

eXpurgate 3.0

**E-Mail-Sicherheit der nächsten Generation
Lösungen für ISPs und Carrier**

E-Mail-Sicherheit der nächsten Generation für ISPs und Carrier

eXpurgate 3.0 ist integrierte E-Mail-Sicherheit der nächsten Generation. eXpurgate 3.0 stellt sicher, dass die E-Mail-Kommunikation in jeder Situation aufrechterhalten bleibt,

schützt zuverlässig vor Spam, Viren, Phishing und anderer Malware, verhindert False Positives und entlastet die E-Mail-Infrastrukturen.

➔ **Höchste Spam-Erkennung bei Zero False Positives**

- » Spam-Erkennungsrate > 99%
- » False-Positive-Rate < 0,00001%

➔ **Höchste Leistungsfähigkeit**

E-Mail-Durchsatz von bis zu mehr als 5.000 E-Mails und Verarbeitung von mehr als 25.000 Verbindungen pro Sekunde: eXpurgate 3.0 ist die weltweit leistungsstärkste E-Mail-Sicherheitslösung für ISPs und Carrier.

➔ **Einsparung von Hardware**

eXpurgate erfordert keine zusätzliche Hardware. Durch die erhebliche Entlastung der E-Mail-Infrastruktur (z. B. im Reject-Modus) können ISPs und Carrier sogar Hardware einsparen.

➔ **Hohe Skalierbarkeit**

eXpurgate ist hoch skalierbar und ideal für ISPs und Carrier mit mehreren Millionen E-Mail-Accounts.

➔ **Einfache Integration in bestehende E-Mail-Infrastrukturen**

eXpurgate kann mühelos in jede bestehende E-Mail-Infrastruktur integriert werden. Dies gilt für die Inhouse-Lösung wie für das SDK.

➔ **Optimaler Datenschutz**

Das eXpurgate Prüfverfahren greift nicht auf die Inhalte der geprüften E-Mail zu und erfüllt damit auch strengste Datenschutzrichtlinien.

➔ **Kein Wartungsaufwand**

Nach der Installation benötigt eXpurgate weder Wartung noch regelmäßige Updates.

➔ **Outbound-Schutz**

eXpurgate bietet die Möglichkeit, auch den ausgehenden E-Mail-Verkehr auf Spam, Viren und andere Malware zu prüfen. Damit wird verhindert, dass die E-Mail-Infrastruktur von ISPs und Carrier zum Malware-Versand missbraucht wird. eXpurgate schützt alle Einlieferungsmöglichkeiten (z. B. Webmail, SMTP).

➔ **Reject-Modus**

Der Reject-Modus ermöglicht die Identifikation und Abweisung von Spam noch während der Einlieferung am E-Mail-Server. Durch den verfahrensbedingten Ausschluss von False Positives bei individuellen E-Mails ist der Reject-Modus auch für ISPs und Carrier problemlos einsetzbar.

➔ **Lückenlose E-Mail-Sicherheit**

Gemeinsam mit der E-Mail-Firewall enSurance und dem eXpurgate Virenschutz mit Virenfrüherkennung bietet eXpurgate einen lückenlosen Schutz der gesamten E-Mail-Infrastruktur.

➔ **Zukunftsfähigkeit**

eXpurgate ist flexibel um neue Funktionen erweiterbar und damit optimal auf zukünftige Herausforderungen und Gefahren vorbereitet.

Die Technologie

Mittelpunkt der eXpurgate Technologie ist der „Bulkcheck“. Ein eigens entwickelter Kontrollsummen-Algorithmus reduziert jede E-Mail auf einen Code von nur wenigen Bytes, der in der eXpurgate Datenbank (eXdb) mit denen anderer E-Mails verglichen wird. Wird der gleiche oder ein ausreichend ähnlicher Code häufig genug gefunden, besteht die hohe Wahrscheinlichkeit, dass es sich um Spam handelt. Mit Hilfe weiterer Prüfverfahren können

unerwünschte (Spam) zuverlässig von erwünschten Massen-E-Mails (z. B. Newsletter) unterschieden werden. Durch das Massen-E-Mail-Kriterium wird sicher verhindert, dass individuelle Nachrichten fälschlich als Spam aussortiert werden (Zero False Positives®). eXpurgate erkennt nicht nur Spam, sondern kategorisiert zuverlässig jede eingehende E-Mail, z. B. als clean, bulk oder spam.

Lösungen für ISPs und Carrier

eXpurgate für ISPs und Carrier ist verfügbar als:

➔ Inhouse-Software-Lösung

➔ SDK zur Integration in eigene Software

eXpurgate.Inhouse

eXpurgate.Inhouse wird als Plug-In in die existierende E-Mail-Infrastruktur des ISPs oder Carriers integriert. Die Prüfung und Kategorisierung der eingehenden E-Mails wird bei eleven durchgeführt, aber auf dem Server des ISPs oder Carriers bearbeitet. Aufgrund des Prüfverfahrens geschieht die Zustellung in der Regel ohne merkliche Verzögerung.

- ➔ Einfache Integration in bestehende E-Mail-Infrastruktur
- ➔ Schnittstellen u. a. für SpamAssassin und Sendmail Militer
- ➔ Keine zusätzliche Hardware nötig
- ➔ Flexible und einfache Konfiguration bis auf Nutzerebene
- ➔ Kompatibel zu allen gängigen Betriebssystemen und Plattformen (Windows, Linux, Solaris)

eXpurgate.SDK

Das eXpurgate Software Development Kit (SDK) erlaubt es, die Spam-Filter- und E-Mail-Kategorisierungstechnologie eXpurgate einfach und effizient in eigene Anwendungen zu integrieren. Die eXpurgate Technologie gewährleistet die Privatsphäre der Anwender und ist insbesondere für Anwendungen mit einem sehr hohen E-Mail-Aufkommen geeignet.

- ➔ Einfache und flexible Integration in eigene Anwendungen
- ➔ Verfügbar als C-Library, API oder SDK-Daemon
- ➔ Minimale Systembelastung

eXpurgate.Inhouse



E-Mail-Firewall enSurance

Die E-Mail-Firewall enSurance stellt die E-Mail-Kommunikation in Zeiten extremer Belastung, zum Beispiel bei Denial-of-Service-Attacken oder Spam-Wellen, sicher. enSurance identifiziert die wichtigsten Kommunikationspartner und behandelt diese in Lastsituationen bevorzugt, während eher nachrangige E-Mails temporär abgewiesen werden. Wichtige E-Mails werden dadurch weiterhin ohne Zeitverzögerung zugestellt. enSurance ist vollständig skalierbar und arbeitet plattformübergreifend.

eXpurgate Virenschutz

Als Teil seines integrierten E-Mail-Sicherheitspakets bietet eXpurgate zusätzlich zum zuverlässigen Spam-Schutz eine umfassende Anti-Virus-Lösung, die aus drei Komponenten besteht, deren Kombination die optimale Identifizierung bekannter Viren ermöglicht:

- ➔ eXpurgate Virus-Outbreak-Detection (Virenfrüherkennung)
- ➔ codebasierter Virenschutz
- ➔ signaturbasierte Anti-Virus-Software AntiVir

E-Mail-Sicherheit Made in Germany

eX Das Unternehmen

eleven ist der führende deutsche Anbieter integrierter E-Mail-Sicherheitslösungen für Unternehmen, ISPs und öffentliche Einrichtungen jeder Größe. eleven bietet ausgelagerte Managed Services sowie Inhouse-Software-Lösungen. Das 2001 in Berlin gegründete Unternehmen prüft täglich mehr als eine Milliarde E-Mails. Weltweit setzen über 30.000 Unternehmen die E-Mail-Sicherheitslösungen „Made in Germany“ ein. Unter den Kunden von eleven befinden sich führende Internet Service Provider (ISP) und Telekommunikationsdienstleister wie T-Online, O2 und Vodafone, namhafte Großunternehmen, darunter Mazda, Air Berlin, DATEV, Tobit Software AG und die Landesbank Berlin, sowie führende Bildungseinrichtungen wie die Freie Universität Berlin.

eXpurgate – bei führenden ISPs und Carriern im Einsatz:



➔ Spam-Erkennungsrate:

über

99%

➔ False-Positive-Rate:

unter

0,00001%

➔ Durchsatz geprüfter E-Mails:

bis zu mehr als
5000
E-Mails/Sek.*

*abhängig von eXpurgate Integration und Hardware

Spotlight: O2

Seit 2007 schützt O2 Germany seine E-Mail-Kommunikation mit integrierter E-Mail-Sicherheit von eleven. O2 hatte nach einer neuen Lösung gesucht, um auch in Zukunft für ein weiter steigendes Spam-Aufkommen gerüstet zu sein. Den Ausschlag für die Entscheidung zugunsten von eXpurgate gaben neben der sehr hohen Spam-Erkennungsrate der verfahrensbedingte Ausschluss von False Positives bei geschäftsrelevanten Nachrichten sowie der geringe Administrationsaufwand und Hardware-Einsatz der Lösung.

„Wir haben eine Lösung gesucht, die sowohl weiteres Spam-Wachstum bewältigen als auch zukünftige neue Spam-Varianten schnell und zuverlässig identifizieren kann. Beides leistet eXpurgate zuverlässig.“

Dr. Klaus Schäfer,

Leiter Mobile Portale der Telefónica O2 Germany

Kostenloser Test

Testen Sie eXpurgate als Managed Service

30 Tage lang - kostenlos!

➔ Bequem auf www.eleven.de

oder kontaktieren Sie unser Vertriebsteam:

➔ E-Mail vertrieb@eleven.de

eleven – Gesellschaft zur Entwicklung und Vermarktung von Netzwerktechnologien mbH

Hardenbergplatz 2 | 10623 Berlin

fon: +49 (0)30/56 00 52 - 0 | fax: +49 (0)30/56 00 52 - 299

e-mail: info@eleven.de | web: www.eleven.de

Stand: Februar 2009