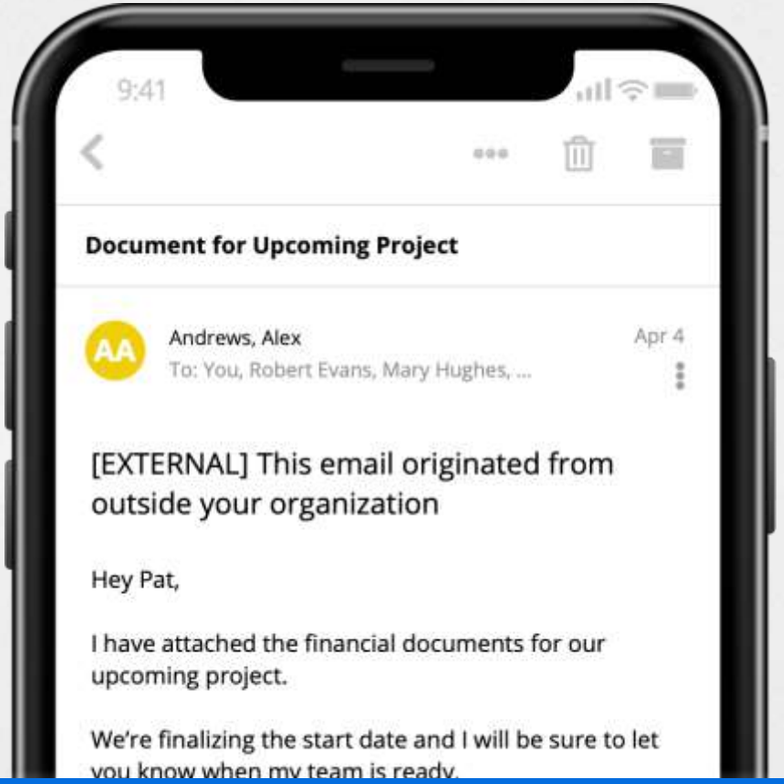
CyberGraph – Warnmeldungen

Kontextbezogene Warnungen

Lernen in Echtzeit

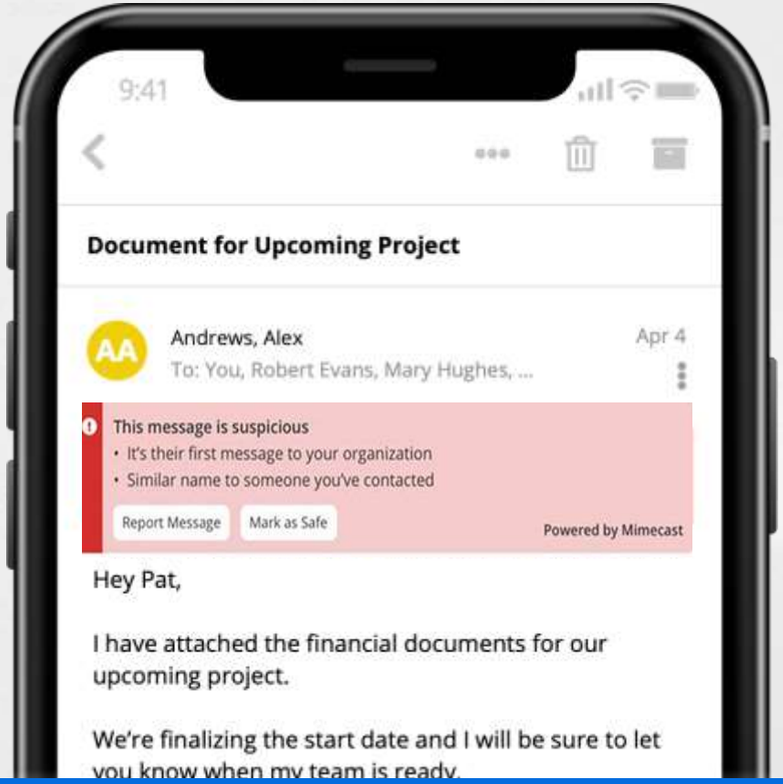
Rückwirkende Warnungen

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

CyberGraph – Warnmeldungen

Kontextbezogene Warnungen

Lernen in Echtzeit

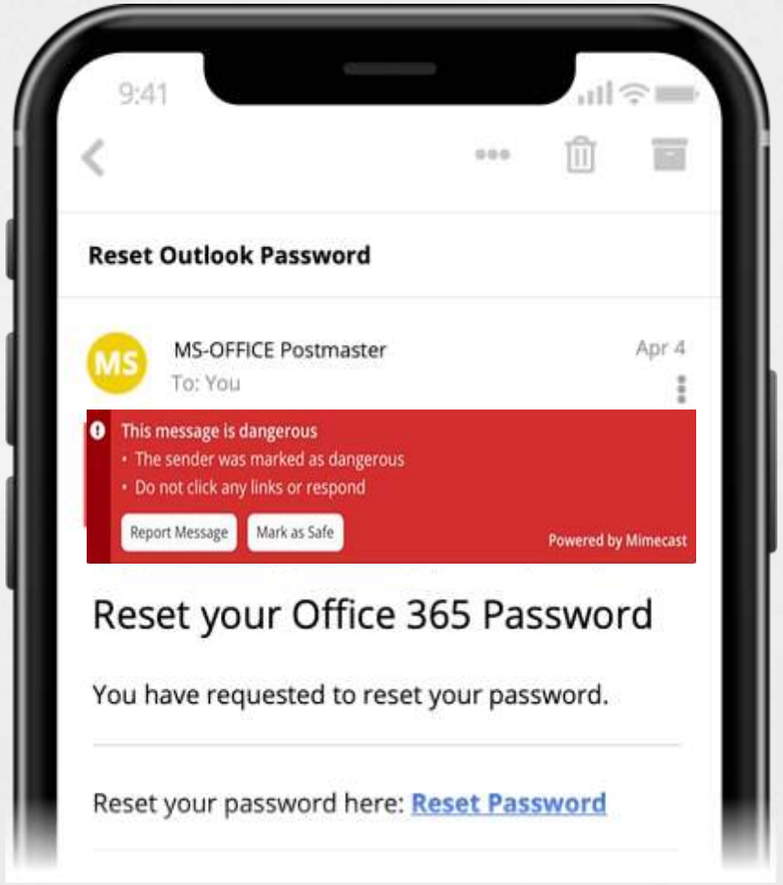
Rückwirkende Warnungen

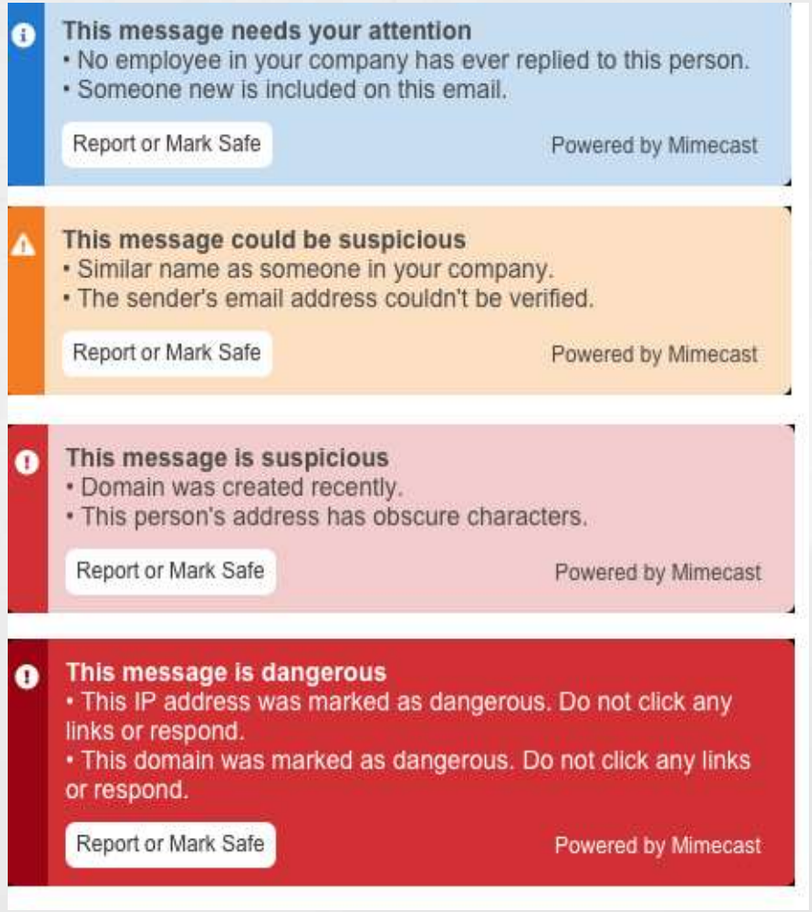
CyberGraph – Warnmeldungen

Kontextbezogene Warnungen

Lernen in Echtzeit

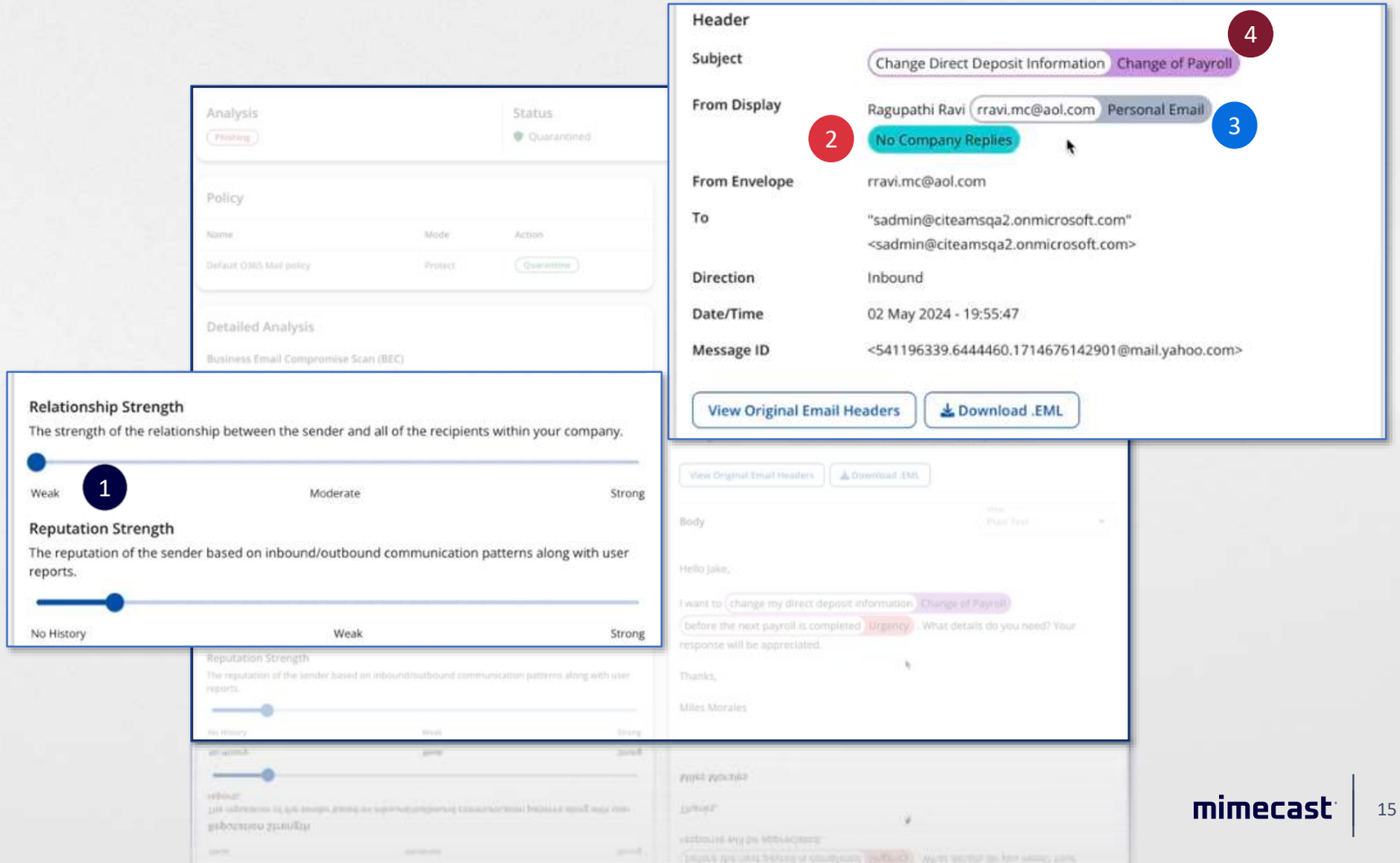
Rückwirkende Warnungen





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



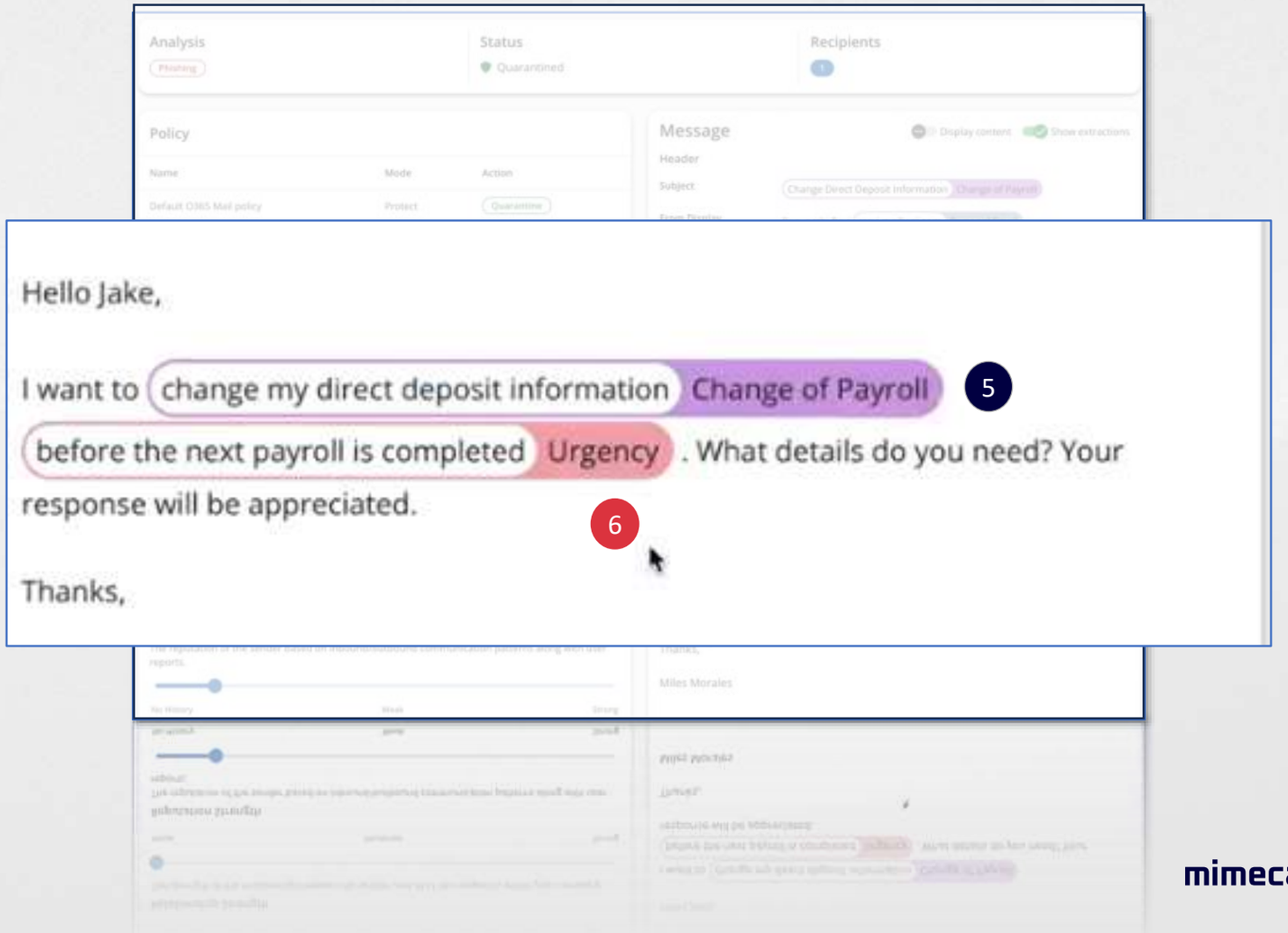
Business Email Compromise (BEC)-Angriffe abwehren

5 **Bedrohungsspezifische Sprache**

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

6 **Nachrichtenintention**

Fokus auf die zugrunde liegende Bedeutung und Absicht



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.

Kostenloser Check Ihrer M365 Postfächer

Unser Stand: 6-112

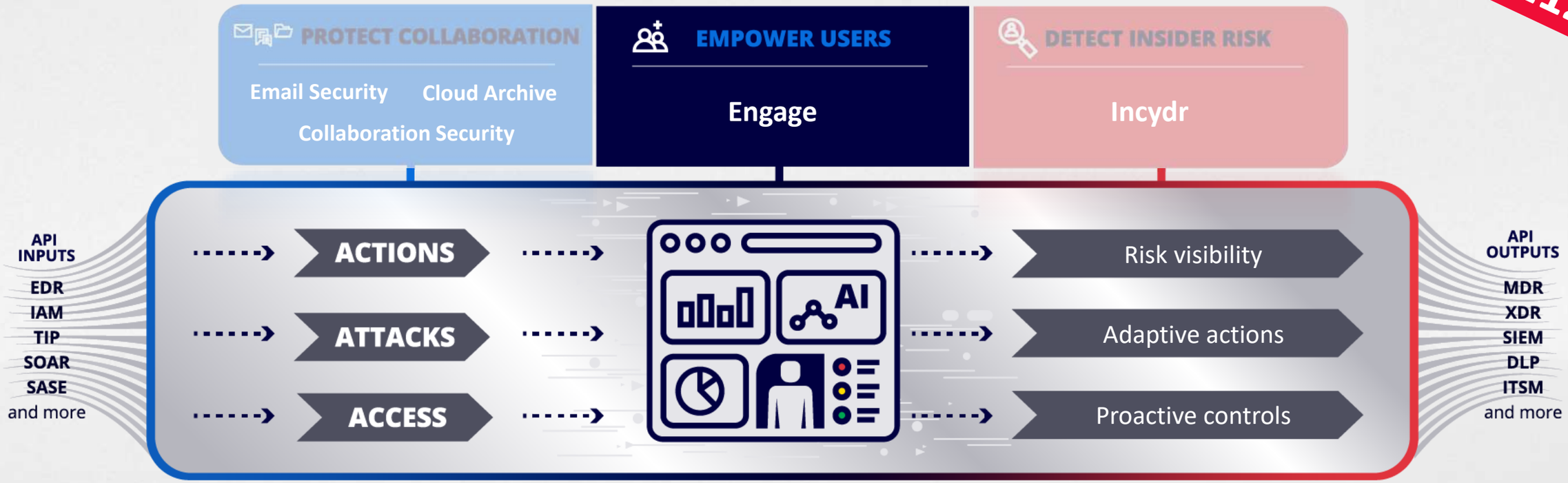
Mimecast Threat Scan jetzt starten!

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

Die Bereitstellung dauert nur zwei Minuten.

Human Risk Management Platform

Unser Stand: 6-112



Es braucht mehr als Schulungen und Simulations-metriken, 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

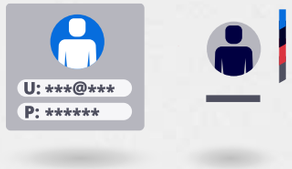
Mitarbeiter B

		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 Sicherheitsignale und Verhaltensanalysen

MONITOR **ACTIONS**

Teilt Login-Daten



Sendet Unternehmensdaten an persönlichen Datei-Speicher

VERSTEHEN **ATTACKS**

Erhält bösartigen Anhang

Ziel von Phishing-Angriffen

BERÜCKSICHTIGEN **ACCESS**

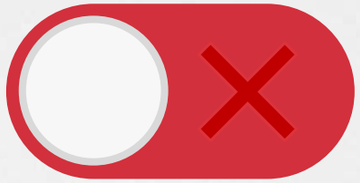
Zugriff auf Finanzdaten

Senior Leadership Rolle

Security Awareness, Re-Envisioned

Traditionelle Lösungen

One-size-fits-all Ansatz.



Output orientiert.

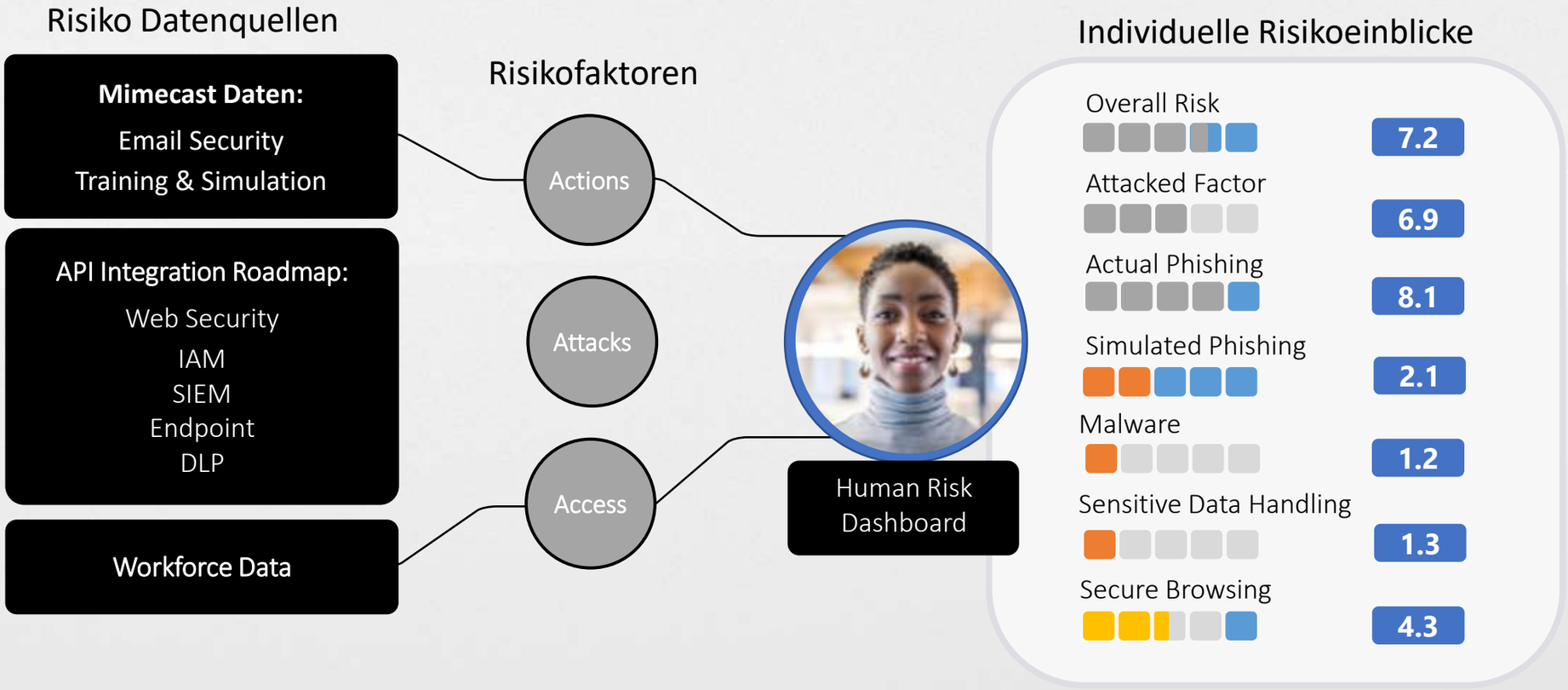
Misst nur simuliertes Risiko

Security Awareness, Re-Envisioned

Traditionelle Lösungen		Powered by a Human Risk Management Platform
One-size-fits-all Ansatz.		**Personalisiert.**
Output orientiert.		**An echten Sicherheitsergebnissen ausgerichtet.**
Misst nur simuliertes Risiko.		**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

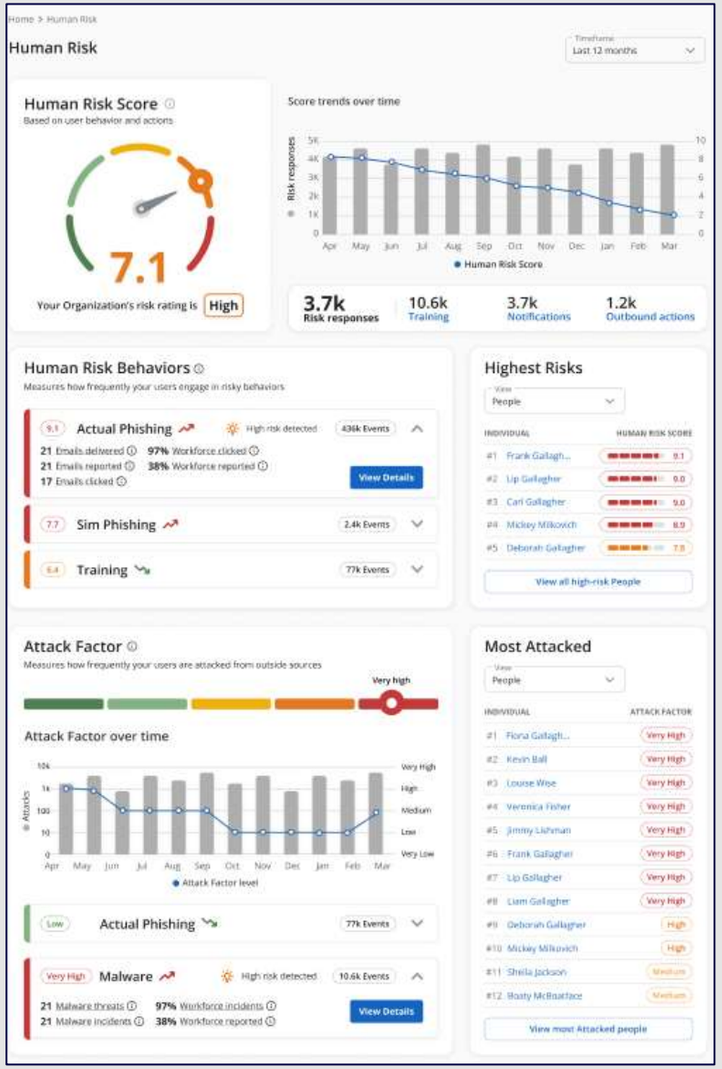
- Individualisiertes Risikoscoring
- Dokumentiert individuelle Risikoreaktionen
- Erfasst Risikoereignisse

Risiko Response Engine

- Organisationales Protokoll der Risikoreaktionen
- Regelbasierte Berichterstattung und Analyse

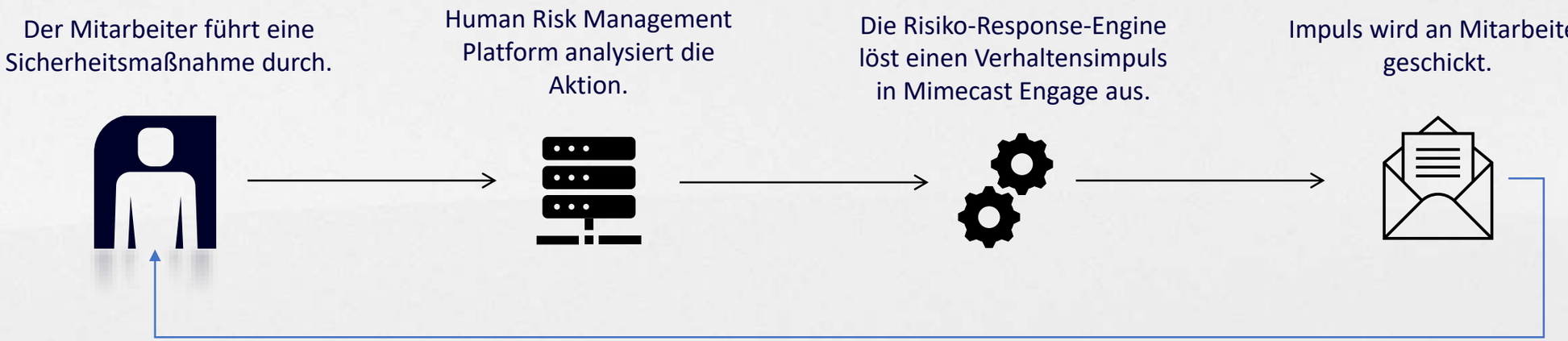
Risiko Analyse Seite

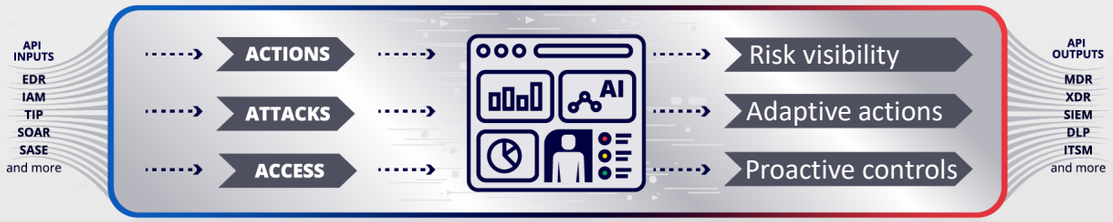
- Tabellarische Ansicht aller Mitarbeiter-Risiken
- Risikobasierte Suche und Filter



Veranlassen Sie echte Verhaltensänderungen

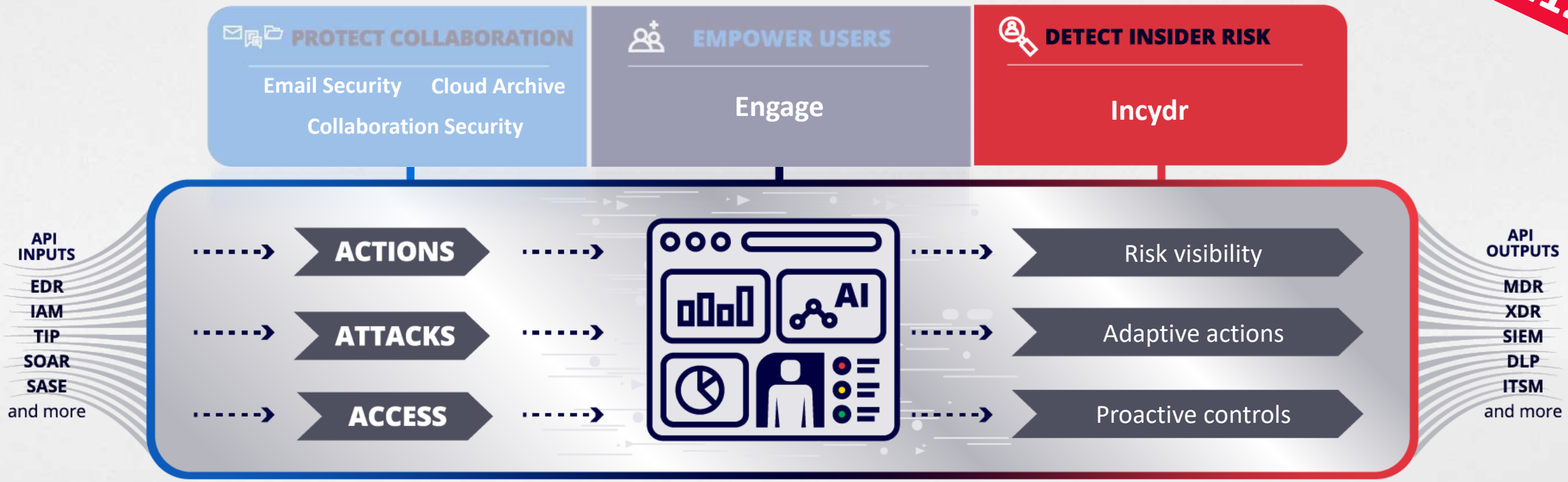
Schneiden Sie Schulungen und Maßnahmen auf die tatsächlichen Verhaltensweisen jedes Mitarbeiters zu.





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

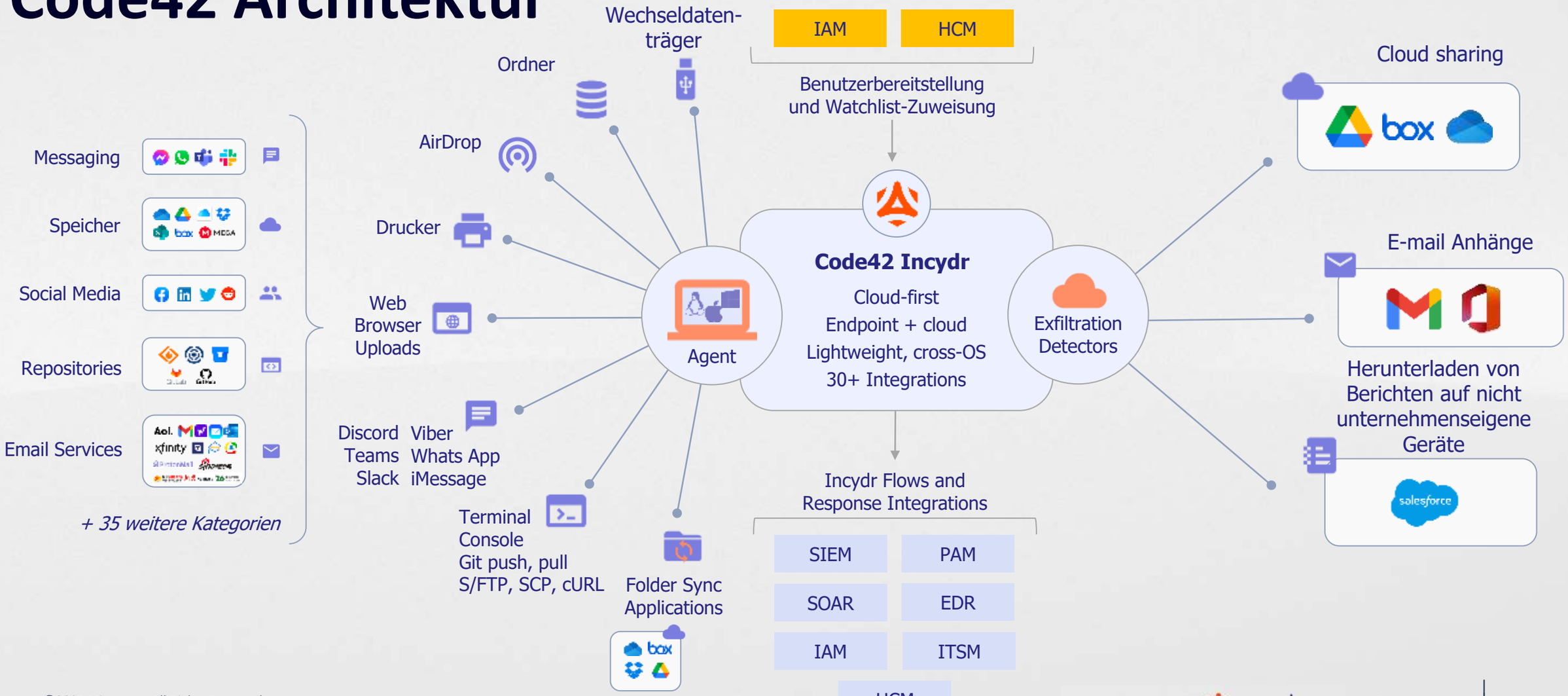
Traditionelle Lösungen **verursachen Arbeit**

und erledigen sie nicht.

- **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-Bedrohungsvorfalls 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

code42 INCYDR

Förderung einer risikobewussten Kultur

code42 INSTRUCTOR

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 DatenschutzverfahrenIhnen 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

Kostenloser Check Ihrer M365 Postfächer

Unser Stand: 6-112

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-Anhägen

Die Bereitstellung dauert nur zwei Minuten.

mimecast®

The Connected Human Risk Management Platform

Kommen Sie zu unserem Stand: 6-112