CLOUDFLARE

PRODUKTÜBERSICHT

E-Mail-Sicherheit von Cloudflare

Autonomer und vielseitiger Schutz für eine sichere Kommunikation am Arbeitsplatz

Schutz vor gezielten Phishing-Angriffen

Mühelos Bedrohungen abwehren und isolieren, die anderen Lösungen entgehen

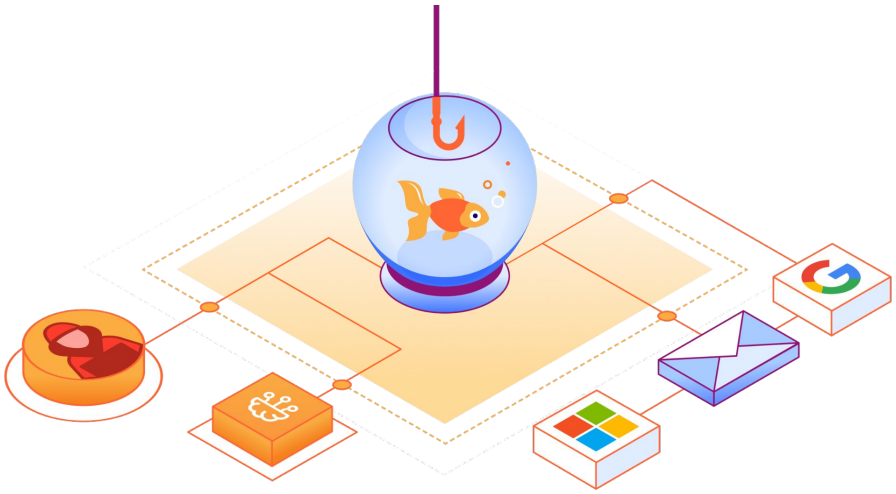
Unter allen Geschäftsanwendungen erfreuen sich E-Mails sowohl bei Nutzern als auch bei Angreifern der größten Beliebtheit. Insofern ist es heute wichtiger denn je, Anwender davor zu schützen, dass ihr Vertrauen durch Phishing missbraucht wird. Um hybrid arbeitende Beschäftigte besser zu unterstützen, 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 wurde speziell dafür entwickelt, mithilfe der vorbeugenden Verwendung von Informationen über Angriffskampagnen, einer KI-gestützten 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-Mail[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 bringt gekaperte oder kompromittierte Konten zutage.

Zeitversetzte Attacken und Multi-Channel-Angriffe isolieren

Nutzer werden vor schädlichen Webinhalten geschützt, die über unbekannte und verschleierte Links aufgerufen werden.

Ransomware und schädliche Anhänge blockieren

So können Erpressungsversuche und Schadcode Ihrem Unternehmen nichts anhaben.

Mehr Schutz, weniger Aufwand

Eine mehrstufige Sicherheitslösung für größeren Schutz zu einem Bruchteil der Kosten

Angesichts immer weiter um sich greifenden Phishing-Angriffen haben Microsoft und Google zusätzliche Funktionen speziell für ihre Produkte entwickelt, die wichtige E-Mail- und Datenschutzaufgaben wie Authentifizierung, Archivierung und clientseitige Verschlüsselung übernehmen. Bedrohungsakteure haben ihre Taktiken jedoch weiterentwickelt, um zielgerichtetere und ausweichende Angriffe durchzuführen, die häufig die integrierten Sicherheitskontrollen umgehen und erfolgversprechender sind.

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 E-Mail-Angriffe verstärken

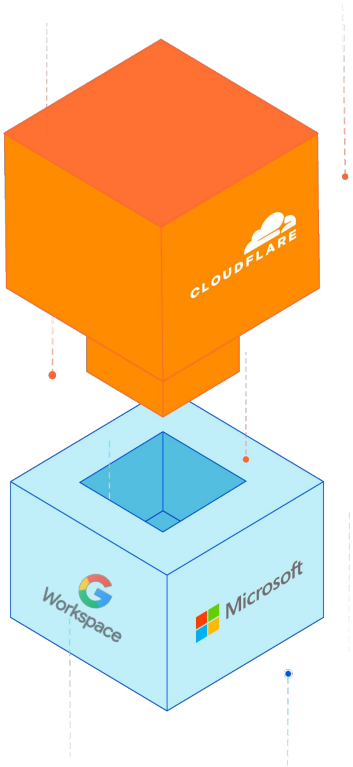
Die cloudnative E-Mail-Sicherheitslösung von Cloudflare lässt sich in wenigen Minuten implementieren. Sie bietet eine Ergänzung zu bestehenden SEG-Lösungen oder integrierten E-Mail-Funktionen von Microsoft und Google. Dafür müssen kaum bis gar keine Anpassungen vorgenommen werden. Unternehmen sind so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

„Seit wir Cloudflare [zusätzlich zu M365] implementiert haben, konnten wir die Zahl der schädlichen oder verdächtigen E-Mails halbieren, die unsere Nutzer täglich erhalten. Dadurch sparen wir viele Stunden Arbeit. In dieser Zeit können wir uns jetzt der Verfolgung anderer Ziele widmen.“

Werner Enterprises
(Fortune 1000)

E-Mail-Sicherheit: Schutz vor gezieltem Phishing und BEC

E-Mail-Provider: Unerlässliche E-Mail- und Datenfunktionen



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, geringere 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.

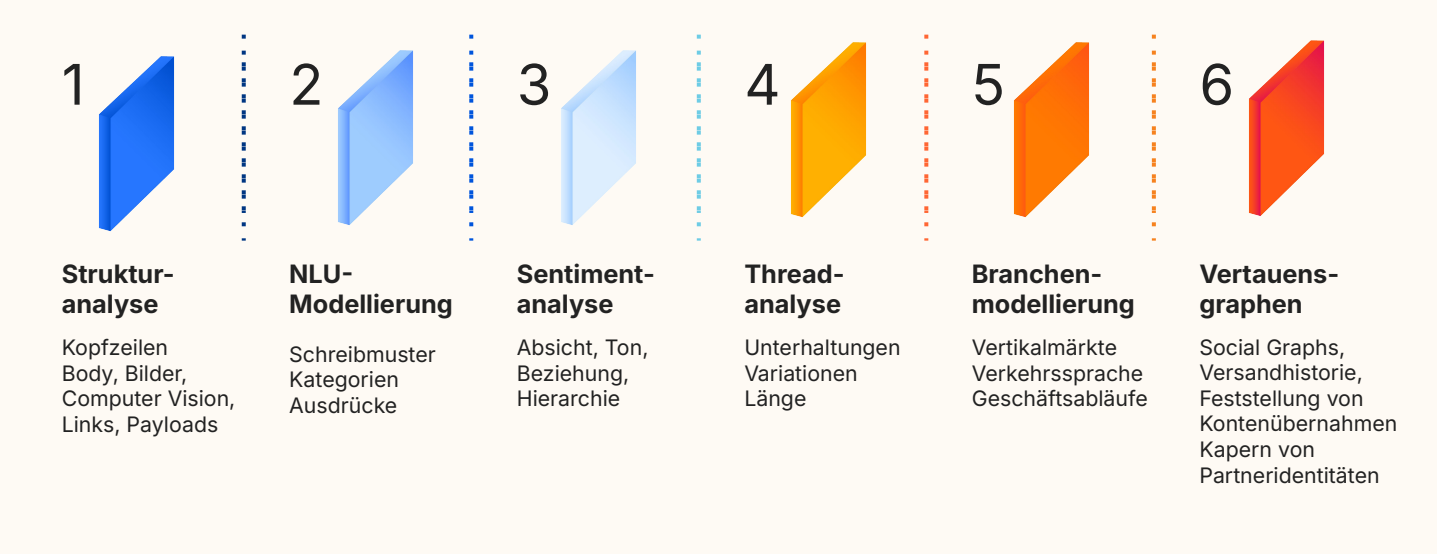


Abbildung 1: Nachrichtenanalyse

Mit ML-gestützter kontextbezogener Analyse BEC erkennen

Die Strukturanalyse 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 3 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.

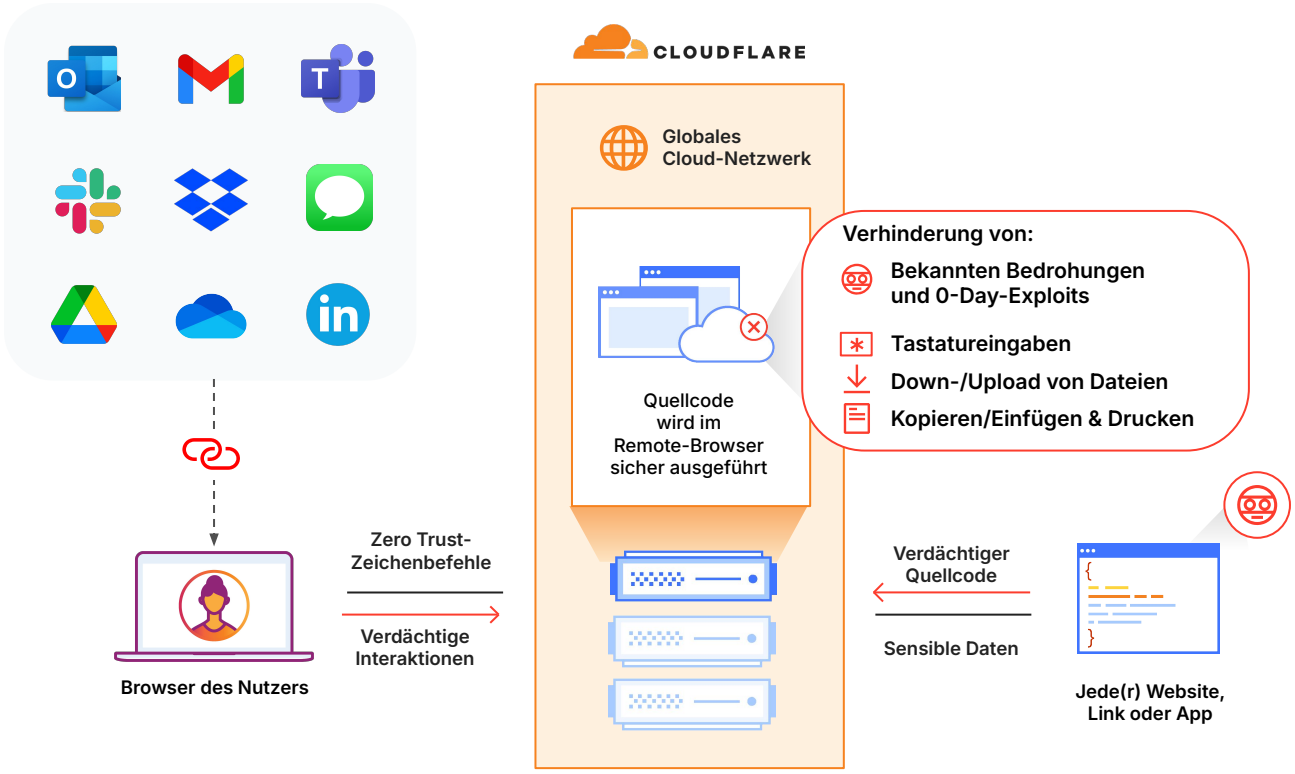
Linkbasierte Angriffe isolieren

Inzwischen sind linkbasierte Angriffe das Mittel der Wahl, wenn Anmeldedaten gestohlen, Malware und Ransomware geladen oder sensible Daten ausgeschleust werden sollen. Dass diese Links ihre Opfer über mehrere Kanäle – per E-Mail, Chat, SMS, über Social Media und andere Apps – gleichzeitig erreichen, macht es komplizierter, Mitarbeitende und Daten vor gezielten Phishing-Angriffen zu schützen.

Cloudflare unterbindet linkbasierte Phishing-Angriffe, indem das Rendering von Quellcode aus dem Web grundsätzlich auf unserem globalen Cloud-Netzwerk erfolgt und nicht lokal auf dem Gerät des Nutzers. Dadurch werden Malware und Zero-Day-Schwachstellen in Browsern neutralisiert. Gleichzeitig wird eine stark ausdifferenzierte Kontrolle über die Aktionen der Nutzer ermöglicht (z. B. durch das Sperren von Tastatureingaben), um den Diebstahl von Anmeldedaten und Datenlecks zu verhindern.

Phishing-Risiko ohne Beeinträchtigung der Mitarbeitenden beseitigen

Durch die Integration von Browserisolierungsfunktionen der nächsten Generation, die auf unserer einzigartigen Network Vector Rendering (NVR)-Technologie aufbauen, kann Cloudflare eine sichere und skalierbare Lösung zur Isolierung potenziell schädlicher Links bieten, die sich nahtlos in das restliche System einfügt. Im Gegensatz zu anderen Verfahren, die sehr viel Bandbreite erfordern, werden bei VNR sichere Draw-Befehle an das Gerät übermittelt. Das trägt dazu bei, das Risiko schädlicher Webinhalte ohne Beeinträchtigung der Endnutzererfahrung zu beseitigen. Dank NVR und des latenzarmen Cloudflare-Netzwerks können Unternehmen Multi-Channel-Bedrohungen neutralisieren und zugleich ein störungsfreies und produktives Arbeiten ermöglichen.



Schnelle Untersuchung und Behebung

Intuitives, unkompliziertes Sicherheitsmanagement

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 Einleitung von Gegenmaßnahmen (PhishGuard)

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 1100

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 Arbeitsaufwand in sieben Jahren für die Konfiguration des E-Mail-Schutzes

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.

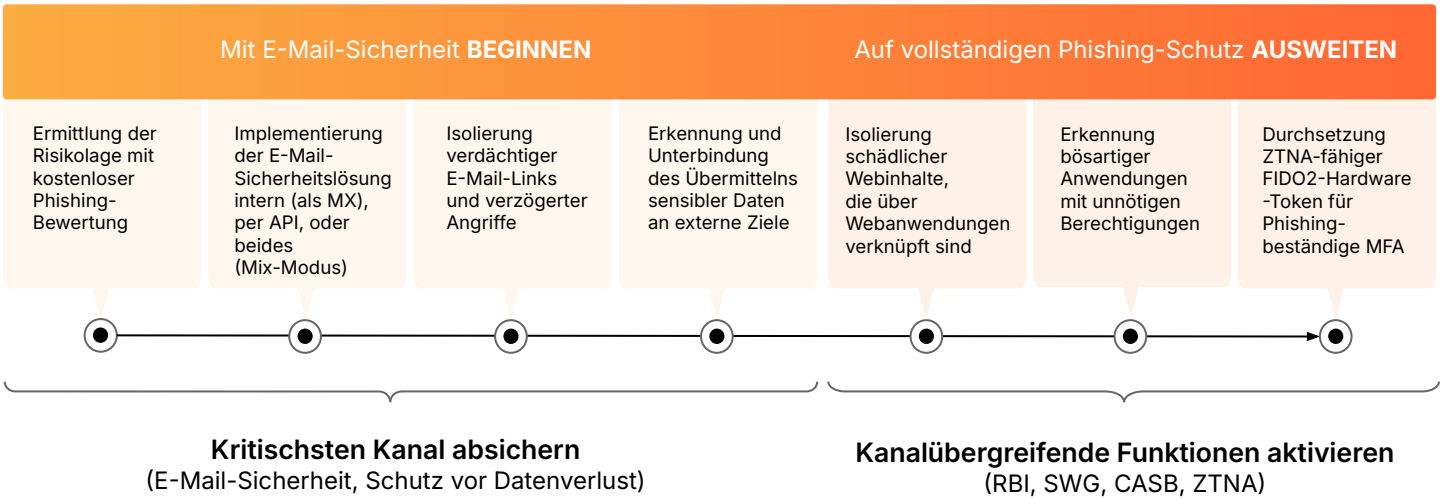
VORTEILE

Umfassender Schutz für sämtliche Kanäle

Phishing-Kampagnen beschränken sich zunehmend nicht mehr auf E-Mails. Deshalb ist es für Unternehmen heute dringender denn je, eine Phishing-Lösung für schnellen und unkomplizierten kanalübergreifenden Schutz zu implementieren.

Mit der Sicherheitsplattform von Cloudflare können Unternehmen zunächst branchenführende E-Mail-Sicherheit implementieren, um das wichtigste Einfallstor für Phishing zu versperren, und anschließend Zero Trust-Dienste aktivieren, um den Schutz auf alle anderen Kanäle auszuweiten. So werden bekannte und neue Phishing-Methoden auf effektive Weise ausgehebelt.

- **Aufwandsarmer, hocheffizienter Schutz:** Branchenführende Effizienz bei der Erkennung reduziert mit geringfügiger Feinabstimmung Phishing auf ein Minimum.
- **Stärkere Bündelung, niedrigere Kosten:** Durch eine einzige, vollständig integrierte Plattform für alle Phishing-Anwendungsfälle sinken die Ausgaben.
- **Schnelle Implementierung, unkomplizierte Verwaltung:** Sofortiger Schutz bei geringerem Zeit- und Arbeitsaufwand für die laufende Verwaltung.



Bewerten und vergleichen

Lassen Sie Ihre aktuelle E-Mail-Abwehr prüfen und finden Sie heraus, welche Bedrohungen zurzeit noch übersehen werden

Mit einem kostenlosen Retro-Scan wissen Sie nach wenigen Minuten, welche Bedrohungen Ihnen in den letzten 14 Tagen entgangen sind. Sie können auch eine Bewertung Ihres Phishing-Risikos vornehmen lassen, um Ihre Posteingänge auf eingehende Phishing-Nachrichten zu überwachen. Vergleichen Sie uns mit anderen Anbietern von E-Mail-Sicherheitslösungen, um zu sehen, wer den schnellsten und unkompliziertesten Schutz bietet.

Retro-Scan anwenden | Bewertung anfordern

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

