



Cisco Expo
2008

Secure Messaging Solutions



Daniel Wolf, Sales Manager / Austria
Achim Kraus, Systems Engineer / Central Europe

Agenda

Aktuelle Bedrohungen

Technische Aspekte und Bedrohungen anhand von aktuellen Beispielen aus der Praxis.

Lösungsansätze

Wege der Gefahrenabwehr durch mehrschichtige und reputationsbasierte Gateway-Lösungen.



Aktuelle Herausforderungen

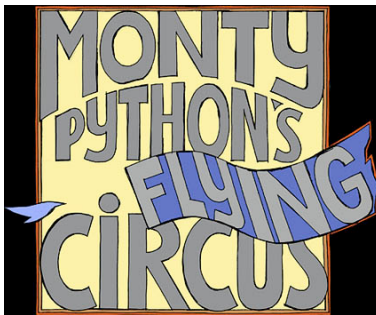
"Spicy Pork And Meat"

Hormel Foods Corporation



Erste Spam-E-mails?

- April 1994



Neues Bot-Netz an einem Tag?

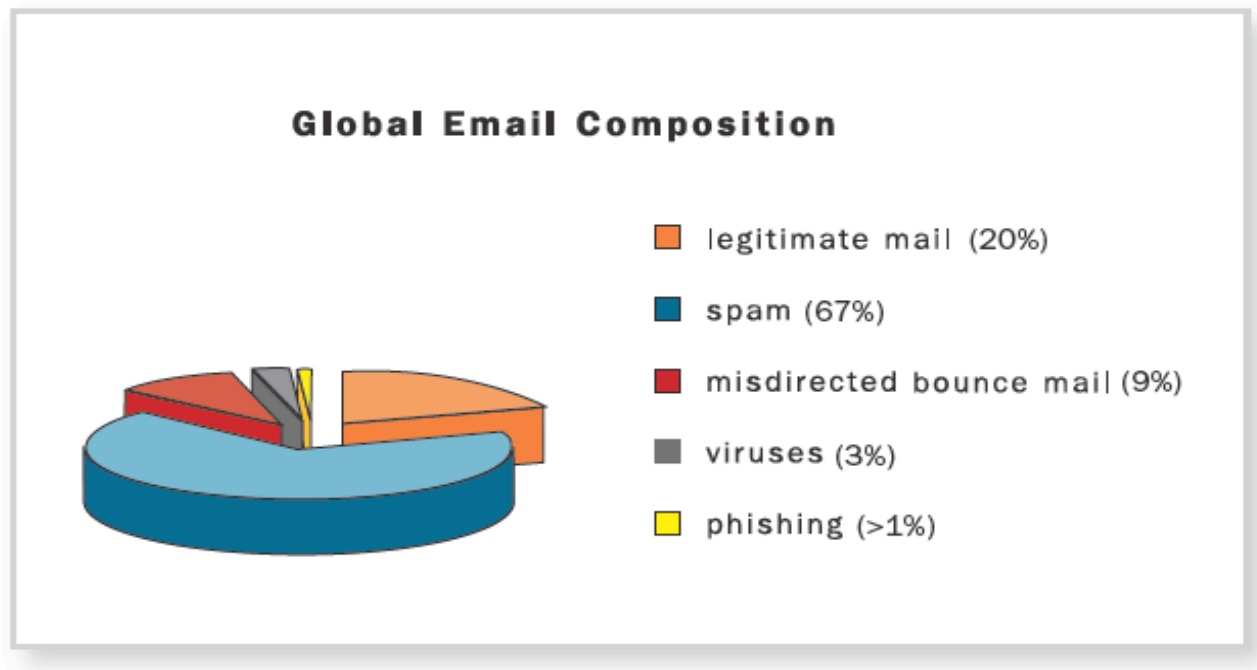
- 23. Mai: 892.565



Infektion um Spam zu versenden?

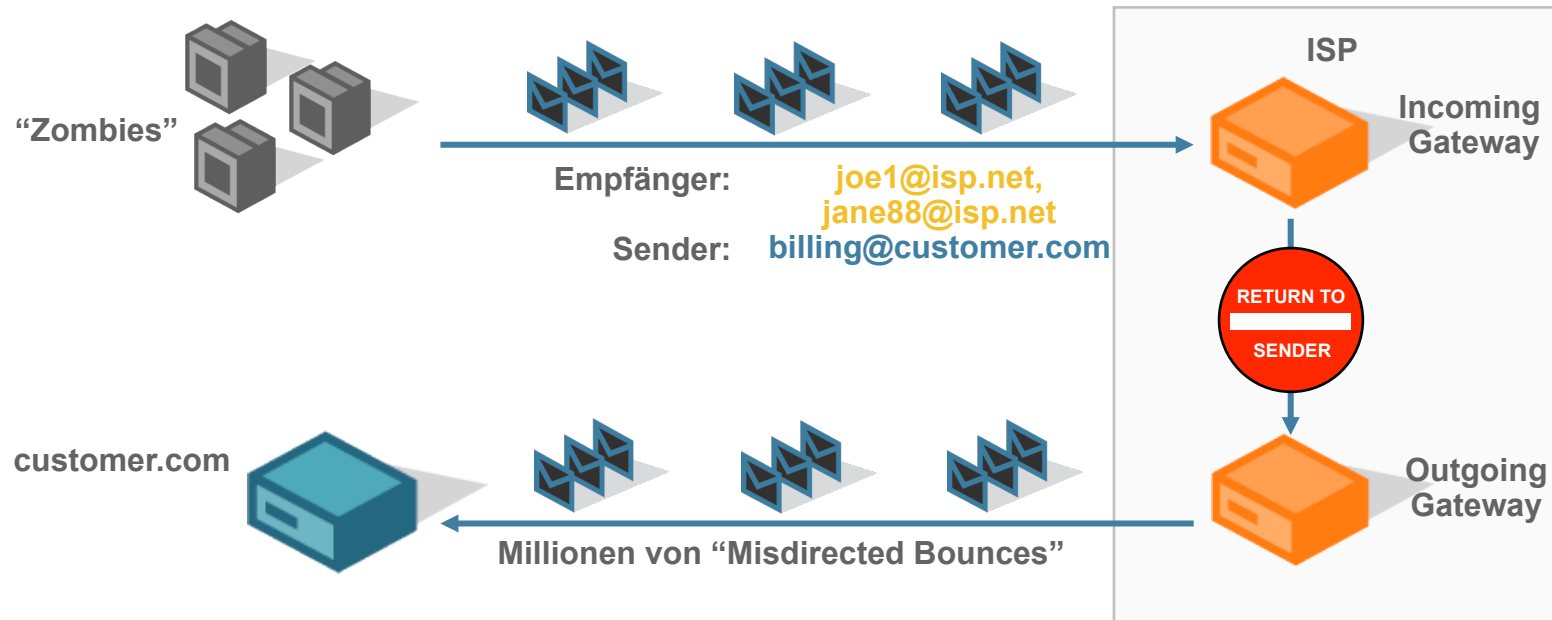
- 36 Sekunden

Unerwünschte Email-Kommunikation



Quelle: IronPort Threat Operations Center (25 – 30% weltweiter Email-Kommunikation)

Misdirected Bounces (4.5 Mrd. täglich)



> 55% der Fortune 500 Unternehmen berichten Ausfälle durch "Misdirected Bounce" Attacken !

Quelle: IronPort Threat Operations Center (25 – 30% weltweiter Email-Kommunikation)

Spam-Varianten

Image-basierend

“Polka-Dots”

*****ATTENTION ALL DAY TRADERS AND INVESTORS*****

INVESTOR ALERT!
IT LOOKS LIKE ANOTHER RUN FOR SWNM!
WATCH SWNM LIKE A HAWK ON Tuesday July 1, 2006

Company Name: SOUTHWESTERN MEDICAL, INC.
Stock Symbol: SWNM
Monday Close: 0.11
Volume: 5,761,702
Change: UP 0.025 (27.78%)
Market Cap: \$33,000,000.00 (Approx)

Goldmark Industries, Inc (GDKI.PK)

THIS STOCK IS EXTREMELY UNDERVALUED

Huge Advertising Campaign this week!
 Breakout Forecast for July, 2006

Current Price: \$5.60
Short Term Price Target: \$12.00
Recommendation: Strong Buy
**300+% profit potential short term*

RECENT HOT NEWS released MUST READ ACT NOW

LOS ANGELES VANCOUVER, British Columbia -- Goldmark Industries, Inc. (GDKI.PK), the Company has recently signed a multi-movie distribution agreement with Mr. Rodriguez's production and distribution company, Polychrome Pictures, for the automatic theatrical and home video distribution of feature length films scheduled for release by Goldmark. Goldmark is making its ascent into the multi-billion

“Slice & Dice”

***** BREAKING NEWS ALERT ISSUED *****

Most stock brokers give out their new issues only to their largest commission paying clients. We assume many of you like to "trade the promotion" and may have made some big, fast money doing so.

Trade Date : Monday, July 31, 2006
 Company : EVER GLORY INTL INC
 Ticker: EGLY
 Rises Over 5% on Friday.
 Volume: 270,947
 Price at Close Friday: \$1.15
 3-6 Day Trading: \$3 - \$4
 Expectations : STRONG BUY

Looking for a company with some good news? Here's one!

Breaking News:
Ever-Glow Signs \$500,000 Deal with Debenhams (Read Yahoo Finance) There is a massive promotion underway this weekend apprising potential eager investors of this emerging situation. Breaking news alert issue - big news coming. We feel this is a "Stock Alert" and you should have this on your Radar. Big news expected. This should invoke LARGE gains. Do this often enough, and your portfolio can double, even TRIPLE in value.

*****BREAKING NEWS ALERT ISSUED*****

Most stock brokers give out their new issues only to their largest commission paying clients. We assume many of you like to "trade the promotion" and may have made some big, fast money doing so.

Trade Date : Friday, July 28, 2006
 Company : EVER GLORY INTL INC
 Ticker : EGLY
 Price : \$1.09
 3-6 Day Trading : \$3 - \$6
 Expectations : BUY

Looking for a company with some good news? Here's one!

Breaking News:
Ever-Glory Signs \$500,000 Deal with Debenhams (Read Yahoo Finance)

There is a massive promotion underway this weekend apprising potential eager investors of this emerging situation. Breaking news alert issue - big news coming. We feel this is a "Stock Alert" and you should have this on your Radar.

Profil dieser Spam Attacke

Spam-Attacke von 20 Milliarden Emails innerhalb von zwei Wochen im Mai 2006

- Zeitweise mehr als 1.5 Milliarden Emails täglich

Vorgehensweise

- Ständig modifizierter Spam-Inhalt einschliesslich URL

Spam Infrastruktur

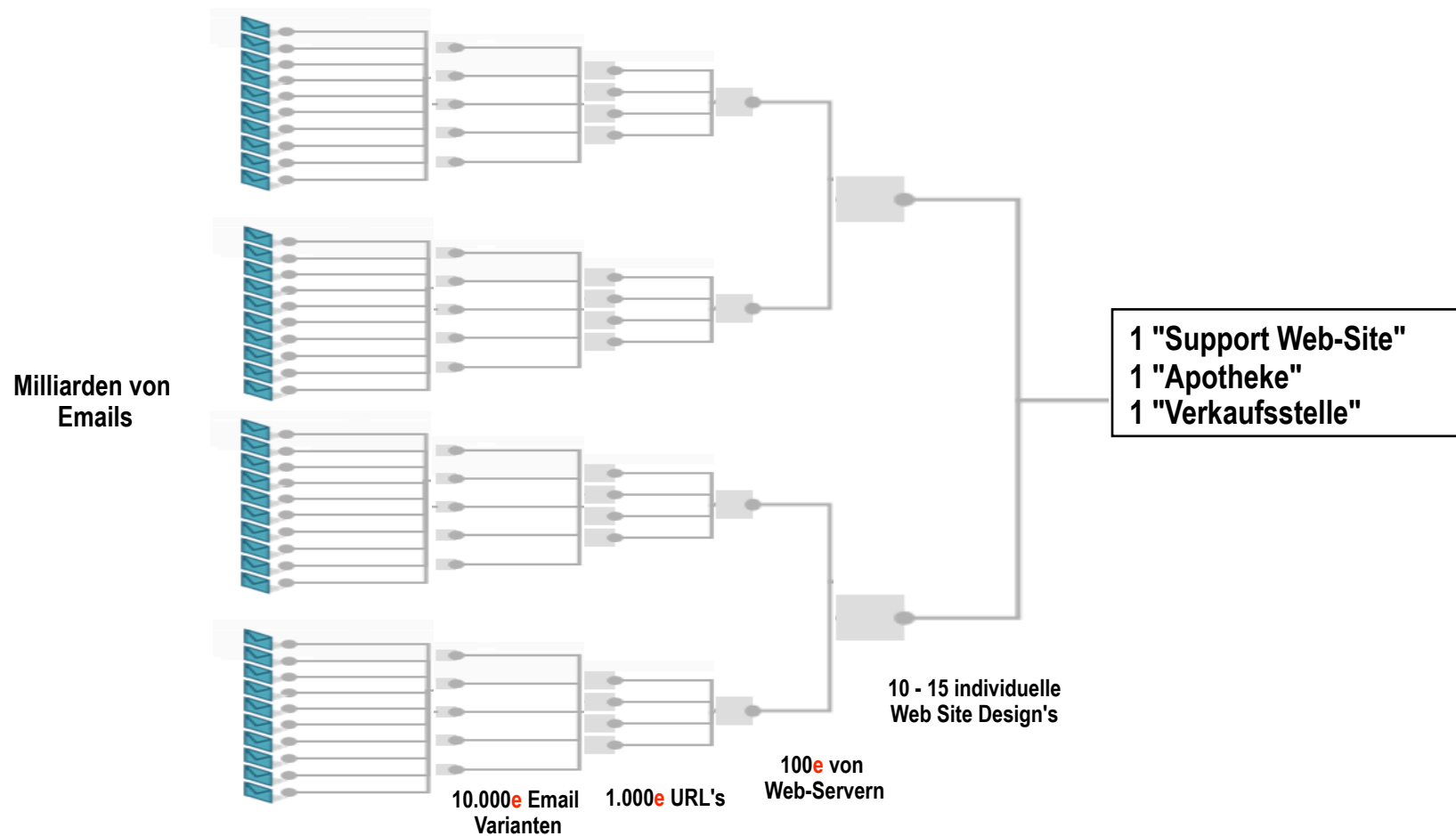
- 100.000 infizierte PC's (Zombies)

"Botnet Command and Control" (C&C) Infrastruktur

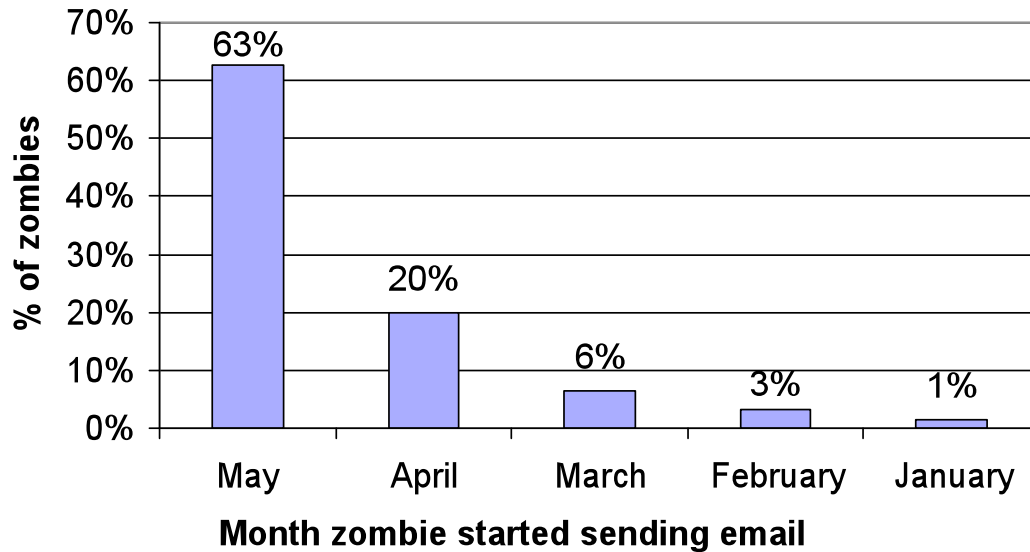
- 1500 Domänen und 100 Web Server

Ein "Geschäftsmodell".

Analyse einer Spam-Attacke



Spam Quelle: 100.000 Zombies



**80% Spam von
Zombies < 30Tage
'alt'**

**Top 10 Netzwerke
senden 28%
weltweiten Spam
Aufkommens**

Rank	Network Owner	Country	%
1	Telefonica de Espana	Spain	6.7%
2	France Telecom	France	4.3%
3	Proxad	France	3.4%
4	Telecom Italia	Italy	2.6%
5	Deutsche Telekom AG	Germany	2.2%
6	Cableuropa - ONO	Spain	2.2%
7	Telemar Norte Leste S.A.	Brazil	1.8%
8	Wanadoo France	France	1.7%
9	Telefonica de Espana SAU	Spain	1.7%
10	TELECOMUNICACOES DE S/	Brazil	1.7%

Botnet “Command & Control Center”

Go to botnet controller

Remark: displayed only online socks (socks that was in online in last 20 minutes)
 Remark: to copy IP or ID to clipboard press button "copy IP" or "copy ID"

Select by country:

Select by state:








Current country selected: all
 Current state selected: all

IP eines infizierten Computers – Verbunden in Echtzeit

List							
IP	SOCKS	ID	COUNTRY	CITY	STATE	CONNECTION	
Copy IP 70.178.130.171	57253	Copy ID XPCNZBSCWZLZCZTZCXFLKHVDJQXPVKO				1	
Copy IP 72.153.6.139	39112	Copy ID NMAWFUNDOTCUJFLZUQUPSCLMFMUATC				1	
Copy IP 86.138.210.148	31295	Copy ID KQAPBQXEYGHBJTYURAHGQUHSPGAPEUR				0	
Copy IP 70.229.125.18	32924	Copy ID DWYFSDPYDIORNSFYXIOSUOAFMDBGHTC				1	
Copy IP 84.9.86.199	51169	Copy ID BSYOUMQEPSSERBFTBIRFOHCKSHJUWKA				1	
Copy IP 68.96.235.136	21535	Copy ID KPNZBYSPUPZENYWEQNFUAUWFLMRSBY	United States	Atlanta	GA	1	
Copy IP 70.232.92.129	17167	Copy ID USPVOTULNTDYFLAZTNJSSUELRFKOPW				1	
Copy IP 87.74.45.27	40415	Copy ID CJKIXMIRLOZTFLSTLQSUZUPUWMJSGOM				1	
Copy IP 24.186.245.152	55147	Copy ID ATOTJDEXFOIDCNDJPALJRXKABULYKEU	United States	Lynbrook	NY	1	
						Total: 10	

Botnet “Command & Control Node”

Index of /uk

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory	03-Aug-2006 13:12	-	
 check.php	12-May-2006 18:43	1k	
 dupes.php	12-May-2006 18:43	1k	
 logger.php	12-May-2006 19:00	1k	
 logger.txt	10-Aug-2006 18:37	211M	
 socks.txt	10-Aug-2006 18:38	1k	
 socks/	25-May-2006 09:55	-	

Apache/1.3.34 Server at www.yops.biz Port 80

211 MB
Datei

Das 'Angebot' – 1 Spam Email

From: Willoughby Hopewell [hopewella@ahihomes.com] Sent: Mon 6/5/2006 6:23 AM
To: Patrick Peterson
Cc:
Subject: test eam

Hi,

SOM &
AMB "EN
MER "DiA
PROZ & C
X & NAX
VAL "UM
LEV "TRA
C "ALiS
V "AGRA

all 50 % off <http://www.stiseermi.com>

The dragon is still alive and in the halls under the Mountain then-or I imagine so from the smoke, said the hobbit. That does not prove it, said Balin, though I dont doubt you are right. But he might be gone away some time, or he might be lying out on the mountain-side keeping watch, and still I expect smokes and steams would come out of the gates: all the halls within must be filled with

"Angebot"

**'Call to Action' – URL
Verlinkung auf eine Web Site**

**"Hashbuster" Text
aus "The Hobbit"**

Irreführung - 6 unterschiedliche Inhalte

The image displays six email screenshots arranged in a 2x3 grid, each illustrating a different phishing technique. Three callout boxes are overlaid on the top row of emails:

- “Angebot”**: Points to the subject line of the top-left email: **Subject: [Ironport SPAM]**.
- ‘Call to Action’ – URL Verlinkung auf eine Web Site**: Points to the URL <http://www.mathareda.com> in the body of the top-left email.
- “Hashbuster” Text**: Points to the text block in the body of the top-left email: *longer making for the main forest-road to the south of his land. Had followed the pass, their path would have led them down the stream from the mountains that joined the great river miles south of the Carrock. At that point there was a deep ford which they might have passed, if they had still had their posies, and beyond that a track led to the skirts of the wood and to the entrance of the old forest road.*

The six email screenshots are as follows:

- Top-Left:** From: Ajeet Tatham [mailto:ajeet@dimensionshealth.or...]; Sent: Tuesday, May 30, 2006 01:01 AM; To: Goldschmidt, Ron; Subject: [Ironport SPAM]. Body contains a URL <http://www.mathareda.com> and a text block about a forest road.
- Top-Middle:** From: Brina Pavlick [mailto:pavleirina@...]; Sent: Monday, May 29, 2006 4:11 AM; To: Zipperstein, Steve; Subject: robi 3649. Body contains a URL <http://www.hisheron.com> and a text block about a hobbit.
- Top-Right:** From: Poncio Wedel [mailto:poncio@ca-sunshine.com]; Sent: Monday, May 29, 2006 10:57 PM; To: Tanouye, Duane; Subject: [Ironport SPAM Positive] Re: 695 swun. Body contains a URL <http://www.carogetha.com> and a text block about a dwarf.
- Middle-Left:** From: Nicolina Krug [mailto:nicolinalkrug@aol.com]; Sent: Monday, May 29, 2006 9:52 PM; To: Maddox, Roderick; Subject: [Ironport SUSPECT SPAM] Re: 240 unshake. Body contains a URL <http://www.romadaque.com> and a text block about a howl.
- Middle-Middle:** From: Sukiie Lawhon [mailto:sukielaw@blaineschools.org]; Sent: Monday, May 29, 2006 9:41 PM; To: Young, Tina; Subject: [Ironport SPAM Positive] Re: 644 Cupi. Body contains a URL <http://www.romadaque.com> and a text block about a troll.
- Middle-Right:** (No callouts, but contains a URL <http://www.mathareda.com> and a text block about a troll).

15 individuell gestaltete Web-Sites

Pharma Sites (9)

My Canadian Pharmacy

International Legal RX

US Drugs

Super Viagra

Viagra Pro

Generic Viagra

Cialis Soft Tabs

Viagra Soft Tabs

Maxaman

Andere Sites (6)

Virility Patch

Super HGH (flash)

SpermaMax

My Replica Rolex

Exclusive Caviar Online

Double Your Dating

Unterschiedliche Web Auftritte

ALL PRODUCTS LIST HOW TO ORDER ABOUT US CUSTOMER SERVICE CONTACT US

Erection Pack

TIME LIMITED OFFER

10 PILLS CIALIS + 10 PILLS VIAGRA + FREE SHIPPING

Try our SPECIAL ERECTION PACK! Two best ED medications in one super pack. Lowest price and FREE shipping. Time limited offer - valid till 10th of June only!

\$129.95 ONLY **ORDER NOW**

PRODUCTS LIST

Men's Health

- Cialis Soft Tabs *bestseller*
- Viagra Professional *bestseller*
- Viagra Soft Tabs *bestseller*
- Cialis *bestseller*
- Generic Viagra *bestseller*
- Levitra *bestseller*
- Maxaman

MOST POPULAR PRODUCTS

Cialis Soft Tabs as low as \$5.78

Just like regular Cialis but specially formulated, these pills are soft and dissolvable under the tongue. The effect of this is more direct absorption into the bloodstream, rather than through the stomach. Result - a powerful, lasting effect of up to 36 hours.

View Cart Order Status Contact Us

for sexual performance

Save up to **80%**

Bulk buy special

Today we have a special on Viagra ST. 5 x Viagra ST 100mg

ONLY \$34.95

Viagra Soft Tablet

	Dosage	Per pill	Price(usd)	
5 Pills	Viagra Soft Tabs 100mg	\$7.99	\$39.95	<input type="button" value="BUY NOW"/>
10 Pills	Viagra Soft Tabs 100mg	\$7.50	\$74.95	<input type="button" value="BUY NOW"/>
30 Pills	Viagra Soft Tabs 100mg	\$5.33	\$159.95	<input type="button" value="BUY NOW"/>
90 Pills	Viagra Soft Tabs 100mg	\$3.33	\$299.95	<input type="button" value="BUY NOW"/>

FREE SHIPPING on ALL ORDERS

FREE SHIPPING on ALL ORDERS

FREE SHIPPING on ALL ORDERS

- Men's health
 - Cialis (Tadalafil)
 - Cialis Soft Tabs
 - Levitra (Vardenafil)
 - Viagra (Sildenafil Citrate)
 - Viagra Gel (Sildenafil Citrate)
 - Viagra Soft Tabs
- Anti Depression
 - Ativan (Lorazepam)
 - Effexor XR
 - Paxil (Paroxetine Hd)
 - Prozac (Fluoxetine)
 - Valium (Diazepam)
 - Xanax (Alprazolam)

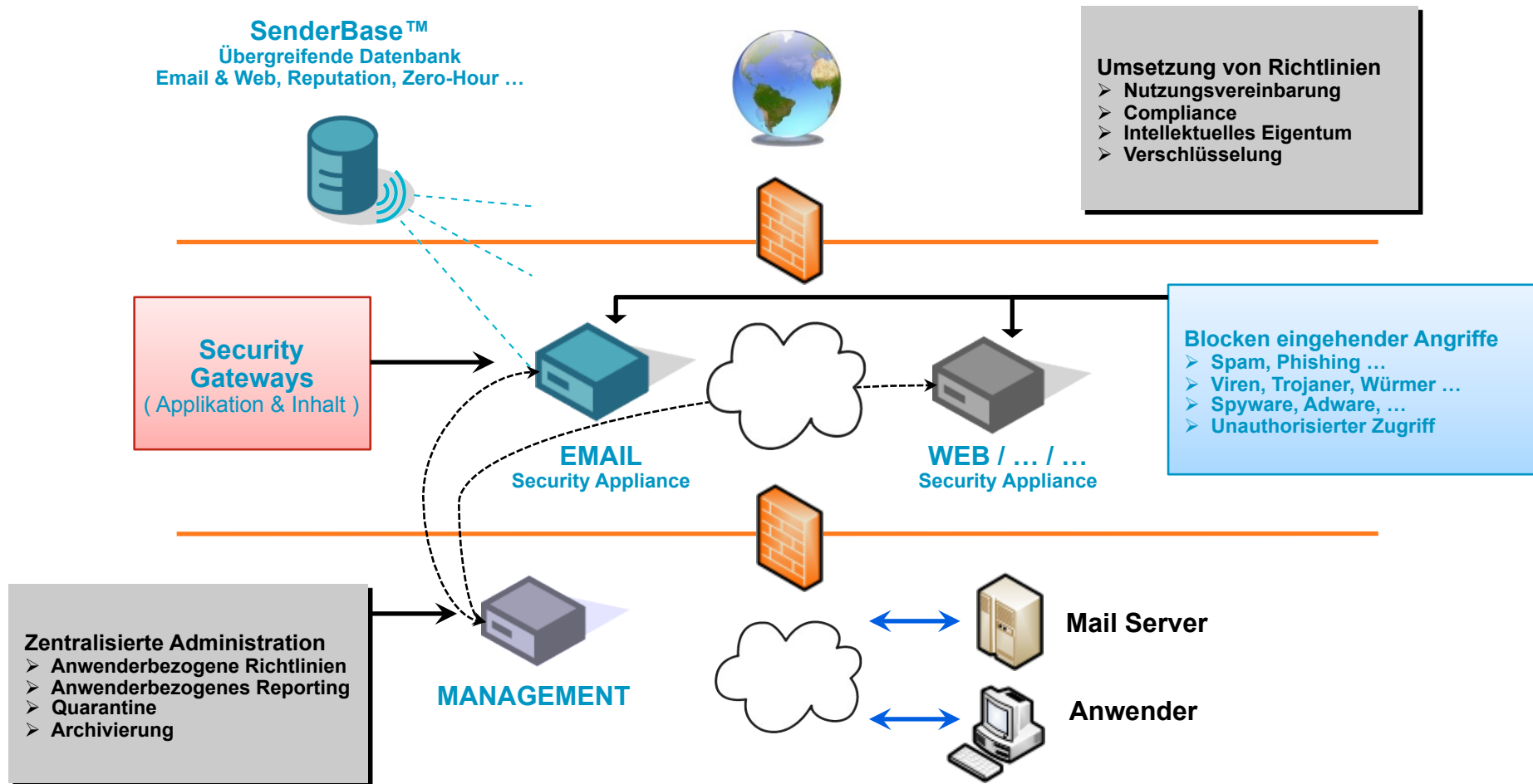
<p>Levitra</p>	<p>Viagra</p>	<p>Cialis</p>
<p>Xanax</p> <p>30 x 1.0mg Xanax (Alprazolam)</p>	<p>Soma</p> <p>80 x 350.0mg Soma (Carisoprodol)</p>	<p>Levitra</p> <p>10 x 20.0mg Levitra (Vardenafil)</p>



Lösungsansatz:

- Globale Konsolidierung**
- Anwendungsoptimierte Security Appliances**

Lösungsansatz: Konsolidierte Applikations Sicherheit



Produktfamilien Security Gateways

E-MAIL-SICHERHEIT

IronPort Systems bietet mit der C-Serie eine führende E-Mail-Sicherheitslösung zum Schutz von Unternehmen jeglicher Größenordnung. IronPorts innovative Technologien kommen in den anspruchvollsten Netzwerken der Welt zum Einsatz und liegen allen E-Mail-Security-Appliances gleichermaßen zugrunde. Die leistungsstarken Plattformen schützen auf Grund der stetigen Weiterentwicklung nicht nur vor aktuellen, sondern auch vor zukünftigen Gefahren.

WEB-SICHERHEIT

Mit dem branchenweit ersten Web-Reputationsfilter bietet IronPorts S-Serie eine leistungsstarke, mehrschichtige sowie herstellerunabhängige Lösung zur Abwehr von sämtlichen webbasierten Bedrohungen, wie beispielsweise Spyware.

SICHERHEITS-MANAGEMENT

Die IronPort M-Serie™ ermöglicht eine zentrale und konsolidierte Verwaltung Ihrer Daten und stellt Administratoren und Endbenutzern eine integrierte Schnittstelle für das Sicherheitsmanagement zur Verfügung.

IRONPORT C100



Technologien der Enterprise-Klasse in einer leistungsstarken und zugleich preiswerten Appliance für die Sicherheit von kleineren Unternehmen und Filialen mit bis zu 1.000 E-Mail-Nutzern.

IRONPORT C300



Höchste Sicherheit für die E-Mail-Kommunikation in mittelständischen Unternehmen und Organisationen mit einer Größenordnung von 1.000 bis 5.000 E-Mail-Nutzern.

IRONPORT C600



E-Mail-Sicherheit auf höchstem Niveau – die C600 kommt bei Netzwerken mit sehr hohen Leistungsanforderungen und mehr als 5.000 E-Mail-Nutzern zum Einsatz.

IRONPORT X1000



Acht der weltweit zehn größten Internet-Service-Provider (ISPs) haben sie bereits im Einsatz: die X1000 bietet eine hochperformante E-Mail-Sicherheitslösung für die anspruchvollsten Netzwerke.

IRONPORT S300



Mit den gleichen Funktionen wie die IronPort S600 bestückt, entspricht diese preiswerte Web-Security-Appliance den Sicherheitsanforderungen von Unternehmen mit bis zu 5.000 Benutzern.

IRONPORT S600



Applikations-Proxies für HTTP, HTTPS und FTP, ein Layer-4-Traffic-Monitor sowie eine ausgeklügelte Scanning- und Vectoring-Engine gewährleisten ein Höchstmaß an Leistung und Effektivität.

IRONPORT M600



Die perfekte Ergänzung der E-Mail- und Web-Security-Appliances von IronPort für das zentrale Management von Sicherheitslösungen mit bis zu 5.000 Benutzern.

IRONPORT M1000



Die zentrale Quarantäne- und Reporting-Appliance mit dem Extra an Speicher und Leistung für Unternehmen mit mehr als 5.000 Benutzern.

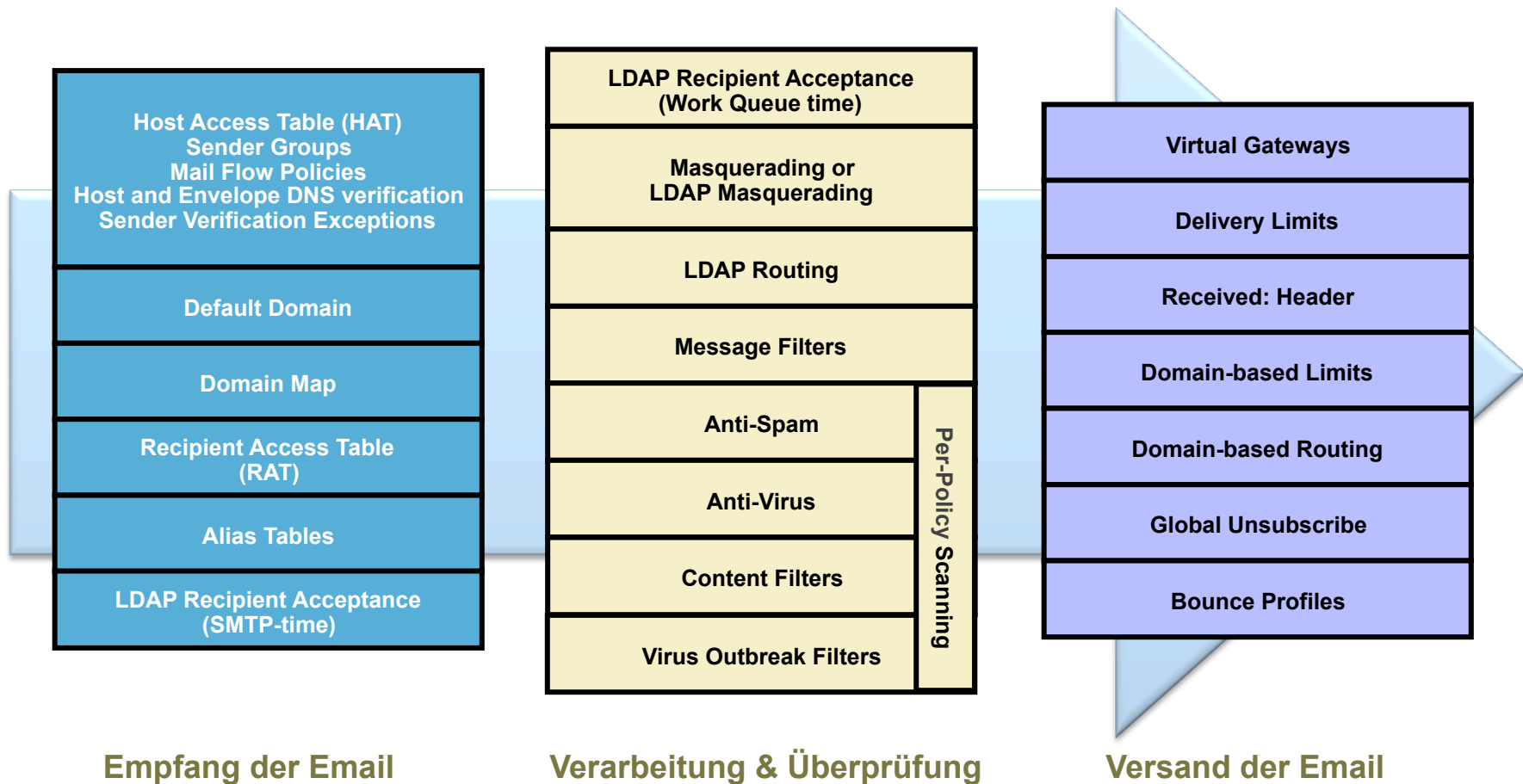
IronPort Architektur

Mehrstufige E-Mail Sicherheit



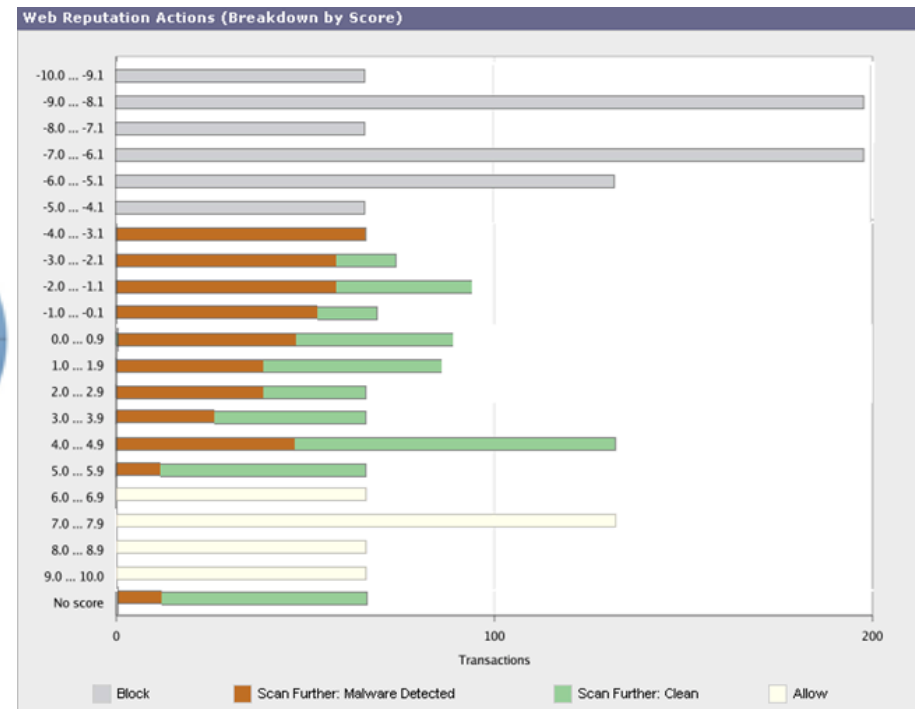
Die IronPort AsyncOS Email Pipeline

[Vereinfacht dargestellt]



IronPort SenderBase Netzwerk - Reputationsdatenbank

Datenbank zur Analyse von E-Mail- und Web-Kommunikation

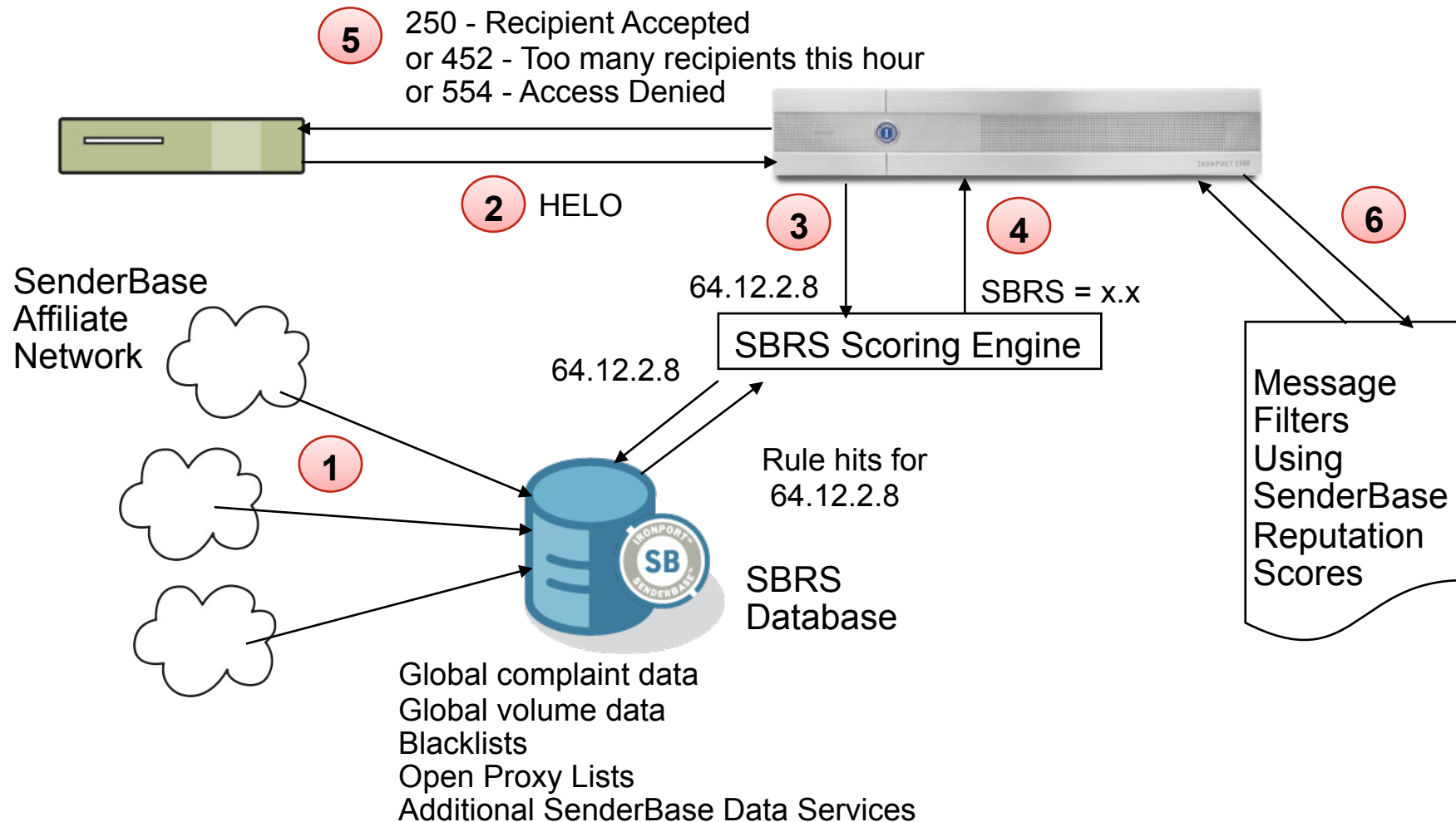


25% des weltweiten E-Mail-Verkehrs

150+ Parameter zur Bewertung von Email- & Web-Ressourcen

5 Milliarden Anfragen täglich (20 Mrd. Emails)

Ermittlung & Anwendung SenderBase Reputation Score (SBRS)



IronPort Reputations-Filter

Mail Flow Monitor & Rate Limiting

Sender Groups (Listener: IncomingMail (172.19.1.11:25))

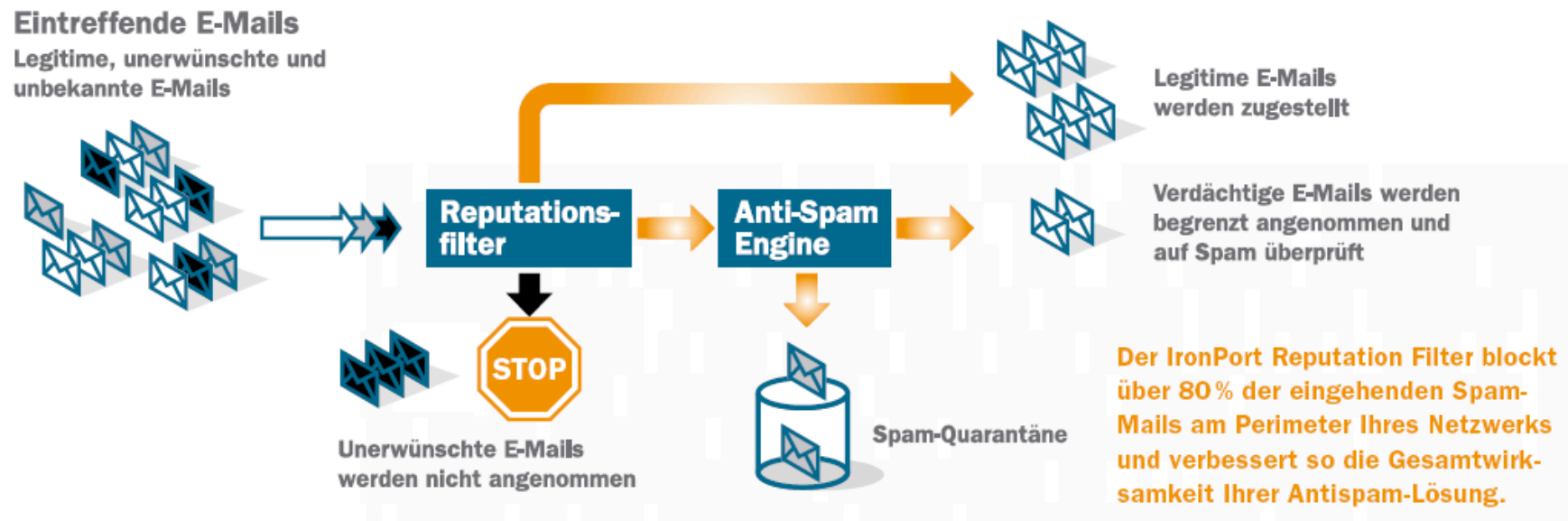
Add Sender Group... Import HAT...

Order	Sender Group	SenderBase™ Reputation Score ?										Mail Flow Policy	Delete
		-10	-8	-6	-4	-2	0	2	4	6	8		
1	WHITELIST											TRUSTED	
2	BLACKLIST											BLOCKED	
3	SUSPECTLIST											THROTTLED	
4	UNKNOWNLIST											ACCEPTED	
	ALL											ACCEPTED	

Edit Order... Export HAT...

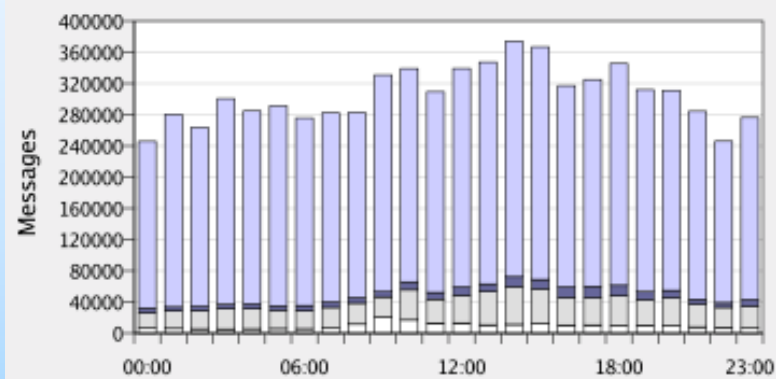
IronPort Reputationsfilter

Stoppt ~ 80% des Spams bereits vor der Annahme



Live Kennzahlen ISP Umfeld

Europa, 24 Stunden, 1 Appliance



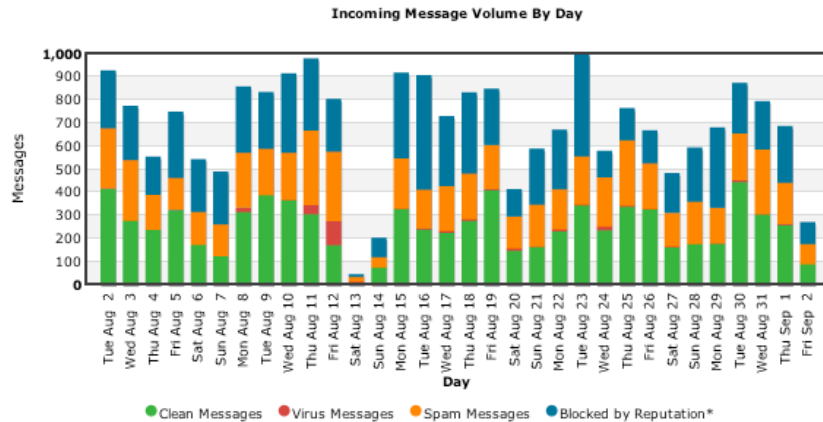
Incoming Mail Category	%	# Messages
Total Attempted Messages		7,330,484
Stopped by Reputation Filtering	83.94	6,153,125
Invalid Recipients	2.78	204,137
Spam Messages Detected	10.18	746,233
Virus Messages Detected*	0.0	0
Total Threat Messages	96.9	7,103,495
Clean Messages Accepted	3.1	226,989



IronPort Mail Traffic Report

For data collected from: Aug 2, 2005 through Sep 2, 2005

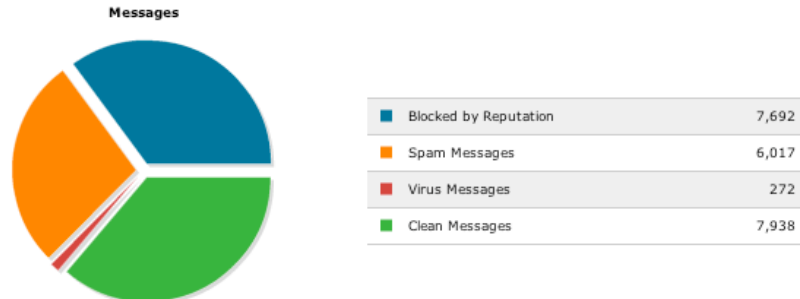
Your IronPort Email Security Appliance is designed to meet the needs of a wide range of customer demands. The IronPort appliance's exclusive **preventative filters** and highly accurate **reactive filters** eliminate spam, enforce corporate policy, secure the network perimeter, and reduce the total cost of ownership (TCO) of your enterprise email infrastructure.



Consolidated

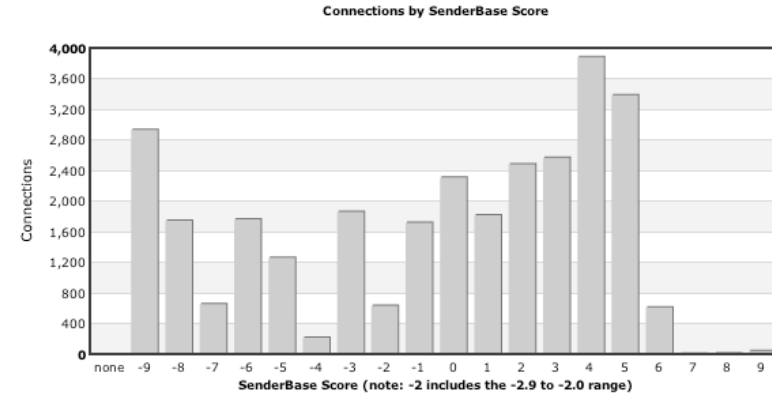
This graph represents the message volume received by your IronPort appliance - including:

- **Messages blocked by Reputation Filtering:** These messages are blocked at the SMTP connection level based on the history of the sending IP address. Reputation Filtering prevents Denial of Service attacks, lowers bandwidth utilization, and reduces computing costs on your IronPort appliance.
- **Messages blocked as Invalid Recipients:** These messages are blocked because they match no valid recipients in your network (determined by querying your directory or the Recipient Access Table configured on the appliance). Blocking invalid recipients at the gateway protects you from directory harvest attacks and reduces the load on your groupware servers.
- **Messages identified to contain spam and/or viruses:** These are messages that are positively identified by IronPort's reactive spam and virus scanning engines. Through policies in the Email Security Manager you determine which messages get scanned. Remember that in many cases, messages containing security threats have already been blocked by the preventive reputation filters above.
- **Clean messages:** These messages have been determined not to contain any security threats, and are then delivered to your internal groupware servers.

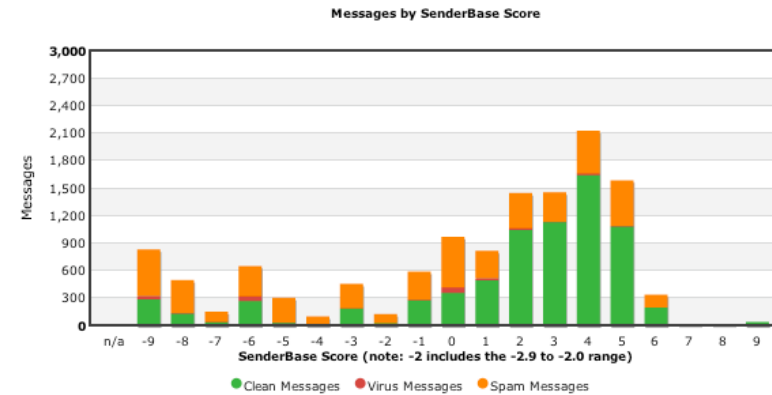


Reputation Filtering

IronPort Reputation Filters provide the outer layer of defense for your email infrastructure. As the IronPort appliance receives inbound mail, it performs a threat assessment of the sender and assigns a proprietary SenderBase Reputation Score (SBRS). Suspicious senders are throttled or blocked while recognized senders, such as customers or business partners, are allowed access. Your IronPort appliance's response is determined by mail flow policies configured in the Host Access Table.



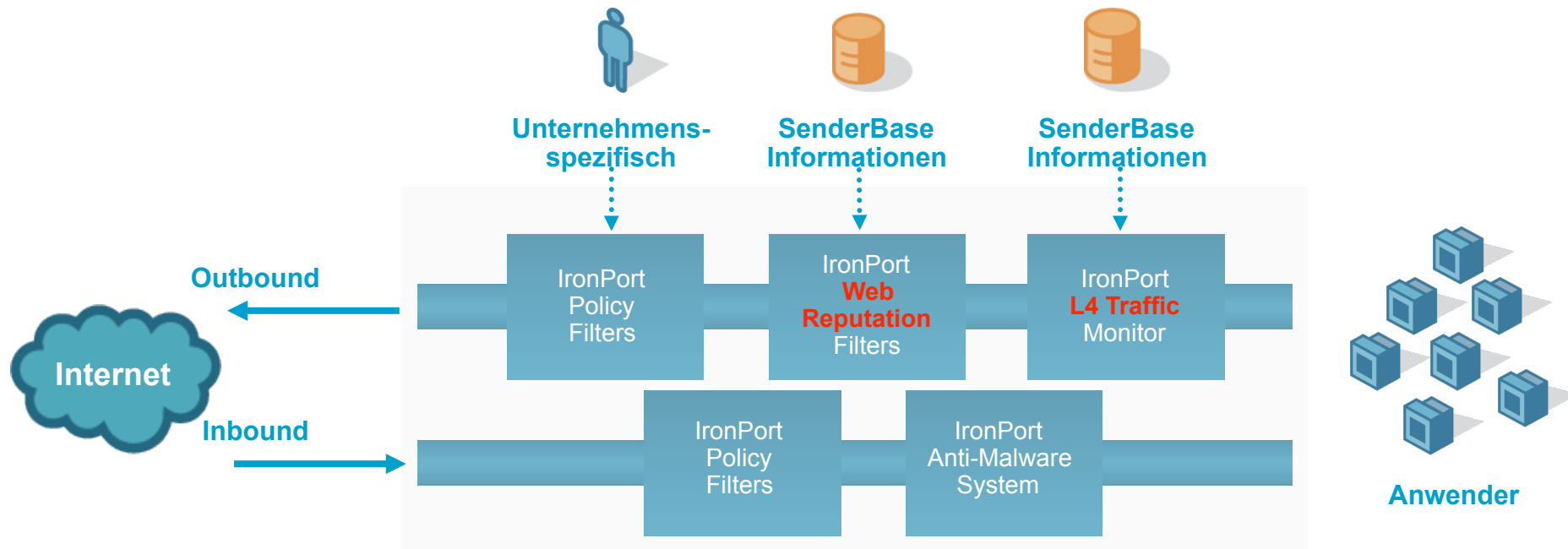
The 'Connections by SenderBase Reputation Score' graph provides a view of the total connections made to your IronPort appliance associated with each senders' SBRS scores. The 'Messages by SenderBase Reputation Score' provides a view into messages actually processed by the appliance, via mail policies and filters.



By contrasting the two graphs, you can see that:

- The portions of the 'Messages by SenderBase Reputation Score' graph where blocking is used and no messages are displayed demonstrates the effectiveness of the IronPort appliances's preventative reputation filters. These filters reduce the traffic load on the appliance by blocking connections to the appliance by disreputable senders - enhancing the availability of your email, even during heavy virus or spam outbreaks.
- The majority of email sent by senders with a lower SBRS (less than 0) but not blocked on connection, is identified as spam. As you become comfortable with the veracity of SenderBase Reputation scoring, you can fine-tune your mail policies to block more email at the SMTP connection.
- Generally, a SBRS of 'None' is assigned to newer IP addresses where no information exists from the SenderBase Reputation Service to make an accurate assessment of the sender's reputation.

HTTP-Transaktionen Multi-Layer & Multi-Vendor



Web Security Manager™

Umsetzung von Unternehmens-Richtlinien

Web Filtering Policies

Policies						
<input type="button" value="Add Group..."/>						
Order	Group	Applications	URL Categories	Objects	Anti-Malware	Delete
1	QA	Block: FTP Block: User Agents	Block: 52 Monitor: 2 Allow: 0	Block: 256 Mb	(global policy)	
2	Engineering	Block: User Agents	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types Block: File Types	(disabled)	
3	Marketing	(disabled)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types	Block: 11 Monitor: 2	
4	Dev	(global policy)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size	(global policy)	
	Global Policy	Block: FTP, HTTPS Allow: HTTP Block: User Agents Allow: Ports 443, 21	Block: 46 Monitor: 8 Allow: 0	Block: 256 Mb Block: Object Types Block: File Types	Block: 13 Monitor: 0	

Key: Global Disabled
 Authentication



Web Security Monitor™

Überwachung von Unternehmens-Richtlinien

System Overview

IRONPORT S650

System Overview

System Resource Utilization

System Status Details

Time Range: Month (30 days)

Total Web Activity

Suspect Transactions Detected

Security Services Summary

Top URL Categories

Top Malware Categories

Search for: Client

Generated: 21 Nov 2006 21:25 (GMT)

Client Detail

IRONPORT S650

Client Detail: jsmith

Web Proxy Activity for Client jsmith

Web Proxy Activity

Malware Risk

Web Transactions by URL Category

Malware Threats Detected

Suspect User Agents Detected

Search for: Client

Generated: 21 Nov 2006 13:24 (GMT)

Web Reputation

IRONPORT S650

Web Reputation Filters

Web Reputation Actions (Trend)

Web Reputation Actions (Volume)

Current Configuration

Web Reputation Actions (Breakdown by Score)

Search for: Site

Generated: 21 Nov 2006 21:29 (GMT)

Q & A



