



What's new in R71

Jani Ekman

June 10, 2010





Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Makes DLP Work



Agenda

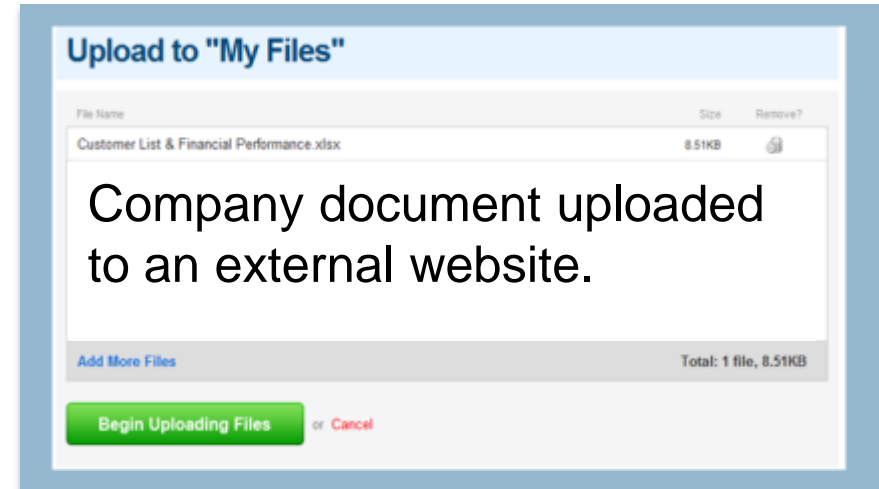
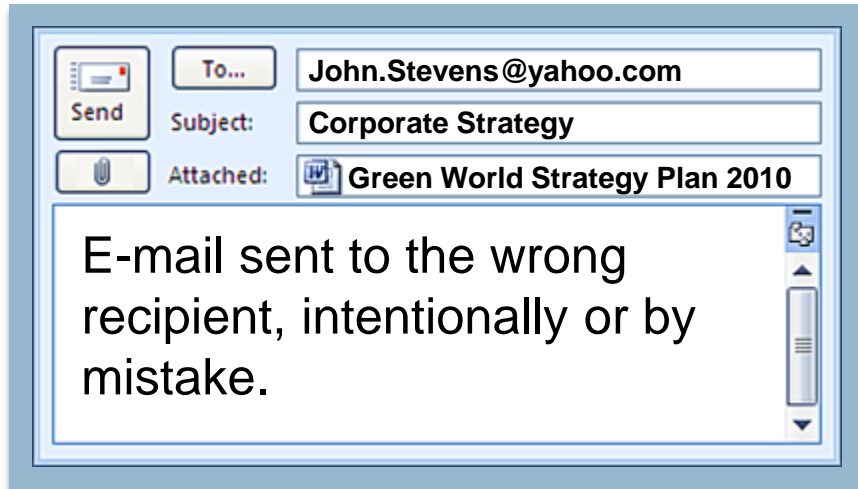
- 1 What is Data Loss?
- 2 Key Challenges of DLP
- 3 Introducing Check Point DLP
- 4 Summary



Check Point DLP
Makes data loss prevention work



What is DLP?



Data breaches have happened to all of us

Data Breaches—Headline Examples

Brand Damage
Compliance
Liabilities
Costly Fines

cnet news

Latest News CNET River Webware Crave Business Tech

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

was in confi

flew behind the

officials of leakin

As the company's

they discovered

BUSINESS TRA

Mail to Wrong Gmail Address, Sues

Categories: Breaches



ROCKY MOUNTAIN BANK

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

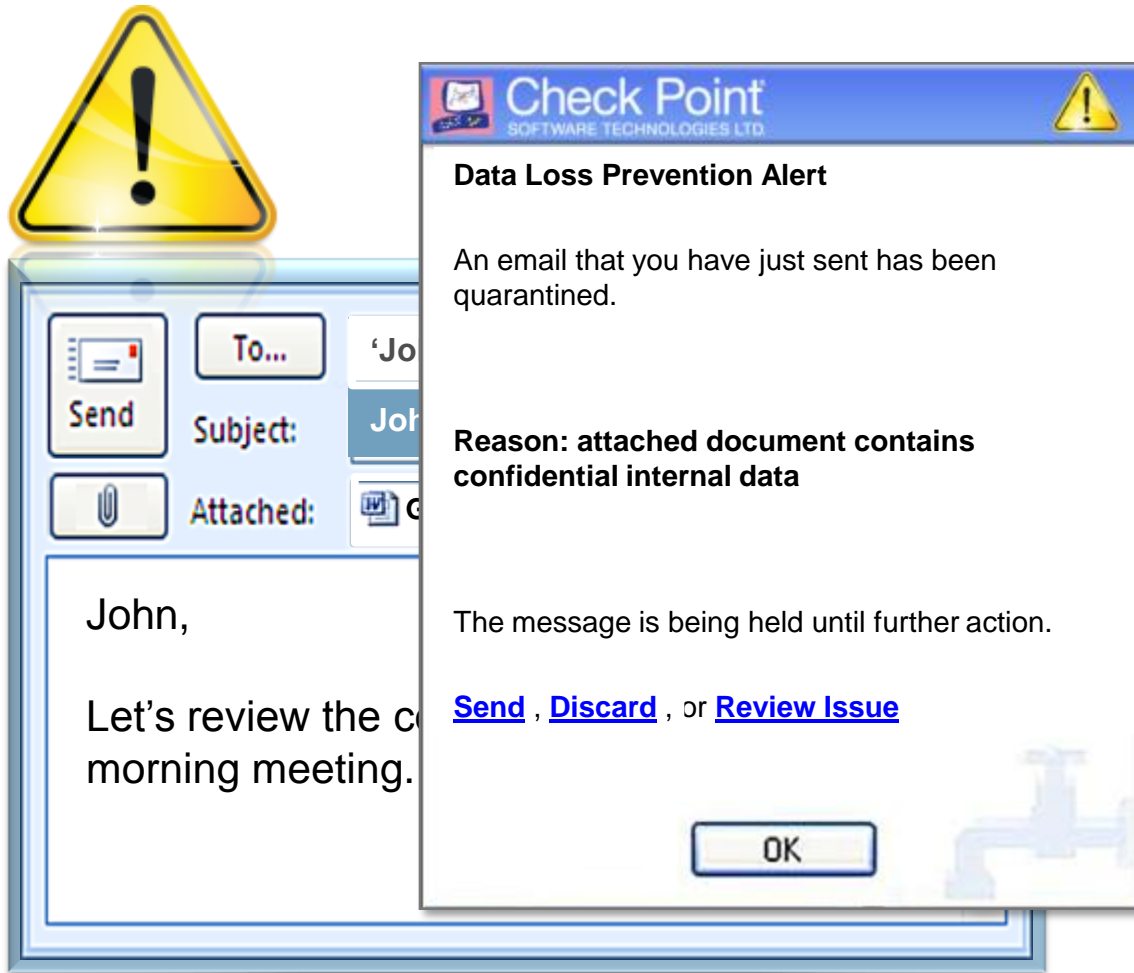


Challenge

Burden of incident handling

Exposure to sensitive data

Check Point Makes DLP Work



**Confidential
data sent to the**

User prompted

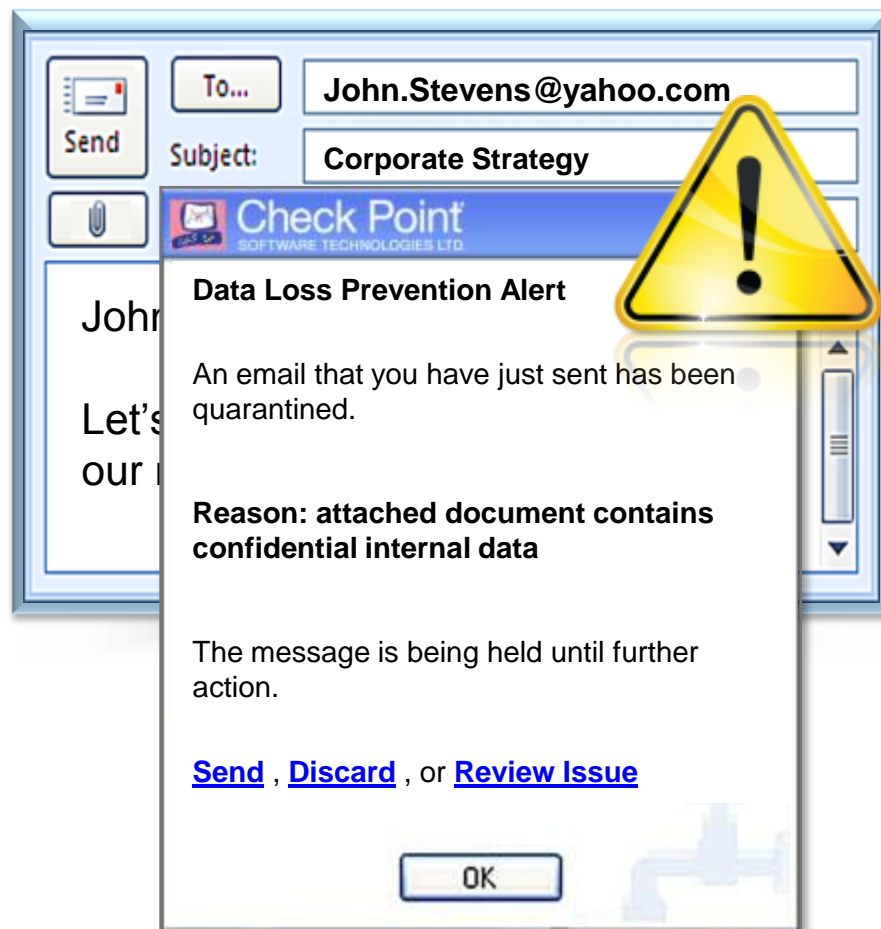
User remediates

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



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

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...							

Data	Source	Destination	Action	Category
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	Log	DLP Blades	Compliance
HIPAA	My Organization	Outside My Org	Prevent	Log	DLP Blades	Compliance

Personally Identifiable Information (2)

Names and Surnames	My Organization	Outside My Org	Detect	Log	DLP Blades	Personally I...
General Personal Data ...	My Organization	Outside My Org	Detect	Log	DLP Blades	Personally I...

Centralized Management



Data Loss Prevention

tion (DLP) Policy

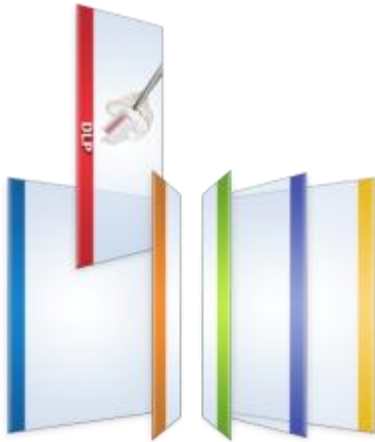
Grouping: By Category

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



On Existing Gateways or
Open Servers

Dedicated Appliance



DLP-1

Network-based Inline Solution



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

Check Point DLP at Work

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

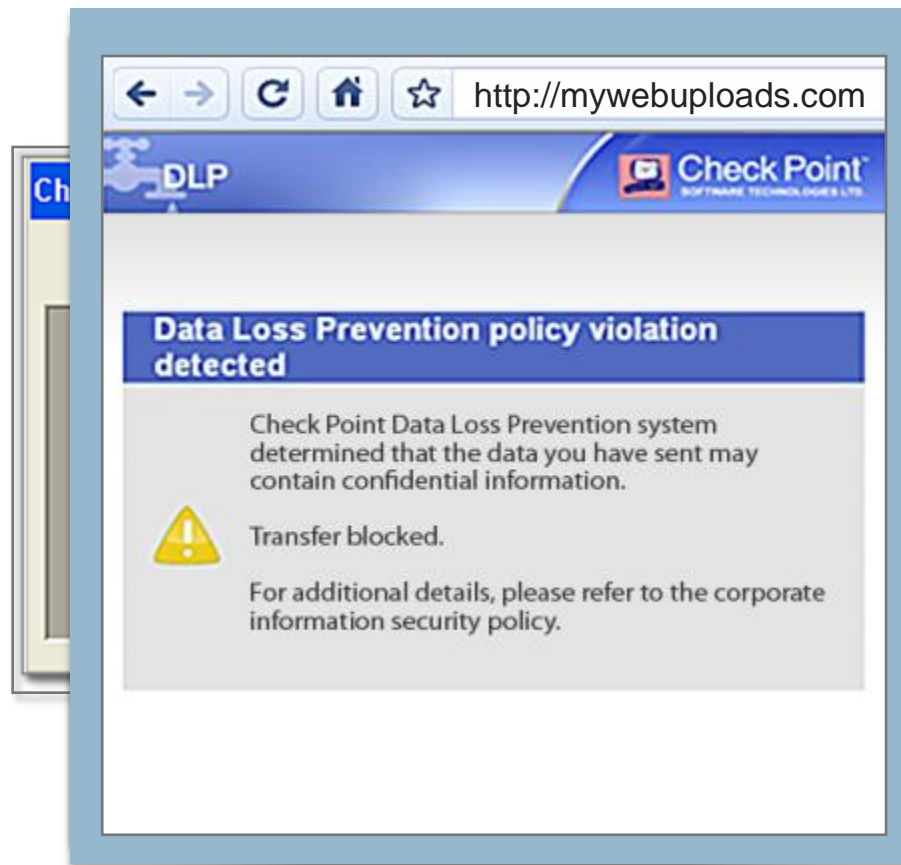
Ask user to confirm and remediate potential breach

Preemptively Prevent Data Breaches

Web Upload of Proprietary Information



Software Developer



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

host site

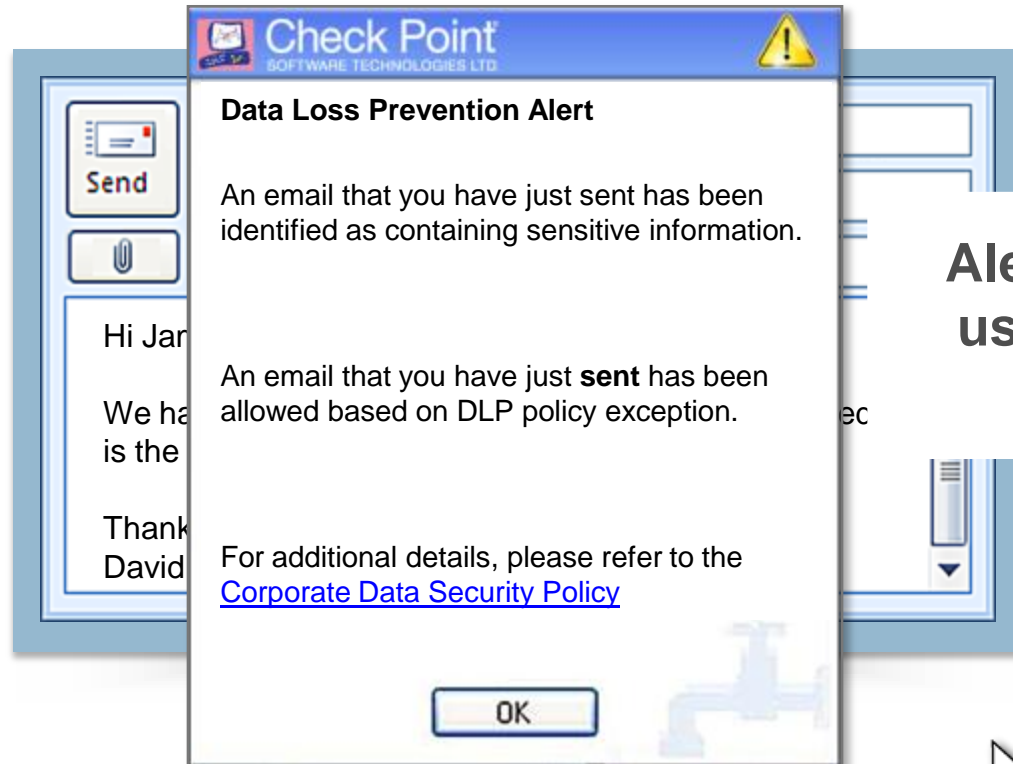


Filter Based on Corporate Data Policies

Policy Exception Allows Email to Pre-selected Recipients



**Corporate
Development
VP**



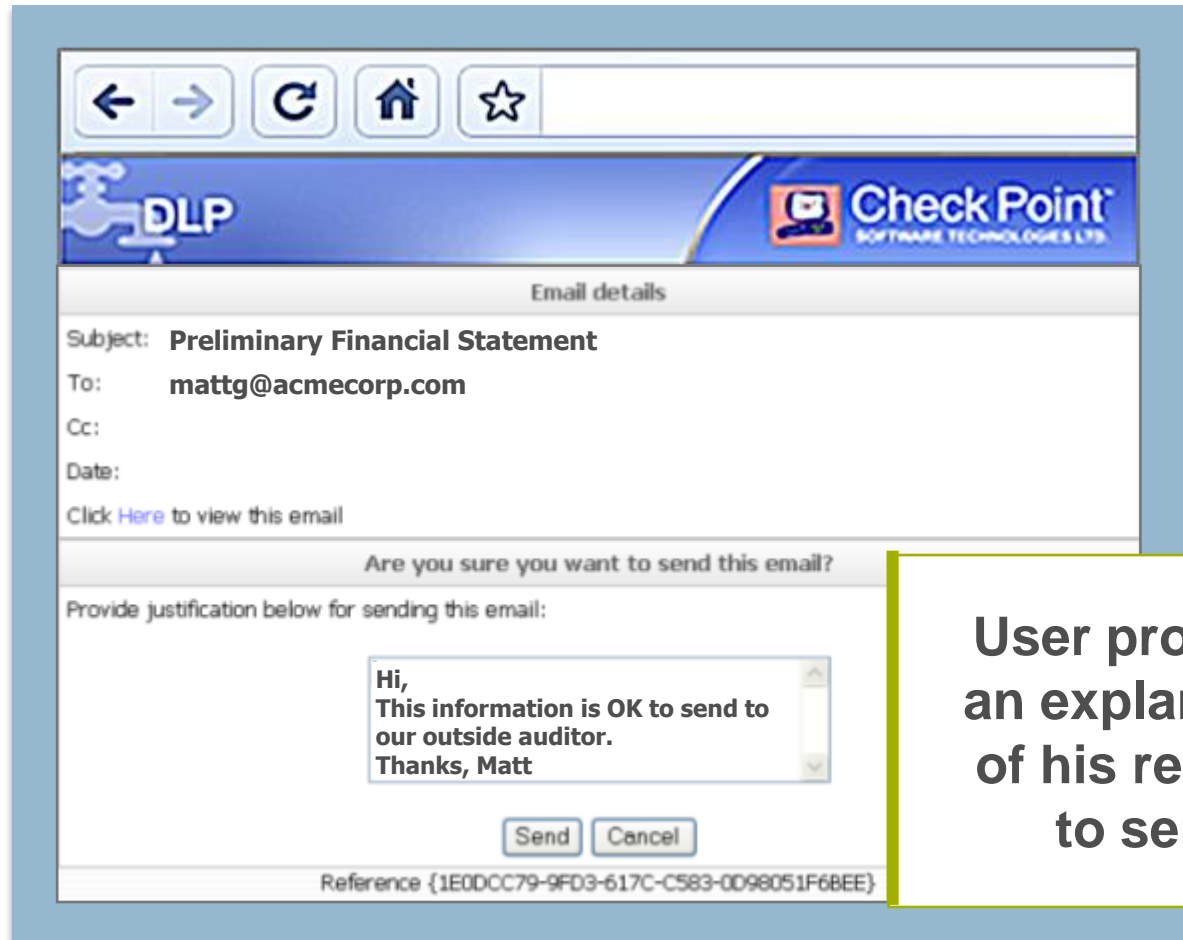
**Alert notifies
user of data
policy**

**M&A contract to
attorney**

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

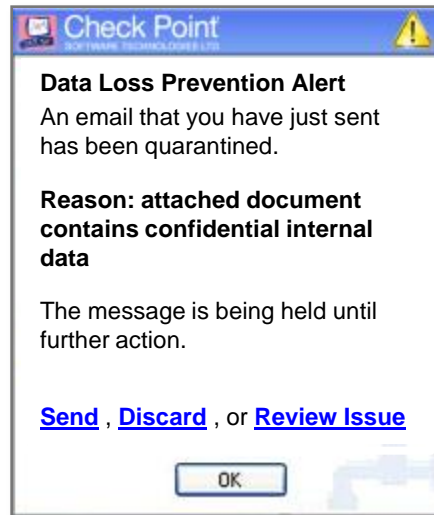
UserCheck Provides User Remediation

1. Mail sent or document uploaded



Non-disruptive

2. User alert



Real-time

3. User remediation



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: [redacted]				
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

Similar

► Recognize sensitive and templates

Data Type Wizard

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



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

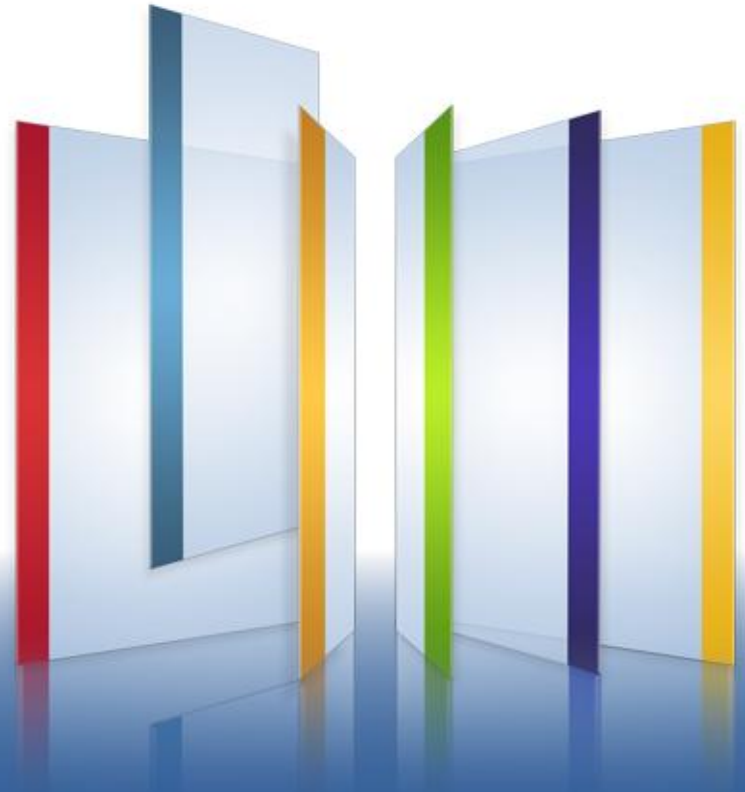
Educate and Alert Users

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!

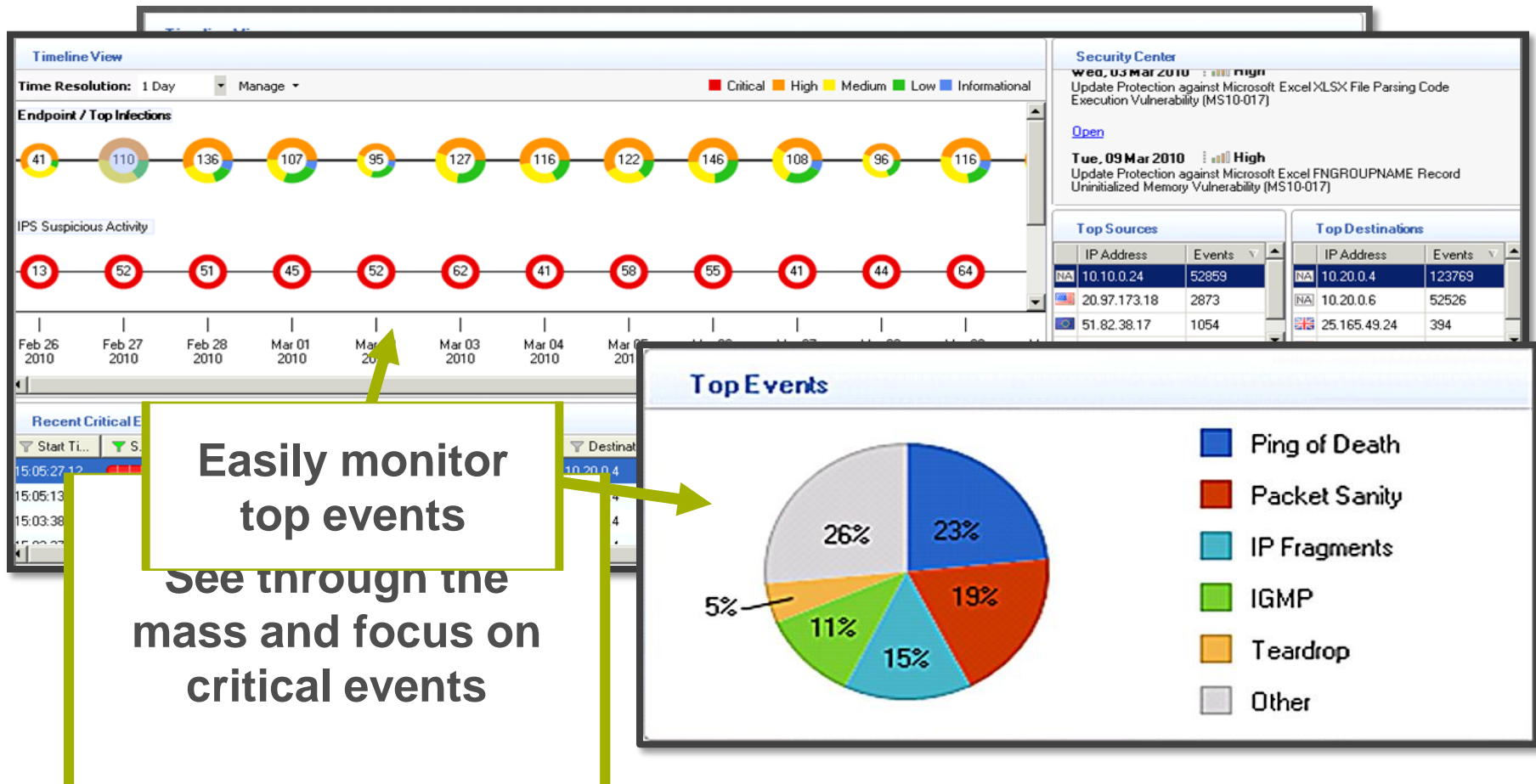


SmartEvent Software Blade



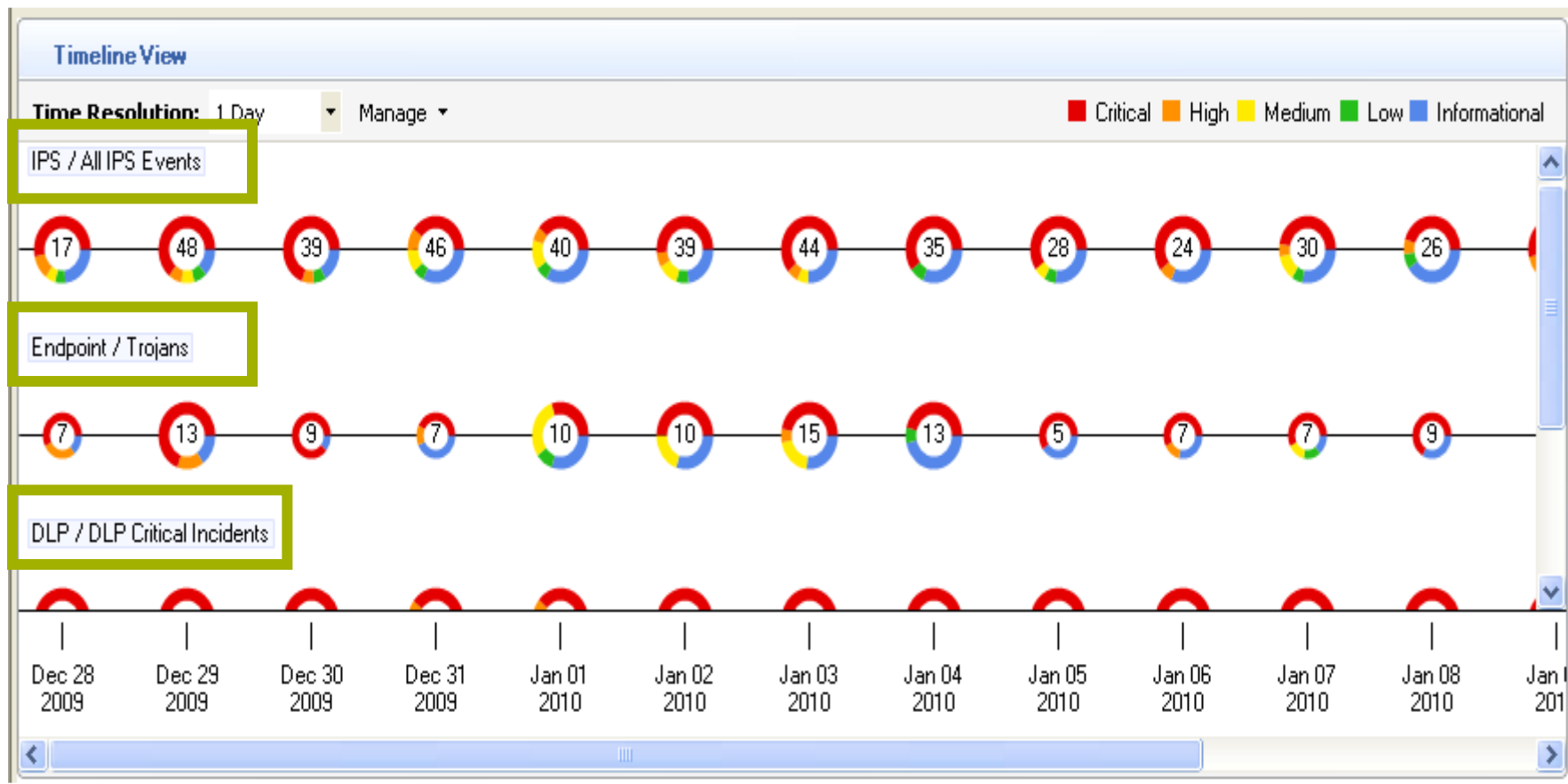
Better Visibility

Monitor ONLY what is important!

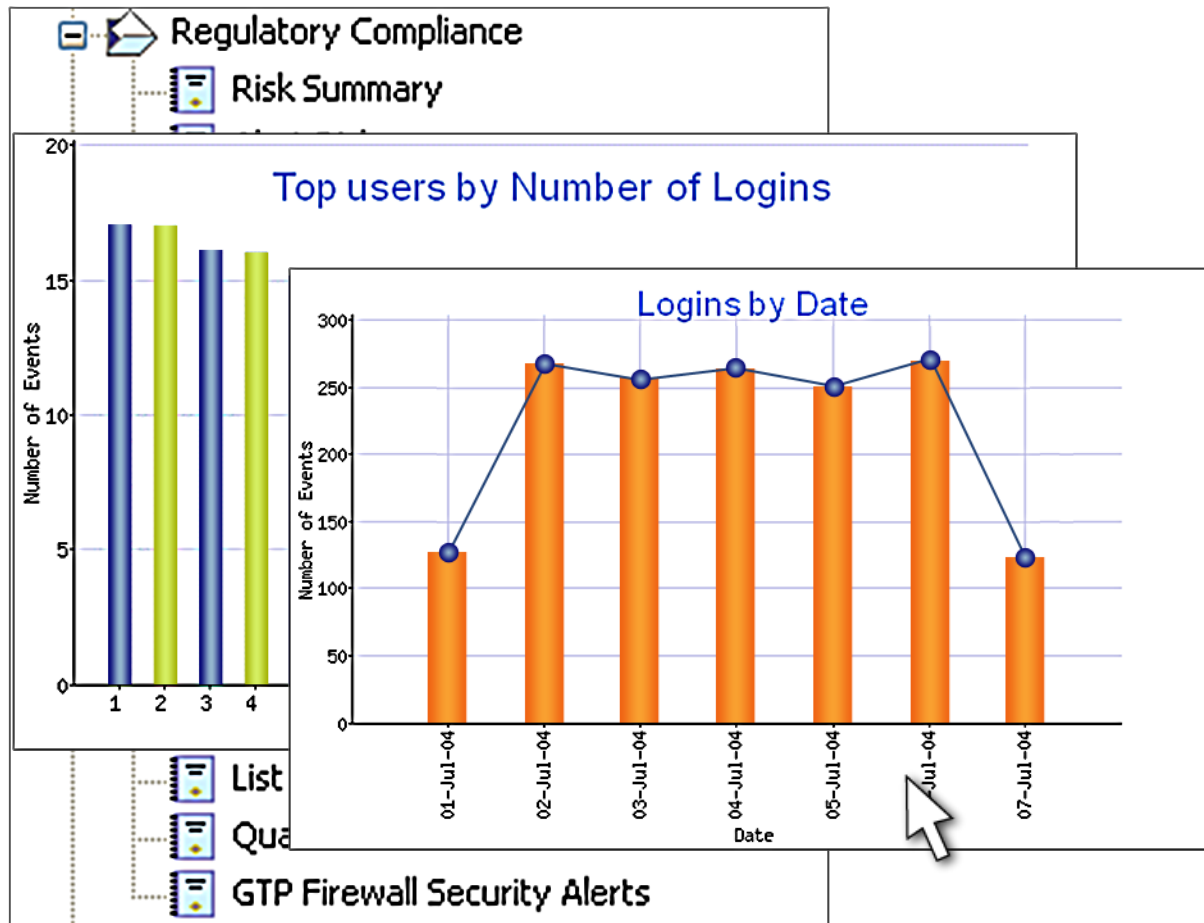


Better Visibility Across Security Systems

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



Unified compliance reporting



SOX Compliance

 **HIPAA**

PCI Compliance

 **AUDIT CHECKLIST**

☒ **Audit Satisfactory**

☐ **Nonconformances Found**

☐ **Observations Made**

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

Edit... | Change Action... | Follow Up... | View Logs



OK | Cancel | Help

Block malicious traffic from rogue nations

Geo Protection
Block network traffic to and from any country.

Profile: Action: Exceptions... View Logs

Policy for Specific Countries




Country	Action	Direction	Track	Comment
 Trojanland	 Block			

Add... Edit... Remove

Policy for Other Countries

Track: Advanced...

Trojanland

-  Trojanland
-  Trojanland
-  Trojanland

Trojanland is now blocked

Identify traffic activity from Trojanland

Block traffic by country with Geo Protection

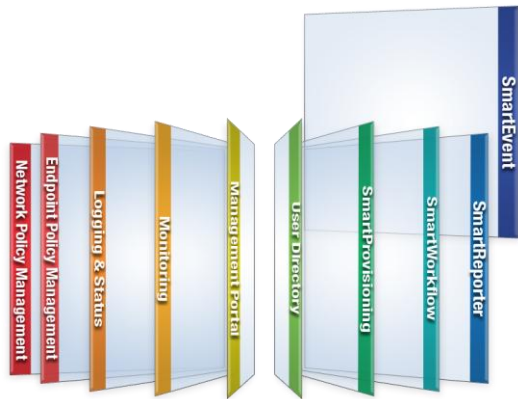
SmartEvent Software Blade



Simple

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 of different sizes (5, 25, and 50) displayed on a blue background. To the left of the appliances are several vertical bars in red, blue, green, and yellow, with the word 'SmartEvent' written vertically on the blue bar. The appliances are shown from a front-three-quarter view, with the 50-unit model being the largest and most prominent.

	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

Summary



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

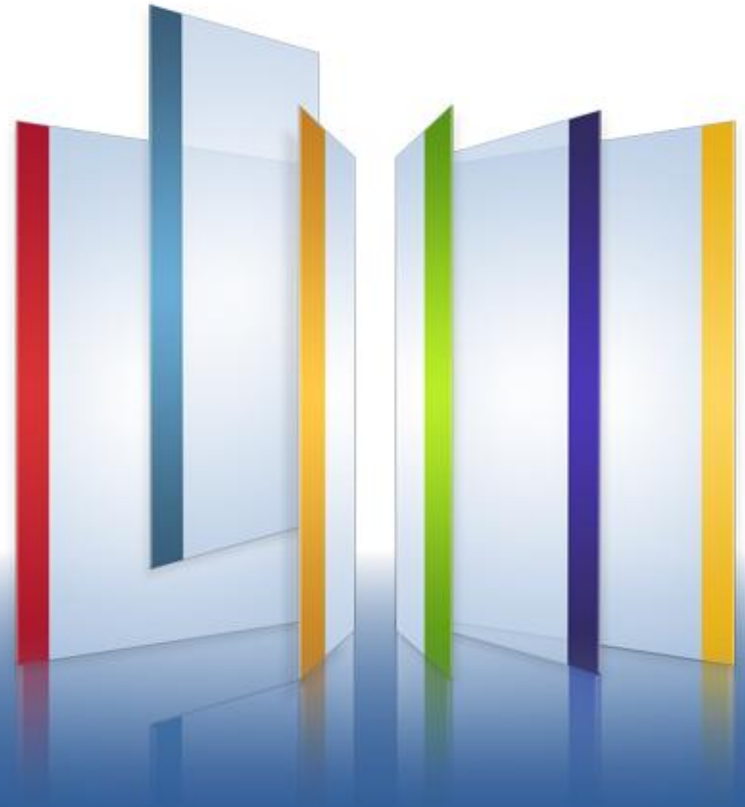
More Visibility
across firewall, IPS, DLP, endpoint and more

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

Raising the bar on UTM-1 performance

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

1-2-3

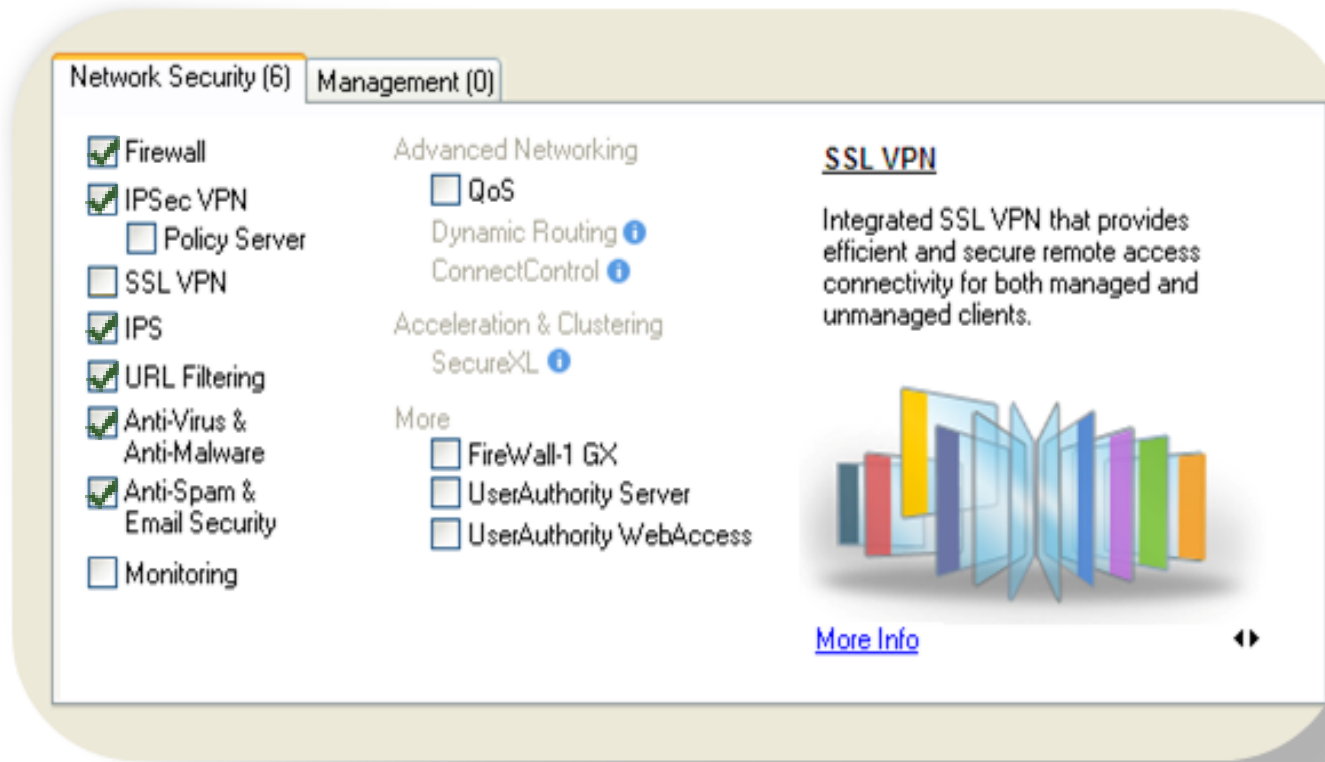
Simple software upgrade to
new R71 release

On same existing system
or gateway

**Immediate protection and
performance boost**

More protection, uncompromised performance

Activate today all layers of security
on your gateway



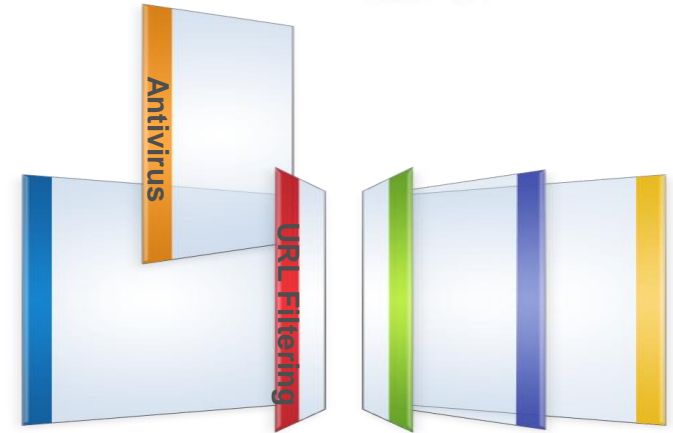
Performance Improvement Summary



Firewall x4

IPS x3

Connection/sec. x4

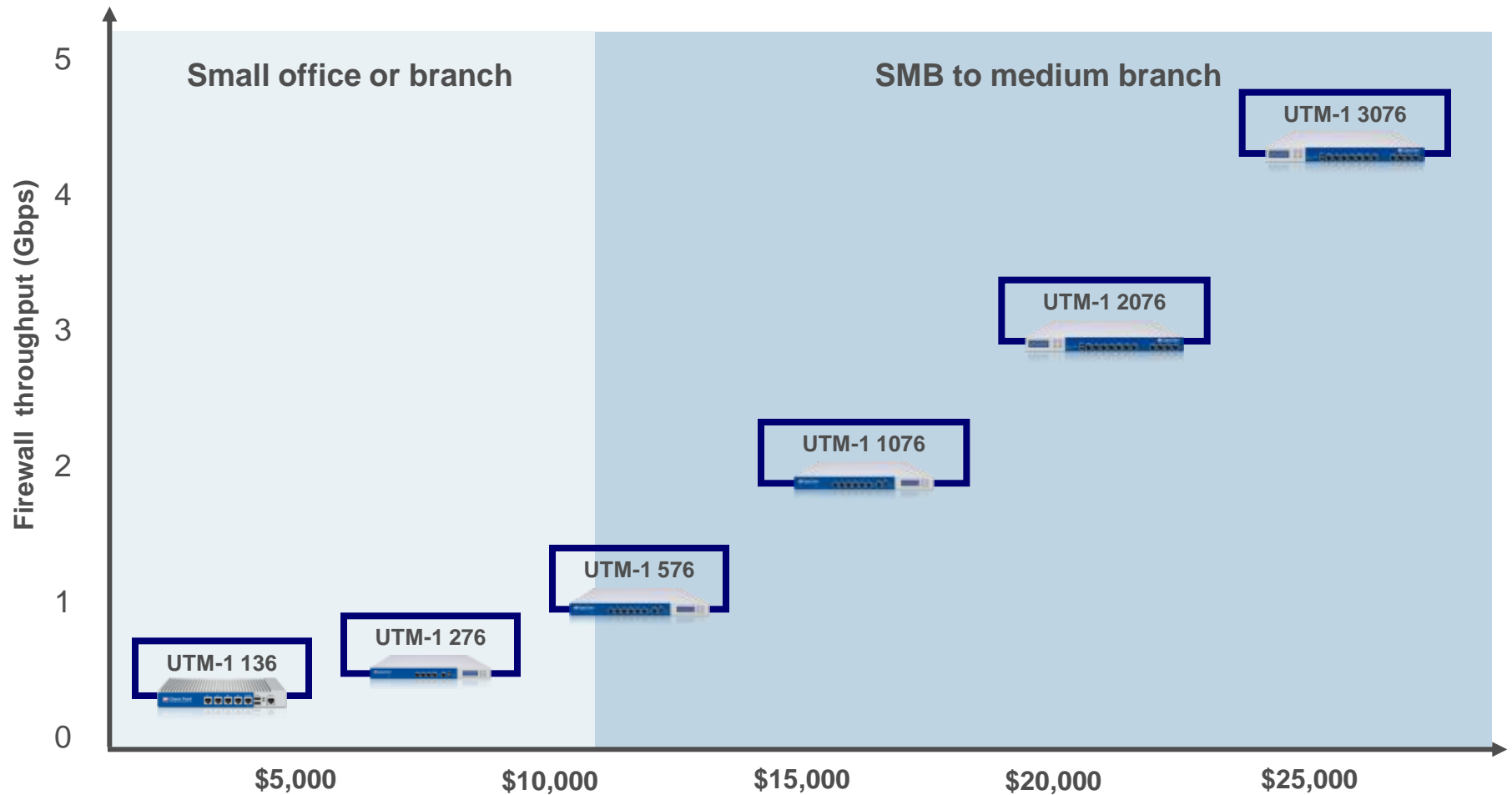


Antivirus x15

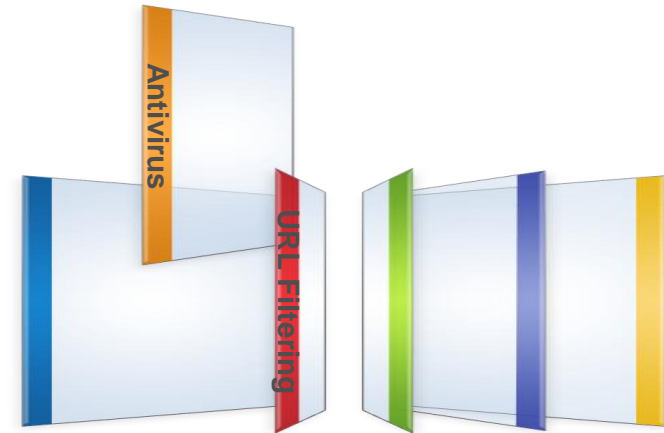
**AV and URLF
connection x80**

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

