Cloudbasierte E-Mail-Sicherheit (CES)

Cloudflare, ein von Analysten anerkannter Marktführer im Bereich E-Mail-Sicherheit, erkennt und stoppt Phishing-Bedrohungen schon im Vorfeld

Schutz vor gezielten Phishing-Angriffen

Mühelos Bedrohungen abwehren oder isolieren, die anderen Lösungen entgehen

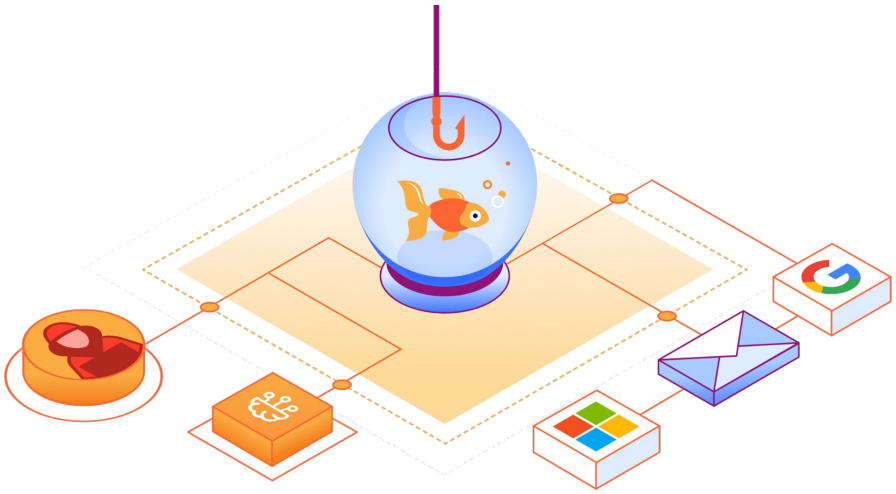
Unter allen Geschäftsanwendungen erfreuen sich E-Mails sowohl bei Nutzern als auch bei Angreifern der größten Beliebtheit. Insofern ist es heute wichtiger denn je, Anwender davor zu schützen, dass ihr Vertrauen durch Phishing missbraucht wird. Um hybrid arbeitende Beschäftigte besser zu unterstützen, setzen Unternehmen zunehmend cloudbasierte E-Mail-Dienste wie Microsoft 365 und Google Workspace ein. Das veranlasst Kriminelle dazu, sich auf kleinere, aber zielgerichtetere Angriffe zu verlegen, die herkömmliche Secure Email Gateways (SEGs) wie Proofpoint und Mimecast umgehen können.

Die cloudnative E-Mail-Sicherheitslösung von Cloudflare (Area 1) wurde speziell dafür entwickelt, mithilfe der vorbeugenden Verwendung von Informationen über Angriffskampagnen, der durch maschinelles Lernen unterstützten Analyse von Inhalten und einer übergreifenden Zero Trust-Plattform Phishing-Angriffe zu stoppen, bevor sie Ihre Mitarbeitenden überhaupt erreichen.

91 %
aller Cyberangriffe beginnen mit einer Phishing-E-Mail1[1]

50 Mrd.
US-Dollar Verlust wurden in den letzten zehn Jahren durch kompromittierte E-Mail-Konten verursacht[2]

81 %
aller Unternehmen haben in den letzten zwölf Monaten einen Multi-Channel-Angriff verzeichnet[3]



Übernahme geschäftlicher E-Mail-Konten verhindern

Eine mehrstufige, durch Machine Learning-unterstützte Kontextanalyse fördert Konten zutage, die gekapert oder kompromittiert wurden.

Zeitversetzte Attacken und Multi-Channel-Angriffe isolieren

Nutzer werden vor schädlichen Webinhalten geschützt, die über unbekannte oder betrügerische Links aufgerufen werden.

Ransomware und schädliche Anhänge blockieren

So können Erpressungsversuche und Schadcode Ihrem Unternehmen nicht gefährlich werden.

Mehr Schutz, weniger Aufwand

Eine mehrstufige Sicherheitslösung für größeren Schutz zu einem Bruchteil der Kosten

Angesichts der immer weiter um sich greifenden Phishing-Angriffe haben Microsoft und Google zusätzliche Funktionen speziell für ihre Produkte entwickelt, die wichtige E-Mail-und Datenschutzaufgaben wie Authentifizierung, Archivierung, Schutz vor Datenverlust (Data Loss Prevention – DLP) und clientseitige Verschlüsselung übernehmen. Bedrohungsakteure haben jedoch ihre Taktiken weiterentwickelt, um zielgerichtetere und ausweichende Angriffe durchzuführen, die häufig die integrierten Sicherheitskontrollen umgehen und größere Chancen auf Erfolg bieten.

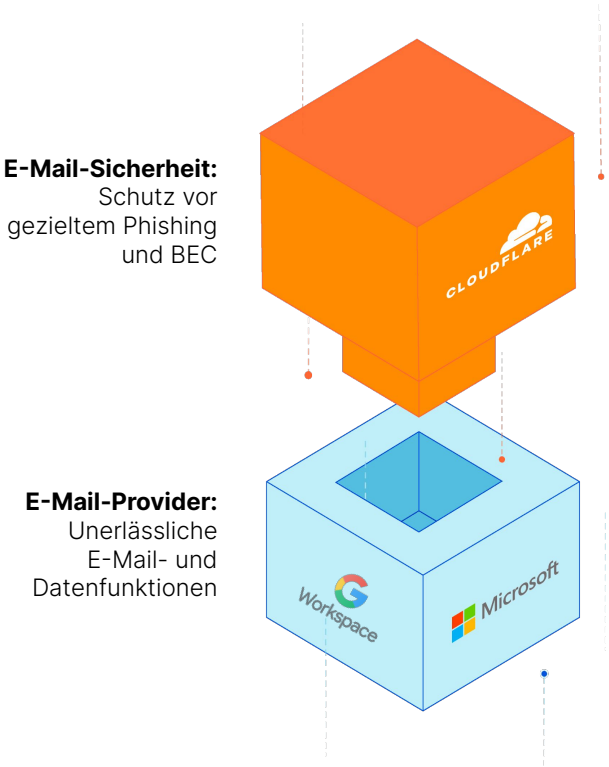
Mit Cloudflare lassen sich gezielte Phishing-Angriffe, bei denen mithilfe schädlicher Links und Anhänge oder kompromittierter E-Mail-Konten vertrauliche Informationen erbeutet und Finanzbetrug begangen wird, automatisch blockieren oder isolieren.

Sicherheitsvorkehrungen gegen eingehende Angriffe verstärken

Die cloudnative E-Mail-Sicherheitslösung von Cloudflare lässt sich in wenigen Minuten implementieren. Sie bietet eine Ergänzung zu bestehenden SEG-Lösungen oder integrierten E-Mail-Funktionen von Microsoft und Google. Dafür müssen kaum bis gar keine Anpassungen vorgenommen werden. Unternehmen sind so nicht nur besser vor Phishing geschützt, sondern verringern auch den mit der Verwaltung der Lösung verbundenen Zeit- und Arbeitsaufwand.

„Seit wir Cloudflare [zusätzlich zu M365] implementiert haben, konnten wir die Anzahl der schädlichen oder verdächtigen E-Mails halbieren, die unsere Nutzer täglich erhalten. Dadurch sparen wir viele Stunden Arbeit. Diese Zeit können wir nun in andere Ziele investieren.“

Werner Enterprises
(Fortune 1000)



Zeitersparnis durch stärkere Automatisierung

Die automatisch arbeitende, schlanke Lösung von Cloudflare fügt sich nahtlos in die Workflows von Microsoft und Google ein. Darüber hinaus bietet sie eine einzige, intuitive Benutzeroberfläche für Analysen.

Erkennungsrate von 99,997 %

Durch eine Verknüpfung der vom E-Mail-Anbieter gebotenen Funktionen mit dem Cloudflare-Schutz vor Phishing und der Übernahme geschäftlicher E-Mail-Konten erhalten Unternehmen eine umfassende Abdeckung bei minimalem Risiko.

Größerer Nutzen zu geringeren Kosten

Werden veraltete, teure und komplizierte Implementierungen durch die interaktionsarme Lösung von Cloudflare ersetzt, können Betriebsaufwand, redundante Funktionen und übermäßiges Nachjustieren verringert werden.

Raffinierte BEC-Angriffe stoppen

Verluste von 50 Mrd. US-Dollar, Tendenz steigend

Übernahmen von geschäftlichen E-Mail-Konten (Business Email Compromise – BEC) waren in den letzten zehn Jahren für schwindelerregende Verluste verantwortlich. Umso erstaunlicher ist es, dass einige Unternehmen dieser wirkungsvollen Form des Finanzbetrugs noch immer keine Priorität einräumen. BEC-Angriffe machen zwar nur einen kleinen Anteil an den Phishing-Bedrohungen aus, doch sie werden von SEGs und cloudbasierten E-Mail-Diensten oft nicht entdeckt, was erhebliche finanzielle Verlusten nach sich ziehen kann. Diese gezielten Angriffe sind nur schwer zu erkennen, weil sie gekaperte oder kompromittierte Konten und einen bestehenden Gesprächskontext nutzen, um sich als Kollegen oder vertrauenswürdige externe Anbieter auszugeben.

Zero Trust-Prinzipien auf E-Mails ausweiten

Wenn Angreifer ein kompromittiertes E-Mail-Konto eines Mitarbeiters oder externen Partners nutzen, können sie damit klassische Sicherheitskontrollen umgehen, mit denen nur versucht wird, sich der Legitimität des Absenderkontos zu vergewissern. Cloudflare geht einen Schritt weiter und analysiert diverse Verhaltensmerkmale, Schreibmuster, Stimmungsindikatoren und den Unterhaltungsverlauf, um die Authentizität des Absenders zu prüfen. Neben der Anwendung von Bedrohungsmodellen, die Machine Learning (ML) einsetzen, sind umfassende Informationen aus dem Cloudflare-Netzwerk die wirkungsvollste Waffe gegen gekaperte Konten, die von Betrügern zum Erschleichen von Zahlungen genutzt werden.

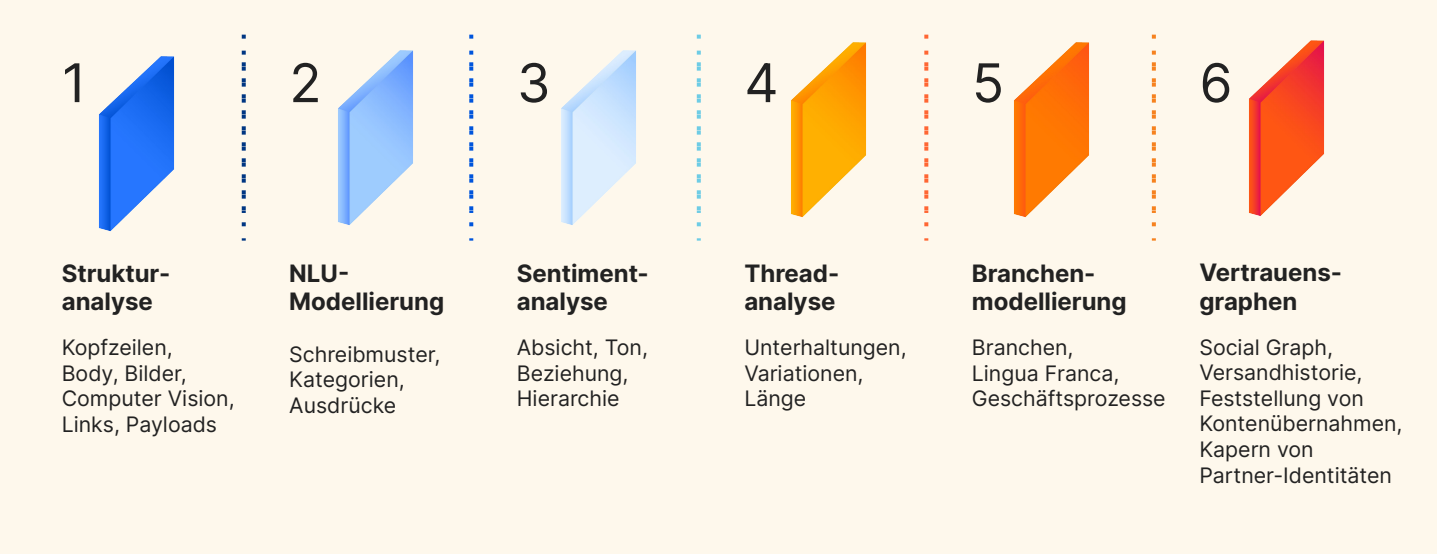


Abbildung 1: Nachrichtenanalyse

BEC mit ML-gestützter kontextbezogener Analyse erkennen

Die strukturelle Analyse von Nachrichten reicht nicht aus, um BEC-Angriffe zuverlässig zu erkennen. Eine erfolgreiche Identifizierung verlangt auch ein detailliertes Verständnis der Variationen im Gesprächsstil und der Absicht. Die umfassende Netzwerktelemetrie von Cloudflare (täglich mehr als 1 Bio. DNS-Anfragen) und die sich weiterentwickelnden ML-Modelle speisen die Small-Pattern-Analyse-Engine. Diese betrachtet die verschiedenen Aspekte einer E-Mail-Nachricht einzeln und bewertet Schreibmuster, Stimmungen, Kontexthistorie und viele andere Variablen, mit denen die Authentizität des Absenders überprüft werden kann.

Gefährliche und betrügerische URLs isolieren

Nutzer vor zweifelhaften E-Mail-Links schützen

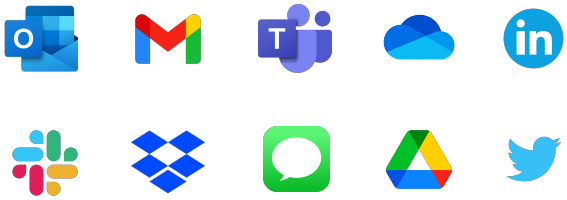
Angesichts der zunehmenden Raffinesse moderner Phishing-Angriffe ist es selbst für die am besten ausgestatteten Sicherheitslösungen schwierig, schädliche Links immer zuverlässig zu erkennen. URL-Shortener verschärfen dieses Problem noch, da sie zeitversetzte Angriffe ermöglichen, bei denen schädliche Links erst nach ihrer Zustellung aktiviert werden. Das führt zu einem Anstieg der:

- **Risiken** durch Anklicken unbekannter Links
- **Störungen** durch die potenzielle Blockierung sicherer Links
- **Kosten** für die Untersuchung verdächtiger Links

Mit einer anpassungsfähigen Isolierung ermöglicht Cloudflare Nutzern den sicheren Zugriff auf zweifelhafte Links: Malware und andere schädliche Webinhalte werden neutralisiert, während zeitaufwendige Untersuchungen und Richtlinienaktualisierungen entfallen.

Phishing-Angrffe über mehrere Kanäle verhindern

E-Mails sind nach wie vor das Mittel der Wahl, wenn es um die Übermittlung schädlicher Links geht. Doch die Angreifer haben ihre Taktik inzwischen erweitert und greifen Nutzer über verschiedene Anwendungen an, die im Geschäftsalltag zur Zusammenarbeit genutzt werden. Unternehmen sind dem aber nicht hilflos ausgeliefert. Wenn sie mit der Zero Trust-Plattform von Cloudflare den E-Mail-Schutz auf andere Bereiche ausweiten, können Sie ihre Nutzer proaktiv vor schädlichen Webinhalten aus folgenden Quellen abschirmen:



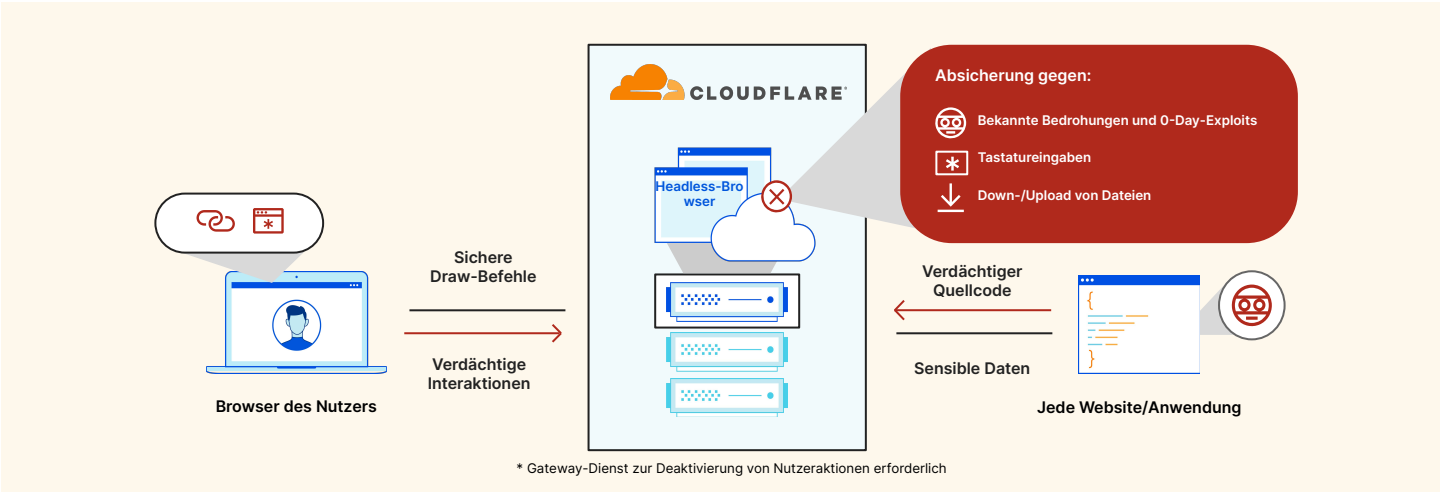


Abbildung 2: Isolierte Sitzung

Sicherheit durch Remote-Browserisolierung neu denken

Die Cloudflare Browser Isolation setzt die von uns selbst entwickelte Network Vector Rendering (NVR)-Technologie ein. Diese bietet eine nahtlos integrierbare, sichere und skalierbare Lösung für die Isolierung verdächtiger Links und Webinhalte. NVR überträgt sichere, schlanke Draw-Befehle an das Gerät, wobei sich isolierte Browsersitzungen auf jedem Server in jedem Rechenzentrum in den über 300 Städten, die von dem Cloudflare-Netzwerk abgedeckt werden, ausführen lassen. So wird vermieden, dass verdächtiger Quellcode auf dem Endgerät des Nutzers ausgeführt wird. Gleichzeitig kann ein transparentes Nutzererlebnis mit einer geringen, für den Anwender nicht spürbaren Latenz geboten werden.

Schnelle Untersuchung und Reaktion

Intuitives, unkompliziertes Lösungsmanagement

Durch eine stärkere Automatisierung und eine minimale Konfiguration, der für optimale Ergebnisse erforderlich ist, reduziert Cloudflare den Zeit- und Arbeitsaufwand für die laufende Steuerung der E-Mail-Sicherheit erheblich. Sicherheitsteams erhalten über das Dashboard sofort einen vollständigen Überblick über alle wichtigen Kennzahlen und Trends. Außerdem haben sie die Möglichkeit, bei gekennzeichneten Nachrichten auf detailliertere Informationen zuzugreifen. Die nähere Aufschlüsselung von Trends erlaubt ein schnelles Aufspüren von Angriffen, die gängigen Mustern folgen. Außerdem lassen sich damit weitere wichtige Informationen sammeln, beispielsweise dazu, welche Führungskräfte im Visier stehen oder welche zeitverzögerten Angriffe abgewehrt wurden.

Alle Analysen, Telemetriedaten, Bedrohungsbeobachtungen und Kompromittierungsindikatoren (Indicators of Compromise – IOC) sind über eine API mit großem Funktionsumfang verfügbar, die eine einfache Integration in bestehende Analyse-Workflows und Orchestrierungstools ermöglicht.

„Ich erzähle meinen Kollegen oft, wie einfach sich Cloudflare als cloudbasierte SaaS-Lösung bedienen lässt und wie zufrieden ich mit der hohen Trefferquote bin.“

Japan Airlines

Verwaltete Erkennung und Abwehr von Phishing

Der verwaltete Cloudflare-Dienst für E-Mail-Sicherheit, PhishGuard, liefert wertvolle Bedrohungsdaten und unterstützt Ihr SOC-Team. So bleibt diesem mehr Zeit, um bei Sicherheitsvorfällen Nachforschungen anzustellen. PhishGuard kann bei der Neutralisierung von Phishing-Kampagnen helfen. Die Lösung bietet Hilfestellung bei Untersuchungen, Bewertungen von Insider-Bedrohungen, der aktiven Betrugsbekämpfung und komplexen Abhilfemaßnahmen. Sie erweitert die Sicherheitsressourcen und das Fachwissen, indem sie aktiv über potenzielle Betrugs- und Insider-Bedrohungen informiert und gleichzeitig eine E-Mail-basierte Gefahrensuche durchführt.

Funktionen und Vorteile von PhishGuard:

- Verwaltete Phishing- und Vorfallreaktion für eine schnellere Lösung
- Proaktive BEC- und Betrugsbenachrichtigungen, damit Unternehmen bereits in der Frühphase eines Angriffs schnell reagieren können
- Eigene Ressourcen für die Echtzeit-Überwachung, regelmäßige Kontoüberprüfungen und kontinuierliche Bedrohungsanalysen
- Benutzerdefinierte Blockiersignaturen, die auf einer Bedrohungsanalyse der verwalteten Umgebung beruhen

Über 1.100

Stunden Zeitersparnis pro Jahr durch Automatisierung der manuellen Triage

Die automatisch arbeitende Lösung von Cloudflare übernimmt manuelle, zeitaufwendige Aufgaben, um die Reaktionszeiten zu verkürzen und den Mitarbeitenden zusätzliche Zeit für andere Tätigkeiten zu verschaffen.

50 %

weniger zugestellte schädliche oder verdächtige E-Mails (mit M365)

Durch den Einsatz von Cloudflare zusätzlich zu Microsoft 365 können Unternehmen gezielte Angriffe abfangen und die Gesamtzahl schädlicher E-Mails reduzieren.

40

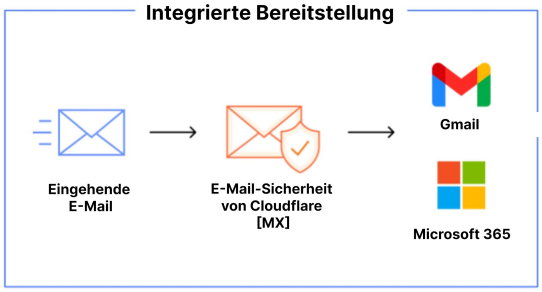
Stunden wurden in sieben Jahren insgesamt für die Konfiguration der E-Mail-Sicherheit aufgewandt

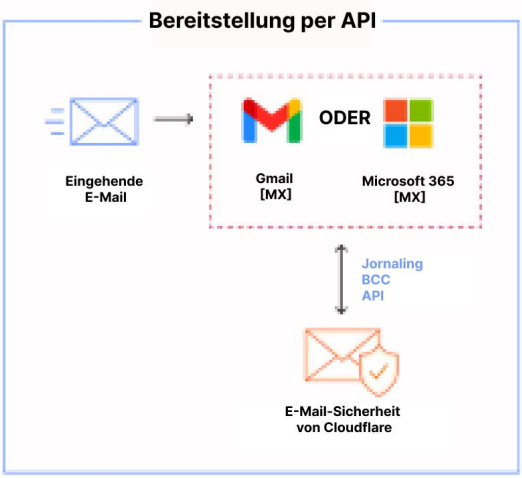
Die unkompliziert einzusetzende E-Mail-Sicherheitslösung von Cloudflare verlangt nur einen geringen Aufwand für die Konfiguration und die kontinuierliche Anpassung. Dafür bietet sie eine hochgradig wirksame, direkt einsetzbare Erkennungsfunktion.

Flexibler, einfach zu implementierender Schutz

Integrierte, API-basierte und und multimodale Optionen für eine schnelle und unkomplizierte Bereitstellung ohne zusätzliches Risiko

Unternehmen können den für ihre Umgebung am besten geeigneten Ansatz wählen und ihn innerhalb weniger Minuten ohne Hardware, Agenten oder Appliances anwenden. Im Gegensatz zu reinen SEG- oder API-Anbietern stellt Cloudflare flexible Optionen bereit, die sowohl den Schutz vor und nach der Auslieferung für eine kontinuierliche Neutralisierung von Bedrohungen als auch eine nahtlose Integration in bestehende SOC-Workflows und SIEM/SOAR-Plattformen ermöglichen.





FORRESTER

Bei Forrester Wave™ als Marktführer („Leader“) im Bereich **E-Mail-Sicherheit für Unternehmen** eingestuft; 2. Quartal 2023

Bewerten und vergleichen

Mit einer Phishing-Risikobewertung finden Sie heraus, welche Angriffe unter dem Radar geblieben sind

Sie können Ihre E-Mail-Umgebung schnell bewerten und feststellen, welche Phishing-Bedrohungen Ihren derzeitigen Abwehrmaßnahmen entgehen. Vergleichen Sie uns mit anderen Anbietern von E-Mail-Sicherheitslösungen, um in Erfahrung zu bringen, welche Lösung den schnellsten und unkompliziertesten Schutz bietet.

Marktführender Schutz vor Phishing

Bewertung anfordern

1. Deloitte-Studie aus dem Jahr 2020: Quelle
2. 2023 FBI IC3 PSA: Quelle
3. 2023 Forrester Opportunity Snapshot: Quelle