Einführung in GFI MailEssentials AI CoPilot: KI-gestützte Datenverlustprävention

E-Mail bleibt der wichtigste Angriffsvektor für Cyberbedrohungen, wobei Phishing weiterhin Wege findet, selbst die besten E-Mail-Sicherheitsmaßnahmen zu umgehen. Wenn ein Angriff erfolgreich ist, besteht ein extrem hohes Risiko, dass sensible Daten über ausgehende E-Mails geleakt werden.

GFI MailEssentials AI CoPilot bietet eine wesentliche letzte Verteidigungslinie, indem KI kontinuierlich Ihren ausgehenden E-Mail-Kanal überwacht, analysiert und schützt.

- Automatisierte Erstellung von DLP-Richtlinien, die auf Ihr Unternehmen zugeschnitten sind
- Reduziert das Risiko von Datenverletzungen und Compliance-Strafen
- Verringert die Belastung der IT-/Sicherheitsteams
- Vereinheitlichte Lösung, die vollständig in GFI MailEssentials AI integriert ist

So funktioniert CoPilot

Mit fortschrittlichem maschinellen Lernen analysiert CoPilot die Details Ihres Unternehmens und die geltenden Vorschriften, um automatisch intelligente DLP-Richtlinien für Ihren ausgehenden E-Mail-Verkehr zu erstellen.

- Geben Sie einfach Details zu Ihrer Organisation an - Branche, Rollen, Arten von Daten usw.
- CoPilot vergleicht dies mit integrierten Richtlinienregeln, die GDPR, HIPAA, PCI-DSS und mehr abdecken.
- Die Verarbeitung natürlicher Sprache erkennt kontextualisierte Daten in E-Mails und wendet DLP-Richtlinien an.
- Richtlinien entwickeln sich durch maschinelles Lernen aus der Überwachung Ihrer Kommunikation.

Mit den automatisierten Funktionen von CoPilot haben Sie eine leistungsstarke zusätzliche Schutzschicht gegen Datenverlust, die das Risiko von Verletzungen verringert und gleichzeitig die Belastung der IT-Teams erleichtert.

Holen Sie sich CoPilot

Urheberrecht © 2024 GFI USA, LLC, Alle Rechte vorbehalten.