MailEssentials

DATENBLATT

14 Anti-Spam-Filter, 3 Anti-Virus-Engines und Malware-Scans in einem einzigen E-Mail-Sicherheitspaket

Mit Milliarden von E-Mails, die jeden Tag gesendet und empfangen werden, ist E-Mail häufig das Mittel eines Eindringlings, um Ihr Unternehmen anzugreifen. GFI MailEssentials ist einfach zu bedienen und bietet umfassende Schutzmaßnahmen zum Schutz Ihres Unternehmens und zur Verbesserung der E-Mail-Produktivität.

Blockieren Sie E-Mail basierte Viren und Malware

Warum sollten Sie einem einzigen Antiviren-E-MailSicherheitssystem vertrauen, wenn Sie ein dreifaches haben können? GFI MailEssentials kann die Leistung führender Marken wie BitDefender, Avira und Sophos nutzen. Jedes System verfügt über eigene Heuristiken und Erkennungsmethoden. Sie erhalten maximalen Schutz für Ihre E-Mails, um von E-Mails übertragene Viren und andere Malware effektiver zu blockieren

Filtern Sie Spam und erkennen Sie Phishing-Angriffe

- Filtern Sie Spam heraus, bevor er in E-Mail-Postfächer gelangt, um Platz auf Ihrem Server und produktive Zeit zu sparen. GfI MailEssentials nutzt 14 fortschrittliche E-MailFiltertechnologien, die Sie in Aktion sehen können. Das Anti-Phishing-Modul von GFI MailEssentials erkennt und blockiert Bedrohungen durch Phishing-E-Mails, indem es den Inhalt des Spam mit einer ständig aktualisierten Datenbank und Phishing-URLs vergleicht.

Machen Sie E-Mails sicher und produktiv... ganz einfach

GFI MailEssentials ist kompatibel mit verschiedene E-Mail-Servern, nicht nur Exchange. Es fügt sich nahtlos in Ihr aktuelles Setup ein - ob lokal, virtuell oder in Ihrer Cloud-Infrastruktur gehostet. IT-Administratoren haben die volle Kontrolle über ihre E-Mail-Sicherheit.

GFI MailEssentials AI

Mit GFI MailEssentials AI, powered by GenAI, definieren Sie E-Mail-Sicherheit neu, indem Sie Intelligenz und Schutz mühelos miteinander verbinden. GFI MailEssentials AI identifiziert schnell echte Bedrohungen, gibt legitime E-Mails frei und markiert den Rest. Zudem passt er Inhaltsfilter dynamisch an, um sensible Daten zu schützen. GFI MailEssentials AI sorgt dafür, dass Ihr Unternehmen nicht nur sicher bleibt, sondern auch die mit Datenschutzverletzungen verbundenen Risiken minimiert.

30 Tage lang kostenlos testen

Bis zu drei Antivirus-Engines

GFI MailEssentials wird mit den leistungsstarken Avira- und BitDefender Antivirus-Engines geliefert. Fügen Sie die Antiviren-Engine von Sophos hinzu, um den ultimativen Schutz zu gewährleisten. Anbieter von Antiviren-Engines haben unterschiedliche Antwortzeiten auf neue Viren und Malware. Die Funktion stellt sicher, dass Ihr System neue Bedrohungen immer in kürzester Zeit erkennen kann.

Erweiterter Malware-Schutz

GFI MailEssentials bietet erweiterten Malware-Schutz mit Scan-Engines, die eine Verbindung zu einem Cloud-Dienst herstellen, wenn unbekannte ausführbare Anhänge gefunden werden. Diese Anhänge werden gründlich gescannt, um festzustellen, ob der Anhang böswillig ist oder nicht.

Ein Arsenal an Anti-Spam-Filtern

GFI MailEssentials bietet eine Vielzahl von Anti-Spam-Technologien. SPF blockiert gefälschte E-Mails. Greylisting blockiert E-Mails, die mit nicht RFC-kompatiblen Techniken gesendet werden, die von Spammern verwendet werden. Der Directory Harvest Protection blockiert E-Mails, die mithilfe zufälliger und umfassender Techniken zur Generierung von E-Mail-Adressen gesendet werden. DNS-Blacklists nutzen eine Fülle von Informationen, die aus verteilten Community-Datenerfassungstechniken stammen, um sich gegen Botnet-Spam zu wehren.

Webkonsole mit integriertem Reporting

Sie können alle Ihre Anti-Spam- und E-Mail-Sicherheitsfunktionen, einschließlich der Quarantäne von Spam und Malware, sowie die Berichterstellung über eine einzige webbasierte Konsole ausführen. Die Konsole enthält das Dashboard, mit dem Sie in Echtzeit eine grafische Darstellung des Softwarestatus sowie des E-Mail-Flusses auf dem Server erhalten.

Quarantänemanagement

Mit GFI MailEssentials können Sie flexibel auswählen, was mit Spam- und Malware-E-Mails geschehen soll. Benutzer können E-Mails als Spam markieren. Sie können verdächtigen Spam unter Quarantäne stellen und Benutzer benachrichtigen. Sie können zentrale Quarantänestellen für Malware einrichten.

Durchsetzung von E-Mail-Inhalten und Verhinderung von Datenlecks

Die Funktion zur Schlüsselwortprüfung in GFI MailEssentials kann verwendet werden, um eingehende und ausgehende E-Mails nach Schlüsselwörtern zu durchsuchen, und die Funktion zur Überprüfung von Anhängen durchsucht E-Mails nach Anhängen.

Sie können alle eingehenden E-Mails mit potenziell böswilligen Anhangstypen blockieren oder Bandbreiten- und Produktivitätsverschwendung wie MP3- und MPEG-Dateien blockieren. Erweiterte benutzerbasierte E-Mail-Filterregeln ermöglichen es Ihnen, E-Mails basierend auf von Ihnen definierten Mustern wie regulären Ausdrücken zu blockieren. Dies ist weitaus leistungsfähiger als die einfache Überprüfung von Schlüsselwörtern.

Schützen Sie Ihr Unternehmen vor E-Mail-Exploits und Trojanern

Der GFI MailEssentials-Trojaner und der ausführbare Scanner erkennen unbekannte, böswillige ausführbare Dateien, indem sie analysieren, was sie tun. Der Scanner verwendet integrierte Informationen, um das Risiko zu bewerten, indem er die ausführbare Datei zerlegt, erkennt, was sie möglicherweise tut, und ihre Aktionen mit einer Datenbank böswilliger Aktionen vergleicht. Der Scanner isoliert dann alle ausführbaren Dateien, die verdächtige Aktionen ausführen, beispielsweise, Netzwerkverbindungen herstellen oder auf das Adressbuch zugreifen.

Schützen Sie Ihre Benutzer vor Phishing und Spyware

Das Anti-Phishing-Modul von GFI MailEssentials erkennt und blockiert Bedrohungen durch Phishing-E-Mails, indem es den Inhalt des Spam mit einer ständig aktualisierten Datenbank und Phishing-URLs vergleicht. Dadurch wird sichergestellt, dass alle aktuellen Phishing-E-Mails erfasst werden. Als zusätzlichen Schutz wird in jeder E-Mail, die an Ihr Unternehmen gesendet wird, nach typischen Phishing-Schlüsselwörtern gesucht.

GFI MailEssentials erkennt auch E-Mail-Spyware über seine Antiviren-Engine, die eine dedizierte Spyware- und Adware-Definitionsdatei enthält, die über eine umfangreiche Datenbank bekannter Spyware, Trojaner und Adware verfügt.