

Bestätigung Externer E-mail-Empfänger

SafeSend löst das Problem falsch adressierter E-Mails

Haben Sie jemals schon einmal eine E-Mail an die falsche Person geschickt? Vielleicht hatten Sie eine automatisch vervollständigte E-Mail-Adresse vor sich, die korrekt aussah, und haben auf Senden gedrückt... Nur, um dann herauszufinden, dass das der falsche "Stefan" war? Den meisten von uns ist das schon mindestens einmal passiert und dieses bedrohliche Gefühl kann unangenehm und peinlich sein. Für öffentliche Organisationen und Unternehmen, die sich an strikte Compliance- und sonstige Bestimmungen halten müssen, wie aus den Bereichen Pharma, Recht, Banken und Gesundheitspflege, kann das auch große finanzielle Auswirkungen haben.

Nutzen Sie SafeSend, um die externen E-Mail-Empfänger und Anhänge zu prüfen, wenn Sie E-Mails mit Microsoft Outlook versenden

VIPRE SafeSend ist ein Outlook-Add-In zur Vermeidung falsch adressierter E-Mails sowie versehentlicher Fehler durch automatische Eintragungen in E-Mails indem Anwender vor dem E-Mail-Versand aufgefordert werden, externe Empfänger und Dateianhänge zu bestätigen.

Mit VIPRE SafeSend können Sie:

- Bestätigen Sie externe Empfänger und Dateianhänge in ausgehenden E-Mails
- Helfen Sie Nutzern proaktiv dabei, die versehentliche Datenweitergabe durch die automatische Vervollständigung und die Nutzung der Funktion Allen antworten zu verhindern
- Erstellen Sie eine weiße Kennzeichnung mit Ihrem Unternehmenslogo und -Design
- SafeSend ist eine sicherheitsfokussierte Lösung, die keine Herausgabe von Unternehmensdaten erfordert. Alle Daten bleiben in Ihrem Netzwerk
- Alle Einstellungen in SafeSend können verändert werden und pro Nutzer/pro Gruppe festgelegt werden
- SafeSend protokolliert alle Ereignisse in einem vollständigen Prüfprotokoll, das lokal oder zentral gespeichert wird
- Unterstützt die lokalen Sprachen von Outlook
- Ergänzen Sie eine DLP-Funktion, um ausgehende E-Mails und Dateianhänge automatisch gleichzeitig zu scannen, um das Risiko zu verringern, dass sensitive Daten Ihr Netzwerk verlassen



5 Millionen
E-Mails jeden Tag

300+
Unternehmen

425,000+
aktive Nutzer



Wichtigste Vorteile Von VIPRE SafeSend

Marktführer	SafeSend hat über 425.000 aktive Nutzer in über 300 Unternehmen.
Schutz vor "Spear Phishing"	Ein externer Absender, der sich mit einer manipulierten E-Mail-Adresse als CEO ausgibt, wird erkannt. Bei der Antwort auf eine "Spear Phishing"-E-Mail wird das SafeSend-Bestätigungsfenster angezeigt, in dem die externe E-Mail-Adresse hervorgehoben wird.
Steigerung des Bewusstseins	Durch Corporate Branding und die Möglichkeit, benutzerdefinierten Text mit einem Link zu Ihrer E-Mail-/Sicherheitsrichtlinie einzugeben, werden Ihre Nutzer daran erinnert, immer besonders auf die Sicherheit zu achten.
Integrierte E-Mail-Verschlüsselung	SafeSend wurde so konzipiert, dass es mit VIPRE E-Mail-Sicherheitsverschlüsselung sowie den Verschlüsselungsdiensten vieler anderer Anbieter zusammenarbeitet. Das Tool kann genutzt werden, um Nutzer zur Verschlüsselung ihrer E-Mails aufzufordern, die besonders empfindliche Daten enthalten, indem sie gefragt werden, ob sie die E-Mail verschlüsseln möchten.
Einhaltung der DSGVO	Die präventive Funktion von SafeSend entspricht Artikel 32 der DSGVO zur "Implementierung geeigneter technischer und organisatorischer Maßnahmen zusammen mit einem Prozess zur regelmäßigen Überprüfung, Bewertung und Auswertung der Wirksamkeit der Maßnahmen zur Sicherstellung der Sicherheit bei der Verarbeitung".
PC und Web Add-Ins	SafeSend ist für PC und Mac erhältlich. Unser PC-Add-In läuft direkt auf Windows-Geräten, während das Web-Add-In die Abdeckung auf Outlook für Mac und Outlook Web Access erweitert.
Nahtlose Integrierung mit Microsoft RMS	SafeSend kann jetzt auch mit Microsoft RMS integriert werden. Dies hat Vorteile, wie die Möglichkeit, verschlüsselte RMSDateien automatisch über das PC Add-In zu scannen, ohne zusätzliche Einstellungen oder Konfigurationen.

Trigger-Optionen

SafeSend kann unter verschiedenen Bedingungen ausgelöst werden. Die gängigste Option ist die Anzeige von SafeSend für alle externen E-Mails, die aus dem Unternehmen herausgeschickt werden. Die zweitgängigste Option ist die Anzeige nur beim Versenden von Dateien nach außerhalb.

SafeSend kann auch so konfiguriert werden, dass es nur ausgelöst wird, wenn es in einer externen E-Mail einen DLP-Treffer gibt. Dies ist hilfreich, wenn Sie bestimmte DLP-Regeln festgelegt haben und den Nutzer nur informieren möchten, wenn es Treffer für eine dieser Regeln gibt.

Systemanforderungen

System Component SafeSend PC Add-in	System Component SafeSend Web Add-in
Minimum Requirement Operating Systems Windows 10, 8.1, 8, 7 Windows Server 2016, 2012, 2008 R2	Minimum Requirement .NET Core 6.0 capable web server Hosting Bundle is required when using IIS Server (Recommended)
Email Clients Outlook 2019, 2016, 2013, 2010 Both 32-bit and 64-bit versions .NET Framework 4.7, 4.6, 4.5, 4.0	Microsoft 365 - Email Clients: Outlook for Mac v16.30+, Outlook for Windows 2019, 2016, Both 32-bit and 64-bit versions
Microsoft .NET 4.7.2 or later is required to be installed but all newer versions of Windows already have this included Please note that .NET 4.7.2 Client Profile is not sufficient to install SafeSend and that the full version of .NET 4.7.2 or later is required	Browsers for OWA - Mozilla Firefox, Google Chrome, Microsoft Edge, Microsoft Edge Chromium, Internet Explorer 11, Safari
	Exchange 2019 - Email Clients: Outlook for Windows 2019, 2016, Both 32-bit and 64-bit versions
	Browsers for OWA - Mozilla Firefox, Google Chrome, Microsoft Edge, Microsoft Edge Chromium, Internet Explorer 11

Optional DLP module

SafeSend mit DLP scannt zusätzlich Dateianhänge und E-Mail-Inhalte auf besonders empfindliche Daten und gibt Unternehmen die Möglichkeit, zusätzliche benutzerdefinierte DLP-Regeln zu erstellen. Mithilfe regulärer Ausdrücke können Sie sensitive Schlüsselwörter oder Datenmuster in E-Mail-Inhalten oder Dateianhängen erkennen, wie beispielsweise Kreditkartennummern, Kontodaten oder Sozialversicherungsnummern. Das DLP-Add-On ist für PC und Web-Add-Ins verfügbar.

- Legen Sie eine Liste mit kundenbezogenen Schlüsselwörtern und freigegebenen Domains fest.
- Schützen Sie Kundendaten davor, an den falschen Kunden geschickt zu werden.
- Geben Sie an Nutzer eine Warnung aus, wenn sie Kundendaten an eine nicht freigegebene Domain schicken.
- Verhindern Sie, dass bestimmte Informationen an nicht zugelassene Domains geschickt werden.



WEITERE INFORMATIONEN. [global.VIPRE.com](https://global.vipre.com)
 +49 (0) 30 22957782 | DACH.Sales@VIPRE.com