FORTRA

Verbesserte Microsoft-Sicherheit mit Fortra Advanced Email Security

Inhaltsverzeichnis

Warum die E-Mail-Sicherheit nach wie vor an erster Stelle steht

Es dürfte nicht überraschen, dass E-Mails nach wie vor die beliebteste Kommunikationsform im Geschäftsleben sind. Daher zielen viele Cyberangriffe auf E-Mails ab. Die E-Mail-Sicherheit muss ein wesentlicher Bestandteil der Cybersicherheitsstrategie eines Unternehmens sein.

E-Mail-Angriffe sind nicht nur beliebt, es gibt auch viele Möglichkeiten, einen E-Mail-Angriff durchzuführen und so Zugriff auf die Daten eines Unternehmens zu erhalten. Hier ein Überblick über die häufigsten Bedrohungen der E-Mail-Sicherheit:

Malware

Dateien oder Links zu Dateien, die bei Ausführung (Anklicken, Herunterladen usw.) einen Computer mit einem Virus, Ransomware oder Spyware infizieren können.

Spam

Unerwünschte kommerzielle E-Mails, die darauf abzielen, den Empfänger zum Kauf von Waren oder Dienstleistungen von möglicherweise illegalen oder gefälschten Websites zu bewegen.

Phishing

Meistens handelt es sich um E-Mails - es können aber auch Textnachrichten, soziale Medien und sogar Telefonanrufe sein -, die eine vertrauenswürdige Person oder Marke imitieren, um sensible Daten zu stehlen oder Zugriff auf das Netzwerk eines Unternehmens zu erhalten.

Spear Phishing

E-Mails, die als vertrauenswürdige Mitteilungen von einer zuverlässigen Quelle, meist innerhalb des Unternehmens, getarnt sind. Eine solche E-Mail kann beispielsweise so aussehen, als käme sie von einer Person mit Vollmacht innerhalb des Unternehmen des Empfängers.

Business Email Compromise (BEC)

Betrügereien wie Executive Spoofing nutzen Social Engineering, um Menschen vorzugaukeln, sie würden mit einem vertrauenswürdigen Absender kommunizieren. Indem sie sich dieses Vertrauen erschleichen, können die Cyberkriminellen Geld auf ihre Konten überweisen lassen, Zugriff auf sensible Daten erhalten oder andere böswillige Aktionen durchführen.

Spyware

Eine Art von Malware, durch die Daten von einem Gerät oder Netzwerk unbefugt übertragen oder kopiert werden. Diese Hacking-Methode kann sehr schwer zu erkennen sein, da sie den normalen Netzwerkverkehr imitiert.

Ransomware

Eine Art von Malware, mit der die Angreifer Daten als Geiseln nehmen und so den Betrieb eines Unternehmens lahmlegen, wenn kein Lösegeld gezahlt wird. Ransomware wird häufig in der Öffentlichkeit thematisiert, da sie Unternehmen zum Stillstand bringen und sehr kostspielig sein kann.

Unbeabsichtigter Datenverlust

Der Verlust von Daten aufgrund von Fehlern, z. B. das Senden von falschen Daten an einen Empfänger oder von Daten an den falschen Empfänger.

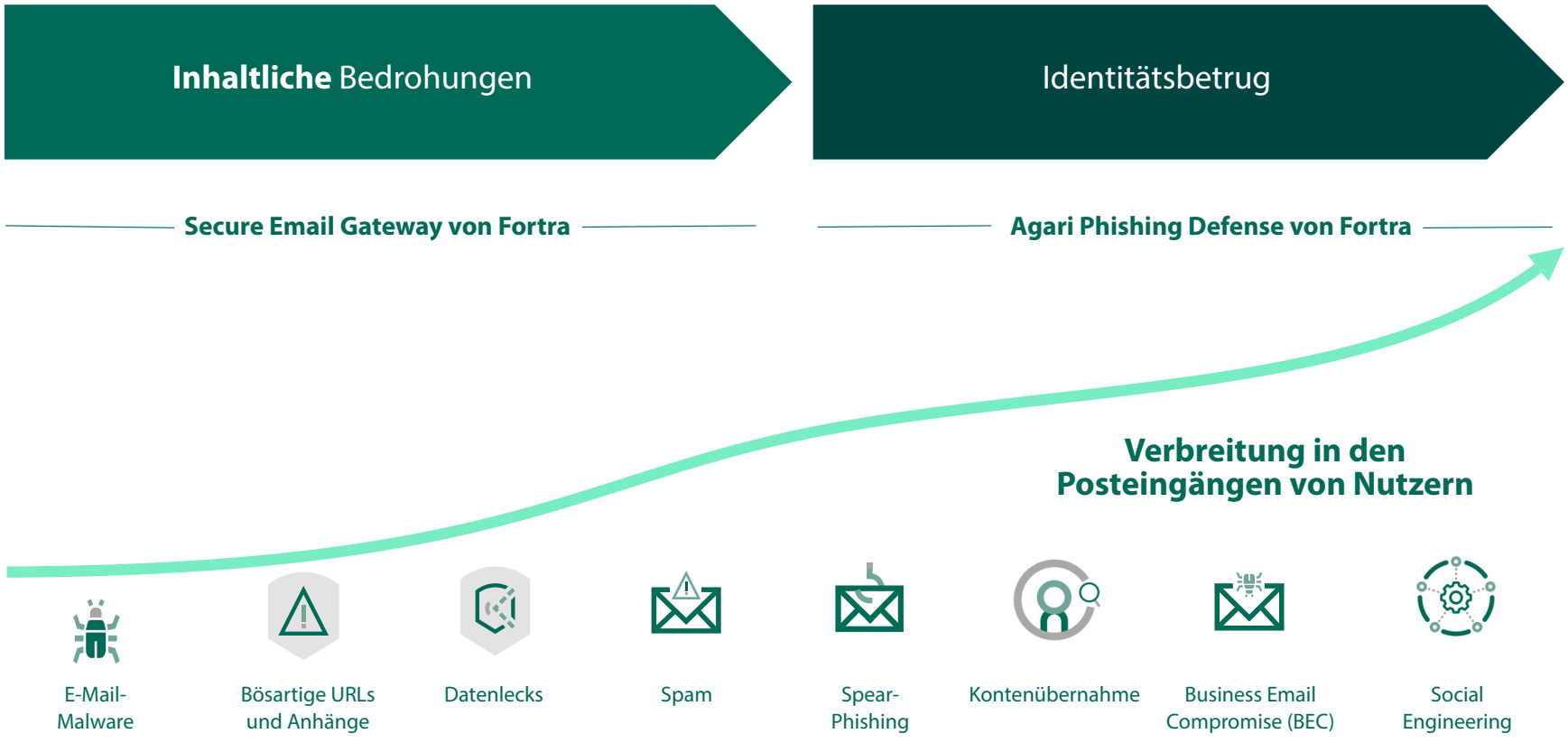
Kontenübernahme

Wurden die Zugangsdaten eines Nutzers erbeutet, melden sich die Täter als der echte Nutzer an und versenden Nachrichten, bei denen sie vorgeben, dieser Nutzer zu sein.

Ein vielschichtiger Ansatz für Ihre E-Mail-Sicherheit

Microsoft 365 steht nach wie vor an der Spitze der E-Mail-Anbieter für Unternehmen weltweit. Laut der Aktionärsversammlung von Microsoft im Januar 2023 hat M365 mehr als 63 Millionen Abonnenten. Angesichts des hohen E-Mail-Datenvolumens in Unternehmen muss unbedingt sichergestellt werden, dass die E-Mail-Sicherheitslösungen mit den täglichen Bedrohungen Schritt halten können, die immer neue Wege suchen, um in das Unternehmen einzudringen. Und obwohl M365 eine Reihe von Sicherheitsfunktionen bietet, sind diese E-Mail-Sicherheitsfähigkeiten allein nicht ausreichend. Es hat sich gezeigt, dass M365 bestimmte Datensicherheitsanforderungen der Kunden nicht erfüllen kann.

Die daraus resultierenden Unzulänglichkeiten machen Unternehmen angreifbar. Fortra kann diese E-Mail-Sicherheitslücken schließen und gleichzeitig eine bestehende E-Mail-Plattform wie M365 ergänzen.



Das Böse in Schach halten - über den gesamten Bedrohungszyklus hinweg

Leider gibt es viele Unzulänglichkeiten im gesamten Bereich des Bedrohungsschutzes - von der Verbreitung von E-Mail-Bedrohungen außerhalb Ihres Unternehmens bis hin zu aktiven Bedrohungen, die im Posteingang landen. Von inhaltsbasierten Bedrohungen bis hin zu Techniken des Identitätsbetrugs - Ihre Sicherheitsarchitektur hat alle Hände voll zu tun, um die schwierigsten Herausforderungen im Bereich der E-Mail-Sicherheit zu meistern.

M365 verfügt zwar über grundlegende Schutzfunktionen für Inhalte wie Virenschutz, Spamschutz, Archivierung und Verschlüsselung, bietet aber nicht die Tiefenprüfung der Inhalte (DCI), die Unternehmen benötigen, um vollständig sicher zu sein. Das liegt daran, dass inhaltsbasierte Bedrohungen nicht nur an der Oberfläche existieren, sondern tief in eingehende Nachrichten eingebettet sein können, z.B. in Dateien, URLs, Anhänge, Bilder usw.

Erschwerend kommt hinzu, dass Techniken zum Identitätsbetrug, wie Spear-Phishing und BEC, speziell dafür konzipiert sind, den Akteuren einen einfachen Zugriff auf die Posteingänge der Nutzer zu ermöglichen. Die meisten Secure Email Gateways sind nicht darauf eingestellt, diesen Arten von Identitätsbedrohungen einen Riegel vorzuschieben. Diese können auf unzählige Arten übertragen werden, sind immer schwieriger zu erkennen und die vom Nutzer gemeldeten Bedrohungsindikatoren reichen im Allgemeinen nicht aus, um sie zu stoppen.

Während einige der M365 Exchange Online Protection-Tarife Defender enthalten (oder zusätzlich gebucht werden können), bieten andere E-Mail-Sicherheitslösungen von Drittanbietern auf dem Markt ein höheres Schutzniveau vor ausgefeilteren, gezielten Angriffen wie Spear-Phishing. In einem Forschungsbericht von Egress aus dem Jahr 2021 wurde festgestellt, dass die herkömmlichen statischen Datenverlustverhütungsregeln (DLP) von Microsoft nicht ausreichen, um mit menschlichen Fehlern umzugehen - erstaunliche 100 % der IT-Leiter gaben an, dass sie darüber frustriert sind.[1]

Außerdem können ausgehende Datenverluste dazu führen, dass vertrauliche Informationen Ihr Unternehmen verlassen, was wiederum Compliance-Mängel und den Verlust vertraulicher geschützter Daten zur Folge haben kann. Der gleiche Bericht von Egress belegte die Häufigkeit von Datenverlusten bei ausgehenden E-Mails, als er feststellte, dass 85 % der Unternehmen, die M365 einsetzen, einen Datenschutzverstoß bei ausgehenden E-Mails verzeichneten.[2]

Glücklicherweise bekämpfen die fortschrittlichen Lösungen für die E-Mail-Sicherheit von Fortra, darunter unser Secure Email Gateway (SEG), Advanced Phishing Defense (APD) und Suspicious Email Analysis (SEA), verschiedene Bedrohungsszenarien, bei denen andere - wie M365 Enterprise Tiers und andere Produkte zum Schutz vor Bedrohungen - versagen.

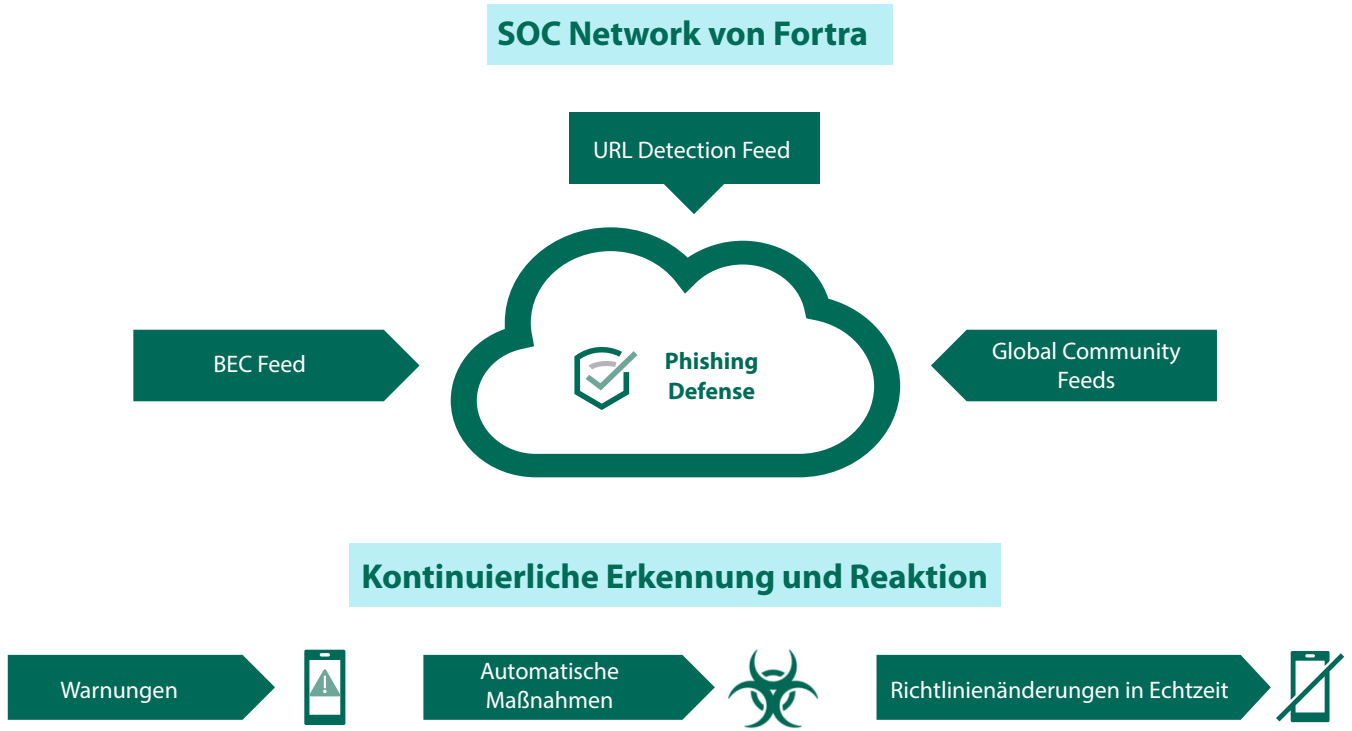
> **"SIE SOLLTEN JEDOCH BEDENKEN, DASS DIE VON MICROSOFT BEREITGESTELLTEN INTEGRIERTEN E-MAIL-SICHERHEITSFUNKTIONEN ALLEIN WAHRSCHEINLICH NICHT AUSREICHEN, UM IHR UNTERNEHMEN VOR ALLEN BEDROHUNGEN ZU SCHÜTZEN, DENEN SIE AUSGESETZT SEIN KÖNNTEN, ZUMINDEST NICHT IN DEM MASSE, WIE DAS ERFORDERLICH WÄRE."**
>
> **— EXPERT INSIGHTS BLOG**

[1]Megan Rees, „Is Microsoft 365 Secure For Business?", **Expert Insights**, 24. November 2022
[2]Derek Belair, „Key Practices to Close the Microsoft 365 Security Gap," **Channel Futures**, 21. Oktober 2022

Bei externen Bedrohungen einen Schritt voraus

Die Advanced Email Security-Lösungen von Fortra unterstützen Unternehmen bei der Bekämpfung einer großen Bandbreite von Bedrohungen, von Spam bis hin zu Spear-Phishing-Angriffen, und besitzen drei wichtige Unterscheidungsmerkmale:

1. DCI, die versteckte eingehende Bedrohungen, die sich tief in E-Mail-Inhalten, angehängten Bildern und Dokumenten verbergen, sowie ausgehende Datenverluste bei sensiblen und regulierten Daten detailgenau identifiziert und stoppt.
2. Identity Threat Detection bietet eine KI-gesteuerte, zusätzliche Sicherheitsebene hinter dem Gateway zum Schutz vor Spear-Phishing und anderen komplexen E-Mail-Angriffen, die an den vordergründigen Sicherheitssystemen vorbeigehen.
3. Global Inbox Threat Intelligence, einschließlich durch Schwarmintelligenz ermittelter Böswilligkeitsindikatoren, die als Fundament dienen, um Ihre Architektur immer unempfindlicher gegenüber den neuesten und relevantesten Bedrohungen machen.



Als erstklassige Phishing-Abwehr

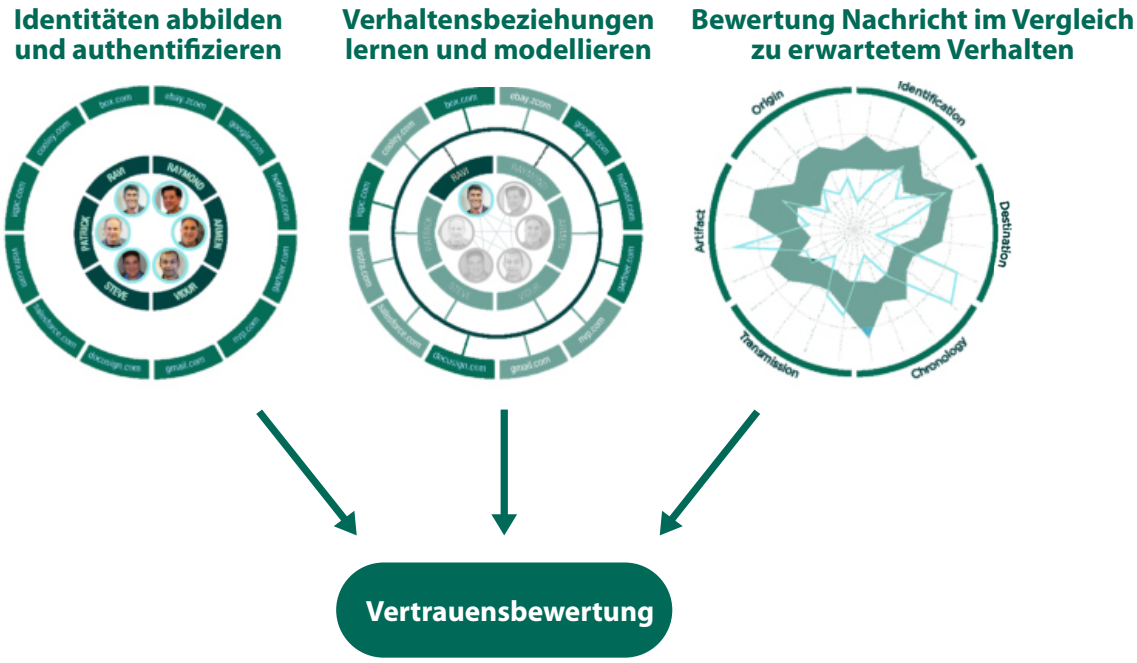
Nutzt Agari Phishing Defense von Fortra maschinelles Lernen, um ein Verständnis für normale, vertrauenswürdige E-Mail-Aktivitäten zu entwickeln, indem Verhaltensbeziehungen untersucht werden, die Identitäten umfassen können, die mit verschiedenen Mailabläufen und gemeinsamen Sendemustern verbunden sind. Die Algorithmen verstehen das Verhalten der Nutzer und bilden es ab, um sicherzustellen, dass die eingehenden Nachrichten rechtmäßig sind. So erkennt Phishing Defense **Betrüger**.

M365 ist im Allgemeinen nicht in der Lage, eine Imitation von Marken und einzelnen Nutzern zu erkennen. Anders als bei APD erfordert eine solche Erkennung eine aufwändige Regelkonfiguration und -pflege durch M365.

BEC trickst arglose Mitarbeiter aus. Daher ist die Phishing-Abwehr so wichtig. Durch die sorgfältige Untersuchung jeder eingehenden E-Mail, die Analyse der menschlichen Beziehungen und Verhaltensweisen und das Verständnis der Identitäten hinter der Nachricht erkennt APD die abweichenden BEC-Verhaltensweisen und verhindert, dass der Angriff den Posteingang erreicht.

APD nutzt künstliche Intelligenz, um Absender aus dem Unternehmen sowie Partner, deren Beziehungen zu Ihnen und das Verhalten von Absendern und Empfängern zu identifizieren und entsprechende Schutzrichtlinien zu erstellen. Dies dient der Abwehr aktueller sowie zukünftiger Bedrohungen, die aufgrund der gewonnenen Erkenntnisse vorhersehbar sind.

Diese E-Mail-Verhaltensmuster sind es auch, mit denen APD gegen Spear-Phishing-Angriffe vorgeht. Durch die Modellierung einer regulären E-Mail-Kommunikation und vertrauenswürdiger Absender kann APD böswilliges Verhalten erkennen und verhindern, dass **Imitationen** den Posteingang des Unternehmens erreichen.

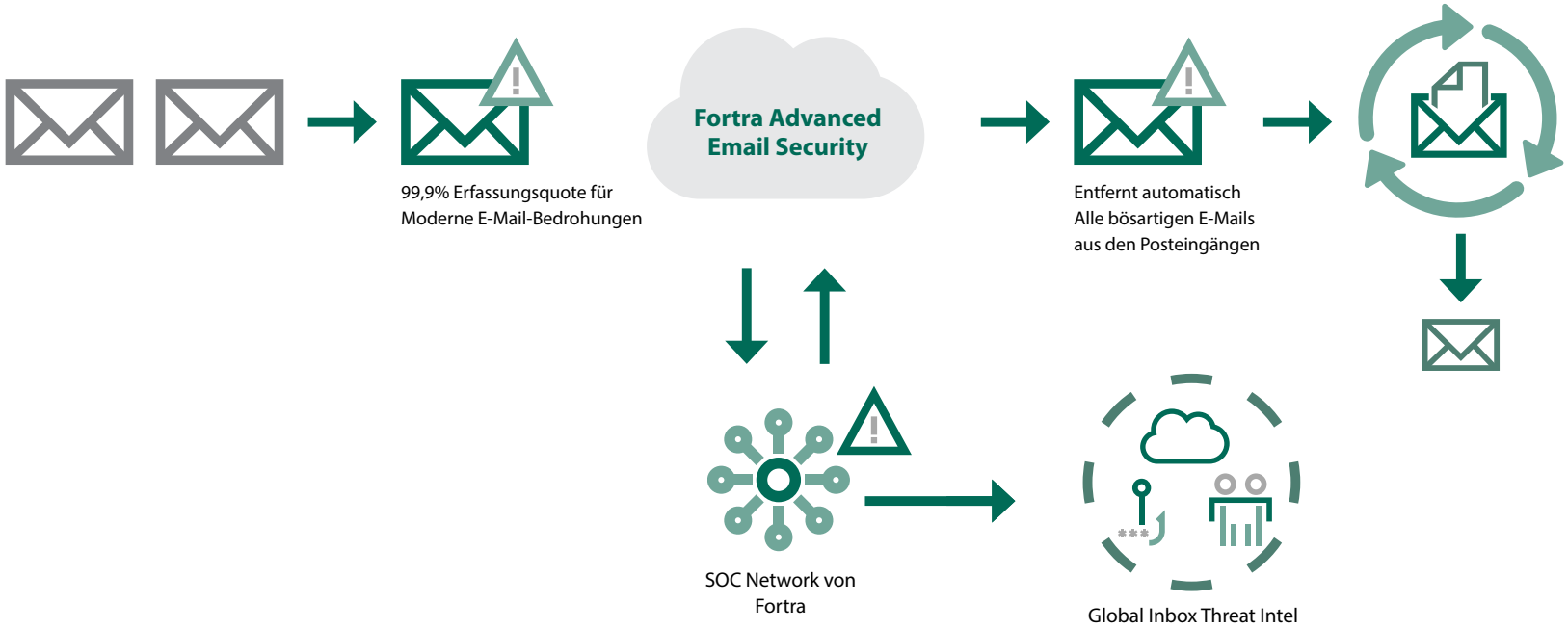


Bei externen Bedrohungen einen Schritt voraus

Search and Destroy ist eine On-Demand-Richtlinie, die schnell und effizient historische E-Mail-Daten durchsucht und Richtlinien implementiert, um E-Mails in Spam-Ordner zu verschieben oder sie zu löschen. Forschungsergebnisse deuten auch darauf hin, dass **Zero-Day-Angriffe** auf dem Vormarsch sind. Da diese Angriffe schwer zu lokalisieren sind, stützt sich Global Inbox Threat Intel von Fortra auf Echtzeitinformationen aus Billionen von E-Mails, die von Ihren Nutzern, unserer globalen Basis und anderen Fortra-Feeds generiert werden, um Verhaltensweisen und Beziehungen verstehen zu lernen.

Dennoch gibt es für Cyberkriminelle Möglichkeiten, zum Ziel zu gelangen. Deshalb hat Fortra eine automatisierte Technologie für die kontinuierliche Erkennung und Reaktion entwickelt, die APD und die Analyse verdächtiger E-Mails (Suspicious Email Analysis, SEA) nutzt, um kontinuierlich nach neuen, von Bedrohungsdaten erkannten Beeinträchtigungsindikatoren (Indicators of Compromise, IOCs) zu suchen und anhand kombinierter Schädlichkeitsindikatoren schnell für Abhilfe zu sorgen.

Herkömmliche E-Mail-Sicherheitskontrollen beruhen auf der Abwehr von Cyberangriffen zu einem einzigen Zeitpunkt, wenn die E-Mail zugestellt wird. Aber manche Bedrohungen werden erst nach der Zustellung, nachdem die E-Mails im Posteingang angekommen sind, aktiv. Continuous Detection and Response nutzt die Ergebnisse erstklassiger Bedrohungsdaten, um kontinuierlich das Wissen über neue IOCs anzuwenden, um nach bösartigen Inhalten in historischen E-Mails zu suchen und gleichzeitig neue eingehende E-Mails zu bewerten und Durchsetzungsmaßnahmen wie Spamzuordnung, Löschen oder beides anzuwenden. Schließlich kann die umfassende Lösung die Rückforderung von E-Mails, die es in den Posteingang geschafft haben, erkennen und automatisieren.



Gründliche Phishing-Reaktion ohne Belastungen

Das SOC-Team von Fortra setzt eine Kombination aus maschineller Analyse und Expertenprüfung ein, um eine genaue Erkennung zu gewährleisten. Anschließend werden die gemeldeten Vorfälle nach Prioritäten geordnet, wobei die verdächtigsten Vorfälle an die Spitze der Liste gesetzt werden. Anschließend wird Ihr Team durch eine reaktionsschnelle Feedbackschleife auf dem Laufenden gehalten, und eine schnelle und gründliche Eindämmung sorgt dafür, dass die Bedrohungen gestoppt werden. Dies geschieht durch:

- Untersuchung der von Mitarbeitern gemeldeten Phishing-Attacken.
- Automatisierung der Phishing-Beseitigung.
- Bereitstellung von Einblicken und Berichten auf CISO-Ebene.
- Verwendung der RESTful-API-Integration mit SIEM/SOAR-Tools.

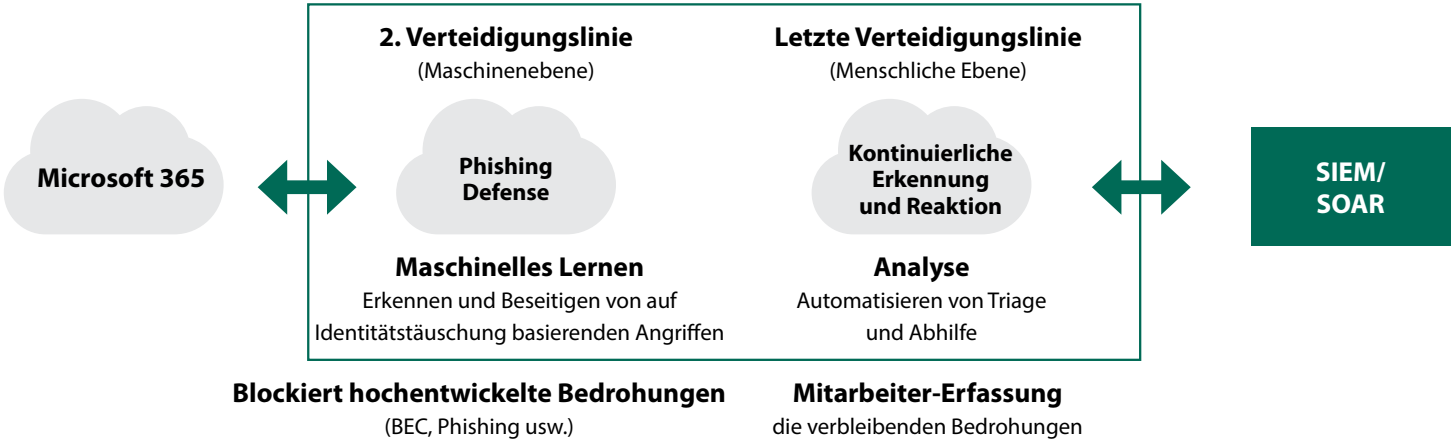
Schnelles Auffinden und Entfernen von bösartigen Domains

Fortra Advanced Email Security verfügt über leistungsstarke Tools zur Bekämpfung von Lookalike-Domains, die häufig für Phishing- und BEC-Angriffe verwendet werden. Hunderttausende Lookalike-Domains werden jedes Jahr von Cyberkriminellen erstellt. DMARC hilft E-Mail-Administratoren dabei, Betrüger daran zu hindern, Domains zu fälschen, indem sie festlegen, ob gefälschte E-Mails von den Empfängern zugelassen, unter Quarantäne gestellt oder zurückgewiesen werden sollen.

DMARC dient als Gatekeeper für einen empfangenden E-Mail-Server und ist Teil von Fortras DMARC Protection. Anhand von Analysen können Nutzer nachvollziehen, woher die E-Mails von ihren Domains stammen und wer sie fälscht. DMARC Protection ist der Goldstandard in der Branche. Die Verwendung von DMARC als Teil eines bewährten E-Mail-Verfahrens ermöglicht Ihnen folgendes:

- Authentifizieren aller authentischen E-Mail-Nachrichten und Quellen für E-Mail-versendende Domänen, einschließlich interner und externer Absender.
- Veröffentlichen einer explizite Richtlinie, die den Mailbox-Anbietern vorschreibt, wie sie Nachrichten, die als nicht authentisch eingestuft werden, zuzustellen oder zu entsorgen haben.
- Erlangen von Informationen über die Verwendung alle ihrer Domains in E-Mail-Nachrichten aus dem gesamten Internet.

Dann durchsucht das Domain Monitoring von Fortra proaktiv die weltweiten Domainregistrierungen und DNS-Daten, um Lookalike-Domains zu finden. Dank eines umfangreichen Netzwerks von vertrauenswürdigen Registrierungspartnern profitieren Fortras Kunden von der höchsten Erfolgsquote und der schnellsten Entfernung bösartiger Domains in der Branche.



Schließen der Lücken bei internen Bedrohungen

Den Datenfluss innerhalb Ihres Unternehmens identifizieren

Wenn es darum geht, Datenverluste über E-Mail zu verhindern, konzentrieren sich Unternehmen oft hauptsächlich auf den ausgehenden E-Mail-Verkehr. Fortras SEG wurde jedoch so konzipiert, dass es ein- und ausgehende Inhalte erkennt und auf Wunsch sogar interne E-Mails scannt.

Unternehmen verfügen über eine Vielzahl von Daten. Dabei kann es sich um sensible Kundendaten, geistiges Eigentum oder sogar als geheim eingestufte Informationen handeln. Die versehentliche Weitergabe falscher Informationen ist ein echtes Risiko, auch intern.

Diese gemeinsame Nutzung und das Zusammenwirken von Informationen ist zwar für die Firma von entscheidender Bedeutung, kann aber auch ein Unternehmen anfällig für versehentlichen Datenverlust machen. Sensible Daten müssen geschützt werden, sei es zu regulatorischen Zwecken (HIPAA, DSGVO, ITAR), zum Schutz personenbezogener Daten (z. B. PII, PCI) oder zum Schutz des Unternehmens, z. B. geistiges Eigentum, Geschäftsgeheimnisse usw.. Das Verhindern versehentlicher Datenverluste sollte ebenso wichtig sein wie der Schutz vor externen Bedrohungen für das Unternehmen.

Die Fortra Advanced Email Security-Lösungen ermöglichen es Managern, den Versand oder die Anzeige bestimmter Daten durch bestimmte Personen einzuschränken. Wenn ein Abteilungsleiter Entscheidungen über die Datenautorisierung trifft, kann dies die Richtlinien zur E-Mail-Sicherheit und zum Schutz vor Datenverlusten stärken, da die IT-Abteilung möglicherweise nicht über die nötigen Kenntnisse über den Kontext der Datenvorschriften verfügt. Dies bedeutet eine große Erleichterung für das Unternehmen.

Mit Hilfe eines zusätzlichen Perimeterschutzes wendet SEG von Fortra DCI auf Nachrichten an. Es gibt mehrere Möglichkeiten, wie SEG dies tut, z.B.:

- Scannen von Inhalten in einem mehrstufigen Prozess:
  - Identifiziert den Dateityp anhand der Dateisignatur
  - Extrahiert Inhalte zur Überprüfung
  - Dekomprimiert Dateien durch Entfernen von Text, Metadaten, Bildern und eingebetteten Dateien aus Dokumenten mithilfe von OCR (Optical Character Recognition)
- Überprüfung der Nachrichtenauthentifizierung mithilfe von SPF, DKIM und DMARC
- Überprüfung von Spam-Inhalten mit Hilfe mehrerer Systeme
- Erkennung und Entfernung bösartiger URLs

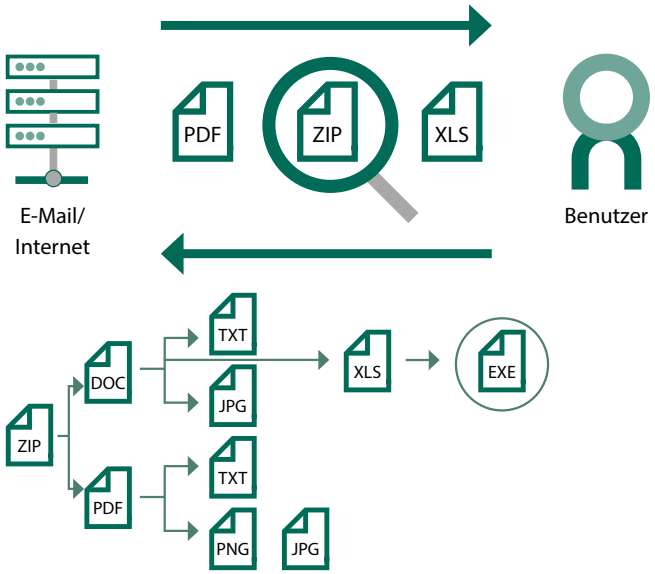
Sobald der Inhalt der Nachricht vollständig extrahiert ist, können Regeln angewendet werden, um den Inhalt zu prüfen und zu bestimmen, was mit der Nachricht geschehen soll. Dann wird sie mit Hilfe eines leistungsstarken Schlüsselwortsuche überprüft, die alle Sprachgruppen unterstützt und einfache Wörter, Phrasen, reguläre Ausdrücke und zusammengesetzte Bedingungen unterstützt. Viele Produkte können nach einfachen Schlüsselwörtern in Nachrichten suchen, aber nur wenige Menschen bedenken, dass diese Sicherheitsmaßnahmen mit einem einfachen Bildschirmausdruck umgangen werden können. Fortras SEG setzt anschließend OCR-Software ein, um Text aus den Bildern zu extrahieren, um sicherzustellen, dass sensible Daten nicht nach außen dringen.

All dies ermöglicht einen äußerst präzisen und flexiblen Ansatz, bei dem Nachrichten blockiert, zurückgehalten oder mit Warnungen versehen zugestellt werden können - und zwar auf der Grundlage von Richtlinien, die selbst den strengsten Anforderungen genügen.

Schließen der Lücken bei internen Bedrohungen

Sogar Bilder können zum Datentransport verwendet werden, indem sie wertvolles geistiges Eigentum verbergen oder Malware durch die Verwendung von **Steganografie-Tools** zum Ausschleusen von Informationen verstecken. Das klingt vielleicht wie etwas, das nur von Spionen und Hackern verwendet wird, aber im Jahr 2022 wurde ein Angestellter von General Electric (GE) wegen Verschwörung zur Wirtschaftsspionage verurteilt, weil er die Dateien in einem digitalen Bild eines Sonnenuntergangs heruntergeladen, verschlüsselt und versteckt hatte, das er dann per E-Mail an sein persönliches E-Mail-Konto schickte. Laut Gerichtsdokumenten dauerte der Verschlüsselungsvorgang nicht einmal 10 Minuten.

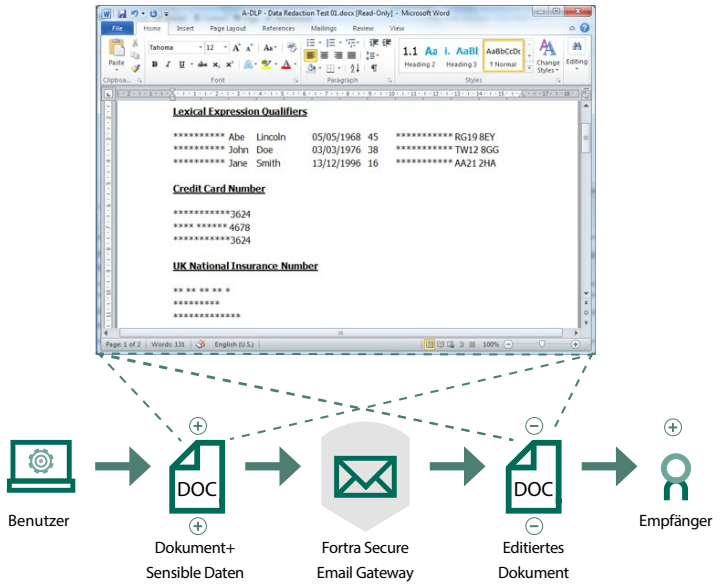
Wie schnell dieser Verstoß ausgeführt wurde, zeigt auf schockierende Weise, warum zusätzliche E-Mail-Sicherheit für den Schutz Ihres Unternehmens unerlässlich ist. Das DCI-System von Fortra bereinigt Bilddateien, um sicherzustellen, dass keine Daten oder Malware mit steganografischen Tools eingebettet wurden.



Schutz von Daten durch eine bessere Sicherung von Inhalten

Kurz gesagt, Fortras SEG kann Daten aufspüren, die nicht vorhanden sein sollten. Die Daten könnten absichtlich ausgeschleust werden oder jemand könnte Inhalte versenden, die ein verborgenes Arbeitsblatt enthalten.

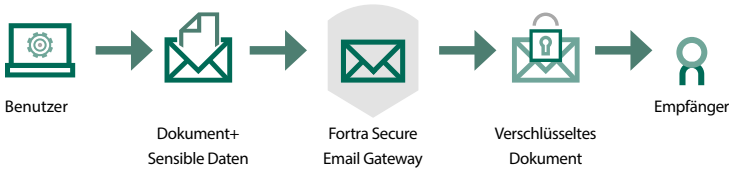
SEG kann Inhalte bereinigen, um sicherzustellen, dass keine sensiblen Daten absichtlich oder versehentlich ausgeschleust werden. Die Bilder können durch das Entfernen aller von Steganografie-Tools hinzugefügten Daten wiederhergestellt werden. In Dokumenten kann sensibler Text automatisch editiert werden, und selbst bei Bildern in Dokumenten kann sensibler Inhalt aus dem Bild editiert und dann im Dokument ersetzt werden. Die Dokumenteigenschaften (Metadaten) können bereinigt werden, z. B. können Sie den Namen des „Autors“ aus allen öffentlich zugänglichen Dokumenten entfernen.



Die Abbildung zeigt, wie ein Anhang mit sensiblen Daten in einer E-Mail von der SEG editiert wurde.

Verschlüsselung, die das Geschäft am Laufen hält

Ein weiterer Bestandteil von SEG von Fortra ist die Verschlüsselung, die automatisch für die Sicherheit und Compliance sorgt, die erforderlich sind, um Daten während der Übertragung zu schützen und gleichzeitig Verzögerungen und Fehler zu vermeiden. Mit den SEG-Verschlüsselungsoptionen können Richtlinien auf Absender, Empfänger, Betreff-Inhalt, Nachrichtentext, Anhangtypen, Anhanginhalte, Nachrichtenkopf oder Dokument-Metadaten basieren.



Durch die Bereitstellung mehrerer Optionen für den sicheren Datenversand können Unternehmen die beste Methode für die Übermittlung von Inhalten an Dritte mit der am besten geeigneten Verschlüsselungsmethode wählen. Bei SEG von Fortra kommen die folgenden Methoden zum Einsatz:

Transport Layer Security (TLS)

Sichert Nachrichten über das Internet zwischen Servern; ist für Endnutzer völlig transparent und daher weit verbreitet.

Kennwort-geschützte Dateien:

Verpackt die Nachricht und Anhänge des Absenders in eine kennwortgeschützte Zip- oder PDF-Datei, die dem Empfänger zugestellt wird. Das Kennwort für den Empfänger wird in einem anderen Format bereitgestellt - per SMS oder in einer zweiten E-Mail.

Secure MIME (S/MIME):

Ein in Europa weit verbreiteter Standard für den sicheren Versand von Nachrichten, der die Public-Key-Kryptographie verwendet, bei der die Nutzer sowohl einen private als auch einen öffentlichen Schlüssel erhalten, die mathematisch miteinander verknüpft sind, so dass eine mit einem öffentlichen Schlüssel verschlüsselte Nachricht nur vom Empfänger mit dem entsprechenden privaten Schlüssel geöffnet werden kann.

Pretty Good Privacy (PGP):

„Pretty Good Privacy“ ist ein ähnlicher Mechanismus wie S/MIME, bei dem Nutzer sowohl private als auch öffentliche Schlüssel haben. Hier werden aber andere Algorithmen verwendet.

Web Pickup Over SSL:

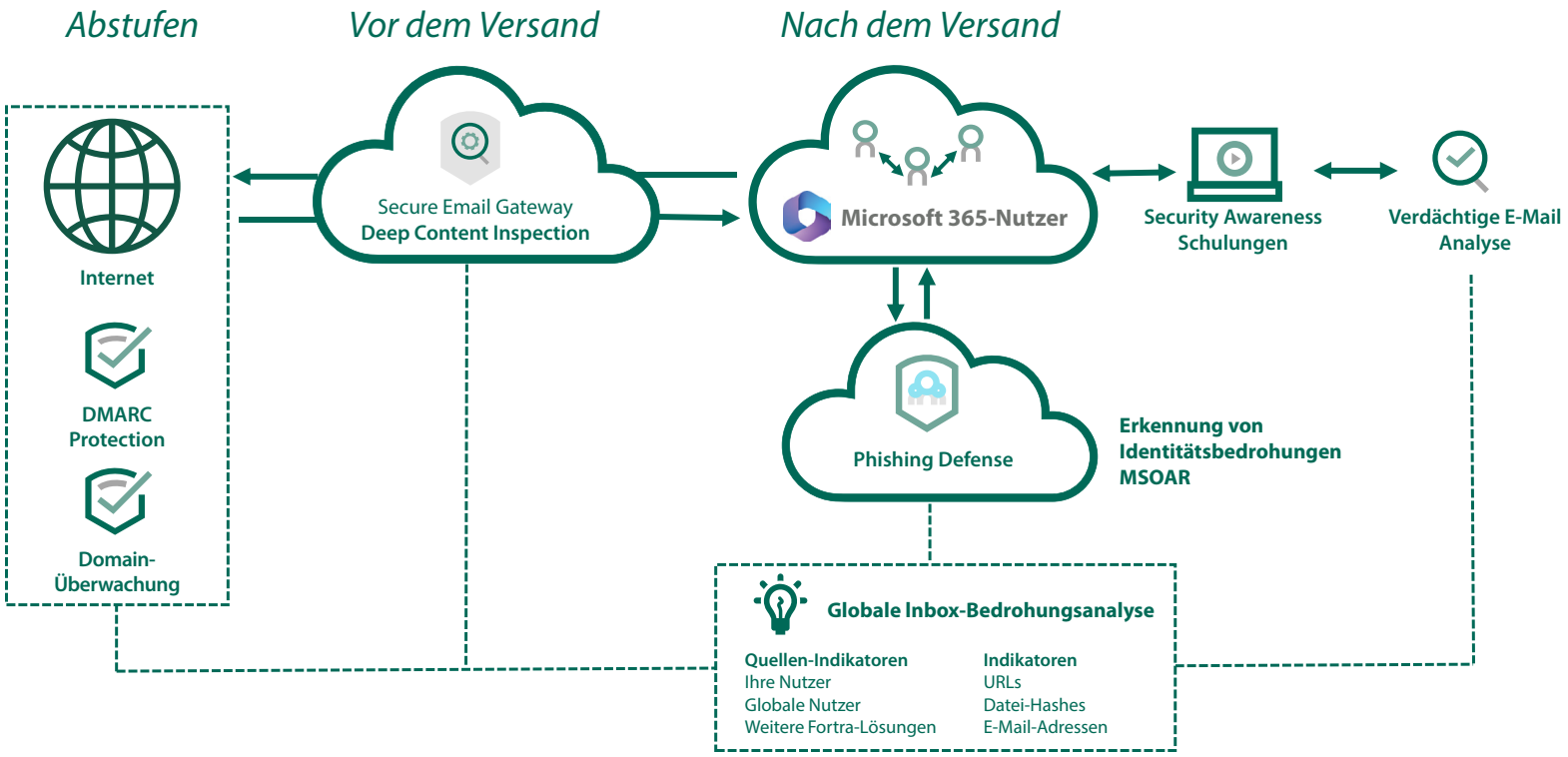
Das gehostete E-Mail-Portal ermöglicht es Absendern, Nachrichten mit einem Webmail-ähnlichen Mail-Client zu versenden und dem Absender auf sichere Weise zu antworten. Es wird in der Regel für ein geringes Nachrichtenvolumen an Benutzer aller Ebenen verwendet.

Methode	Nutzungshäufigkeit		Empfänger		Sicherheitsstufe
	Regelmäßig	Adhoc	Unternehmen	Verbraucher	
TLS	✔	✔	✔	✔	Über Netzwerk
Kennwort	✔	✔	✔	✔	Über Netzwerk
S/MIME & PGP	✔		✔		Zum Benutzer
Web Portal Pickup		✔	✔	✔	Zum Benutzer

Eine solide Kombination

Sicherlich verfügt M365 über viele E-Mail-Sicherheitsfunktionen, aber es hat auch seine Schwächen. Und diese Schwächen haben sehr reale Folgen. Der Schutz von Unternehmen vor Daten- und finanziellen Verlusten mit integrierter und anpassungsfähiger E-Mail-Sicherheit durch mehrschichtige Schutzfunktionen schließt die Lücken, die eine bestehende E-Mail-Plattform wie M365 hinterlässt. Fortras APD deckt Identitätsbetrug auf und schützt vor Phishing-Angriffen, während Fortras Continuous Detection & Response effektiv Berichte erstellt und die IT-Abteilungen entlastet. SEG bietet Schutz vor eingehenden, ausgehenden und internen Nachrichten, einschließlich Angriffen auf Inhalte und Datenverlusten. All dies kann über die Cloud, ortsgebunden oder als Hybridlösung erfolgen.

Fortra Advanced Email Security kann zusammen mit M365 eingesetzt werden, um sicherzustellen, dass die wertvollen Daten Ihres Unternehmens sicher bleiben - egal ob sie vor Ort, in der Cloud oder in einer hybriden Umgebung gespeichert sind. Es stellt genau die Unterstützung zur Verfügung, die Ihr Unternehmen braucht, damit Sie ohne E-Mail-Sicherheitsprobleme und Kopfschmerzen arbeiten können.



Sind Sie bereit, Ihre E-Mail-Sicherheit zu verbessern? Vereinbaren Sie einen Vorführtermin zu einer Ihnen genehmen Zeit.

FORTRA

Über Fortra

Fortra Cybersicherheits-Unternehmen wie kein zweites. Wir schaffen eine einfachere, stärkere Zukunft für unsere Kunden. Unsere bewährten Experten und unser Portfolio an integrierten und skalierbaren Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Wir führen positive Veränderungen herbei und sind Ihr unermüdlicher Verbündeter, der Ihnen bei jedem Schritt Ihrer Reise in Sachen Cybersicherheit ein sicheres Gefühl gibt. Erfahren Sie mehr auf fortra.com.

fta-corp-gd-0123-r2-vm