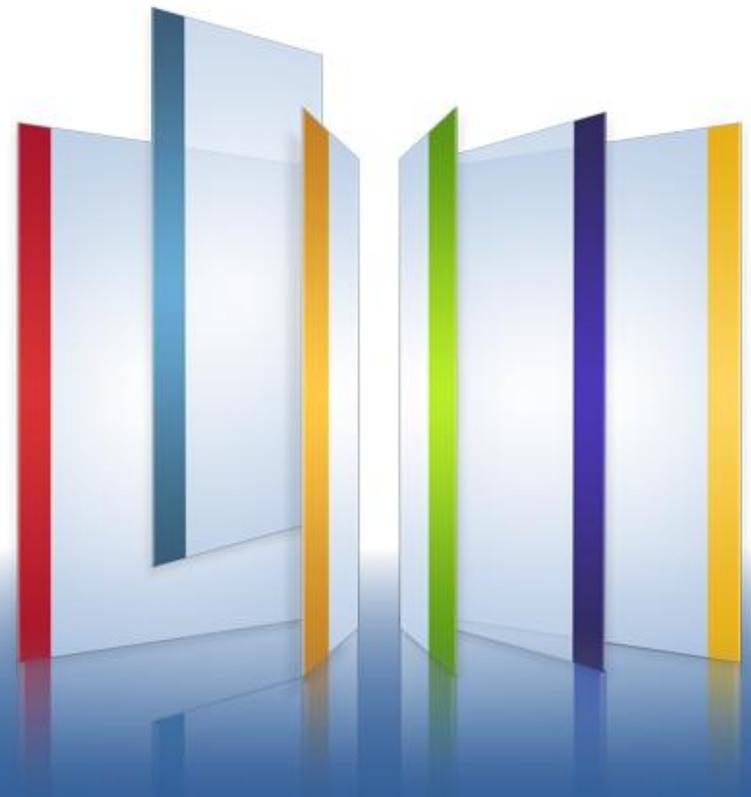




What's new in R71

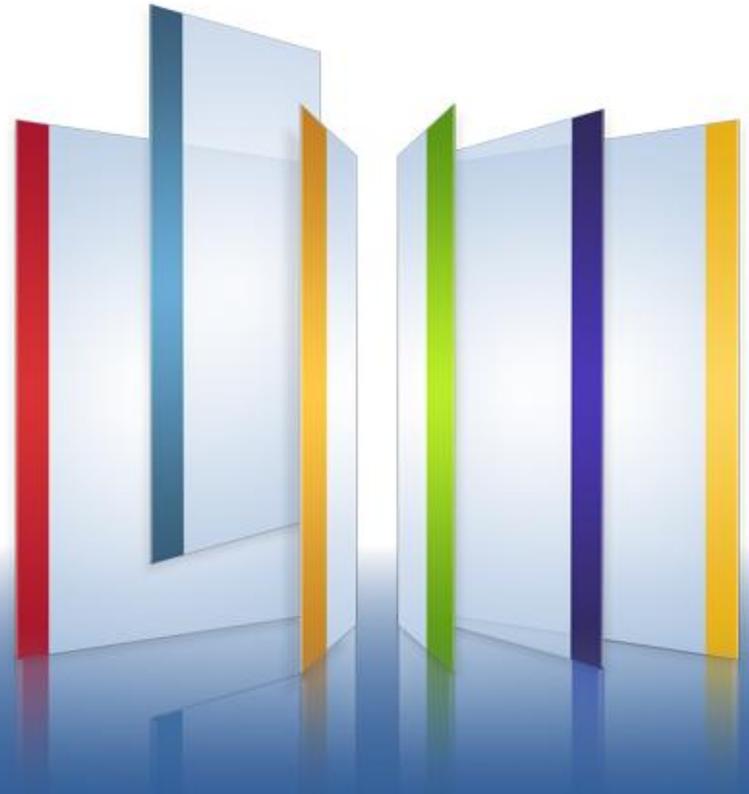
Jani Ekman

June 10, 2010





Check Point Makes DLP Work



Agenda

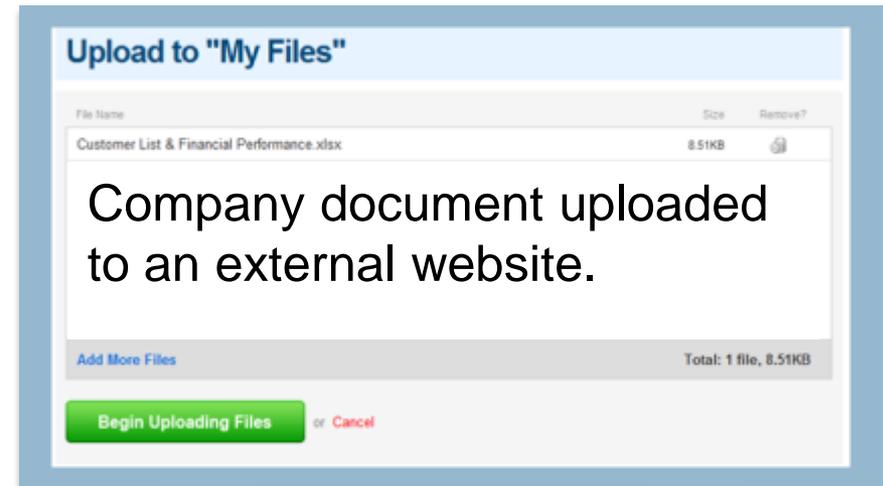
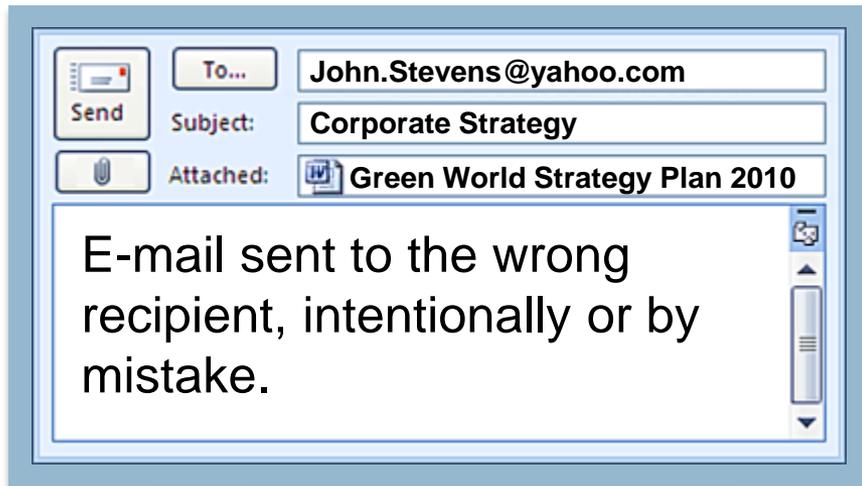
- 1 What is Data Loss?
- 2 Key Challenges of DLP
- 3 Introducing Check Point DLP
- 4 Summary



Check Point DLP
Makes data loss prevention work



What is DLP?



Data breaches have happened to all of us

Data Breaches—Headline Examples



Home > News > Privacy & data protection

August 25, 2006 5:11 PM PDT

Verizon gaffe lets customer detail

By Joris Evers
Staff Writer, CNET News

Related Stories

Theft of laptop puts thousands of identities at risk
August 11, 2006

Portfo

BUSINESS NE

HOME

Lilly's

by Katherine
A secret
When the M
was in conf
flew behind th
officials of leakin

As the company's law
... they discovered

BUSINESS TRA

mail to Wrong Gmail Address, Sues

Categories: Breaches



According to a court document in the case, in August a customer of the Rocky Mountain Bank asked a bank employee to send certain loan statements to a representative of the customer. The employee however, inadvertently sent the e-mail to the wrong Gmail address. Additionally, the employee had attached a sensitive file to the e-mail that should not have been sent at all.



It's Not Just About Regulatory Compliance

Compliance

- ▶ Customer data
- ▶ Corporate data
- ▶ Patient data



Chief Compliance
Officer

Security

- ▶ Intellectual property
- ▶ Strategic plans
- ▶ Internal data



Chief Security
Officer

DLP Has Not Yet Been Solved!

Technology



Challenge

Computers can not reliably understand human content and context

IT Staff

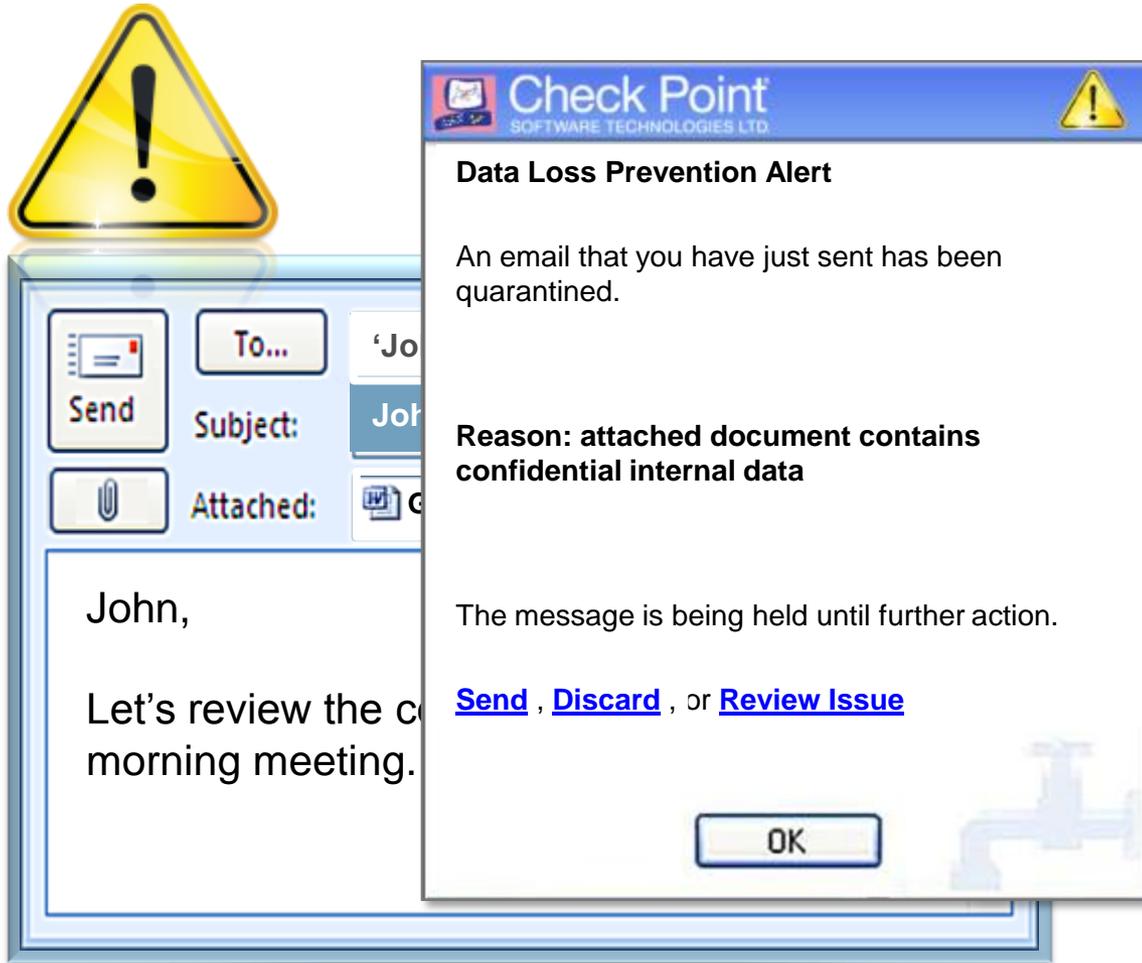


Challenge

Burden of incident handling

Exposure to sensitive data

Check Point Makes DLP Work



**Confidential
data sent to the**

User prompted

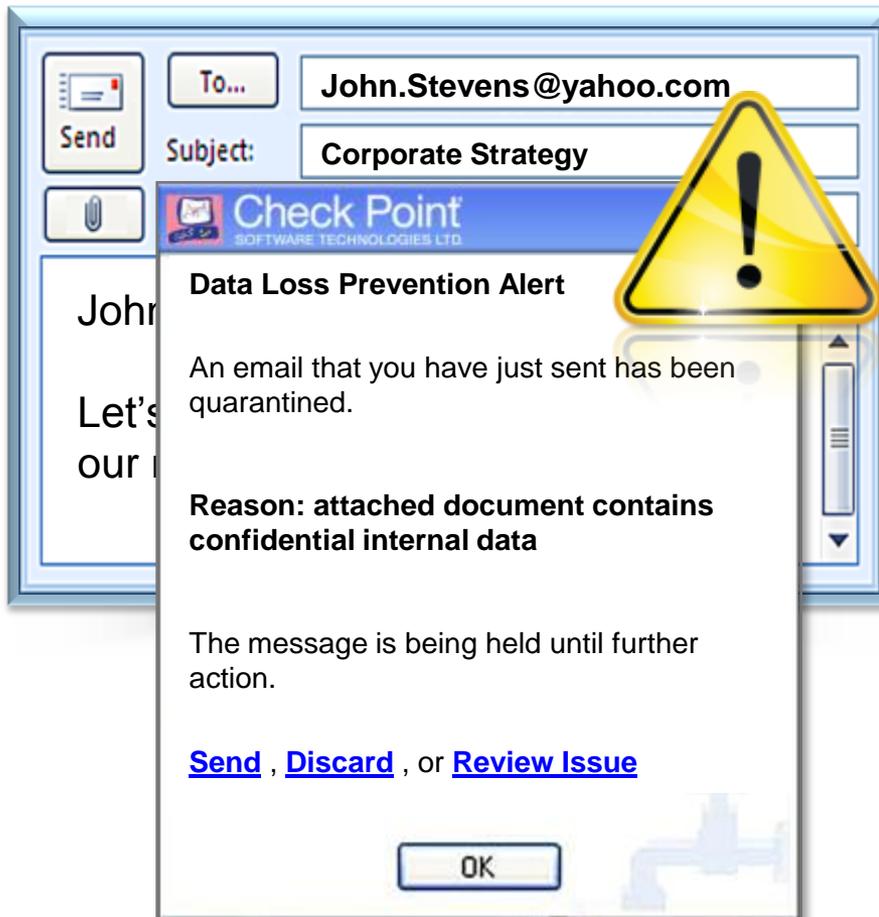
User remediates

Introducing Check Point Data Loss Prevention



Check Point Combines Technology and Processes to Make DLP Work

NEW!



Prevent

Move from detection to prevention

Educate

Users on corporate data policies

Enforce

Data loss business processes

New UserCheck™ Technology



Technology Challenge

Empowers users to remediate incidents in real time



IT Staff Challenge

Educates users on DLP policies without involving IT staff

How Does Check Point DLP Work?



MultiSpect™ Detection Engine

Simple Rule-based Policy Management

Full Network Enforcement



New MultiSpect™ Technology

MultiSpect Detection Engine

Correlates data from multiple sources using open language

250+ Data Types



The image shows a close-up of a Texas Department of Transportation Social Security card resting on a computer keyboard. The card is blue and white with the Texas state flag and the text 'TEXAS DEPARTMENT OF TRANSPORTATION' and 'SOCIAL SECURITY'. The keyboard keys are visible in the foreground and background.

Detects more than 600 file formats

Over 250 pre-defined content data types

Detect and recognize proprietary forms and templates

Simple Rule-based Policy Management



Easily Define Policy to Detect, Prevent or Ask User

Firewall | NAT | IPS | Anti-Spam & Mail | SSL VPN | Data Loss Prevention | Anti-Virus & URL Filtering | IPSec VPN | QoS | Desktop

Overview | Policy | Enforcing Gateways | Data Types | My Organization | Additional Settings

Data Loss Prevention (DLP)

New Rule | Delete | Grouping: Category | Type to Search

Data	Source	Destination	Action	Exceptions	Track	Install On	Category
General Business Records	My Organization	* Outside My Org	Prevent	None	Log	* DLP Blades	Business Inf...
Employee Names	My Organization	* Outside My Org	Ask User	None	Log	* DLP Blades	Business Inf...
Employee Email Address...							
Business Plan	My Organization	* Outside My Org	Ask User				Business Information
Credit Card Numbers	My Organization	* Outside My Org	Prevent				Compliance
Compliance (2)							
Credit Card Numbers	My Organization	* Outside My Org	Prevent	None	Log	* DLP Blades	Compliance
HIPAA	My Organization	* Outside My Org	Prevent	None	Log	* DLP Blades	Compliance
Personally Identifiable Information (2)							
Names and Surnames	My Organization	* Outside My Org	Detect	None	Log	* DLP Blades	Personally I...
General Personal Data ...	My Organization	* Outside My Org	Detect	None	Log	* DLP Blades	Personally I...

Centralized Management



Data Loss Prevention

tion (DLP) Policy

Grouping: By Category

Source	Destination	Action	Comments
My Organization	* Outside	Detect	
My Organization	* Outside	Ask user	
My Organization	* Outside	Inform user	
My Organization	* Outside	Detect	
My Organization	* Outside	Detect	

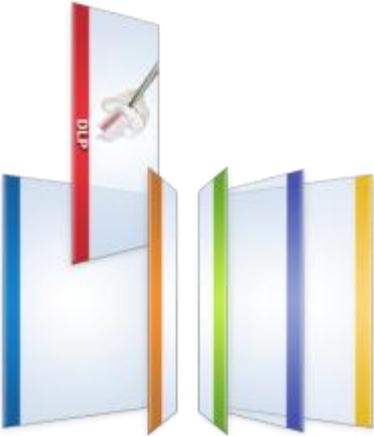
**For Unified Control
Across the Entire
Security Infrastructure**

Ease-of-Deployment

Software Blade

Dedicated Appliance

**Network-based
Inline Solution**



On Existing Gateways or
Open Servers



DLP-1



Be Up and Running
Day-1!

Move from Detection to Prevention

Proactively block intentional and unintentional data loss



Inline network-based Software Blade running on any existing Check Point gateway



Supporting HTTP, SMTP and FTP protocols



UserCheck notification using either thin agent or a returning email to the user



Scaling from hundred to thousands of users



Check Point combines technology and processes **to make DLP work**



Prevent Data Breaches
Move from detection to prevention

Enforce Data Policies
Across the entire network

Educate and Alert Users
Without involving IT staff

Check Point DLP User Scenarios

Key DLP Technologies

Scenario 1: Prevent

Block Web upload of proprietary information

Scenario 2: Enforce

Filter communications of confidential information based on policy exception

Scenario 3: Alert, Ask and Educate

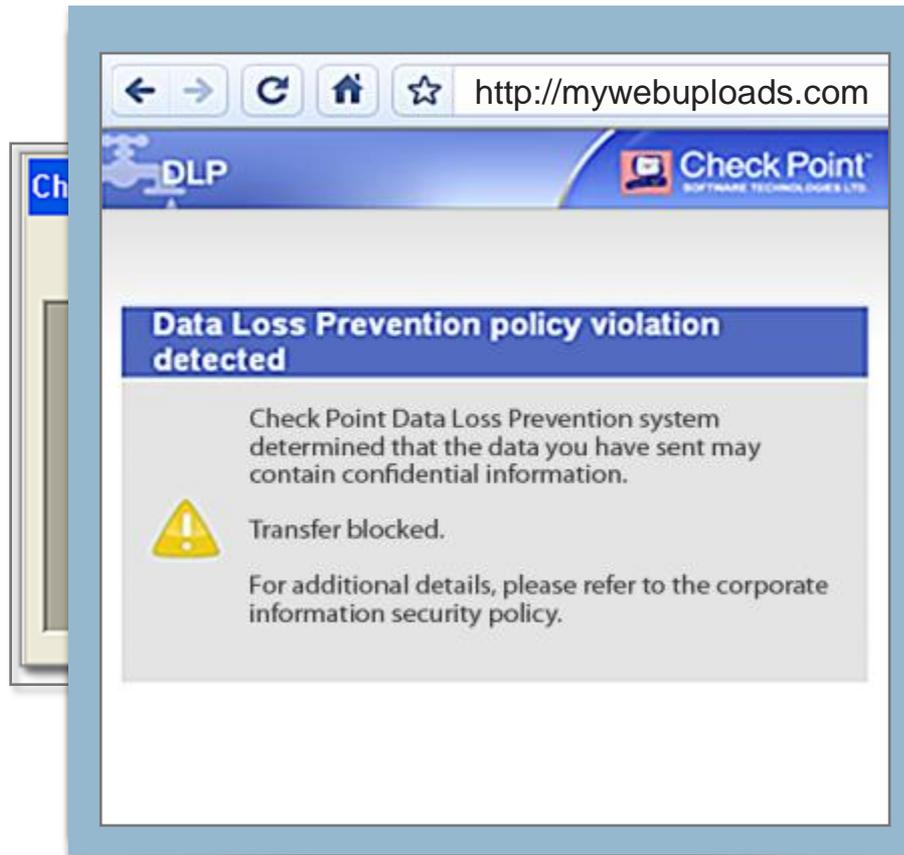
Ask user to confirm and remediate potential breach

Preemptively Prevent Data Breaches

Web Upload of Proprietary Information



Software Developer



**Check Point
DLP blocks
upload and
notifies user**

host site

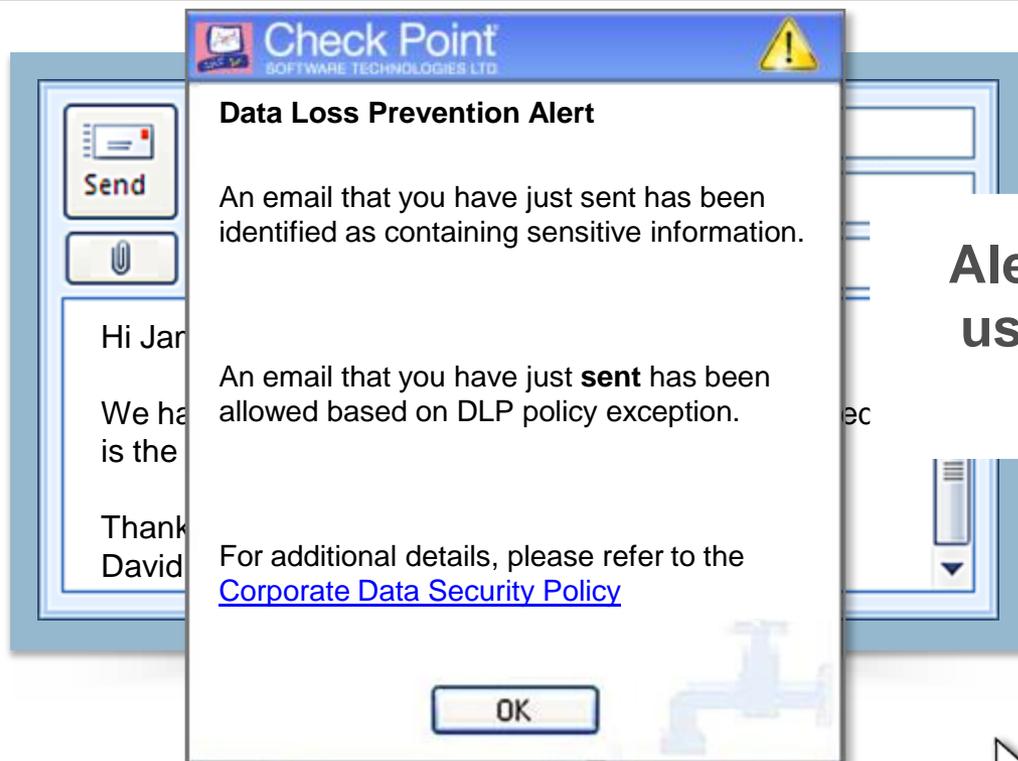


Filter Based on Corporate Data Policies

Policy Exception Allows Email to Pre-selected Recipients



Corporate Development VP



Data Loss Prevention Alert

An email that you have just sent has been identified as containing sensitive information.

An email that you have just **sent** has been allowed based on DLP policy exception.

For additional details, please refer to the [Corporate Data Security Policy](#)

OK

Alert notifies user of data policy

M&A contract to attorney

Alert, Ask and Educate Users

Check Point Brings User Remediation to DLP



Chief
Financial
Officer

← → ↻ 🏠 ☆

DLP **Check Point**
SOFTWARE TECHNOLOGIES LTD.

Email details

Subject: **Preliminary Financial Statement**
To: **mattg@acmecorp.com**
Cc:
Date:
Click [Here](#) to view this email

Are you sure you want to send this email?

Provide justification below for sending this email:

Hi,
This information is OK to send to
our outside auditor.
Thanks, Matt

Send Cancel

Reference {1E0DCC79-9FD3-617C-C583-0D98051F6BEE}

User provides
an explanation
of his request
to send



UserCheck™ provides User Remediation

Align DLP Rules to Your Policies and Processes

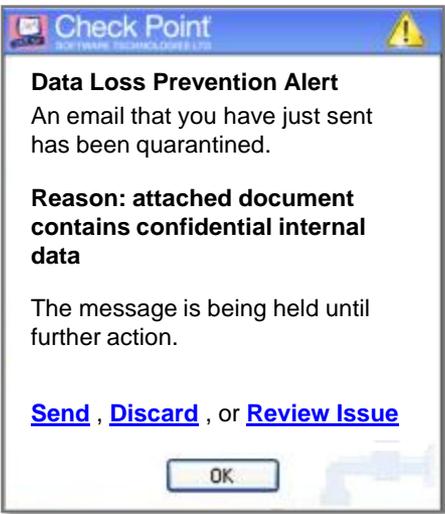
MultiSpect™ Detection Engine

UserCheck Provides User Remediation

1. Mail sent or document uploaded

2. User alert

3. User remediation



Non-disruptive

Real-time

Educational

Adapts to Your Processes and Environment

Suspicious Communications



Identify unconventional business communication behavior

Examples

- ▶ Spreadsheets with over 500 rows
- ▶ More than 5 financial terms
- ▶ External recipients in BCC
- ▶ More than 10 company names
- ▶ Profanity

Multi-data Correlation Prevents Potential Violations

Correlates a combination of data types

PAYROLL SUMMARY SHEET



FROM: []

Item No.	Name	Social Security Number	Job Title	Gross Pay
1	John Smith	987-65-4320	CEO	\$ 200,000.00
2	Kevin Brian	987-65-4221	VP R&D	\$ 150,000.00
3	Margret White	769-65-7522	VP Marketing	\$ 153,000.00
4	Bob Johns	342-62-3323	CFO	\$ 140,000.00
				180,000.00

Prevents sending sensitive data to wrong recipients



Detect and Recognize Your Proprietary Forms

Forms F

Documents Based on a Corporate Template

INSURANCE CLAIM FORM

Any person who knowingly and with intent to injure, defraud, or deceive any insurance company or other person submits an insurance application or statement of claim containing any materially false, incomplete or misleading information may be committing a crime and may be subject to civil or criminal penalties.

Group Plan or Program: _____
Policyholder Policy Number Certificate/I.D. Number

Present Address: _____
No. and Street City or Town State Zip Code Country

Home Address: _____
No. and Street City or Town State Zip Code Country

Telephone Number: _____ Date of Birth: _____ Male Female (Circle One)

If payment was made to someone other than the Insured, who is to receive payment? _____

Relationship to insured: _____ Address: _____

Date of Accident or Sickness: _____ Nature of Accident or Sickness: _____

If accident, describe fully how and where accident occurred: _____

If injured in play or practice of sport, indicate what sport: _____

Is the insured covered under any other group plan, health maintenance organization, government plan, or insurance policy?
Yes No Insurance Company Policy Number: _____

Are you covered as a dependent under this policy? Yes No

Are you covered under your school's domestic student accident and sickness insurance plan? Yes No Name of School _____

Upl

Similar

► Recognize sensitive and temporary

Extended Data Type Creation

Custom Data Type



- ▶ Open Scripting Language

- ▶ Create completely new data types
- ▶ Enhance existing data types
- ▶ Flexibly tailor DLP to your environment

DLP-1 Appliance Specifications



	DLP-1 2571	DLP-1 9571
	Performance	
Number of users	1,000	5,000
Messages/Hour	70K	350K
Throughput	700 Mbps	2.5 Gbps
	Specifications	
Storage	500 GB	2 x 1 TB (RAID 1)
NICs	6 Copper 1GbE	10 Copper 1GbE
Optional Bypass card	4 ports - 2 segments (pre-packaged appliance)	4 ports - 2 segments (orderable as accessory)

Check Point combines technology and processes **to make DLP work**



Prevent Data Breaches
Move from detection to prevention

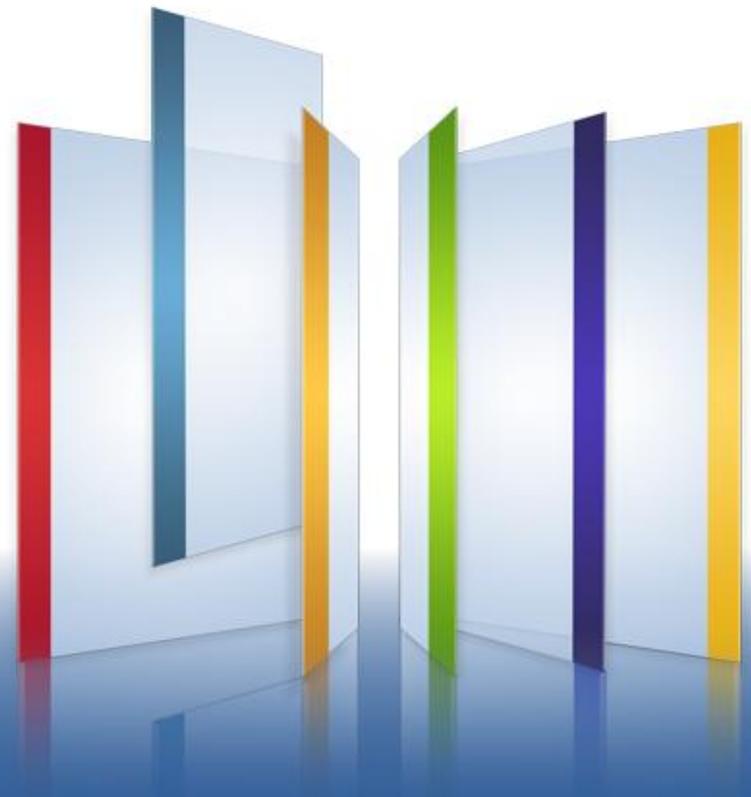
Enforce Data Policies
Across the entire network

Educate and Alert Users
Without involving IT staff



Turn Security Information into Action

Introducing SmartEvent Software Blade



1

Security Management Challenges

2

Introducing SmartEvent

3

SmartEvent Key Benefits

4

Summary

**Getting Actionable
Information**

**Leveraging Information
to Stop Attacks Across
the Enterprise**



Security management that provides



More Visibility

To monitor critical
events across
security systems



Faster Remediation

With more
actionable
information



More Simplicity

For more
efficiency and
easy deployment

Introducing SmartEvent Software Blade



SmartEvent translates
security information
into **action**



More Visibility



Faster Remediation



Simple!

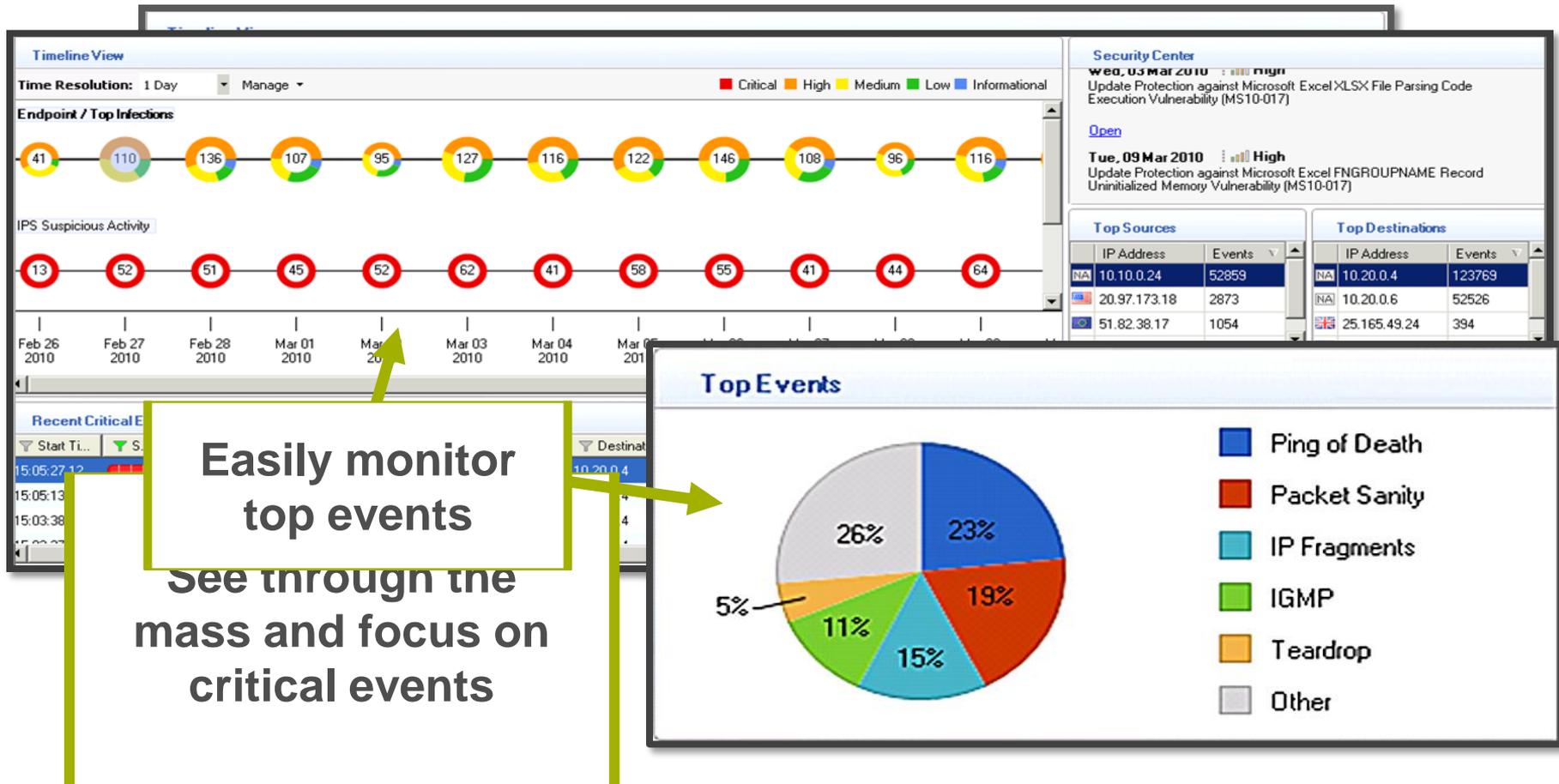
SmartEvent Software Blade



Better Visibility



Monitor ONLY what is important!



The screenshot displays the Security Center interface. The 'Timeline View' shows a sequence of events from Feb 26 to Mar 04, 2010. The 'Endpoint / Top Infections' row shows 11 circular gauges with values ranging from 41 to 146. The 'IPS Suspicious Activity' row shows 11 circular gauges with values ranging from 13 to 64. The 'Security Center' panel on the right lists updates for Microsoft Excel vulnerabilities. Below the timeline, a 'Recent Critical Events' table is partially visible. A 'Top Events' pie chart is overlaid on the bottom right, showing the distribution of event types.

Timeline View
Time Resolution: 1 Day | Manage

Endpoint / Top Infections

IPS Suspicious Activity

Security Center
Wed, 03 Mar 2010 | High
Update Protection against Microsoft Excel XLSX File Parsing Code Execution Vulnerability (MS10-017)
[Open](#)
Tue, 09 Mar 2010 | High
Update Protection against Microsoft Excel FNGROUPNAME Record Uninitialized Memory Vulnerability (MS10-017)

Top Sources

IP Address	Events
10.10.0.24	52859
20.97.173.18	2873
51.82.38.17	1054

Top Destinations

IP Address	Events
10.20.0.4	123769
10.20.0.6	52526
25.165.49.24	394

Recent Critical Events

Start Time	Destination
15:05:27.12	10.20.0.4
15:05:13	
15:03:38	
15:03:27	

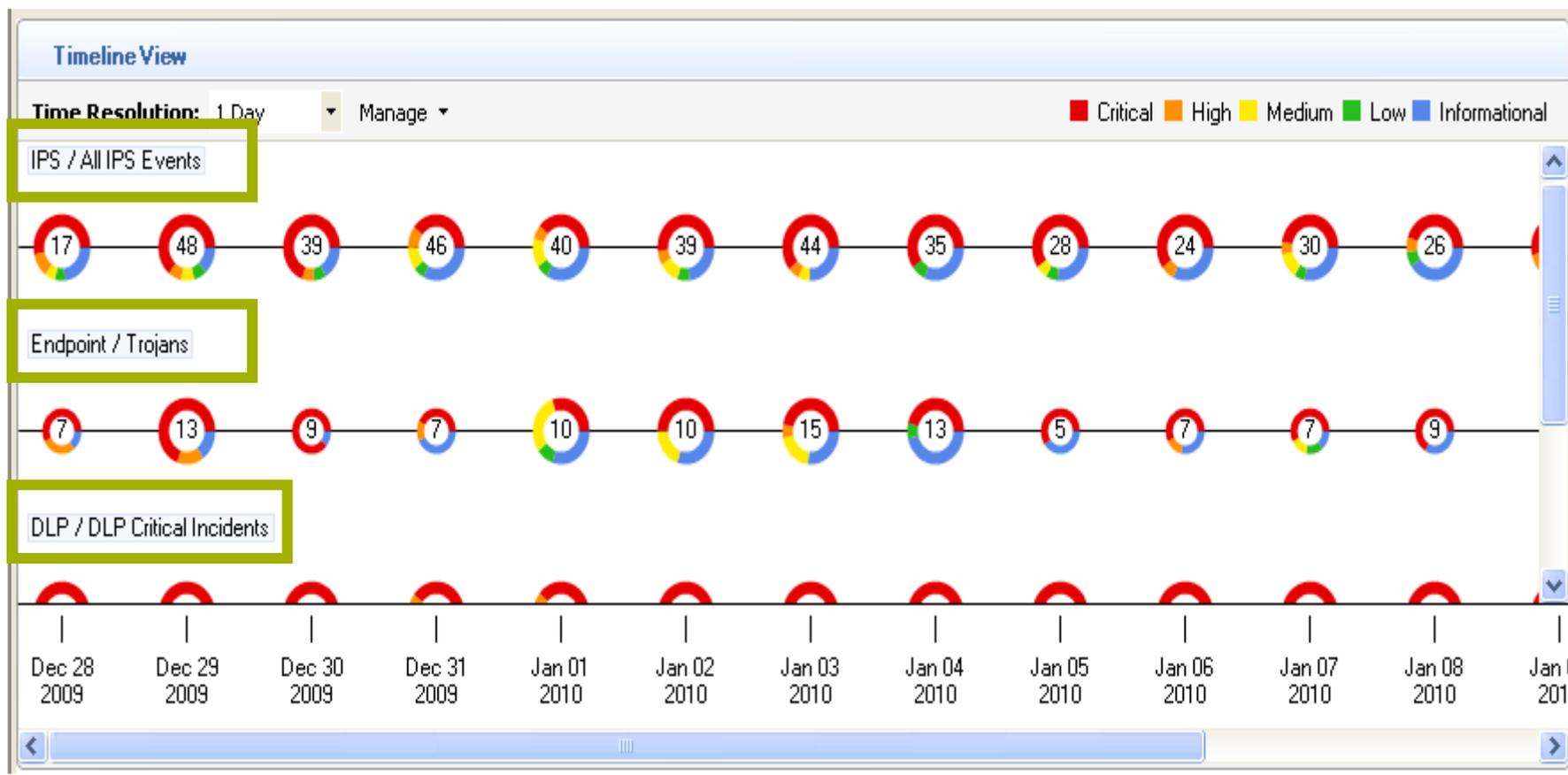
Top Events

- Ping of Death: 23%
- Packet Sanity: 19%
- IP Fragments: 15%
- IGMP: 11%
- Teardrop: 5%
- Other: 26%

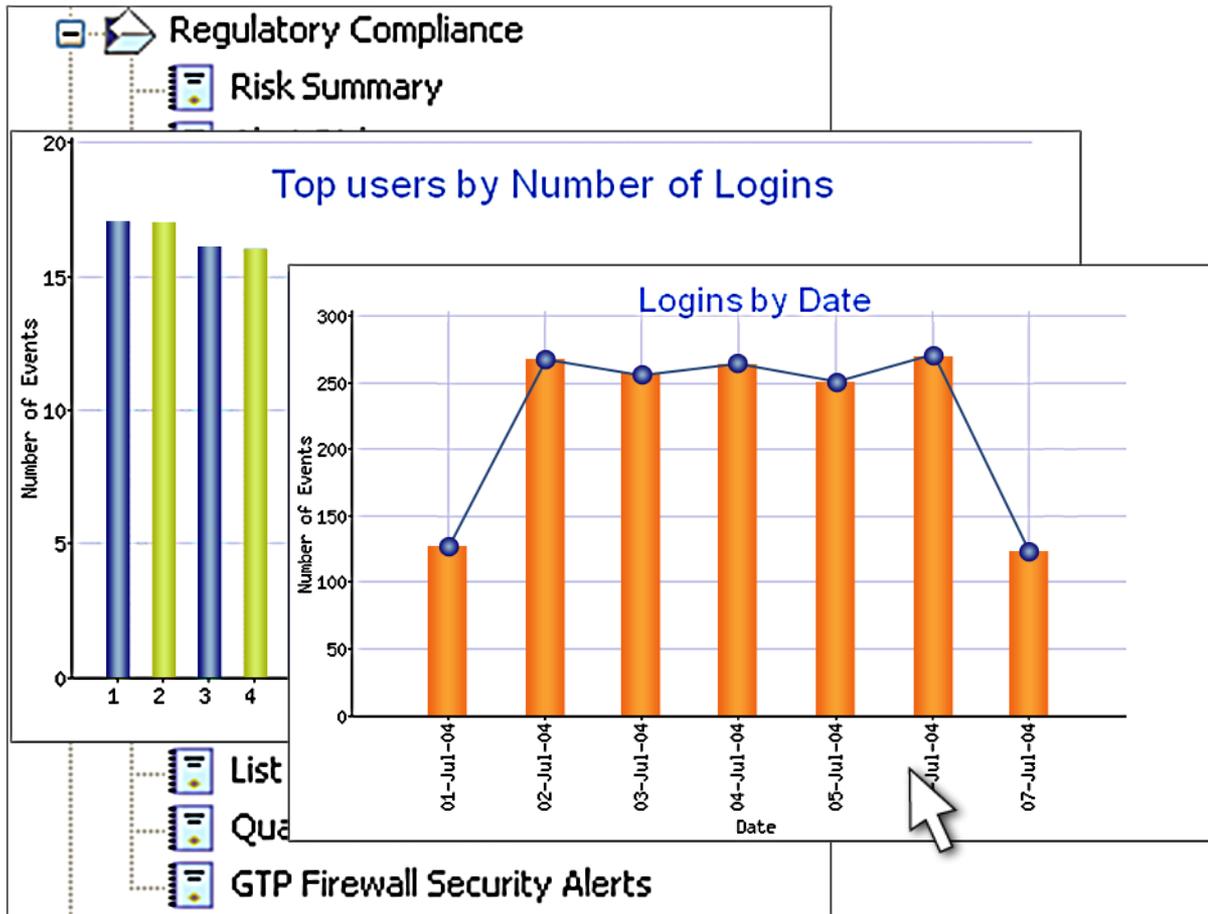
Easily monitor top events
See through the mass and focus on critical events

Better Visibility Across Security Systems

View unified events for firewall, IPS, DLP, endpoint and more in a single console



Unified compliance reporting



SOX Compliance



PCI Compliance



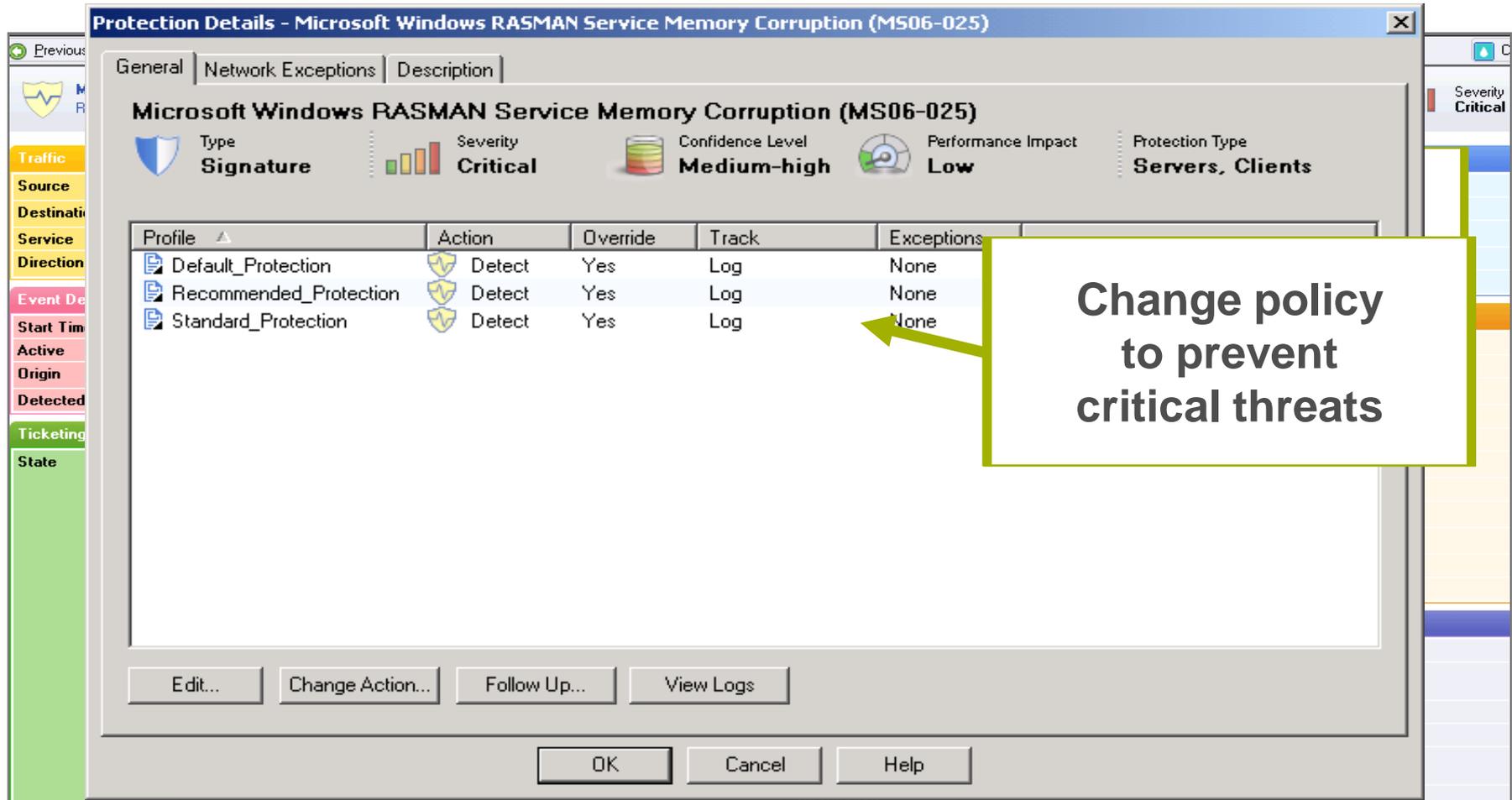
SmartEvent Software Blade



**Faster
Remediation**



Stop attacks straight from the event screen



Protection Details - Microsoft Windows RASMAN Service Memory Corruption (MS06-025)

General | Network Exceptions | Description

Microsoft Windows RASMAN Service Memory Corruption (MS06-025)

Type: **Signature** Severity: **Critical** Confidence Level: **Medium-high** Performance Impact: **Low** Protection Type: **Servers, Clients**

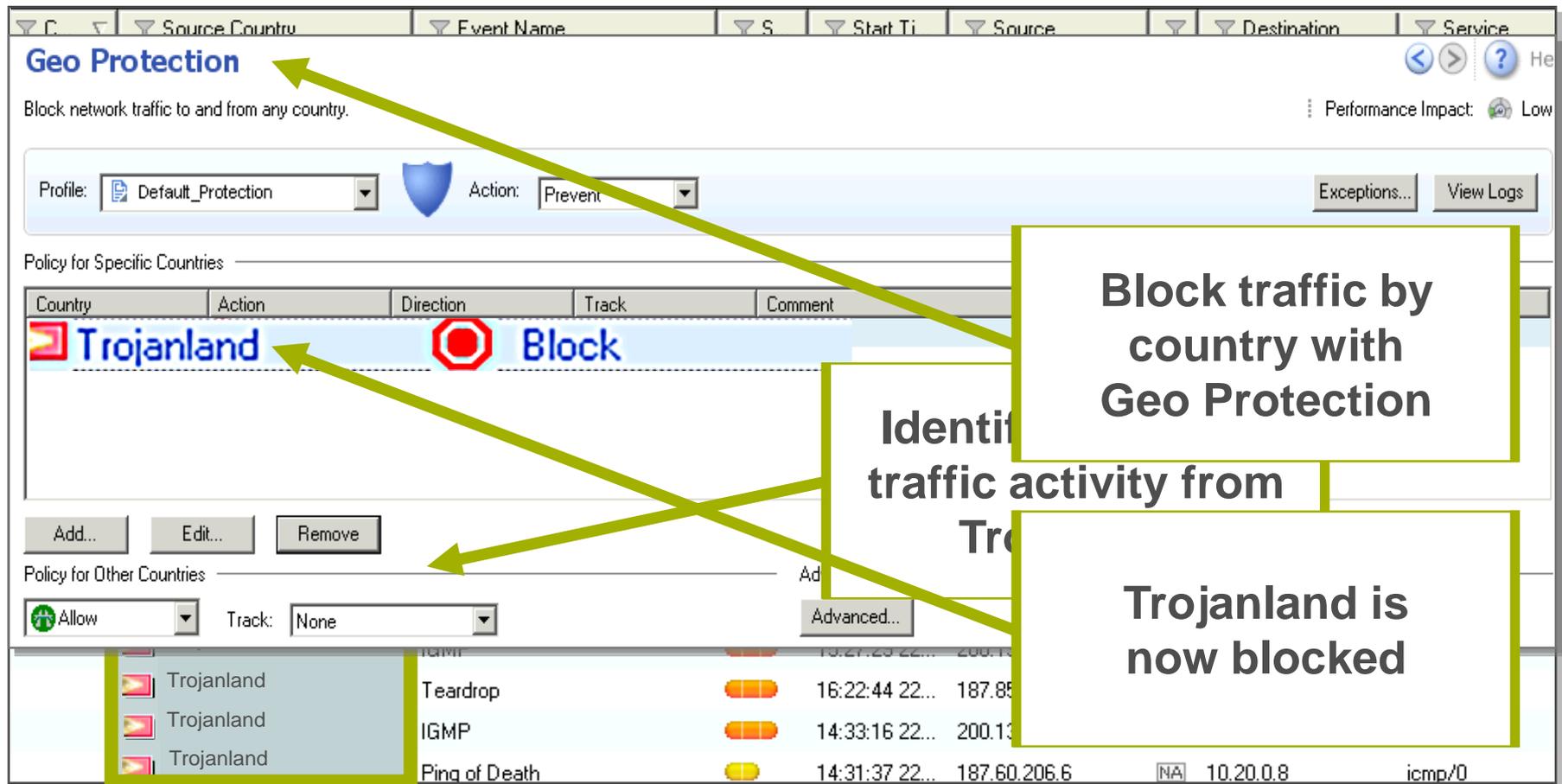
Profile	Action	Override	Track	Exceptions
Default_Protection	Detect	Yes	Log	None
Recommended_Protection	Detect	Yes	Log	None
Standard_Protection	Detect	Yes	Log	None

Change policy to prevent critical threats

Buttons: Edit... Change Action... Follow Up... View Logs

Buttons: OK Cancel Help

Block malicious traffic from rogue nations



The screenshot shows the Geo Protection configuration page in the Check Point management console. The page title is "Geo Protection" and the description is "Block network traffic to and from any country." The "Profile" is set to "Default_Protection" and the "Action" is set to "Prevent".

Under "Policy for Specific Countries", a table lists countries and their actions:

Country	Action	Direction	Track	Comment
Trojanland	Block			

Below this table are buttons for "Add...", "Edit...", and "Remove".

Under "Policy for Other Countries", the "Allow" option is selected and "Track" is set to "None".

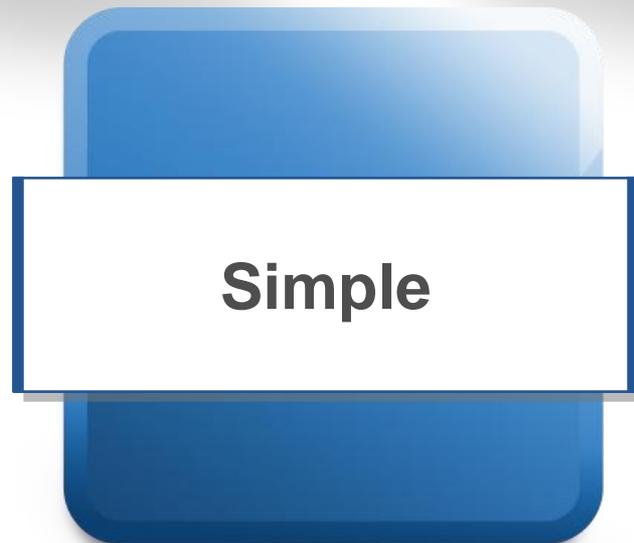
At the bottom, a list of traffic events is shown:

Country	Service	Direction	Track	Time	IP	Destination	Service
Trojanland	Teardrop			16:22:44	22...	187.85	
Trojanland	IGMP			14:33:16	22...	200.13	
Trojanland	Ping of Death			14:31:37	22...	187.60.206.6	NA 10.20.0.8 icmp/0

Three callout boxes with yellow borders and arrows pointing to the interface:

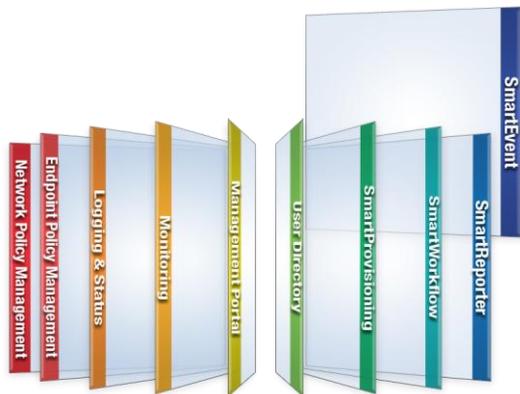
- Top box: "Block traffic by country with Geo Protection" (points to the "Geo Protection" title)
- Middle box: "Identify traffic activity from Trojanland" (points to the "Trojanland" entry in the table)
- Bottom box: "Trojanland is now blocked" (points to the "Block" action in the table)

SmartEvent Software Blade



Deployment Options

Software Blade



Easily add to your existing security management

All-in-One Dedicated Appliance



Pre-configured and plug-and-play



Smart-1 SmartEvent Appliances



The image shows three Smart-1 SmartEvent appliances (5, 25, and 50*) in a row, with a central monitor displaying the SmartEvent interface. To the left, there are vertical bars representing storage capacity. The appliances are housed in a rack-like structure.

	Smart-1 SmartEvent 5	Smart-1 SmartEvent 25	Smart-1 SmartEvent 50*
Storage	1 x 0.5 TB	4 x 0.5 TB	4 x 1 TB
Managed GWs (Recommended / Max)	5 / 25	25 / 50	50 / 150
Logging Capacity (Recommended)	2GB per day	10GB per day	25GB per day



Check Point SmartEvent
translates security
information into **action**

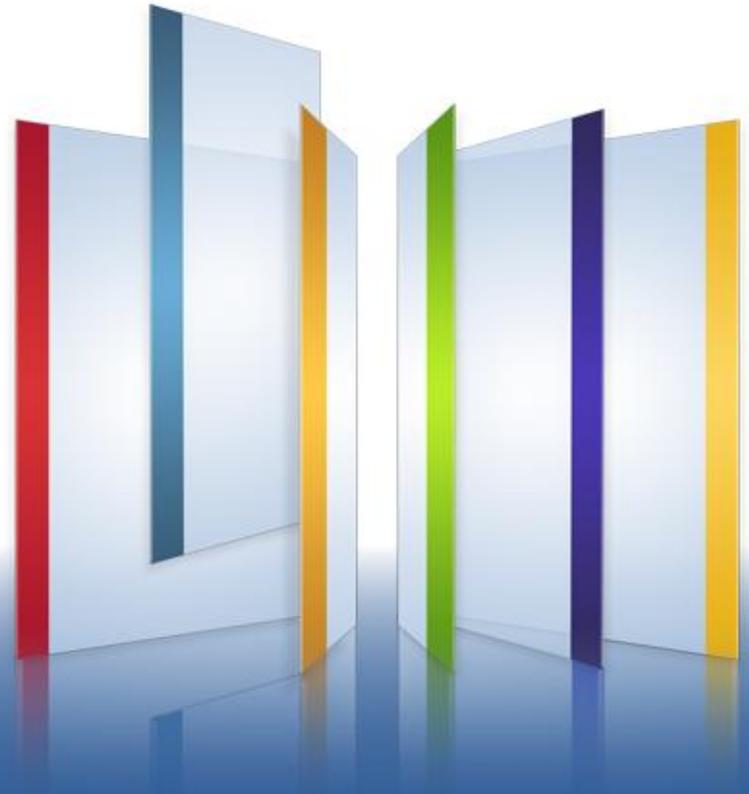
More Visibility
across firewall, IPS, DLP, endpoint and more

Faster Remediation

Easy To Deploy



Raising the bar on UTM-1 and UTM software blades performance



Agenda

1

Raising the bar on Antivirus and URL
Filtering software blades performance

2

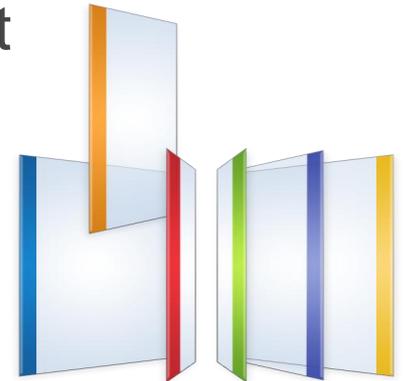
UTM-1 firewall performance improvement

3

How to benefit from boost

3

Summary



New Performance Levels

AV & URLF software blades

Amazing boost for Antivirus and URL filtering software blades performance across systems

UTM-1

Enhanced firewall performance for 5 UTM-1 models

Simple Upgrade

Simply upgrade your existing UTM-1 device or software blades to new R71 software release



Raising the Bar on Antivirus & URL Filtering Software Blades Performance



Antivirus throughput 2-core system

X 15 Antivirus throughput improvement

AV & URLF Concurrent Sessions

600000

Up to 80 X Anti-virus & URL Filtering connection capacity improvement

Better protection with better performance

NEW!



Up to 4x **Firewall** throughput improvement

AND

Up to 3x **IPS** throughput improvement

AND

Up to 4x **connection/second** improvement

Simple Software Upgrade

Simple Upgrade



Simple software upgrade to
new R71 release

On same existing system
or gateway

**Immediate protection and
performance boost**



More protection, uncompromised performance

Activate today all layers of security
on your gateway



The screenshot displays the configuration interface for a Check Point gateway. It is divided into two tabs: "Network Security (6)" and "Management (0)".

Network Security (6) features:

- Firewall
- IPSec VPN
 - Policy Server
- SSL VPN
- IPS
- URL Filtering
- Anti-Virus & Anti-Malware
- Anti-Spam & Email Security
- Monitoring

Advanced Networking features:

- QoS
- Dynamic Routing ⓘ
- ConnectControl ⓘ

Acceleration & Clustering features:

- SecureXL ⓘ

More features:

- FireWall-1 GX
- UserAuthority Server
- UserAuthority WebAccess

SSL VPN section:

SSL VPN

Integrated SSL VPN that provides efficient and secure remote access connectivity for both managed and unmanaged clients.

[More Info](#) ⓘ

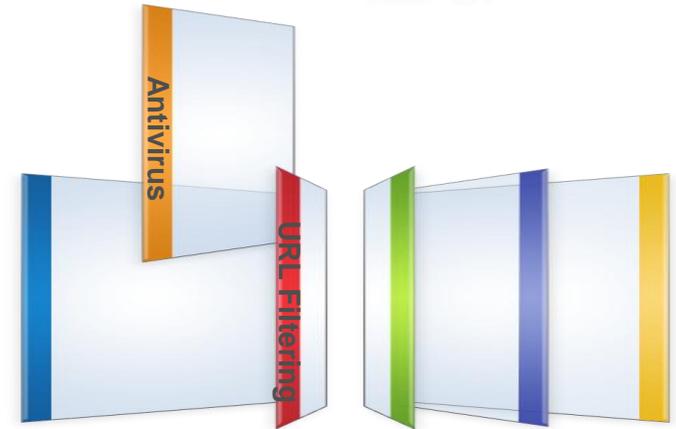
Performance Improvement Summary



Firewall x4

IPS x3

Connection/sec. x4

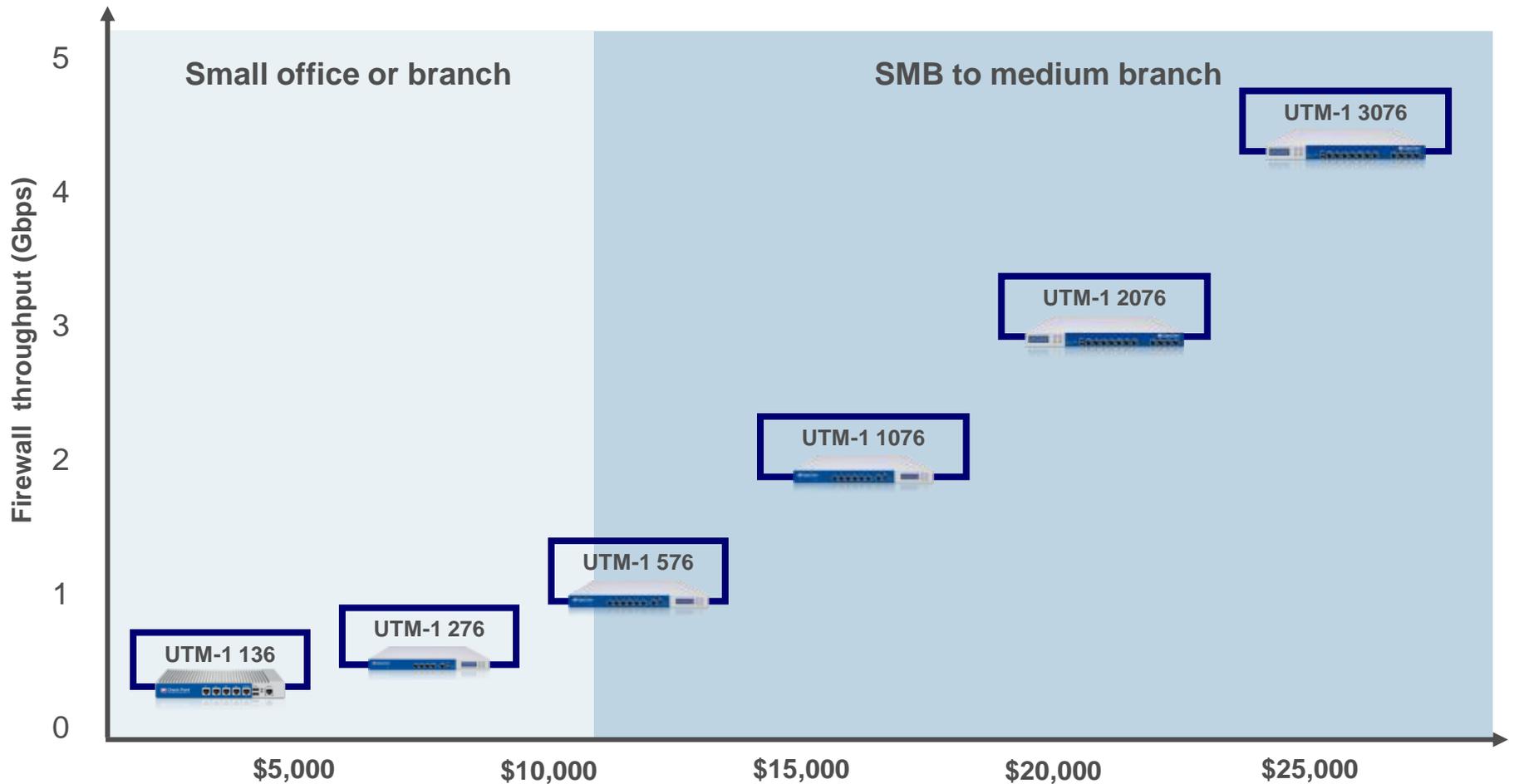


Antivirus x15

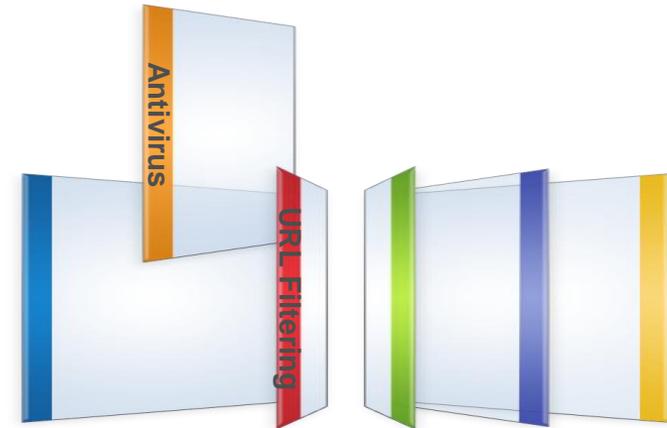
**AV and URLF
connection x80**

Raising the Bar on UTM-1 Performance

Up to 4x Firewall throughput improvement



Performance Improvement Summary



Firewall x4

Antivirus x15

**AV and URLF
connection x80**



Thank You!



Jani.ekman@checkpoint.com