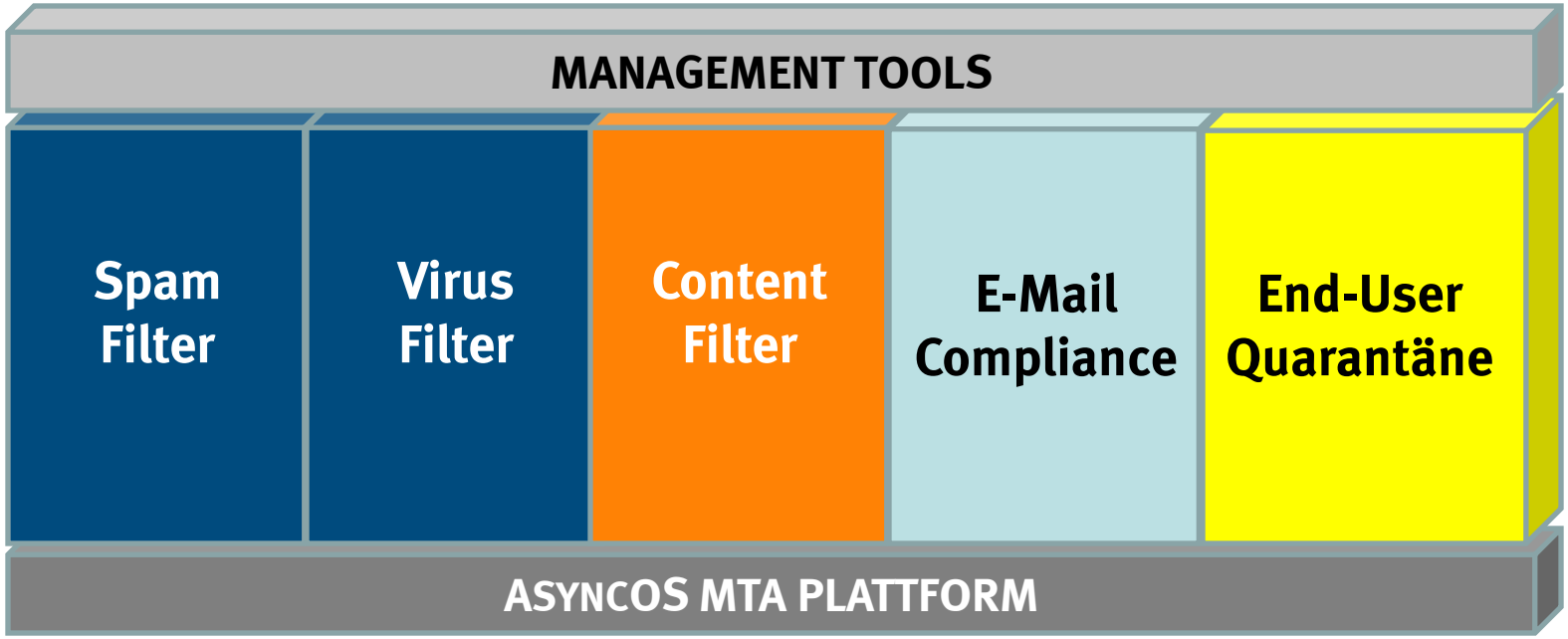
SECUR TEC
SYSTEMHAUS

IronPort E-Mail Security

SECUR TEC SYSTEMHAUS

IronPort E-Mail Security



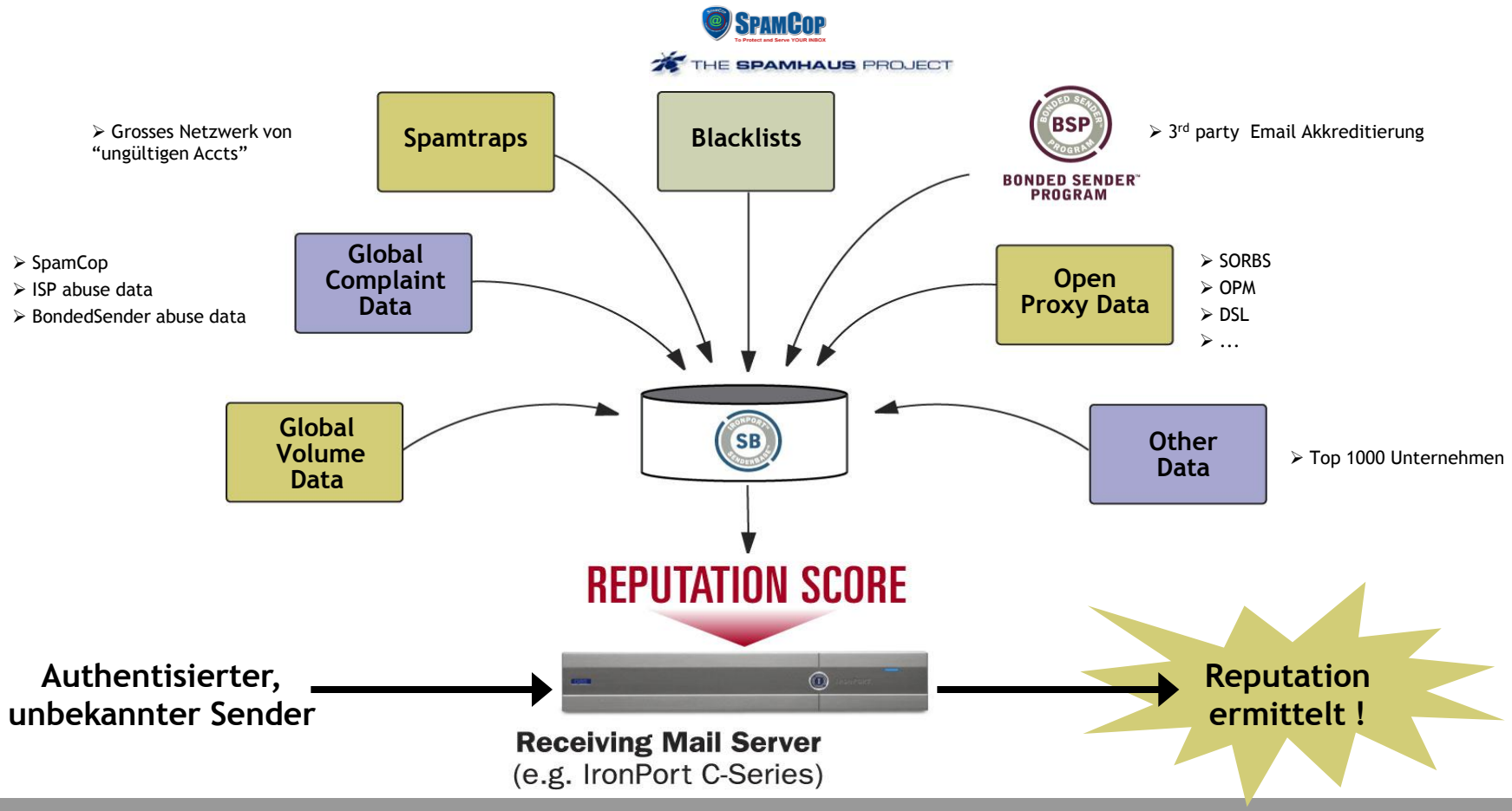
SECUR TEC
SYSTEMHAUS

IronPort SenderBase® Netzwerk

› 30% des globalen Email-Volumens
› 100.000 zuliefernde Netzwerke
› 5 Mrd. Anfragen täglich
› 110 Detail-Parameter

Beobachtung & Beurteilung des weltweiten Email- and Web-Verkehrs

SenderBase Quellen



Reputation Tracking

SECUR TEC SYSTEMHAUS

SenderBase Network

Sophisticated Security Modeling

Reputation Scores (-10 to +10)

90+ Parameters	• Global volume data • Message composition data • Spam traps, complaints • Blacklists, whitelists • Compromised host lists • Open proxy lists	→	**Sender Reputation Score**
45+ Parameters	• URL blacklists and whitelists • HTML Content Data • Domain Registrar Information • Network Owners • Known Threats URLs • Web Site History…	→	**Web Reputation Score**

„Host Access Table": Positive & negative Reputation

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

Add Sender Group... | Import HAT...

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

Edit Order... | Export HAT...

SECUR TEC SYSTEMHAUS

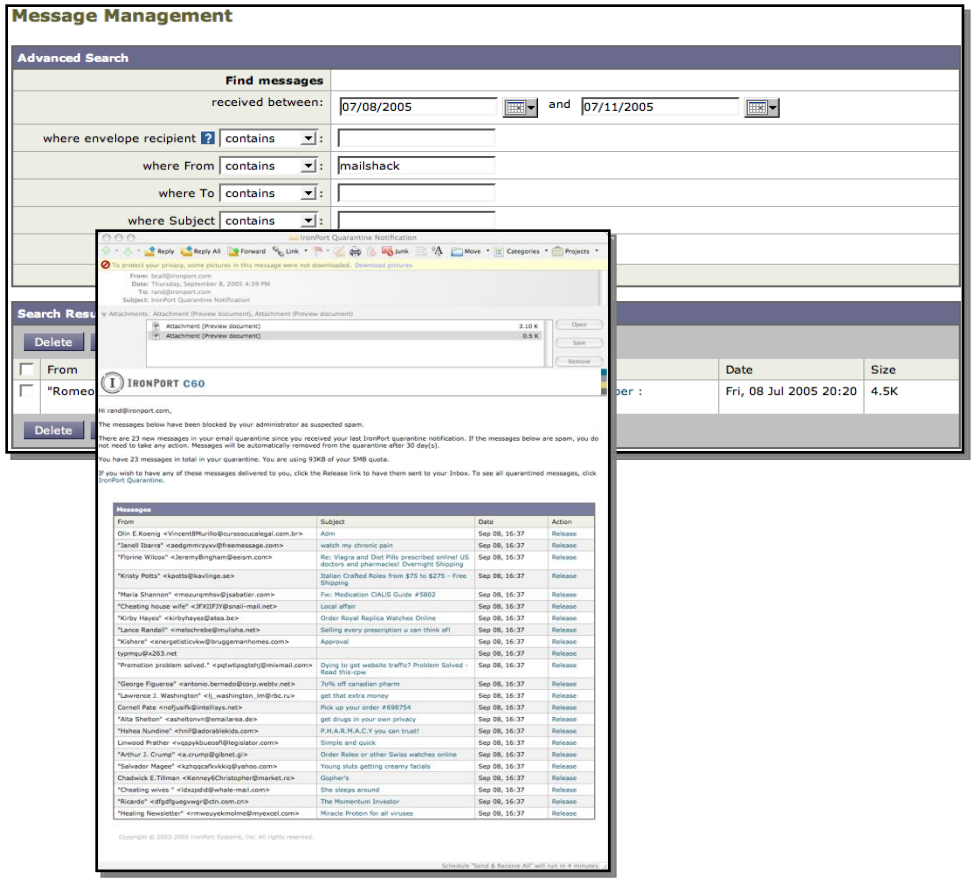
IronPort's CASE

	IronPort Anti-Spam	Andere Anbieter
Was? **Email Inhalt** Welchen Inhalt hat die Email?	✔	✔
Wie? **Email Struktur und Aufbau** Wie wurde die Email erzeugt?	✔	✔
Wer? **Email Reputation** *Wer ist der Absender der Email?*	✔	✔
Wohin? **Web Reputation** *Wohin verweisen die Web Links (URLs)?*	✔	

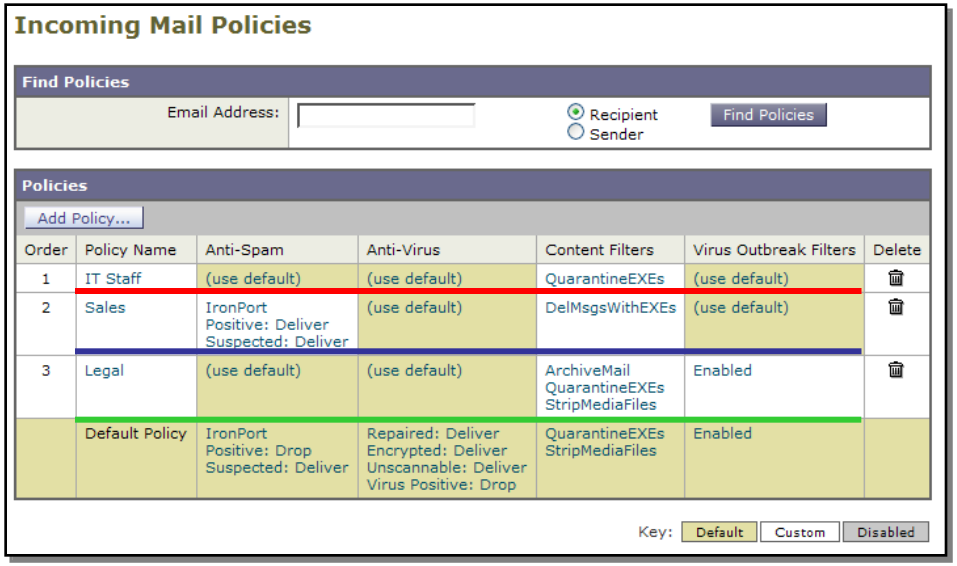
SECUR TEC SYSTEMHAUS

IronPort Spam Quarantäne

- **Flexibel einsetzbar**
  - On-box oder zentrale Quarantäne (M-Serie)
  - IronPort Anti-Spam
- **Großer Funktionsumfang**
  - Authentisierung der User mittels LDAP, AD, oder IMAP/POP
  - Automatisches Speicherplatzmanagement
  - End-User Zugriff
  - Benachrichtigungsfunktion



IronPort Email Security Manager



Incoming Mail Policies

Find Policies

Email Address: Recipient / Sender — Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	IT Staff	(use default)	(use default)	QuarantineEXEs	(use default)	
2	Sales	IronPort Positive: Deliver Suspected: Deliver	(use default)	DelMsgsWithEXEs	(use default)	
3	Legal	(use default)	(use default)	ArchiveMail QuarantineEXEs StripMediaFiles	Enabled	
	Default Policy	IronPort Positive: Drop Suspected: Deliver	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	QuarantineEXEs StripMediaFiles	Enabled	

Key: Default | Custom | Disabled

Kategorien:

- **Domäne (Sender & Empfänger)**
- **Username (Email-Adresse)**
- **LDAP**

➢ **Medien-Dateien**
➢ **EXE in Quarantäne**

IT

➢ **Spam markieren & zustellen**
➢ **EXE löschen**

Vertrieb

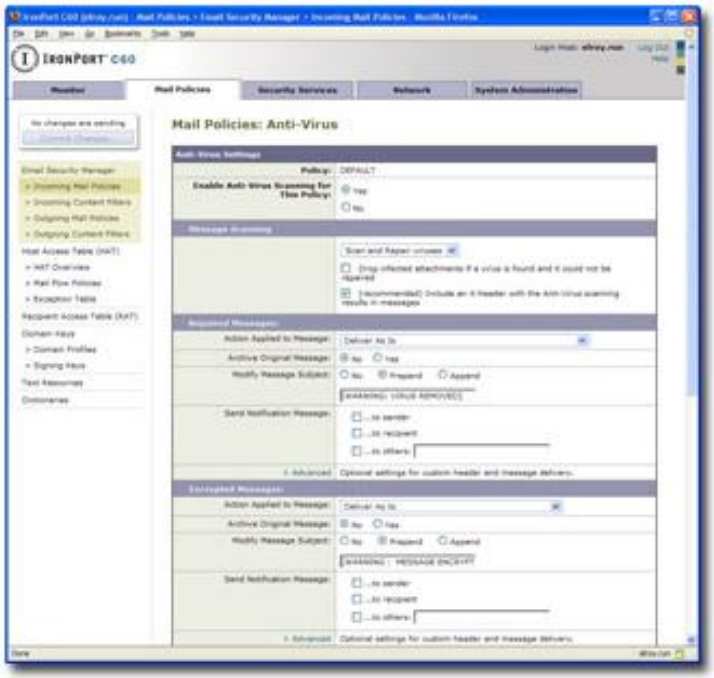
➢ **Archivierung aller Emails**
➢ **VOF inaktiv für .DOC**

Rechts-abteilung

SECUR TEC SYSTEMHAUS

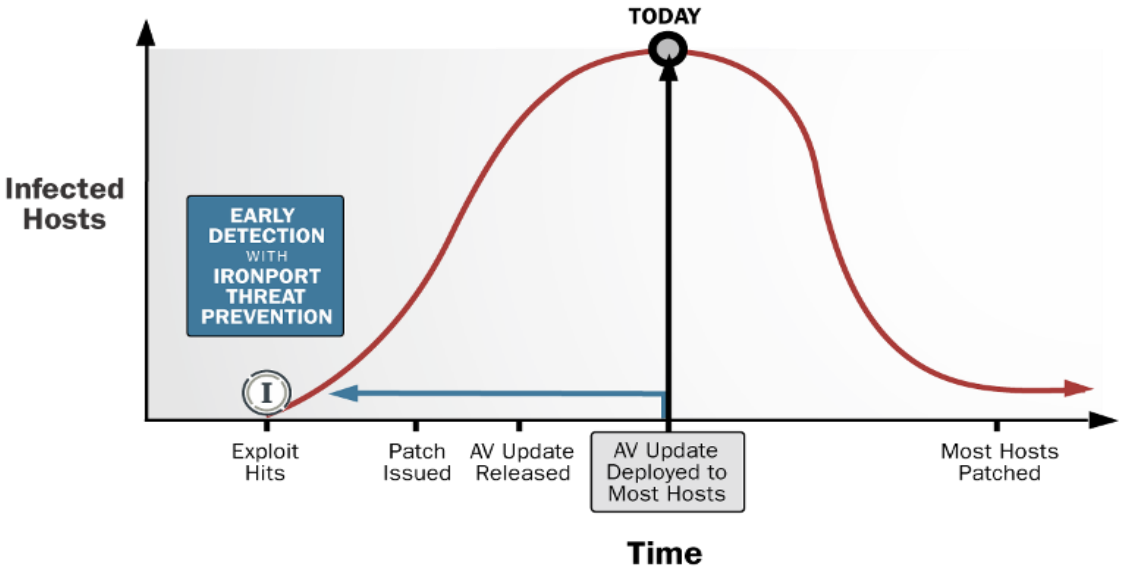
Sophos Anti-Virus

- **Integrierte Sophos® Antivirus Engine**
  - Hochperformante Scanengine
  - Schnelle IDE Updates
  - Ausgezeichnete Erkennungsrate
- **Einfache Administration**
  - Intuitives Benutzerinterface
  - Komplett in Mail Flow Monitor integriert
  - Automatische IDE und Engine Updates
  - Unschlagbare TCO durch integrierte Lösung



Virus Outbreak Filter

SECUR TEC SYSTEMHAUS

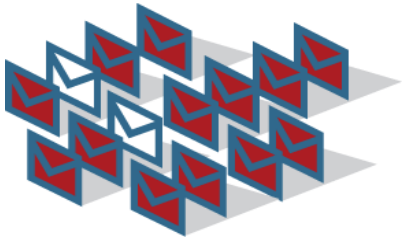


VIRUS NAME	IRONPORT'S EARLY DETECTION ADVANTAGE
Multiple "Bagle" Variants	DETECTED 41:43 hours BEFORE ANY OTHER TECHNOLOGY
"MyTob.EC"	DETECTED 15:22 hours BEFORE ANY OTHER TECHNOLOGY
"Sober.J"	DETECTED 10:23 hours BEFORE ANY OTHER TECHNOLOGY
"Zotob-C"	DETECTED 2:51 hours BEFORE ANY OTHER TECHNOLOGY

Funktion Virus Outbreak Filter

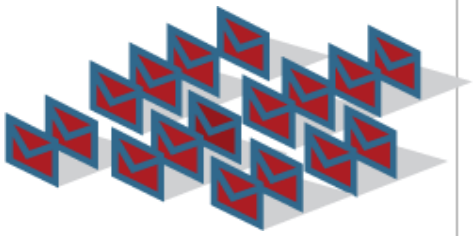
T = 0

> zip (exe) files



T = 5 Min.

> zip (exe) files
> Größe: 50 bis 55 KB



T = 10 Min.

> zip (exe) files
> Größe: 50 bis 55KB
> z.B. “Price” im
> Dateinamen

Nachrichten gescanned & gelöscht

T = 8 Std.

> Freigabe der Nachricht, sobald Signatur verfügbar

SECUR TEC SYSTEMHAUS

Outbreak Quarantäne

IRONPORT C60

Monitor | Mail Policies | Security Services | Network | System Administration

No changes are pending
Commit Changes...

- Incoming Mail Overview
- Incoming Mail Details
- Outgoing Mail Overview
- Outgoing Mail Details
- System Overview
- System Status
- Quarantines
- Scheduled Reports

Outbreak Quarantine Summary

Manage by Rule Summary

All Select	Rule ID	Rule Description	Number of Messages	Average Message Size	Total Size	Capacity
	OUTBREAK_0002189_03	Testing Outbreak rules.	72	4 KB	0.3 MB	0.1%
	OUTBREAK_0002187_03	This is an example Outbreak rule.	62	2 KB	0.1 MB	0.0%
	OUTBREAK_0002188_03	Another Outbreak rule.	36	5 KB	0.2 MB	0.1%
	VOF_ADAPTIVE_RULES	N/A	36	1 KB	0.0 MB	0.0%
	Totals		206	12 KB		

Select Action... Submit

Emails nach Regel-Typ aufgeführt

Information nach Regel-Typ kategorisiert

SECUR TEC SYSTEMHAUS

Quarantäne Management

IRONPORT C60

Monitor | Mail Policies | Security Services | Network | System Administration

No changes are pending
Commit Changes...

- Incoming Mail Overview
- Incoming Mail Details
- Outgoing Mail Overview
- Outgoing Mail Details
- System Overview
- System Status
- Quarantines
- Scheduled Reports

Quarantined Message

Quarantine Details

All Select	Quarantine	Reason	Time Received	Time Scheduled to Exit
	All	Message Filter: 'allq'	13 Jun 10:47	21 Sep 10:47
	All2	Message Filter: 'allq2'	13 Jun 10:47	21 Sep 10:47
	Outbreak	OUTBREAK_0002189_03	13 Jun 10:47	25 Jun 10:47

Select Action... Submit

< Back to Message List

Message Details

Test for Viruses: Start Test

Send Copy To: E-Mail Address: Send a Copy to IronPort Systems Send

Envelope Sender: user123@test14.eng

Recipients: aprils@spaceneedle.com.d1.test14.eng
tlcorvel@att.net.d1.test14.eng

```
Return-Path: <paklaovawerkok-2b-2-l.z@adbsys.no>
X-Original-To: sonictrap@bondedsender.org
Delivered-To: sonictrap@bondedsender.org
Received: from eth0.b.lds.sonic.net (eth0.b.lds.sonic.net [209.204.159.5])
      by dumpster.senderbase.org (Postfix) with ESMTP id 8A41F25164
      for <sonictrap@bondedsender.org>; Sat, 13 Sep 2003 00:42:55 +0000 (GMT)
Received: from b.mx.sonic.net (eth0.b.mx.sonic.net [209.204.159.4])
      by eth0.b.lds.sonic.net (8.12.9/8.12.9) with ESMTP id h8D7bobG017671;
      Sat, 13 Sep 2003 00:37:50 -0700
Received: from 209.204.159.4 ([200.90.80.222])
      by b.mx.sonic.net (8.12.9/8.12.7) with SMTP id h8D7bOUc023191;
      Sat, 13 Sep 2003 00:37:32 -0700
Received: from [218.236.233.132] by 209.204.159.4 for <onceler@sonic.net>; Sat, 13 Sep 2003 00:34:48 +0400
```

Test mit neuester AV-Signatur

An IronPort zur Auswertung senden

Nachricht auswerten

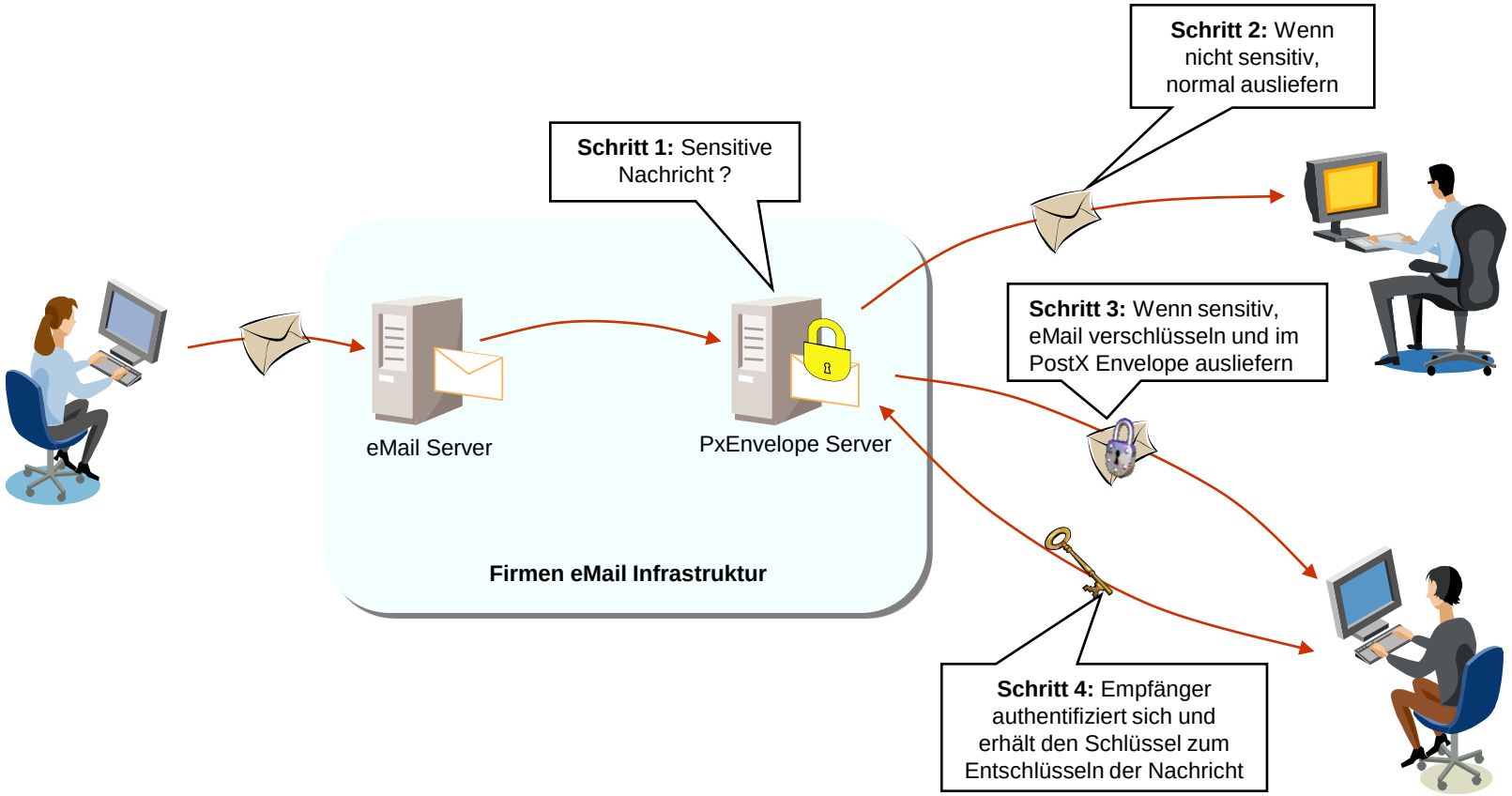
SECUR TEC SYSTEMHAUS

Compliance Filter

- **Sofortiger Einsatz vordefinierter Filter bei ausgehenden Nachrichten**
  - Filterung ausgehender Nachrichten zur Richtlinieneinhaltung
  - Minimiert False-Positives
  - Einzigartiges Pattern-Matching nach mehreren Kategorien

- **Vertrauliche Kommunikation**
  - Verschlüsselung von E-Mailverkehr mit TLS
  - Einfache Integration mit Verschlüsselungsfunktion am Desktop

PXEnvelope Verschlüsselung

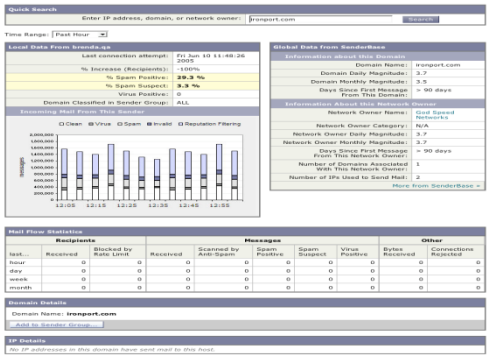


Reporting

SECUR TEC SYSTEMHAUS

IronPort Exklusive **Mail Flow Monitor™**

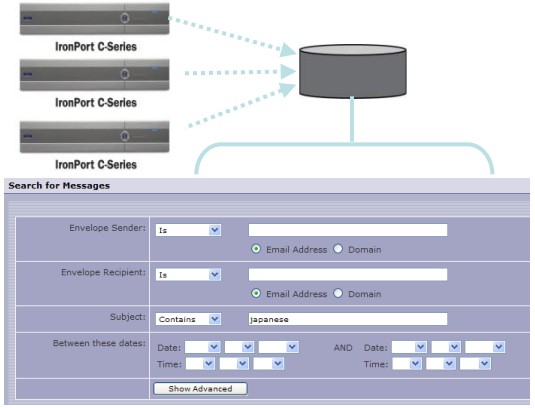
- **Sicherheit durch Sichtbarkeit**
- Zeigt Anomalien
- Identifiziert Sender und Empfänger
- Speichert Email-Statistiken



Auf einen Blick:
"Werden wir angegriffen?"
"Fließt der Email-Verkehr?"

IronPort **Mail Flow Central™**

- **Zentralisierte Visualisierung von Informationen mehrerer Gateways**
- Nachrichtenverfolgung (Tracking)
- Periodische Reports



Auf einen Blick:
"Wurde die Nachricht zugestellt?"
"Wer bekommt den meisten Spam?

Tracking

SECUR TEC SYSTEMHAUS

- **Suche nach:**
  - Sender
  - Empfänger
  - Subject
  - Zeit
  - Message ID
  - IronPort Appliance

Message Details

Envelope and Header Information	
Sender:	jwinsel@gmx.de
Recipient(s):	wwiggles@[redacted]
Subject:	"I've_got your EMail on my_account!"
Message-ID Header:	822e.c5bed9f80aa@gmx.de
Message Size:	113.73 (KB)
Receiving IP:	10.160.38.200
Received Time:	April 19, 2005 20:46:05
SMTP Authenticated User Id:	N/A

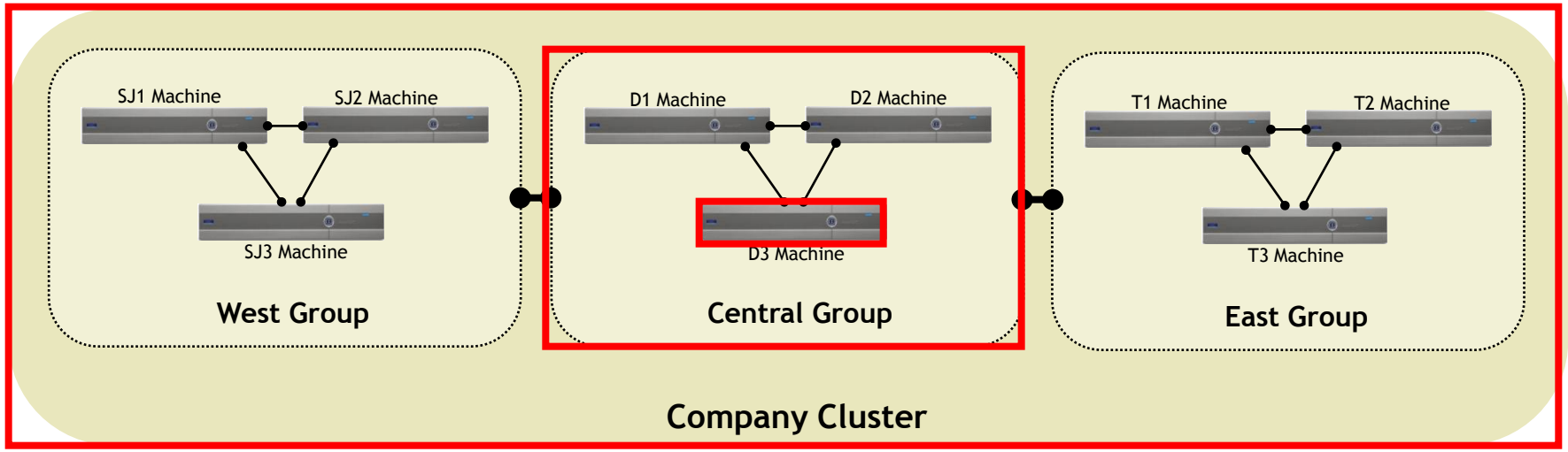
Sending Host Information	
IP Address:	10.99.1.103
Reverse DNS hostname:	sfh15110a14.[redacted] (Verified)
SBRS score:	None

Message Processing	
April 19, 2005 20:46:05	Message enqueued
April 19, 2005 20:46:05	Message matched all recipients using policy 'DEFAULT' in the 'inbound' table
April 19, 2005 20:46:05	Message processed by Brightmail Anti-Spam. Verdict: Negative
April 19, 2005 20:46:05	Message processed by Sophos Anti-Virus. Verdict: Negative
April 19, 2005 20:46:05	Message quarantined in the Outbreak quarantine as a result of rule '.exe file in zip'
April 20, 2005 08:59:37	Message released from the Outbreak quarantine due to expiration of retention period
April 20, 2005 08:59:37	All quarantine processing for message is complete
April 20, 2005 08:59:37	Message matched all recipients using policy 'DEFAULT' in the 'inbound' table
April 20, 2005 08:59:37	VOF antivirus scan positive
April 20, 2005 08:59:37	Message dropped due to Antivirus verdict

Centralized Management

Mehrere Ebenen verfügbar

- **Cluster:** aufteilbar in mehrere Gruppen
- **Gruppe:** beinhaltet eine oder mehrere Appliances
- **Maschine:** Appliance



IronPort Appliances

SECUR TEC SYSTEMHAUS

IronPort X1050

- Multi Prozessor System
- 4 Drives; RAID 10 (je 146 GB)
- Für Global 2000 Unternehmen & ISPs

IronPort C650

- Dual Prozessor System
- 4 Drives; RAID 10 (je 146 GB)
- Für größere Unternehmen

IronPort C350

- Ein Prozessor System
- 2 Drives; RAID 1 (je 146 GB)
- Für mittelgroße Unternehmen

IronPort C100

- Ein Prozessor System
- 2 Drives; RAID 1 (je 80 GB)
- Für Firmen bis zu 1000 Mitarbeitern