CLOUDFLARE
AREA 1 SECURITY

KURZDARSTELLUNG DER LÖSUNG

Erweitern Sie die E-Mail-Sicherheit in Microsoft 365 mit Cloudflare Area 1

Erweitern Sie Zero Trust auf Ihr wichtigstes Kommunikationstool — E-Mail in der Cloud

Schützen Sie Microsoft-Postfächer vor Bedrohungen – mit präventiver, Cloud-nativer E-Mail-Sicherheit

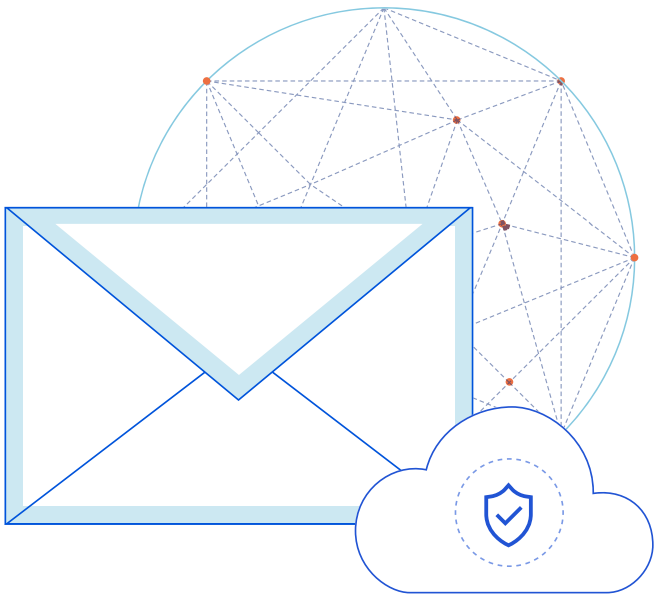
Microsoft 365 bietet einen ausgezeichneten Schutz vor durch hohes Datenvolumen geprägte Bedrohungen wie Spam und Viren und bietet zusätzlichen Schutz für Kunden von Microsoft Advanced Threat Protection (ATP).

Dennoch stellt Gartner® fest, dass[1], „mit der Verbesserung der integrierten Sicherheit … auch die Bedrohungsakteure immer raffinierter werden und oft gefälschte Anmeldeseiten verwenden, um Anmeldedaten zu sammeln. Zu den ausgefeilten E-Mail-Bedrohungen gehören kompromittierte Websites und bösartige Dokumente, die zur Verbreitung von Malware verwendet werden. Viele Ransomware-as-a-Service-Banden nutzen E-Mails als ersten Einstiegspunkt. Neben Malware nehmen auch die Bedrohungen durch Business Email Compromise (BEC) und die Übernahme von Konten weiter zu, was zu erheblichen finanziellen Verlusten führt.“

Ausgefeilte Bedrohungen mit geringem Volumen, wie die oben genannten, werden zuerst mit Angriffsinfrastrukturen und -techniken aufgebaut, die Cloudflare Area 1 auf einzigartige Weise im Internet entdecken kann. Durch die Identifizierung und automatische Blockierung von Kampagnen in einem frühen Stadium des Angriffslebenszyklus (durchschnittlich 24 Tage vor dem Start) hält Area 1 die Posteingänge frei von Bedrohungen.

Als Teil der Cloudflare Zero Trust-Plattform umfasst der Area 1 E-Mail-Sicherheitsdienst auch:

- **Aufdeckung von Finanzbetrug ohne Malware**, der oft über mehrere E-Mail-Konversationen mit „vertrauenswürdigen“ Anbietern/Lieferanten erfolgt
- **Blockierung bislang unbekannter Angriffe in Echtzeit**, ohne dass Sie eine SEG „optimieren“ oder auf Signatur-/Richtlinien-Updates warten müssen
- **Entdeckung kompromittierter Konten und Domains** sowie neue, ähnlich aussehende und nahe gelegene Domains, die Angreifer zur Umgehung von DMARC/SPF/DKIM verwenden
- **Isolierung und Blockieren kombinierter und verzögerter** Angriffe durch Integration in Cloudflare Browserisolierung (Beta)



Übersicht der Lösung

In einer Cloud-first-Welt sind herkömmliche sichere E-Mail-Gateways (SEGs) unflexibel und ineffektiv gegenüber sich ständig weiterentwickelnden Bedrohungen wie Business Email Compromise, Spoofing und Ransomware.

Cloudflare Area 1 bietet präventive, Cloud-native E-Mail-Sicherheit, um diese und andere gezielte Phishing-Angriffe umfassend zu stoppen.

Unternehmen, die Microsoft 365 mit Cloudflare Area 1 übereinander lagern, erhalten:

- **Umfassenden Phishing-Schutz** für internen und externen E-Mail-, Web- und Netzwerk-Traffic
- **Geringere IT-Komplexität** und kürzere Reaktionszeiten bei Phishing-Vorfällen
- **Einfache Bereitstellung in wenigen Minuten** mit einem auf APIs fokussierten Ansatz
- **Beschleunigte SOC-Überprüfungen** mit Post-Delivery Message Retractions und SIEM/SOAR-Integrationen

Wie können Sie mit dem Area 1-Ansatz für Cloud-E-Mail-Sicherheit mehr Bedrohungen abwehren?

Microsoft 365 bietet großartige Sicherheit für E-Mail-Bedrohungen mit hohem Volumen; jedoch können sehr gezielte Phishing-Angriffe mit geringem Volumen, die für mehr als 90 % der Datenschutzverletzungen im Internet verantwortlich sind, immer noch unbemerkt bleiben.

Wie sollten Unternehmen, die Microsoft 365 nutzen und immer noch von übersehenen Phishing-Angriffen geplagt werden, mit modernen Bedrohungen umgehen?

Hier kommen Lösungen für **integrierte Cloud-E-Mail-Sicherheit** (ICES) ins Spiel. Hierzu meint Gartner®: „Lösungen, die über eine API direkt in die Cloud-E-Mail integriert werden und nicht als Gateway fungieren, erleichtern die Bewertung und Bereitstellung und verbessern die Erkennungsgenauigkeit, während sie gleichzeitig die Vorteile der Integration des Großteils des Phishing-Schutzes in die Kernplattform nutzen."[2]

„Bis 2023 werden mindestens 40 % aller Unternehmen integrierte Schutzfunktionen von Cloud-E-Mail-Anbietern anstelle eines sicheren E-Mail-Gateways (SEG) nutzen, gegenüber 27 % im Jahr 2020.

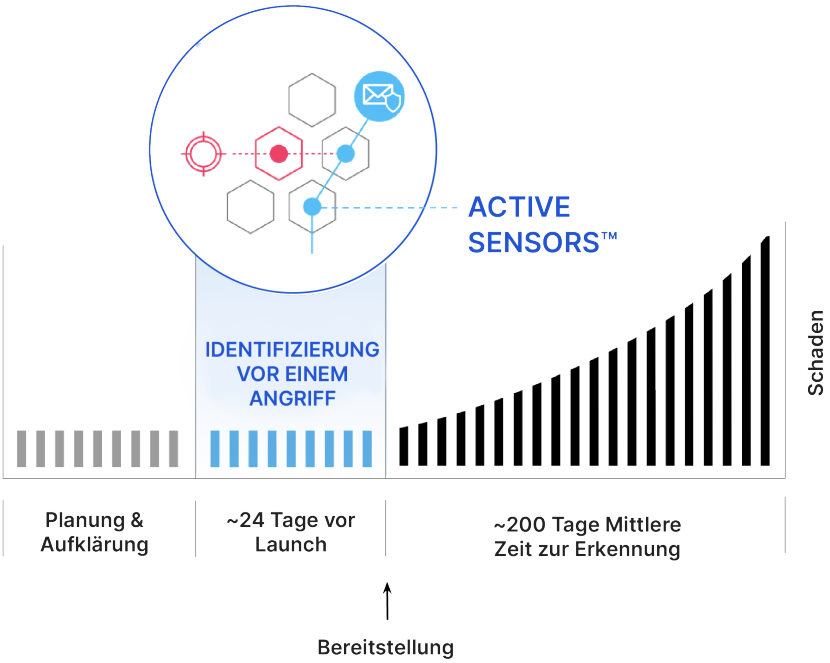
„Bis 2025 werden 20 % der Anti-Phishing-Lösungen über eine API-Integration mit der E-Mail-Plattform bereitgestellt werden, heute sind es weniger als 5 %."

— 2021 Gartner® „Market Guide for Email Security"

Area 1 Horizon (jetzt Cloudflare Area 1 E-Mail-Sicherheit) ist ein maßgeblicher Anbieter („Representative Vendor") in der Kategorie Integrated Cloud Email Security (ICES) im Gartner-Marktleitfaden.

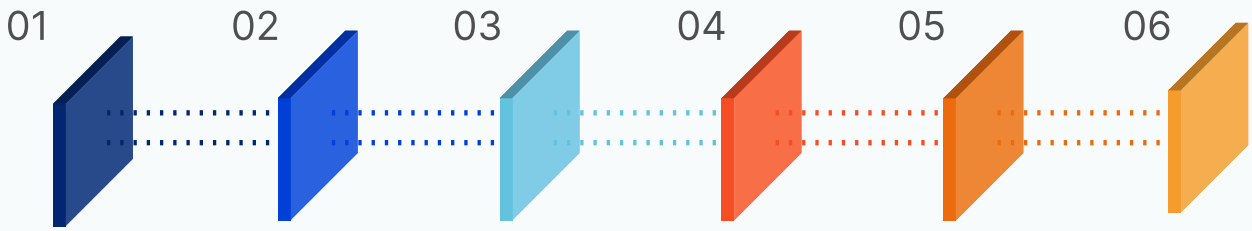
Im Gegensatz zu anderen Lösungen **durchforstet Area 1 kontinuierlich und proaktiv das Internet**, um neue Phishing-Kampagnen und die Infrastruktur von Angreifern „in freier Wildbahn“ zu entdecken. Im Durchschnitt erkennt Area 1 bösartige Websites und Nutzdaten volle 24 Tage vor dem Start von Angriffen.

Abbildung 1: Stoppen Sie Phishing-Angriffe präventiv – bevor sie Ihren Posteingang erreichen – mit Cloudflare Area 1



Area 1 verwendet auch eine Reihe von **fortschrittlicheren Erkennungstechniken**, darunter NLU, NLP, Social Graph Analysis (Muster der E-Mail-Kommunikation) und Bilderkennung, um die raffiniertesten Angriffe zu erkennen und zu stoppen – einschließlich brandneuer sehr gezielter Bedrohungen, die Nutzer im Verhältnis 1:1 bedrohen, anstatt solcher, wo ein Angreifer zahlreiche Nutzer bedroht.

Abbildung 2: Analysieren Sie den Inhalt, den Kontext und die sozialen Graphen der E-Mail-Kommunikation, um moderne Bedrohungen wie BEC zu stoppen



01 Struktur-analyse
Kopfzeilen
Body, Bilder, Computervision
Links, Nutzlasten

02 NLU-Modellierung (Natural Language Understanding)
Schreibmuster
Kategorien
Ausdrücke

03 Sentiment-analyse
Intent, Ton, Beziehung, Hierarchie

04 Gesprächs-analyse
Gespräche
Variationen
Länge

05 Branchenmodel-lierung
Branchen
Lingua Franca
Geschäftsprozesse

06 Vertrauen Graphen
Soziale Graphen von Partnern, Sendeverlauf
Erkennung von Konto-übernahmen
Imitationen von Partnern

Einfache Bereitstellung in wenigen Minuten

Mit einem auf APIs fokussierten Ansatz, der sich nahtlos in Microsoft 365 integriert, ist Area 1 in wenigen Minuten einsatzbereit. Erkennen und blockieren Sie Phishing genauer und effektiver – ohne die IT-Komplexität, die für die ständige „Optimierung" einer ineffektiven traditionellen SEG erforderlich ist.

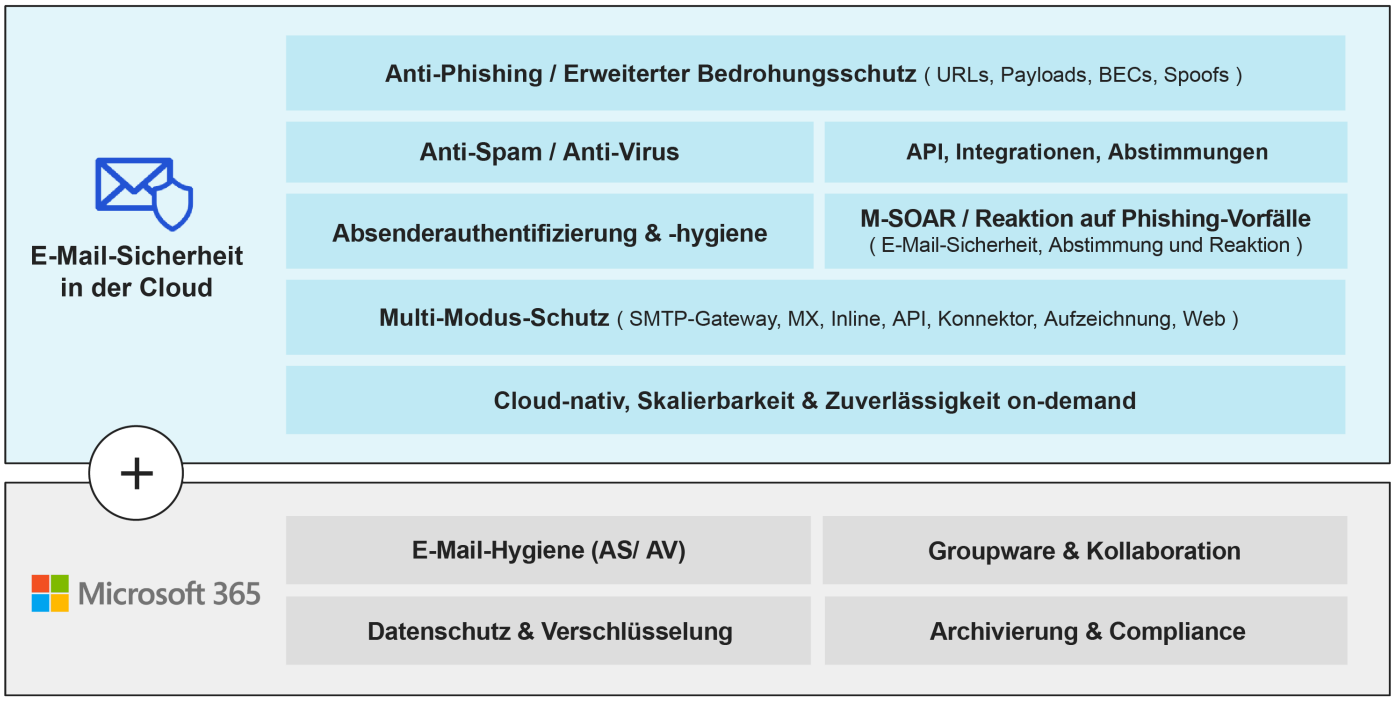
Abbildung 3: Beispiel für die Option zur Bereitstellung von E-Mail-Sicherheit im Bereich 1

Area 1:

- Kann in weniger als fünf Minuten bereitgestellt werden, ohne dass eine Installation erforderlich ist und ohne Auswirkungen auf Ihre bestehende Infrastruktur;
- Bietet im Vergleich zu anderen Lösungen flexiblere Bereitstellungsoptionen (einschließlich MX/Inline, Connector und API);
- Integriert sich nahtlos in die anderen E-Mail-Sicherheitsfunktionen von Microsoft 365 wie Anti-Spam, DLP, Verschlüsselung und Archivierung;
- Kann mühelos alle bösartigen Nachrichten direkt aus Microsoft 365-Postfächern mit integrierter Abhilfemaßnahme und Rückruf der Nachrichten entfernen; und
- Ist für Ihre Nutzer völlig transparent und bietet gleichzeitig eine umfassende, durchgängige Phishing-Erkennung und -Behebung.

Die Vorteile des Schutzes Ihrer Microsoft 365-E-Mail-Umgebungen mit Cloudflare Area 1 umfassen:		
Branchenführende Cloud-E-Mail-Sicherheit	**Nahtlose Arbeitsabläufe**	**Gesteigerte betriebliche Effizienz**
• Erweitert die nativen Microsoft-Schutzmechanismen für einen umfassenden Schutz vor modernen Bedrohungen wie BEC, Angriffen auf die E-Mail-Supply-Chain, kompromittierten Anbieterkonten, Insider-Bedrohungen und mehr. • Ein umfassenderer Einblick in Bedrohungen und Forensik verbessert die Untersuchungen und Reaktionszeiten.	• Tiefgreifende Integration in Microsoft-Umgebungen, APIs und Arbeitsabläufe. • Integrieren Sie mit ADFS, senden Sie Warnmeldungen an Teams und leiten Sie Protokolle an Azure Sentinel weiter. • Endnutzer bleiben in den nativen Microsoft-Dashboards, damit diese weiterhin produktiv sind und nicht abgelenkt werden.	• Basiert auf einer Cloud-nativen, dynamisch skalierbaren Infrastruktur, um Cloud-Traffic-Spitzen zu bewältigen. • Ersetzt herkömmliche SEGs für mehr Sicherheit und betriebliche Effizienz. • Erweiterte Erkennung, Triage und Reaktion in einer einzigen Plattform für eine umfassende Verteidigung.

Halten Sie Ihre Posteingänge frei von Bedrohungen – dank umfassender, integrierter Cloud-E-Mail-Sicherheit:



Microsoft + Cloudflare: für eine sicherere und private Cloud

Cloudflare hat tiefgreifende Integrationen mit Microsoft aufgebaut, um Unternehmen dabei zu helfen, den nächsten Schritt in ihrer Umstellung auf Zero Trust zu setzen. Diese Integrationen ermöglichen es Unternehmen, Kundenimplementierungen betrieblich effizient zu gestalten und gleichzeitig ein nahtloses Nutzererlebnis zu bieten und den Betrieb zu skalieren.

Zusätzlich zu Area 1 gehören zu den Zero Trust-Services von Cloudflare auch Integrationen:

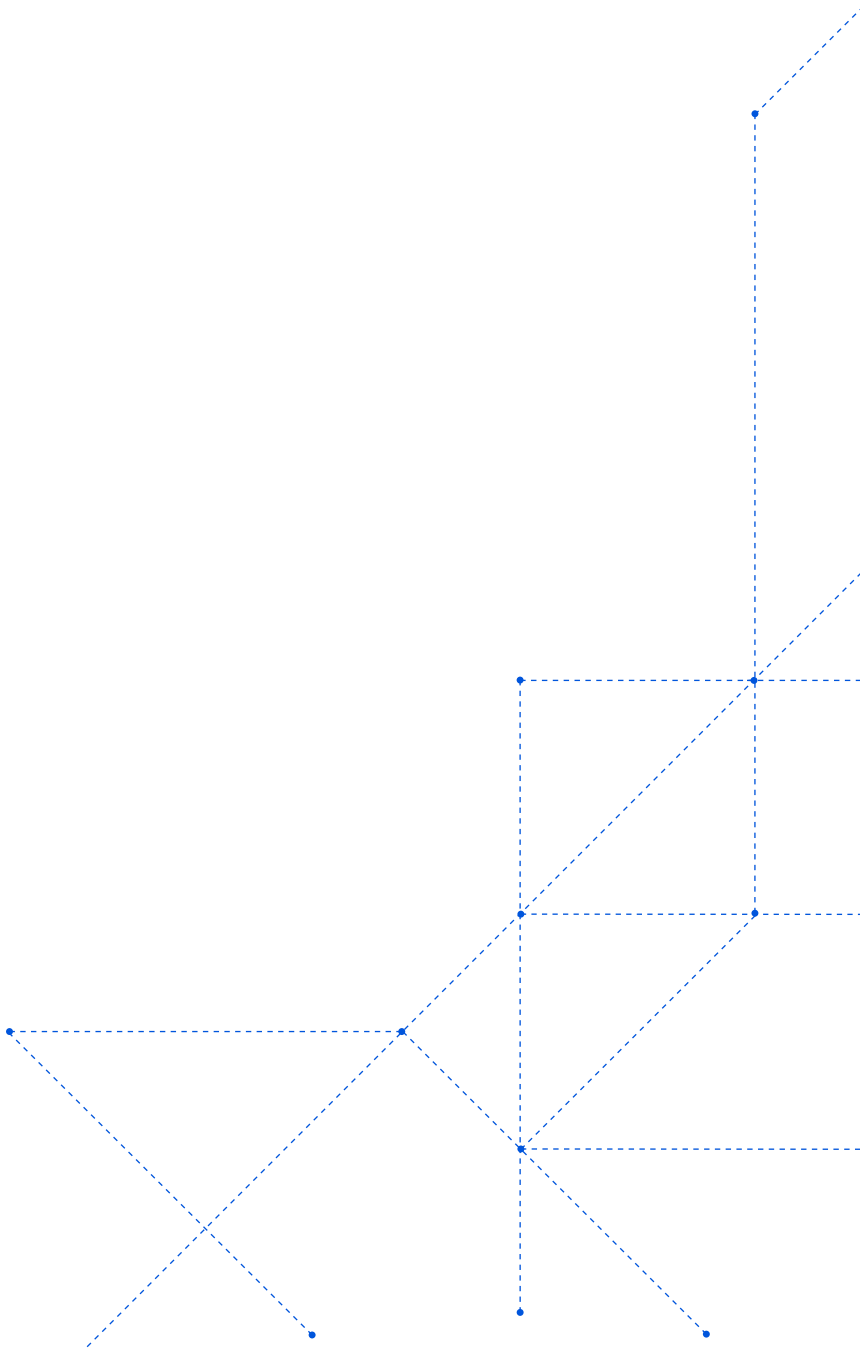
- **Azure Active Directory (AD)** — Nutzen Sie leistungsstarke Authentifizierungstools, einschließlich Multi-Faktor-Authentifizierung (MFA), bedingte Zugriffsrichtlinien und risikobasierte Kontrollen.
- **Microsoft Cloud-App-Sicherheit (MCAS)** — Starten Sie die M365-Integration, um nach neuen Sicherheitsproblemen im Zusammenhang mit M365-Nutzern, -Daten und -In-App-Diensten zu suchen und sie den Kunden zu präsentieren.
- **Zero Trust für Azure Apps** — Ermöglichen Sie den sicheren Zugriff auf lokale Anwendungen oder auf in Azure gehostete Anwendungen – kein VPN erforderlich.
- **Microsoft Endpoint Manager** — Bewertung des Status des Clients zum Zeitpunkt der Anmeldung über Microsoft Intune, so dass Cloudflare den Zugriff auf der Grundlage von Sicherheits- oder Geräte-Stellungsmeldungen zulassen oder verweigern kann.
- **Microsoft 365** — Bieten Sie ein schnelleres und sichereres Nutzererlebnis, indem Sie die Konnektivität der Nutzer zu Microsoft 365 über Cloudflare und das Networking Partner Program von Microsoft optimieren.

Sie möchten mehr über Partner-Integrationen von Cloudflare mit Microsoft erfahren? Dann kontaktieren Sie uns.

Sie möchten erfahren, wie Cloudflare Area 1 Ihren Microsoft 365 Phishing-Schutz verbessern kann? Dann fordern Sie hier eine individuelle Risikobewertung an.

Quellen

1 & 2 Gartner, „Market Guide for Email Security," 7. Oktober 2021, Mark Harris, Peter Firstbrook, Ravisha Chugh, Mario de Boer



CLOUDFLARE
AREA 1 SECURITY

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV:BDES-3778/2022SEPT07