

*eSafe ist eine Lösung für Secure Content Management,
die weit über das Leistungsangebot der wichtigsten
Wettbewerber hinausgeht.*

IDC, 2004

eSafe®

PROACTIVE CONTENT SECURITY



- ***Umfassende Content Security***
- ***Sicheres Web-Browsing***
- ***Anti-Spyware***
- ***Proaktive E-Mail-Sicherheit***
- ***Spam-Management***

Aladdin®
SECURING THE GLOBAL VILLAGE

+ Content Security im Zeitalter von Malware

Ein sicherer Datenverkehr ist grundlegend für den Erfolg von Unternehmen. Es gibt zahlreiche Bedrohungen, die über das Web oder per E-Mail ins Netzwerk gelangen können: Spyware, Spam, neue und unbekannte Viren, Würmer, File-Sharing Applications, Blended Threats, unproduktive Internetinhalte u.v.m.

Als Sicherheitsverantwortlicher Ihres Unternehmens möchten Sie sicherlich nicht Ihre gesamte Zeit damit verbringen, den aktuellen Virenupdates hinterherzulaufen oder Spyware-infizierte Rechner von Angestellten zu bereinigen. Sie müssen sich darauf verlassen können, dass Dateninhalte, die in Ihr Unternehmensnetzwerk gelangen, sicher sind.

Laut Analysten betrug im Jahr 2004 der finanzielle Schaden durch Content Security Verletzungen, inklusive Malicious Code, Viren, Trojaner, Spyware etc. - bis zu \$169 Milliarden, einigen Statistiken zufolge sogar \$204 Milliarden. Daher wurde 2004 als das Jahr mit den bisher meisten Angriffen eingestuft. Diese Zahlen beinhalten Faktoren wie Helpdesk Support-Kosten, Überstundenbezahlung, eingeschränkte Produktivität, Wiederherstellungskosten und Software-Upgrades. Bei ungefähr 600 Millionen Windows-basierten Rechnern weltweit ergibt das eine Schadenssumme zwischen \$281 und \$340 pro Rechner* – eine Summe, die Unternehmen in Ihrem Endgewinn beeinflusst.

Dabei sind verlorene Zeit, Geld und die Verlangsamung der Netzwerk-Performance nicht die einzigen Gründe, worüber sich Security Manager Sorgen machen müssen. Wirksame Content Security für Unternehmen umfasst ein mehrschichtiges Schutzkonzept von proaktivem Anti-Virus über E-Mail Compliance bis zu Web/URL-Filter und mehr. Falls Ihre Lösung nicht über all diese Schutzmechanismen verfügt, ist Ihr Netzwerk Gefahren ausgesetzt.

*Quelle: mi2g, 2004

eSafe bietet eine umfassende Plattform für den Schutz vor einer Vielzahl unterschiedlicher Angriffe, anstelle einzelner Punktlösungen. Für zahlreiche Kunden ist es daher eine sehr gefragte Lösung.

Chris Christiansen
Program Vice President, IDC



PROACTIVE
CONTENT
SECURITY

+ Mehrschichtige Content Security

eSafe ist eine leistungsstarke Content Security-Lösung, die Ihr Netzwerk schnell und proaktiv vor bekannten und unbekanntem böswertigen Codes, Spam sowie unproduktiven und unerwünschten Inhalten schützt. Mit dieser Lösung verfügen Sie über eine mehrschichtige Schutzstrategie, die sich dank der umfassenden Integrationsmöglichkeiten einfach implementieren und verwalten lässt. eSafe ist eine umfassende Sicherheitslösung, die alle Ebenen der Content Security abdeckt. Sie beinhaltet:

Proaktiver Virenschutz: Blockt den Großteil an "Zero-Hour" böswertigen Codes, einschließlich Würmern und Trojanern. Signaturbasierter Virenschutz: Blockiert gemäß ICASA- und Checkmark-Zertifizierung 100 % aller In-The-Wild-Viren (ITW)

Exploit-/Hacker-Schutz: Blockt proaktiv Angriffe auf Sicherheitslücken über E-Mails und Webseiten.

- Scannen des HTTP-Protokolls und Erkennung von Exploits
- HTML -Überprüfung hinsichtlich böswertiger Skripts und Exploits in Webseiten, Webmail und E-Mail-Text
- E-Mail-Standardisierung gemäß RFC-Standards verhindert das Ausnutzen bekannter und unbekannter Exploits

E-Mail-Sicherheit: Schutz des E-Mail-Verkehrs durch Überprüfung von Text und Dateianhängen

Web-/URL-Filtering basierend auf Kategorien, Inhalten und Dateitypen

Application-Filtering für Würmer, Spyware, IM, P2P, Remote-Access-Anwendungen und Tunneling

Spam-Management filtert ungewünschte Massen-E-Mails heraus und spart Zeit und Geld

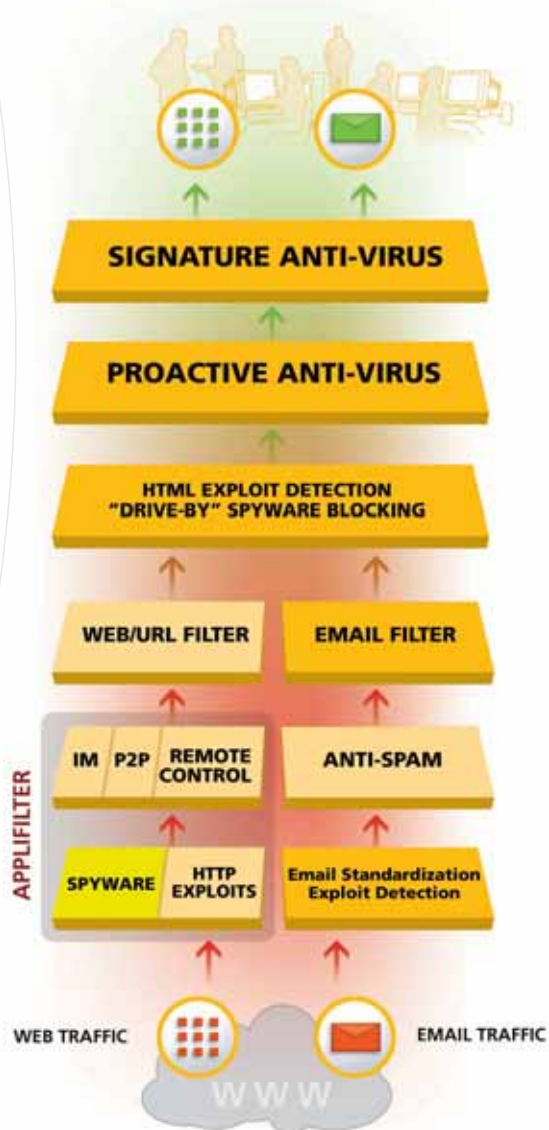
Spyware-Abwehr auf vier Ebenen

Ebene 1: Blockierung von unbewussten Spyware-Installationen

Ebene 2: Blockierung des Spyware-Downloads

Ebene 3: Blockierung anhand der Spyware-Signatur

Ebene 4: Blockierung der Spyware-Kommunikation



+ Secure Content Management (SCM)

Die Implementierung von Content Security im Zeitalter des schnellen Internet

Die Anforderungen an die Perimetersicherheit lassen sich in Netzwerksicherheit und Secure Content Management (SCM) untergliedern. Netzwerksicherheit wird durch Firewalls, VPN und IDS/IPS geleistet und muss die Masse an Internetgefahren abwehren. Sie muss schnell sein, ohne zusätzlich mit Inhaltsprüfungen belastet zu werden. Content Security ist naturgemäß sehr vielseitig. Hier werden bereits in das Netzwerk gelangte Inhalte detailliert analysiert. Die Überprüfung auf dieser Ebene ist sehr zeit- und ressourcenaufwändig, so dass hierfür eine eigenständige, spezialisierte Lösung verwendet werden sollte.

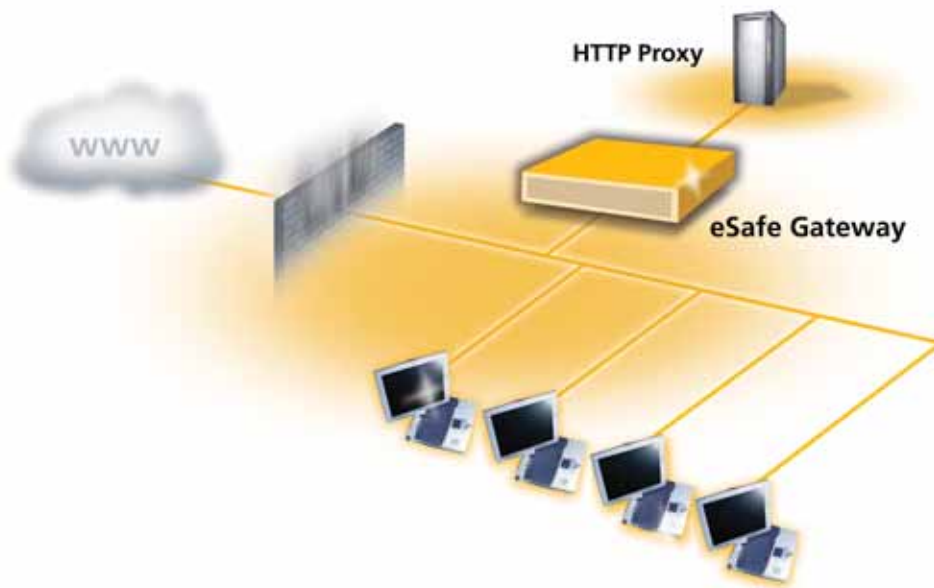


Es sind eben nicht alle Netzwerke gleich: Content Security für beliebige Netzwerkkonfigurationen

Im Gegensatz zu anderen Lösungen, die auf einer einzigen Konfiguration aufsetzen, bietet eSafe eine Auswahl verschiedener Betriebsmodusarten, die auf fast alle Netzwerkkonfigurationen jeglicher Größe angewendet werden können.

- **Sicheres SMTP-Relay:** überprüft alle E-Mails, verwaltet Spam und schützt vor SMTP-Hackerattacken
- **NitroInspection Bridge:** echtes Plug-and-Play, transparente Implementierung.
Keine Veränderungen am Netzwerk erforderlich!
- **NitroInspection Router:** Inline-Implementierung mit Lastverteilungs- und Hochverfügbarkeitslösungen anderer Hersteller
- **Forwarding Proxy:** rasche und einfache Implementierung in einer Proxy-Umgebung, kein Single-Point-of-Failure
- **eSafe Security Cluster:** bietet hohe Verfügbarkeit und Lastenverteilung
- **ICAP:** ermöglicht die ICAP-Integration mit Proxy-Lösungen von BlueCoat, Cisco CE und NetApp.
- **Check Point CVP-Modus:** ermöglicht OPSEC-Integration mit Check Point FireWall-1, einschließlich Unterstützung für Check Point ELA sowie AMON-Prüfung und Berichtsfunktionen für die Firewall

SAMPLE DEPLOYMENT MODE Bridge Mode with Proxy



Das Dilemma in Breitband-Netzwerken

Die Verbindungsgeschwindigkeiten in das Internet werden in kleinen Unternehmen zunehmend schneller, von Großunternehmen gar nicht zu sprechen. Unternehmen, die mit Hochgeschwindigkeit ins Internet gehen, stehen vor der Herausforderung, alle Inhalte des gesamten Web-Verkehrs zu überprüfen. Viele Unternehmen setzen hier nur unzureichende Lösungen ein oder nehmen im schlimmsten Fall gar keine Überprüfungen vor.

Die eSafe-Lösung

eSafe ist die einzige praktikable Lösung für eine umfassende Content Security für Highspeed-Internetverbindungen und mehrere tausend gleichzeitig erfolgende Zugriffen.

Advanced NitroInspection™ : 10X Performance

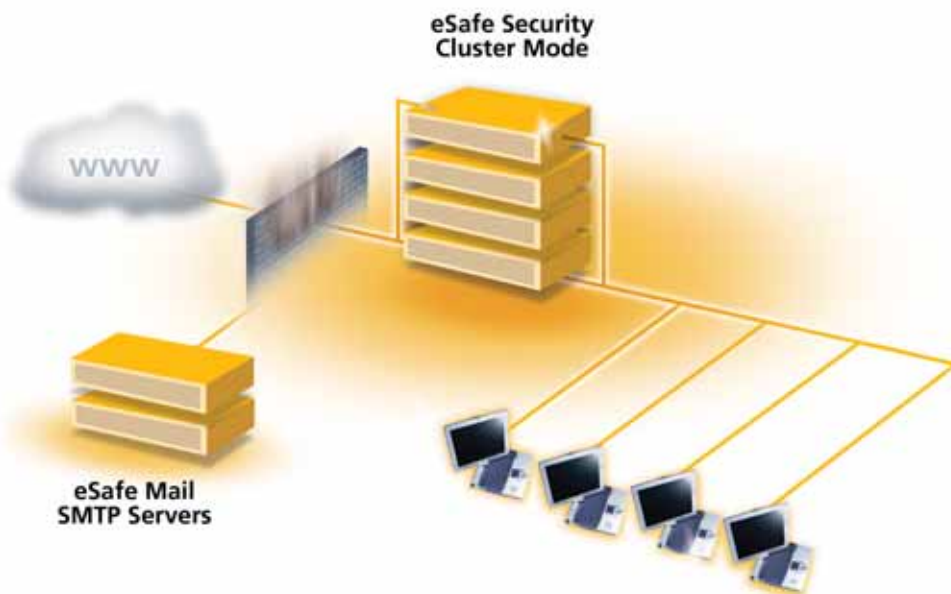
Die zum Patent angemeldete NitroInspection-Technologie sorgt dafür, dass eSafe im Vergleich zu anderen Anbietern mit einer zehnmals schnelleren Performance aufwarten kann. Im Gegensatz zu Proxy-Lösungen muss NitroInspection Inhalte vor der Prüfung nicht zuerst im Cache speichern. Die Prüfung erfolgt sofort. Die Systemleistung wird nicht ausgebremst, es gibt keine Timeouts, keine Beschwerden über zu langsame Internetverbindungen – und es wird trotzdem maximale Sicherheit gewährleistet.

10X höherer Datendurchsatz: Kompletter Content Security-Check, einschließlich aller HTML-Seiten, bei einem kontinuierlichen HTTP-Datendurchsatz von bis zu 38 Mbps je eSafe-Maschine.

10X mehr Verbindungen: Jeder einzelne eSafe-Rechner kann mehr als 1.500 gleichzeitige Verbindungen verarbeiten; dies entspricht ca. 4.000 bis 8.000 Mitarbeitern in einem Unternehmen.

eSafe Cluster: Mit integrierter Loadbalancing und Failover-Funktionalität; eine eSafe-Cluster-Konfiguration mit acht Rechnern ermöglicht eine umfassende Überprüfung des Internetverkehrs bei Geschwindigkeiten von über 200Mbps.

Mehr Sicherheit: Mit einer transparenten Überprüfung des Datenverkehrs auf allen Ports kann eSafe auch nicht-dateiebasierte Würmer und Angriffe auf Anwendungen abwehren sowie die Security Policy-Einstellungen effizient durchsetzen.



+ Proaktiver Virenschutz

Die zertifizierte Antivirus-Engine von eSafe blockt sowohl 100% der In-The-Wild Viren, als auch mehr als 100.000 Malware-Varianten (Viren, Würmer, Trojaner etc.). eSafe scannt alle MIME-Typen und komprimierten Dateien. Die Antivirus-Engine von eSafe ist ICSA Labs und WestCoast Labs Check-Mark zertifiziert und garantiert so die Einhaltung gängiger Anti-Viren-Standards.

eSafe-Antivirentechnologie

eSafe umfasst die Proactive Security Engine (PSE). Durch die Kombination verschiedener Technologien blockiert eSafe mit PSE sogar den Großteil aller "Zero-Hour" bösartigen Codes. Das Ergebnis ist ein hochperformantes System, denn langsame und nicht effiziente Lösungen sind für die heutigen schnellen Netzwerke nicht tragbar. NitroInspection™ von eSafe ist eine Hochgeschwindigkeitslösung, die alle Schlüsseltechnologien am Gateway des Unternehmens effizient einsetzt.



Die proaktive Security Engine (PSE) von eSafe gewährleistet in Verbindung mit der NitroInspection Technologie eine Hochgeschwindigkeitslösung zur Inhaltsprüfung ohne dabei die kleinsten Sicherheitsanforderungen zu vernachlässigen

Ghost Machine® bietet proaktiven Schutz vor hochentwickelten, verschlüsselten, verborgenen und polymorphen Viren. Ghost Machine blockiert zudem die Mehrheit aller Remote-Access Spionage-Trojaner, noch bevor ein Update verfügbar ist.

SmartScript™ sorgt für eine proaktive Blockierung aller bösartigen Scripts in E-Mails und auf Webseiten. Die Funktionsfähigkeit aller anderen Scripts bleibt gewährleistet.

Macro Terminator™ bietet heuristische Erkennung und Blockierung von bekannten und unbekanntem Microsoft Office®-Makroviren.

Schutz gegen bösartigen Code – eSafe inspiziert alle Webseiten und heruntergeladenen Dateien sowie das gesamte E-Mail-Aufkommen und eliminiert bösartige Java-, ActiveX- und Script-Vandalen.

Schutz für Office-Dokumente – Entfernung von Makros und eingebetteten Objekten, wie z.B. selbstausführende Objekte in Microsoft Office®-Dokumenten aus ungesicherten Quellen.

+ Internetsicherheit

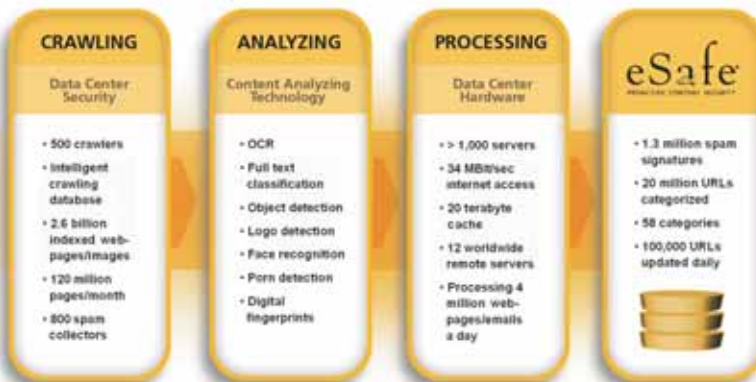
Über den herkömmlichen Virenschutz hinaus

Fälschlicherweise wird allgemein davon ausgegangen, dass die Bedrohung beim Surfen im Netz von Viren ausgeht. Tatsache ist, dass ein Virusbefall eher selten ist, falls nicht gerade Seiten mit Virusarchiven aufgesucht und Viren manuell heruntergeladen werden. Die tatsächliche Bedrohung im Internet stellen bösartige aktive Codes, Spyware und Exploits dar, die im HTTP-Protokoll und HTML-Inhalt eingebettet sind und versuchen, sich automatisch auf dem Benutzerrechner zu installieren oder zu starten. Neben der Erkennung aller standardmäßigen Viren und Anti-Spyware sowie URL-Filterung setzt eSafe zudem Richtlinien für das sichere Web-Browsing im Unternehmen mittels folgender Maßnahmen durch:

- Entfernen bösartiger und als unsicher eingestufter Scripts (SmartScript Filtering)
- Blockieren aller Script-Viren und Exploits
- Blockieren bekannter HTML- und HTTP-Exploits (XploitStopper)
- Optionales Entfernen von ActiveX-Tags
- Optionales Zulassen ausschließlich vorinstallierter, vertrauenswürdiger ActiveX-Objekte
- Optionales Entfernen von Java Applets
- Optionales Entfernen von Cookies
- Optionales Blockieren von HTML-Seiten mit vordefinierten Schlüsselwörtern
- Optionale Inhaltsprüfung verschlüsselter SSL-Seiten durch Partnerlösungen
- ... und weitere Funktionen

eSafe ermöglicht eine umfassende Internetsicherheit ohne Performance-Einbußen. Die NitroInspection -Technologie von eSafe bietet eine Echtzeitprüfung von Web-Inhalten ohne Beeinträchtigung des Benutzers. eSafe prüft nicht nur herunterladbare Dateien, sondern ermöglicht eine umfassende Prüfung von HTML-Inhalten sowie das Scannen aller Bilddateien hinsichtlich bekannter Exploits von JPG- und BMP-Formaten. eSafe ist die skalierbarste auf dem Markt erhältliche Content Security-Lösung und kann als Bridge, Router oder Proxy installiert werden. Zudem enthält sie einen integrierten Lastenausgleich.

Website-Filtering



Das optionale URL-Filtermodul von eSafe baut auf die weltweit größte und konsistenteste Datenbank klassifizierter URLs auf, die über 20 Millionen Einträge, 58 Kategorien und mehr als 100.000 tägliche Updates umfasst.

+ Spyware-Abwehr auf vier Ebenen

Die Bedrohung

Spyware ist mehr als nur eine Belästigung. Sie stellt eine ernst zu nehmende Gefahr für Unternehmen dar, weil sie:

- Private und persönliche Informationen sammelt
- Sich urheberrechtlich geschützte oder vertrauliche Daten aneignet
- Irreparable Systemschwächen erzeugt
- Rechtmäßig installierte Anwendungen oder Prozesse schädigt oder stört
- Eine Hintertür zu infizierten Systemen öffnet
- Spyware-Betreibern die Möglichkeit gibt, Kontrolle über ein infiziertes System zu erlangen



eSafe Applifilter bietet vier Schutzebenen gegen Spyware. Das Spyware Neutralizer Add-on entfernt per Remote Spyware, die auf Client-PC installiert wurde.

+ Application-Filtering

eSafe, die umfassende proaktive Content Security-Lösung, enthält den AppliFilter™ – eine neue Technologie, die vor folgenden Bedrohungen auf Applikationsebene schützt:

- Gateway-basierte TCP/IP, nicht dateigebundene Angriffe mittels bössartigen Codes wie Nimda und CodeRed
- P2P (Peer to Peer)-Filesharing wie KaZaa, eDonkey und BitTorrent
- Instant Messengers wie ICQ, MSN, AOL und Yahoo! Messengers
- Adware/Spyware-Komponenten, wie sie in zahlreicher kostenloser und kommerzieller Software zu finden sind
- Unautorisiertes HTTP-Tunneling und Durchsetzung von HTTP-Protokollen

Einige der Vorteile der AppliFilter™-Technologie sind:

- Echtzeit-Filterung von unterschiedlichem Malicious Internet Content beim Versuch, in das Unternehmensnetzwerk einzudringen
- Ähnliche Funktionsweise wie ein aktives Intrusion Detection System (IDS): jeglicher Inhalt wird überprüft, für den Endanwender bleibt der Vorgang transparent
- Einfache Handhabung und Anwendung
- Ermöglicht der eSafe NitroInspection-Engine, den gesamten Verkehr am Gateway zu überprüfen. Die durchlaufenden Datenpakete werden analysiert und Traffic blockiert, der als bössartig, unangemessen oder anderweitig unzulässig eingestuft wird

Instant Messaging verbreitet sich in Unternehmen immer mehr und gibt Anlass zu neuen Sicherheitsbedenken.

Instant-Messaging-Systeme sind ideale Angriffspunkte für Hacker. Diese nutzen die Instant Messenger als Tunnel, durch den sie die Firewall von Unternehmen umgehen und mühelos in das System eindringen können.

Information Week

APPLICATION
FILTERING

+ E-Mail-Sicherheit

eSafe Mail pr oaktiver Schutz vor E-Mail-Inhalten und Spam-Management

eSafe Mail ist ein sicheres Mail-Relay, das eine umfassende und integrierte E-Mail-Sicherheit und schnelle Performance bietet. eSafe Mail schützt alle ein- und ausgehenden SMTP- und POP3-Verbindungen und kann sowohl als sicheres Stand-alone Mail-Relay oder als Teil von eSafe Gateway implementiert werden. Bei Verwendung mit eSafe Gateway werden Webmails ebenfalls blockiert.

Sieben E-Mail-Bedrohungen: Ein Schutzsystem

- 1. Viren** – Bekannte Viren werden mit der leistungsstarken Anti-Virus-Engine von eSafe abgewehrt. Unbekannte Viren und andere Malicious Codes (ActiveX, Java) werden durch den Einsatz verschiedener proaktiver eSafe-Technologien blockiert.
- 2. Exploits** gefährden die Sicherheit und werden von Hackern für die Übertragung sich rasch verbreitender bösartiger Codes verwendet. eSafe erkennt und blockiert Malicious Codes, die sich über Sicherheitslücken Zugang zum System verschaffen möchten.
- 3. Bösartige Scripts** können einfach, rasch erstellt und verbreitet werden. eSafe blockiert proaktiv ALLE bösartigen Scripts.
- 4. Spam** stellt ein erhebliches Ärgernis dar, das Unternehmen nicht nur Zeit sondern auch Ressourcen kostet. eSafe blockiert die Mehrzahl aller Spams und ermöglicht so Zeit- und Kosteneinsparungen.
- 5. Cookies** können vertrauliche Daten speichern und damit Spam fördern. eSafe blockiert Cookies aus nicht vertrauenswürdigen Quellen und aus allen E-Mails.
- 6. MS Office-Dokumente** können Makroviren und eingebetteten bösartigen Code enthalten. eSafe entfernt Makros und eingebettete Objekte aus verdächtigen Quellen.
- 7. Hacker-Attacken** sind vielfältig: angefangen bei Denial of Service (DoS)-Attacken über E-Mail-Spoofing bis hin zur Fälschung und Manipulation von Anhängen – eSafe bietet zahllose integrierte Schutzmechanismen.

Transparente POP3-Überprüfung

POP3 ist ein gängiges E-Mail-Protokoll zum Herunterladen von E-Mails aus Remote-Access Mail-Servern und für den Zugriff auf E-Mails, die von Service Providern gehostet werden. POP3 kann auch als Sicherheitsmerkmal in Unternehmen genutzt werden, die keinen offenen Port auf dem Mail-Server verwenden möchten. Der Schutz von E-Mail-Inhalten ist ohne eine POP3 E-Mail-Prüfung unvollständig. eSafe Gateway ermöglicht eine vollkommen transparente POP3 E-Mail-Prüfung, ohne dass POP3 Server- und Account-Details definiert und verwaltet werden müssen.

Webmail-Sicherheit

Web-basierte E-Mail-Services sind sehr beliebt. Die Benutzer loggen sich über einen Web Browser in ihren E-Mail-Account ein, und die E-Mails stehen dann als HTML-Webinhalt zur Verfügung, der mittels des HTTP-Protokolls übertragen wird. Ohne Web-Mail-Überprüfung ist keine E-Mail-Sicherheitslösung vollständig. eSafe Gateway und eSafe Web prüfen den gesamten HTTP-Verkehr einschließlich Webmails. Alle Inhalte, einschließlich der Dateianhänge, werden in Bezug auf bösartigen Code überprüft.

EMAIL
SECURITY

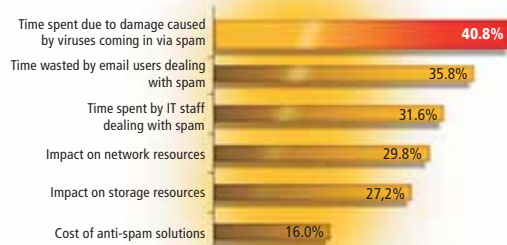


+ Spam-Mangement

Spam nimmt rapide zu, so dass Anti-Spam-Dienste immer wichtiger werden. Schätzungen zufolge betragen Spam-Mails mittlerweile über 70 % im E-Mail-Aufkommen eines Unternehmens. Internet Service Provider sehen sich mit einer deutlich wachsenden E-Mail-Flut konfrontiert, die nicht nur einen erheblichen Anteil der einem Unternehmen zur Verfügung stehenden Bandbreite belegt, sondern zudem auch negative Auswirkungen auf die Auslastung und Produktivität der Mitarbeiter hat.

Convergence of Spam and Virus

Survey Question: Rate the cost impact of various Spam related factors by severity.

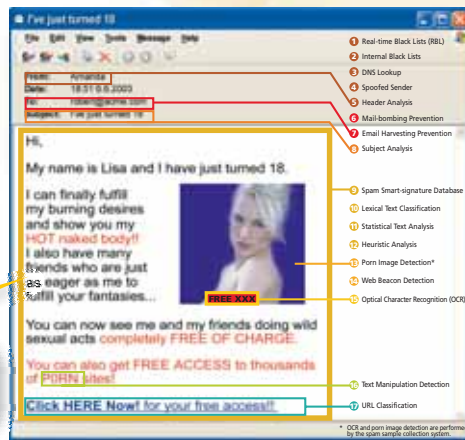


Source: The True Cost of SPAM and Value of Anti-SPAM Solutions Survey, IDC 2004

Modern spam is also a prominent source of various malicious code.

Das erweiterte Anti-Spam-Modul von eSafe eliminiert mehr als 95 % des Spam-Aufkommens mit einer False-Positives-Rate von unter 0,5 %. eSafe umfasst erweiterte Funktionen für Anti-Spam, Quarantäne-Verwaltung und Spam Tagging.

eSafe bietet eine Vielzahl an Anti-Spam-Mechanismen zur Reduzierung des Spam-Aufkommens mit einer hohen Erfolgsquote



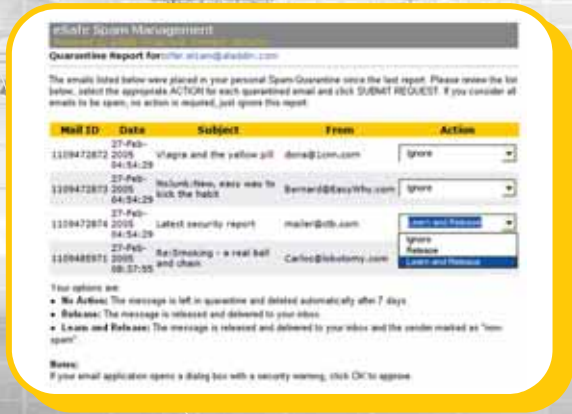
Phishing Prevention

Phishing ist eine besondere Form des Spam. Phisher bedienen sich gefälschter E-Mails und betrügerischer Websites, um sich persönliche Daten des Empfängers, wie etwa Kreditkartennummern, Bankverbindungen, Passwörter etc. des Empfängers zu erschleichen. Durch die illegale Verwendung von Firmennamen renommierter Banken, Versandhäuser und Kreditkartengesellschaften können Phisher bis zu 5 % aller Empfänger dazubringen, ihnen zu antworten. In diesem Zusammenhang sei darauf hingewiesen, dass Phishing selten mit bösartigen Inhalten verbunden ist, sondern im Rahmen von Betrugsdelikten stattfindet.

eSafe blockiert die meisten Phishing-E-Mails als Spam. Andere Phishing-Angriffe werden durch den Einsatz leistungsstarker Anti-Phishing-Methoden blockiert oder neutralisiert.

Erweiterte eSafe Funktionen für das Spam-Management

Spam-Management-Funktion	Kundenvorteil
Blockiert Spam in anderen Sprachen	Es gehen viele fremdsprachige Spam-Nachrichten ein, die nicht zum normalen E-Mail-Aufkommen des Unternehmens passen.
Entfernung von Bildern aus Spam-Nachrichten	Verhindert das Herunterladen von Bildern in Spam-E-Mails, wenn eine E-Mail als Spam gekennzeichnet ist; sie kann jedoch noch vom Empfänger angezeigt werden.
Integrierte "Honigtöpfe" für Spam	Ermöglicht den Einsatz lokaler, ausschließlich Spams vorbehaltenen Accounts, mit denen unerwünschte Spam-Nachrichten ermittelt werden können, die an das Unternehmen gesendet werden.
Anti-Spoofing-Prüfung des Absenders	Verhindert Spam, falls der Absender innerhalb der Domain angesiedelt ist.
Entfernung von E-Mail-Cookies	Verhindert künftige Spam-Angriffe nachdem ein Cookie aktiviert wurde.
Web Beacon-Erkennung	Blockiert E-Mails mit eindeutigen Identifikatoren in Bildern und Links, die dem Spammer signalisieren, dass eine E-Mail-Adresse aktiv ist.
Optical Character Recognition (OCR)* für Spam- und URL-Sammler	Erkennt Spam-Inhalte anhand von Text in Bildern. * Hierbei handelt es sich um eine Datacenter-Servicefunktion, die im Aladdin-Backend ausgeführt wird.
Erkennung von pornografischen Inhalten* für Spam und URL-Sammler	Spam- und URL-Datenbanken enthalten Signaturen von automatisch erkannten pornografischen Bildern, die von den Datenbank-Bots erfasst wurden. * Hierbei handelt es sich um eine Datacenter-Servicefunktion die im Aladdin-Backend ausgeführt wird.
URL Spam-Datenbank mit aktiven Links*	Ermittelt URLs in Spam-E-Mails und vergleicht diese mit einer Datenbank über indizierte Websites.
Vom Benutzer verwaltete Spam-Mails in Quarantäne-Verzeichnissen	Geringerer IT-Aufwand und Möglichkeit der Feinabstimmung bei der Spam-Filterung



Die sich selbstverwaltende Spam-Quarantäne entlastet Administratoren, trägt entscheidend zur Benutzerzufriedenheit bei und ermöglicht, dass Benutzer blockierte E-Mails selbst freigeben und "White Lists" erstellen können.

+ eSafe-Partnerlösungen

eSafe Appliance

Macht in 15 Minuten aus jeder beliebigen Server-Hardware eine eSafe Appliance!

eSafe[®] VIRTUAL APPLIANCE
PROACTIVE CONTENT SECURITY



Unsere Partner für eSafe-Lösungen bieten Ihnen eine Vielzahl an Hardware-Plattformen und Produktintegrationen



IBM



hp HEWLETT[®] PACKARD



SECUDOS



SecureGUARD

Hochverfügbarkeitslösungen

Crossbeam

Crossbeam-Lösungen sind Security Switches (Chassis-basiert) in modularer Bauweise. Die einzigartige Architektur mit zweistufiger Paketverarbeitung ermöglicht einen effizienten Einsatz von eSafe Clustern und eine Skalierbarkeit für besonders hohe Performance, Verfügbarkeit und Port-Dichte.

Crossbeam X-Serie

Die X-Serie von Crossbeam bietet hochwertige Sicherheitsservice-Switches für die Datenzentren großer Unternehmen und Service Provider.

CROSSBEAM[®] SYSTEMS



IBM Blade Center ist eine herausragende Hardware-Plattform für eSafe Cluster. Diese modulare Hardware braucht wenig Platz, Strom und Verkabelung und verbessert die Investitionskosten und Kapitalrendite.

BladeFusion

Blade Fusion bietet ein Diskless-Blade-System für auf IBM BladeCenter Hardware verwaltete eSafe Cluster. Ermöglicht werden sofortige und automatische Anwendungs- und Blade-Failover, Wartung und Service im laufenden Betrieb, Software- und Blade-Upgrades ohne Ausfallzeiten und Risiken, automatisches Rollback, Wiederherstellung, Replizierung und Überprüfung des Systems, automatische Leistungsüberwachung und Netzwerklastenausgleich.

BLADEFUSION
security without limits



Radware CID (Content Inspection Director)

Radware CID ist ein intelligentes Application-Switching mit ausgereifter Rerouting-Funktionalität, das eine nahtlose Integration mit eSafe Gateway und HTTP-Kapazität bis zu 2,5 Bbps bietet. Mit der herausragenden Funktionalität von CID kann der Internetverkehr eines Benutzers anhand von Benutzererkennung und Attributen (z.B. RADIUS-Attribute) umgeleitet werden, sodass ISPs nun in der Lage sind, die Inhaltsprüfung für den gesamten Internetverkehr (einschließlich HTTP) als zusätzliche Serviceleistung anzubieten. Leistungsüberwachung und Netzwerklastenausgleich.

 **radware**
availability | performance | security



Lösungen für die Überprüfung des verschlüsselten SSL-Verkehrs

Radware Certain

Radware Certain ist ein System für die Beschleunigung und Prüfung verschlüsselter Inhalte. SSL-Verkehr kann mit Gigabit-Geschwindigkeit ver- und entschlüsselt werden und bietet so umfassende Inhaltstransparenz und Überprüfungsmöglichkeiten sowie Abschirmung gegen verborgene Angriffe. Der entschlüsselte Verkehr wird zur Überprüfung an eSafe weitergeleitet. Die Identifizierung und der Abbruch ungültiger SSL-Sitzungen schützt in Echtzeit vor bösartigen SSL-Paketen und Sicherheitsverletzungen und bietet so eine umfassende Transaktions- und Netzwerksicherheit.

 **radware**
availability | performance | security



Microdasys SCIP

Die Kombination von Microdasys SCIP und eSafe bietet eine vollständige Erfüllung der Sicherheitsanforderungen verschlüsselter Inhalte durch:

- Zertifikatprüfung in Echtzeit entsprechend der Sicherheitsvorgaben und beständig aktualisierter Sperrlisten für jede aufgebaute Verbindung
- Inhaltsprüfung für den Ausschluss bösartiger, unproduktiver oder unangemessener Inhalte

Dank dieser Lösung können alle bislang übersehenen verschlüsselten Pakete, wie etwa verschlüsselte Webseiten, Web-basierte E-Mails, Instant Messaging und Chat-Inhalte, nun vollständig auf ihre Inhalte überprüft und – wenn als bösartig erkannt – blockiert werden, bevor sie in das Netzwerk des Unternehmens gelangen.

MICRODASYYS
BRIDGING THE GAP IN CONTENT SECURITY



Komplette Installation auf einem Rechner:
eSafe Gateway im Forwarding Proxy Mode mit Microdasys SCIP

eSafe
PARTNER

+ eSafe-Lösungen

eSafe ist besonders für größere Unternehmen mit hohen Sicherheitsanforderungen geeignet. Eine Vielzahl von Banken und Behörden sowie verschiedene Service Provider setzen auf eSafe und seine bewährte Kombination von hoher Sicherheit, leistungsstarker Performance sowie einfache Implementierung und Handhabung.

Lösung	Produktpositionierung	Besondere Unterscheidungsmerkmale
Sicheres Web-Browsing	<ul style="list-style-type: none"> • Anti-Spyware • Blockierung nicht autorisierter Applikationen (P2P, IM) • Blockierung von Malicious Active Content • Webmail-Sicherheit • URL-Filterung 	<ul style="list-style-type: none"> • Besonders hohe Durchsatzrate • Transparentes Tool NitroInspection™ • Integrierter Lastenausgleich und Failover • Mehrschichtige Anti-Spyware Features • AppliFilter™ • XploitStopper™
E-Mail-Sicherheit und Spam-Management	<ul style="list-style-type: none"> • Proaktiver Antivirenschutz für E-Mails • Schutz vor Exploits • E-Mail-Sicherheit und Anti-Phishing • Spam-Management 	<ul style="list-style-type: none"> • Proaktiver Schutz gegen neue Viren • XploitStopper™ • Umfassende E-Mail-Sicherheit • Spam-Management
Plattform für Services Providers (xSP)	<ul style="list-style-type: none"> • ISP: mehrstufige Mehrwertdienste für Endbenutzer (AV, AS, URLFiltering, AF) • MSP: SCM-Lösung mit Remote-Steuerung 	<ul style="list-style-type: none"> • Hoher Durchsatz • Skalierbare Lösung für jegliche bestehende Infrastruktur • Integration mit Drittanbietern zur Bereitstellung mehrstufiger Dienstleistungen • Strategische Allianz mit Anbietern von Blade-Servern

Kostenlos: Testen Sie eSafe 30 Tage lang, einschließlich vollständigem technischen Support. Weitere Informationen finden Sie auf unserer Homepage www.Aladdin.de/eSafe oder unter www.eSafe.de

Zertifizierungen



Partner



+ Über Aladdin

Aladdin Knowledge Systems (NASDAQ: ALDN) ist weltweit einer der führenden Anbieter im Bereich IT-Security und entwickelt und vertreibt auf Hard- und Software basierende Produkte und Komplettlösungen für die Bereiche Software- und Internet-Sicherheit. Das Unternehmen ist eine 100%ige Tochter der Aladdin Knowledge Systems Ltd. in Tel Aviv/ Israel. Aladdin Knowledge Systems Ltd. unterhält acht internationale Niederlassungen und ein Vertriebsnetz mit mehr als 50 Distributoren



Weitere Informationen erhalten Sie unter www.Aladdin.de/eSafe

Deutschland	T: +49-89-894 221-77	F: +49-89-894 221-40
North America	T: 1-800-562-2543, 1-847-818-3800	F: 1-847-818-3810
International	T: +972-3-636-2222	F: +972-3-537-5796
UK	T: +44-1753-622-266	F: +44-1753-622-262
Benelux	T: +31-30-688-0800	F: +31-30-688-0700
France	T: +33-1-41-37-70-30	F: +33-1-41-37-70-39
Spain	T: +34-91-375-99-00	F: +34-91-754-26-71
Israel	T: +972-3-636-2222	F: +972-3-537-5796
Asia Pacific	T: +852-2166-8605	F: +852-2166-8999
Japan	T: +81-426-607-191	F: +81-426-607-194