

Proofpoint: E-Mail-Sicherheit und Data Loss Prevention [Vorbeugung vor Datenverlust] der nächsten Generation



Mit Proofpoint übernehmen Sie auf Abruf, oder ständig bei sich im Unternehmen, die Kontrolle über E-Mail-Risiken



Egal ob Proofpoint bei Bedarf zum Einsatz kommt, oder ständig im Unternehmen angewandt wird, die E-Mail-Sicherheitslösungen schützen gegen eingehende Datenübertragungsgefährdungen, verhindern das Durchsickern sensibler Informationen, verschlüsseln Nachrichten und helfen bei der Optimierung Ihrer Nachrichteninfrastruktur. Die vereinheitlichte Struktur, der modulare Schutz und die Management-Oberfläche schützen Unternehmen gegen alle Arten von E-Mail-Risiken—direkt an der Schnittstelle zum Unternehmen.

abwehren, vorbeugen, verschlüsseln, analysieren

Weshalb noch eine weitere Punktlösung? Proofpoints einheitliche Plattform für E-Mail-Sicherheit und Data Loss Prevention [Vorbeugung vor Datenverlust] bietet umfassenden Schutz gegen sowohl eingehende Gefährdungen, als auch Sicherheitsrisiken beim Versand von Inhalten nach außen – und mit Proofpoints modularer Architektur, können Sie mit der Veränderung Ihres Bedarfs ganz leicht neue Schutzkomponenten einsetzen.

Sämtliche Eigenschaften von Proofpoint – einschließlich Anti-Spam, Anti-Virus, protokollübergreifender Content-Sicherheit, richtlinienbasierter Verschlüsselung und Berichtsfunktionen – werden zentral über eine einzige grafische Benutzeroberfläche gesteuert und in einer einheitlichen Architektur umgesetzt. Die Funktionen können in nahezu jeder Konfiguration angewandt werden, um den einzigartigen Bedürfnissen Ihres Unternehmens nachzukommen.

Egal ob Ihre Installation an einem Standort, oder an mehreren Standorten auf dem ganzen Globus vertreten ist, sämtliche Bestandsmanagement- und Verwaltungsaufgaben werden durch Proofpoints zentrale, webbasierte Managementkonsole kontrolliert.

Flexible Installationsoptionen

Proofpoints E-Mail-Sicherheitslösungen und Data Loss Prevention können bei Bedarf ständig, oder in Hybridkonfigurationen installiert werden. So hat man maximale Flexibilität.

- **SaaS:** Die Proofpoint ENTERPRISE™ und Proofpoint PROTECT™ Software-as-a-Service-Lösungen bieten Proofpoints E-Mail-Sicherheits-Funktionen und DLP-Funktionen als kostengünstigen Service auf Abruf. Diese Lösungen auf Abruf werden in den High-End-Rechenzentren von Proofpoint gehostet und bieten maximale Sicherheit in Verbindung mit den niedrigsten Gesamtkosten.
- **Hardware-Geräte:** Der Proofpoint Messaging Security Gateway ist eine Hardware, welche absolut sicher ist und sich innerhalb von Minuten installieren lässt. Es gibt eine ganze Reihe von Modellen, mit denen Unternehmen jeder Größenordnung ausgerüstet werden können.
- **Virtuelle Geräte:** Proofpoints virtuelle Version bietet den gleichen erstklassigen Schutz wie Proofpoints Hardware-Geräte. Dazu kommen die zahlreichen Kosten- und Verwaltungsvorteile der Virtualisierung. Die virtuelle Anwendung läuft auf jeder Standard x86 Hardware mit VMware Server oder VMware Infrastruktur.
- **Software:** Der Proofpoint Protection Server bietet Proofpoints E-Mail-Security-Plattform als Software für das Red Hat Linux Enterprise Betriebssystem.

Sicher. Effektiv. Einfache Installation.

Das sind nur einige Stichpunkte, die Proofpoints einheitliche Email-Sicherheits- und Data Loss Prevention Plattform beschreiben. Es ist die leistungsstärkste Lösung der Branche—zur Anwendung als SaaS, als Hardware, als virtuelles Gerät, oder als Software—die Folgendes bietet:

- Unschlagbare Spamerkennung und Verbindungsmanagement
- Virenschutz und Schutz vor Massenangriffen von Weltrang
- Umfangreiche Multi-Protocol Data Loss Prevention und Content Security
- Richtlinienbasierte E-Mail-Verschlüsselung
- Erweiterte Berichts- und Analysefunktionen
- Einheitliches Policy Management
- Leistung für Unternehmen als Zielgruppe
- Schnelle Installation und schneller Zugang
- Optimal skalierbare Architektur

„Pacific Sunwear hat eine große Anzahl an Anti-Spam-, Anti-Viren- und Content Scanning-Lösungen ausgewertet. Proofpoint war das erste Unternehmen, das eine Plattform bietet, die alle unsere Anforderungen in den Bereichen E-Mail und Nachrichtenübertragung in einer einzigen, einfach zu installierenden und zu verwaltenden Lösung erfüllt. Die Anwendung Message Security Gateway hat unseren E-Mail-Kanal wieder zu dem Kanal für Geschäftskommunikation gemacht der er sein sollte. Er stellt nicht mehr die Drehtür für aus den Nachrichten übertragene Bedrohungen dar.“

Ron Ehlers
VP für Informationssysteme
Pacific Sunwear

Proofpoint: E-Mail-Sicherheit und Data Loss Prevention der nächsten Generation

Kompletter Schutz

Proofpoint MLX-Technologie

Fortgeschrittenes maschinelles Lernen

Die Stärke hinter Proofpoints Nachrichtensicherheitslösungen für Unternehmen – Proofpoint MLX – ist ein fortgeschrittenes, zum Patent angemeldetes, maschinelles Lernsystem, das von Wissenschaftlern des Proofpoint Attack Response Centers entwickelt wurde. Es basiert auf fortschrittlichen statistischen Methoden, einschließlich logistischer Regression und Informationszuwachsanalyse. Damit ermöglicht Proofpoint MLX die akkurate Klassifizierung und Identifikation von nicht strukturierten Inhalten, wie sie sich in E-Mails und anderen Dokumenten finden.

Einzigartige Genauigkeit

Proofpoint MLX sorgt für die einzigartige Anti-Spam-Genauigkeit von Proofpoint Spam Detection. Mit Hilfe von MLX analysiert Proofpoint hunderttausende strukturelle Eigenschaften, Bild-, Text- und Reputationseigenschaften, um zwischen Spam und echten Nachrichten zu unterscheiden. Traditionelle Anti-Spam-Lösungen werten nur eine begrenzte Zahl von Eigenschaften aus und sind zu einer deutlichen Klassifizierung von Spam nicht in der Lage, was zu geringer Effektivität und einer großen Zahl falscher Positivmeldungen führt.

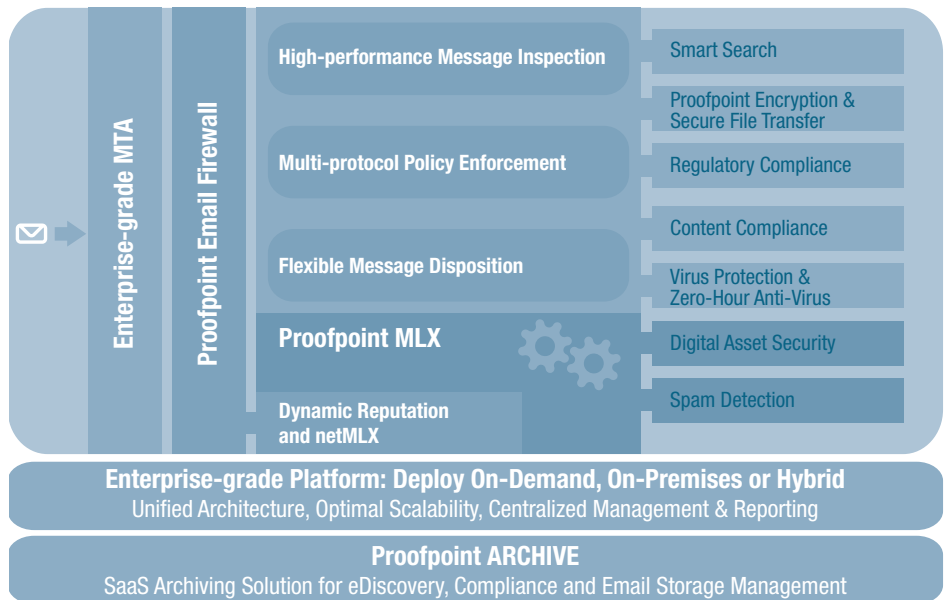
Zukunftssichere Intelligenz

Proofpoints Anti-Spam-Technologie aktualisiert sich fortlaufend selbst, um vor neuen Arten von Spam zu schützen. Kontinuierliches Selbsttraining und von den Proofpoint-Wissenschaftlern entwickelte Methoden ermöglichen MLX, neue Arten von Spam bei deren Auftauchen zu erkennen und sich auf sie einzustellen. Alle Kunden erhalten automatisch fortlaufend die MLX Updates.

Dadurch bietet Proofpoint MLX eine Wirksamkeit von mindestens 99,8 Prozent, selbst bei schwierigen Arten von Spam, einschließlich von Bildern, PDF, Anhängen, „Backscatter“ und fremdsprachigem Spam.

Anders als bei anderen Anti-Spam-Lösungen lässt die Wirksamkeit von Proofpoint beim Schutz vor Spam mit der Zeit nicht nach – und die Updates an der MLX Anti-Spam-Engine werden Ihrem Unternehmen regelmäßig automatisch übermittelt. Proofpoint entwickelt sich ständig weiter, um entstehenden Bedrohungen zu begegnen und sicherzustellen, dass Ihre Nachrichteninfrastruktur sowohl gegen die Spammer von morgen, als auch gegen die von heute gesichert ist.

Proofpoint MLX unterstützt auch die fortgeschrittenen Content Security-Funktionen von Proofpoint Digital Asset Security und die intelligenten Sicherheitsmerkmale des Proofpoint E-mail Firewall und Dynamic Reputation Service. Proofpoint ist der einzige Anbieter, der diese wirkungsvollen maschinellen Lernmethoden in den Bereichen E-Mail-Sicherheit und Data Loss Prevention einsetzt.



Verteidigung gegen eingehende Bedrohungen

Fortgeschrittene Spamererkennung, powered by Proofpoint MLX™

Proofpoint Spam Detection™ wird von der zum Patent angemeldeten Proofpoint MLX Technologie für maschinelles Lernen unterstützt und überprüft hunderttausende Attribute in jeder E-Mail – einschließlich des Nachrichtenheaders und der Struktur, Bilder, Reputation des Absenders, sowie den unstrukturierten Inhalt der Nachricht – zur Abwehr von Spam, Bild-Spam und Phishing-Angriffen. Außerdem passt es sich auf neue Angriffe bei deren Erscheinen an. Der **Proofpoint Dynamic Update Service™** aktualisiert Ihren Spamschutz automatisch, so dass jederzeit maximale Wirksamkeit gewährleistet ist. Individuell steuerbare Einstellungen für Spam und Inhalte für Erwachsene ermöglichen die Durchsetzung von Nulltoleranzregelungen gegenüber pornografischem Spam. Anti-Phishing-Eigenschaften (einschließlich DKIM-Signatur für ausgehende Nachrichten) stoppen die Verbreitung von Phishing-E-Mails und beugen dem Diebstahl persönlicher Mitarbeiterinformationen vor. Die Bounce Management-Eigenschaften, einschließlich Bounce Address Tag Validation (BATV) Spezifikationsunterstützung blocken „Backscatter“-Spam (Nichtzustellbarkeitsmeldungen) zu 100 %.

Proofpoint Spam Detection ist mehrsprachig und bietet hervorragende Genauigkeit gegen Spam in jeder Sprache – einschließlich schwer zu analysierender Sprachen mit Mehrfach-Byte-Zeichen, wie beispielsweise Japanisch und Chinesisch. Die Anti-Spam-Richtlinien können global, für Gruppen und Endnutzer festgelegt werden. Eine Integration mit LDAP oder Active Directory vereinfacht die laufende Verwaltung.

Integrierter E-Mail-Firewall-Schutz

Die **Proofpoint E-mail Firewall™** bietet eine zustandsabhängige, „first line of defence“ gegen Spam und schädliche Verbindungen, indem sie zahlreiche Datenpunkte in der Verbindung überprüft, einschließlich DNS, MX Record-Verifizierung, SPF, Empfänger-Verifizierung, Proofpoint Dynamic Reputation-Informationen und optional auch netMLX (Netzwerkreputation).

Innovatives Verbindungsmanagement

Sämtliche Proofpoint-Installationen verfügen über eine eingebaute, vorausschauende Verhaltensanalyse des lokalen IP-Traffic, die in Echtzeit reagiert und durch gezielte Angriffe verursachte E-Mail-Verkehrsspitzen beseitigt, sowie schädliche Verbindungen von Botnets blockiert, oder drosselt.

Proofpoint Dynamic Reputation™ oder **Proofpoint SHIELD™** können das eingehende Verbindungsvolumen um 80 % und mehr reduzieren. Proofpoint unterhält die genaueste und aktuellste Datenbank der Branche über die Reputation von IP-Adressen, die E-Mails im Internet übertragen. Es ist der einzige E-Mail-Reputationsservice, der mit einer Kombination aus lokaler

Proofpoint: E-Mail-Sicherheit und Data Loss Prevention der nächsten Generation

Verteidigung gegen eingehende Bedrohungen (Fortsetzung)

Reputation, erwarteten Verhaltensdaten und global beobachteter Reputation arbeitet—analysiert von leistungsstarken maschinellen Lernalgorithmen—um eingehende Verbindungen von schädlichen IP-Adressen zu blocken. Jede Minute werden hunderte von Datenpunkten für sämtliche IP-Adressen mit fortgeschrittenen maschinellen Lernalgorithmen analysiert. Daraus wird eine Punktzahl generiert, die die Reputation des Absenders anzeigt. Proofpoint Dynamic Reputation nutzt diese Punktzahlen dann, gemeinsam mit den lokalen Verhaltensdaten, um intelligente Entscheidungen über Akzeptanz, Drosselung oder Ablehnung der eingehenden E-Mail-Verbindungen zu treffen.

Virenschutz und Zero-Hour Antivirenschutz

Durch strategische Partnerschaften mit führenden Anbietern von Antivirenlösungen bietet **Proofpoint Virus Protection™** eine komplette Virenschannerfunktion. Die Virus-Engines sind tief in Proofpoints Plattform integriert und bieten komfortable, zentrale Verwaltung der Antivirenrichtlinien über die gleiche Oberfläche, mit der auch die Spam- und Contentrichtlinien verwaltet werden. Nachrichten werden parallel mit Spam und Nachrichteninhalten auf Viren überprüft. So wird der Endnutzer vor Viren, Würmern und anderen bösartigen Codes geschützt. Außerdem schützt **Proofpoint Zero-Hour Anti-Virus™** vor aufkommenden Viren schon im frühesten Stadium ihrer Ausbreitung—so werden sie schon Stunden vor der Reaktion von Konkurrenzprodukten gestoppt.

Vorbeugung von Informationslecks über mehrere Protokolle hinweg

Proofpoints fortschrittliche Data Loss Prevention-Funktionen können sowohl ausgehende E-Mails, als auch zusätzliche Nachrichtenströme, wie beispielsweise webbasierte E-Mails, Blogpostings, Beiträge auf Messageboards und weitere HTTP- bzw. FTP-basierte Aktivitäten, schützen.

Content Compliance: Easily Enforce Acceptable Use Policies

Proofpoint Content Compliance™ macht die Definition und Durchsetzung von Richtlinien für die angemessene Benutzung von Nachrichteninhalten und -anhängen einfach. Mit einer praktischen Point-und-Klick-Oberfläche wird das Festlegen komplexer Regeln hinsichtlich Dateitypen, Nachrichtengröße und Nachrichteninhalte vereinfacht. Mit Hilfe dieser Eigenschaften kann man eine Reihe ein- und ausgehender Richtlinienverletzungen feststellen—einschließlich Beleidigungen, Belästigung, File-Sharing und Verletzung externer Richtlinien.

Regulatory Compliance: Sorgen Sie für die Sicherheit privater Daten

Unternehmen müssen mehr als je zuvor auf den Datenschutz und die Sicherheit von Kunden- und Mitarbeiterdaten achten. **Proofpoint Regulatory Compliance™** setzt die besten Standards zur Sicherung privater Daten um und schützt Ihr Unternehmen vor der Haftung, die im Zusammenhang mit Gesetzen aus den Bereichen Datenschutz und Datensicherheit stehen (wie beispielsweise HIPAA, GLBA, PCI, SEC und weitere). Anpassbare Regeln, verwaltete Wörterbücher und „kluge Identifier“ scannen nichtöffentliche Informationen automatisch—wie beispielsweise geschützte Gesundheitsinformationen und Informationen zu persönlichen Finanzen—und lehnen Nachrichten ab, bzw. verschlüsseln sie angemessen.

Proofpoints kluge Identifier sind raffinierter als einfache reguläre Formeln. Sie suchen nach der richtigen Anzahl an Ziffern bzw. Zeichen, aber führen auch komplexe Algorithmen aus, um eine hohe Genauigkeit bei der Identifizierung mit einer minimalen Anzahl falscher Positivmeldungen zu erreichen.

Digital Asset Security: Vertrauliche Dokumente schützen

Seit E-Mail, Webmail und andere Nachrichtensysteme zu den wichtigsten Kommunikationskanälen geworden sind, sind sie auch zu einem Kanal für die Freigabe sensibler, bzw. vertraulicher Informationen geworden. **Proofpoint Digital Asset Security™** schützt wertvolle Unternehmensressourcen und vertrauliche Daten davor, per E-Mail oder anderer Nachrichtenprotokolle aus Ihrem Unternehmen verschickt zu werden. Die starke maschinelle Lerntechnologie MLX analysiert und klassifiziert Ihre vertraulichen Dokumente und überwacht dann den ausgehenden Datenstrom für diese Informationen (bzw. Teile dieser Informationen)—so wird die Verletzung der Contentsicherheit gestoppt bevor sie passiert.

Multi-protocol Data Loss Prevention

Erweitern Sie mit **Proofpoint Network Content Sentry™** den Wirkungsbereich von Proofpoints Data Loss Prevention-Funktionen auf HTTP und FTP Streams.

Zentrales Management

Webbasiertes Richtlinienmanagement, Verwaltung und End-user Kontrolle

Die Proofpoint Messaging Security Console™ bietet eine zentrale, zu 100 % webbasierte Verwaltungsoberfläche für Proofpoints einheitliches Policy Management-System. So wird die ständige Anwendung der Unternehmensrichtlinien für Nachrichten sichergestellt. Die Konsole macht die Überwachung und Kontrolle der Nachrichteninfrastruktur, sowie die Definition von Nachrichtenrichtlinien einfach. Sie können sogar unterschiedliche Richtlinien für verschiedene Gruppen von Endnutzern oder Domains definieren und durchsetzen. Wenn Sie Ihrer Installation weitere Proofpoint-Funktionen hinzufügen, wird die gleiche praktische Oberfläche für das Richtlinienmanagement angewandt.

Das Ajax-basierte Interface bietet „Drag and Drop“-Anpassung der Berichte, Statusinformationen, RSS Feeds und die Anzeige weiterer Komponenten. Man kann sogar „Mashups“ aus Informationen externer Quellen erstellen.

Proofpoints ausgesprochen einfache Bedienbarkeit gilt auch für den Endnutzer. Leicht verständliche Berichte und Kontrollen, wie beispielsweise Proofpoints Digest für Endnutzer, webbasierte Quarantäne und individualisierte Listen für sichere und geblockte Inhalte geben den Nutzern die komplette Kontrolle über ihre eigenen Spameinstellungen. Die Endnutzeroberfläche kann mit Proofpoints Verwaltungsoberfläche einfach individuell angepasst und markiert werden.

Umfangreiche Auswertung

Die Konsole bietet auch Zugang zu über 60 grafisch dargestellten Echtzeitberichten und Benachrichtigungen, die einen kompletten Einblick in den Zustand des Nachrichtensystems Ihres Unternehmens gewährleisten. Die Berichte können einfach als HTML oder XML per E-Mail versandt oder veröffentlicht werden. Proofpoints „aktive“ Berichte liefern Schlüsselinformationen und erlauben den Administratoren auch sofortiges Eingreifen (beispielsweise einfach per Klick auf einen Link einen missbräuchlichen Absender blockieren).

Null Administration

Immer aktueller Schutz, einfache Administration

Proofpoints Anwendungen bieten die Vorteile von Proofpoints Cloud Computing-Ressourcen, die ihr Unternehmen sicher machen. Gleichzeitig wird die laufende Wartung minimiert. Der Proofpoint Dynamic Update Service stellt sicher, dass das Netzwerk immer den bestmöglichen Schutz vor E-Mail-basierten Bedrohungen hat. Es bietet laufende Updates für jede Komponente Ihrer Proofpoint-Installation, einschließlich der Hardware OS und MTA, Spam- und Virus-Engines, Compliance Dictionaries, Anwendungskomponenten und individuelle Hot Fixes.

Proofpoint: E-Mail-Sicherheit und Data Loss Prevention der nächsten Generation

Sensible Informationen verschlüsseln

Proofpoint Encryption™ fügt Ihrem Proofpoint-Paket leistungsstarke richtlinienbasierte E-Mail-Verschlüsselungsmöglichkeiten hinzu. So werden Nachrichten automatisch gemäß den Richtlinien Ihres Unternehmens verschlüsselt. Die Anwendung setzt die Verschlüsselungsrichtlinien automatisch und durchgängig um, ohne dass der Endnutzer spezielle Aktionen durchführen muss. Die Proofpoint ENTERPRISE SaaS-Lösung und Proofpoints Hardwaregeräte und virtuelle Geräte unterstützen auch digitale Zertifikate und ermöglichen sicheren Transfer von Gateway zu Gateway, sowie den Empfang von E-Mail mit Transport Layer Security (TLS).

Optimieren Sie Ihre Nachrichteninfrastruktur

Erweitern Sie Ihr Proofpoint-Paket mit einer Reihe von Erweiterungen, die die Benutzerfreundlichkeit und Handhabbarkeit Ihrer E-Mail-Infrastruktur verbessern.

Die On-Demand **Proofpoint ARCHIVE™**-E-Mail-Archivlösung kümmert sich um Speicherverwaltung, Beweissicherung und die Einhaltung gesetzlicher Richtlinien, ohne den Aufwand eines E-Mail-Archivs im eigenen Unternehmen. Die patentierte DoubleBlind Encryption™ sorgt für die Sicherheit Ihrer Daten bei der Übertragung und in der On-Demand-Lösung. **Proofpoint Smart Search™** erweitert Proofpoints eingebaute Protokoll- und Berichtsfunktionen mit fortschrittlichster Nachrichtenverfolgung, Forensik und Protokollanalysemöglichkeiten – so bietet es einfache Echtzeitsichtbarkeit des Nachrichtenflusses. Suchen, analysieren und exportieren Sie Nachrichtenprotokolle von einer komfortablen, einfach zu bedienenden Benutzeroberfläche aus – selbst über global verteilte Proofpoint-Installationen hinweg. **Proofpoint Secure File Transfer™** bietet zusätzlich sichere, hohe Dateitransferkapazitäten für Ihre Proofpoint-Installation. Mit dieser Anwendung können die Endnutzer große Dateien, bzw. Dateien mit hoher Sicherheitsstufe schnell und einfach versenden – ohne dass diese Anhänge in Ihren E-Mail-Server gelangen.

Hohe Leistung, einfache Installation, optimale Skalierbarkeit

Proofpoint wurde entwickelt, um die einzigartigen Bedürfnisse großer Unternehmen, Internetdienstleister, Universitäten und Regierungsorganisationen zu erfüllen. Egal ob Sie es als SaaS, Gerät oder Software verwenden, Proofpoint bietet alle Leistungs-, Flexibilitäts-, Skalierbarkeits-, Anpassungs- und Endnutzerkontrollfunktionen, die für Installationen im großen Rahmen notwendig sind.

Jede einzelne Komponente des Proofpoint-Systems ist dazu entwickelt, die strengen Anforderungen von Unternehmensvorgaben zu erfüllen. Von der Hardware, dem nachrichtenoptimierten OS in Proofpoint-Geräten, bis hin zu Proofpoints einzigartiger „queue-less“ Architektur, bei der sämtliche Scanfunktionen in den Nachrichten im Speicher ausgeführt werden können, bietet Proofpoint die hohe Leistung und Sicherheit, die in den anspruchsvollsten Anwendungen benötigt wird.

Die Proofpoint-Anwendungen skalieren unbegrenzt und können pro Tag mehrere Millionen Nachrichten unterstützen. Sie können einfach in Master/Agent-Konfigurationen eingesetzt werden, um komplexe oder geografisch voneinander entfernte Rechenzentren zu unterstützen – so bieten Sie die Sicherheit von 100 %-iger Redundanz kombiniert mit der Bequemlichkeit einer einzigen Verwaltungsoberfläche. Proofpoint unterstützt sogar hybride Installationen, bei denen Hardware, virtuelle Geräten und SaaS zusammenarbeiten.

Mit Proofpoints optimal skalierbarer Architektur können Sie sämtliche Agent-Server von einer einzigen Master-Konsole aus bedienen. Automatische Konfigurationsübertragung, eine zentrale Nachrichtenquarantäne und zentrale Berichte vereinfachen die Wartung und reduzieren die Gesamtbetriebskosten.

Proofpoint reduziert die Gesamtbetriebskosten außerdem dadurch, dass es sich leicht in jede IT-Infrastruktur integrieren lässt, egal wie sie verbreitet ist. Eine auf einer grafischen Benutzeroberfläche basierende LDAP-Kommandokonsole und Microsoft Active Directory®-Unterstützung machen die Verzeichnisserverintegration einfach. Proofpoint ist auch kompatibel mit – und minimiert die Last auf – überlasteten E-Mail-Server-Lösungen, einschließlich Microsoft Exchange®, Lotus Notes®, bzw. jedem anderen SMTP-E-Mail-Server.

kostenlose Testversion—testen sie heute!

Überzeugen Sie sich selbst von Proofpoints Stärken. Besuchen Sie www.proofpoint.com/trial und registrieren Sie sich für den Download einer 45-Tage-Testversion von Proofpoints Virtual Edition. Oder besuchen Sie www.proofpoint.com/trypod und registrieren Sie sich für einen kostenlosen Test unserer Vorzeige-SaaS-E-Mail-Sicherheitslösung Proofpoint ENTERPRISE.

Proofpoint spricht Ihre Sprache

Zusätzlich zu hervorragenden Leistungen gegen Spam in jeder Sprache, erkennen und „verstehen“ Proofpoints Richtlinien- und Contentscanner Text in jeder Sprache, einschließlich Multi-Byte-Sprachen. Die Data Loss Prevention-Richtlinien können nichtenglische Schlüsselwörter und Terminologie aus Wörterbüchern in internationalen Schriftsprachen, einschließlich Japanisch, Chinesisch und Kyryllisch abgleichen. Die Administratoren können Richtlinien erstellen, die je nach der Sprache, die in einer E-Mail entdeckt wird, greifen. Sie können beispielsweise sprachspezifische Disclaimer zu ausgehenden Nachrichten hinzufügen – je nach der Sprache, in der die Nachricht geschrieben wurde.

Die Endnutzerinterfaces für Message Digests und webbasierte Quarantäne sind in Deutsch, Chinesisch (Traditionell und vereinfacht), Niederländisch, Englisch, Finnisch, Französisch, Italienisch, Japanisch, Polnisch, Portugiesisch, Russisch, Spanisch, und Schwedisch verfügbar.

Proofpoints administrative grafische Benutzeroberfläche, die Produktdokumentation und die Onlinehilfe sind momentan in Englisch und Japanisch verfügbar. Genau wie bei Proofpoints Endnutzerinterfaces können die Administratoren Ihre bevorzugte Sprache individuell einstellen.

Geräteversionen

Das Proofpoint Messaging Security Gateway-Gerät ist in einer Vielzahl von Hardware-Konfigurationen erhältlich, welche Installationen jeder Größe unterstützen können. Für aktuelle Informationen über die Proofpoint Geräteversionen besuchen Sie bitte:

www.proofpoint.com/products/msg.php

Unterstützte Browser

Sämtliche Konfigurations- und Verwaltungsaufgaben geschehen über Proofpoints zu 100 % browserbasierte Oberfläche. Unterstützte Browser umfassen:

Microsoft® Internet Explorer 6.0 oder höher
Mozilla Firefox 2.0 oder höher
Safari 3.1.1 (nur Endnutzer-Interface)

©2009 Proofpoint, Inc. Proofpoint und Proofpoint Protection Server sind eingetragene Marken von Proofpoint, Inc. in den USA und anderen Ländern. Proofpoint on Demand, Proofpoint Messaging Security Gateway, Proofpoint Email Firewall, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Dynamic Update Service, Proofpoint MLX, Proofpoint Dynamic Reputation, Proofpoint netMLX, Proofpoint Smart Search, Proofpoint ENTERPRISE, Proofpoint PROTECT, Proofpoint SHIELD, Proofpoint ARCHIVE und Proofpoint Messaging Security Console sind eingetragene Marken von Proofpoint, Inc. in den USA und anderen Ländern. Alle anderen hierin genannten Marken sind im Besitz Ihrer jeweiligen Eigentümer. 09/09