

HOSTED WEB SECURITY

ANALYSTENSTIMME

“Das Internet hat sich zur bevorzugten Angriffsplattform von Hackern und Cyberkriminellen entwickelt, über die sie Malware in Umlauf bringen und Identitätsdiebstahl, Finanzbetrug und Industriespionage begehen.”

IDC Worldwide IT Security Software, Hardware, and Services 2009 – 2012 Forecast and 2007 Vendor Shares: The Big Picture

DER MESSAGELABS-UNTERSCHIED

- Fortschrittliche Architektur für unübertroffenen Schutz bei minimaler Auswirkung auf die Netzwerkleistung
- Hervorragende Service-Level-Vereinbarungen (SLAs) mit Rückerstattungsanspruch, falls vereinbarte Servicequalitätsstufen nicht eingehalten werden
- Zentrale Verwaltungskonsole und protokollübergreifende Bedrohungsinformationen für E-Mail-, Internet- und Instant Messaging-Dienste für mehr Schutz, Übersicht und Kontrolle
- Kostenloser, rund um die Uhr und in 10 Sprachen verfügbarer weltweiter Support durch SaaS-Spezialisten

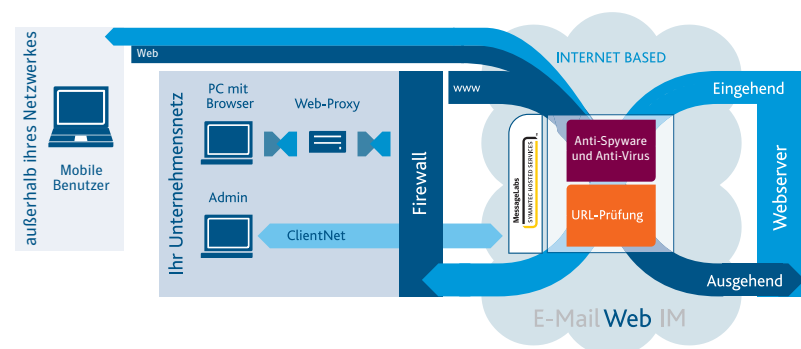
WIE ÜBERWACHEN UND SCHÜTZEN SIE DEN INTERNETDATENVERKEHR IN IHREM UNTERNEHMEN?

Das Internet gehört in vielen Unternehmen zum Geschäftsalltag. Doch noch nie waren die Risiken größer. Angreifer nutzen das Internet inzwischen als Hauptplattform zur Verbreitung von Viren und Spyware. Benutzer, die infizierte Websites besuchen, können unwissentlich Malware herunterladen, die es auf vertrauliche Informationen abgesehen hat.

Unternehmen haben zudem erkannt, dass es unerlässlich ist, Richtlinien für die Nutzung des Internets festzulegen und durchzusetzen, um eine optimale Produktivität zu erreichen, Datenverluste einzugrenzen und rechtliche Risiken zu vermeiden. Mit der weit verbreiteten Nutzung von Web 2.0-Anwendungen und sozialen Medien steigen auch die Chancen für einen Missbrauch des Internets.

Der MessageLabs Web Security-Service blockiert über das Internet übertragene Viren, Spyware-Programme und Phishing-Bedrohungen und kontrolliert den Internetdatenverkehr mithilfe von URL-Filtertechnologien. Unternehmen sind so in der Lage, ihre Nutzungsrichtlinien für die unternehmensinterne Internetnutzung durchzusetzen. Der MessageLabs Web Security-Service arbeitet auf der Internetebene und blockiert Bedrohungen, bevor sie Ihr Netzwerk erreichen. Mithilfe von URL-Filtern lässt sich der Internetzugriff nach Kategorie, Benutzer, Uhrzeit, URL oder Dateityp einschränken. Der Roaming User Support weitet den Schutz und die Richtlinien durchsetzung auf Mitarbeiter aus, die von außerhalb des Unternehmensnetzwerks auf das Internet zugreifen.

INTERNETSICHERHEIT UND -KONTROLLE – DIE MESSAGELABS-LÖSUNG



Der MessageLabs Web Security-Service wird unter minimaler Auswirkung auf die Netzwerkleistung über unsere globale Infrastruktur aus hoch verfügbaren Rechenzentren mit Lastverteilung bereitgestellt. Sie erhalten so einen schnellen, effizienten und lückenlosen Schutz, ohne dass die Produktivität Ihrer Benutzer beeinträchtigt wird. Die Lösung lässt sich sehr einfach installieren und verwalten. Die Bereitstellung des Service erfolgt auf der Grundlage hervorragender Service-Level-Vereinbarungen (SLAs). Kostenloser, rund um die Uhr und in 10 Sprachen verfügbarer weltweiter Support durch SaaS-Spezialisten vervollständigt das Angebot.

WIE FUNKTIONIERT DER SERVICE?

- Internetanfragen werden über MessageLabs geleitet und mit Ihren unternehmensinternen Nutzungsrichtlinien abgeglichen.
- Wird kein Verstoß gegen die Richtlinien festgestellt, kann die Anfrage passieren.
- Kommt es zu einem Richtlinienverstoß, wird die Anfrage entweder protokolliert und anschließend freigegeben, oder der Zugriff auf die angeforderte Webseite wird blockiert.
- Angeforderte Websites werden von MessageLabs geladen und auf bekannte sowie neu auftretende Internetbedrohungen gescannt, bevor sie in Ihr Netzwerk zugestellt werden.
- Neue und konvergierende Malware-Bedrohungen werden von Skeptic™ identifiziert, während die Identifizierung von bekannten Bedrohungen mithilfe mehrerer Malware-Signatur-Engines erfolgt.
- Wird eine Bedrohung erkannt, wird der Zugriff auf die angeforderte Webseite verweigert.
- Wird keine Bedrohung erkannt, wird die Seite dem Benutzer ohne merkbliche Verzögerung zugestellt.

SERVICE-LEVEL-VEREINBARUNG (SLA)

MessageLabs kann unterschiedliche Service-Level zu folgenden Aspekten anbieten:

- Erkennungsrate für bekannte Viren
- Durchschnittliche Scan-Zeiten
- Serviceverfügbarkeit
- Technischer Support/Reaktion auf Vorfälle: Reaktionszeiten für kritische, schwere und geringfügige Vorkommnisse.

DER NÄCHSTE SCHRITT

Sprechen Sie mit einem Produktspezialisten:
 DACH: +49 800 66 47 453
 info@messagelabs.com



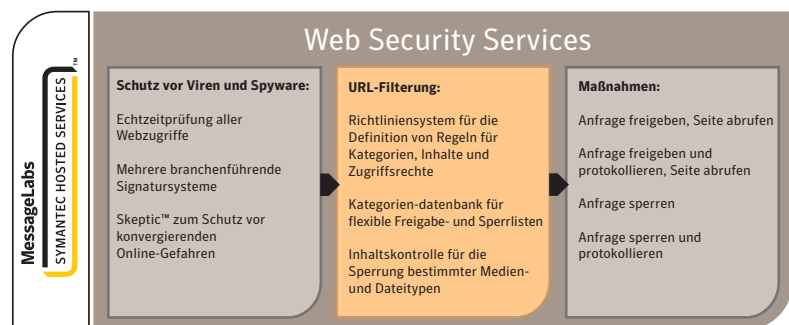
Confidence in a connected world.

MessageLabs Web Security umfasst zwei Kernkomponenten:

Mehrstufige Sicherheit – Mehrere handelsübliche Anti-Spyware- und Anti-Virus-Engines scannen Internetinhalte auf Malware. Diese Engines werden fortlaufend von MessageLabs aktualisiert, so dass bekannte Bedrohungen zuverlässig erkannt werden. Darüber hinaus schützt die unternehmenseigene heuristische Skeptic™-Technologie von MessageLabs vor neuen und konvergierenden Bedrohungen, die Internetbenutzer über andere Protokolle wie E-Mail und Instant Messaging angreifen können.

URL-Filter – Sämtliche Internetanfragen werden mit einer hochentwickelten Richtlinien-Engine und URL-Kategorisierungsdatenbank abgeglichen, um sicherzustellen, dass zulässige Inhalte verfügbar bleiben und eingeschränkte Inhalte eine sorgfältige Kontrolle durchlaufen. Die hochflexible und intuitive Richtlinien-Engine ermöglicht es Unternehmen, Richtlinien für bestimmte Benutzer und Gruppen zu erstellen und deren Verhalten zu überwachen.

MessageLabs bietet eine zentrale integrierte Verwaltungskonsolle für E-Mail, das Internet und Instant Messaging. Die Vorteile sind eine vereinfachte Verwaltung, niedrigere Gesamtbetriebskosten und ein besserer Überblick über das Benutzerverhalten. Bedrohungsinformationen werden gemeinsam von verschiedenen Kommunikationsprotokollen genutzt, so dass der Schutz weiter verbessert wird.



FUNKTIONEN	VORTEILE
Mehrstufige Anti-Virus- und Anti-Spyware-Abwehr, die auf der Internetebene ansetzt	Blockiert Viren und Spyware, bevor sie in Ihr Netzwerk eindringen
Unternehmenseigene heuristische Skeptic™-Technologie mit Rasterverarbeitung	Schützt vor neuen und konvergierenden Malware-Bedrohungen, die sich auf E-Mail-, Internet- und Instant Messaging-Protokollplattformen verbreiten
Verteilte globale Architektur für minimale Auswirkungen auf die Netzwerkleistung	Ermöglicht sicheres Surfen ohne merkbliche Verzögerungen
Vielseitig konfigurierbare Engine für die Erstellung von URL-Filterrichtlinien	Ermöglicht es Unternehmen, durch Einschränkung des Zugriffs auf unerwünschte Websites und Inhalte eine unsachgemäße Nutzung des Internets zu unterbinden
Roaming User Support	Weitet den Schutz und die Richtliniendurchsetzung auf Mitarbeiter außerhalb des Unternehmensnetzwerks aus
Cache-Filter für Suchmaschinen	Identifiziert die Herkunft von Cache-Inhalten und wendet entsprechende Kontrollrichtlinien an
Dashboard-, Übersichts- und Detailberichte sowie Berichterstellung nach Terminplan	Bietet eine bessere Übersicht und Kontrolle über die Effektivität des Service
Zentrale Verwaltungskonsolle für E-Mail-, Internet- und Instant Messaging-Sicherheit	Vereinfacht die Verwaltung und bietet ein hohes Maß an Schutz, Kontrolle und Übersicht