



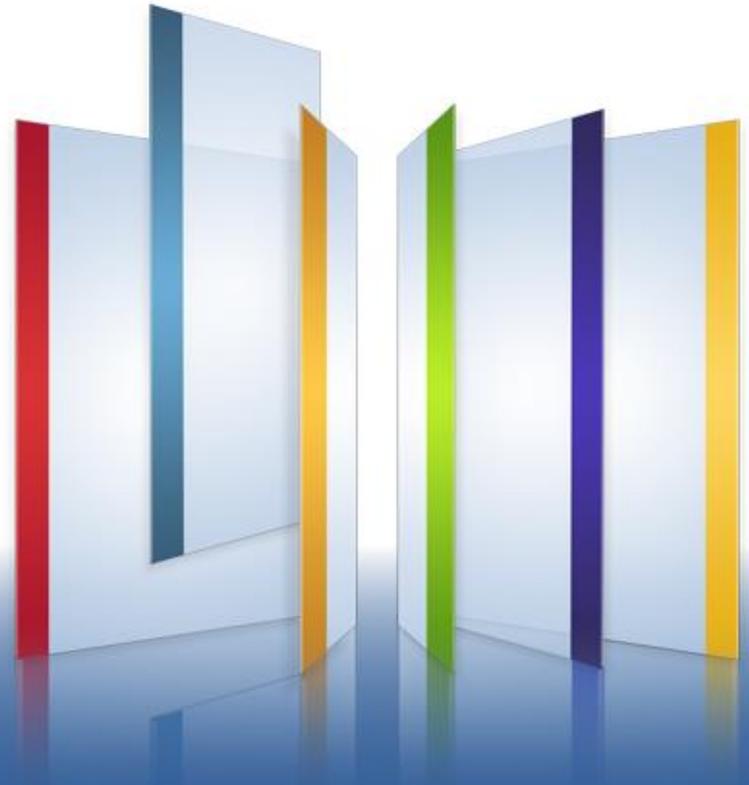
Check Point

SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Check Point Mobile Information Protection, Data Loss Prevention

Petr Kadrmas, SE Eastern Europe



Data Travel Fast — Smartphones and Sharing Apps



**90% of organizations
allow storing business
data on smartphones¹**

**69% of businesses
share data using
public cloud services²**



Data leaving to uncontrolled environments

Source

¹ Check Point Mobility Survey, Dec. 2012

² Check Point Security Report



Control the Access and Usage of Business Data



Endpoint and USB Devices



Smartphones and Tablets



Data Collaboration

**Available
anywhere**

Encrypt Data in Uncontrolled Environments

Set Authentication & Access Rights to Data

Be Able to Revoke Access to Data if Needed

Mobile Information Protection Solution



Mobile Security



Document Security



Data Loss Prevention



Media Encryption



Full Disk Encryption

Check Point Mobile Security



Check Point Mobile Enterprise



Available on the
App Store

ANDROID APP ON
Google play

- ✓ Protected Business communication
- ✓ Single Sign On
- ✓ Online/Off-line access



Check Point Mobile VPN



Available on the
App Store

ANDROID APP ON
Google play

- ✓ VPN tunnel for any App
- ✓ Automatic connect
- ✓ IPsec or SSL VPN



Share documents securely with
authorised co-workers & business partners

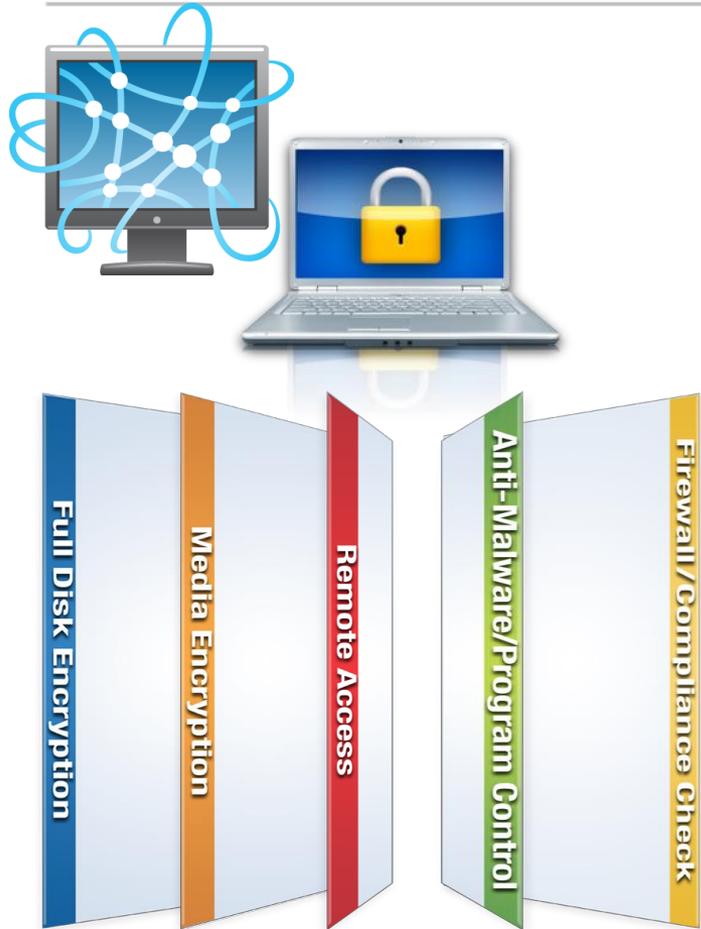


The security policy follows
the document and its entire content



Simple access to documents from
PC, Mac, Smartphones and tablets

Check Point Endpoint Security



Automatically and transparently secure all information on endpoint hard drives



Centrally enforceable encryption of removable media and port control



Provide secure, seamless access to corporate networks remotely



Protects your endpoint from unsecure, malicious and unwanted applications

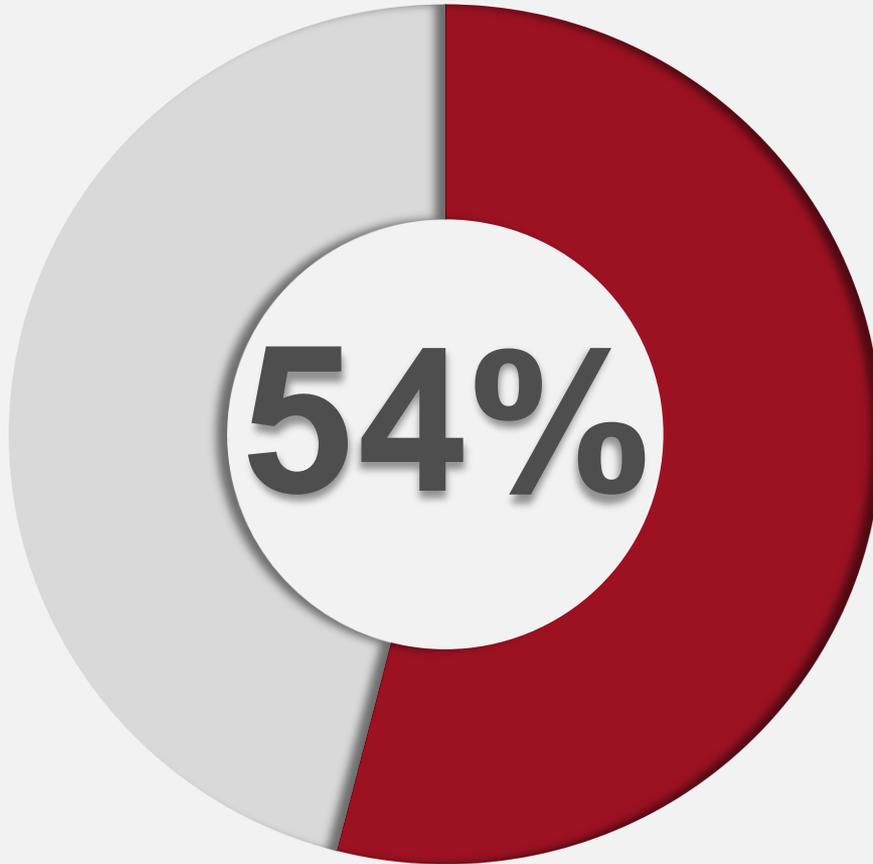


Stop unwanted traffic, prevent malware and block targeted attacks

Unified Security Management with true visibility

Secure Business Data in Motion: Check Point DLP Blade



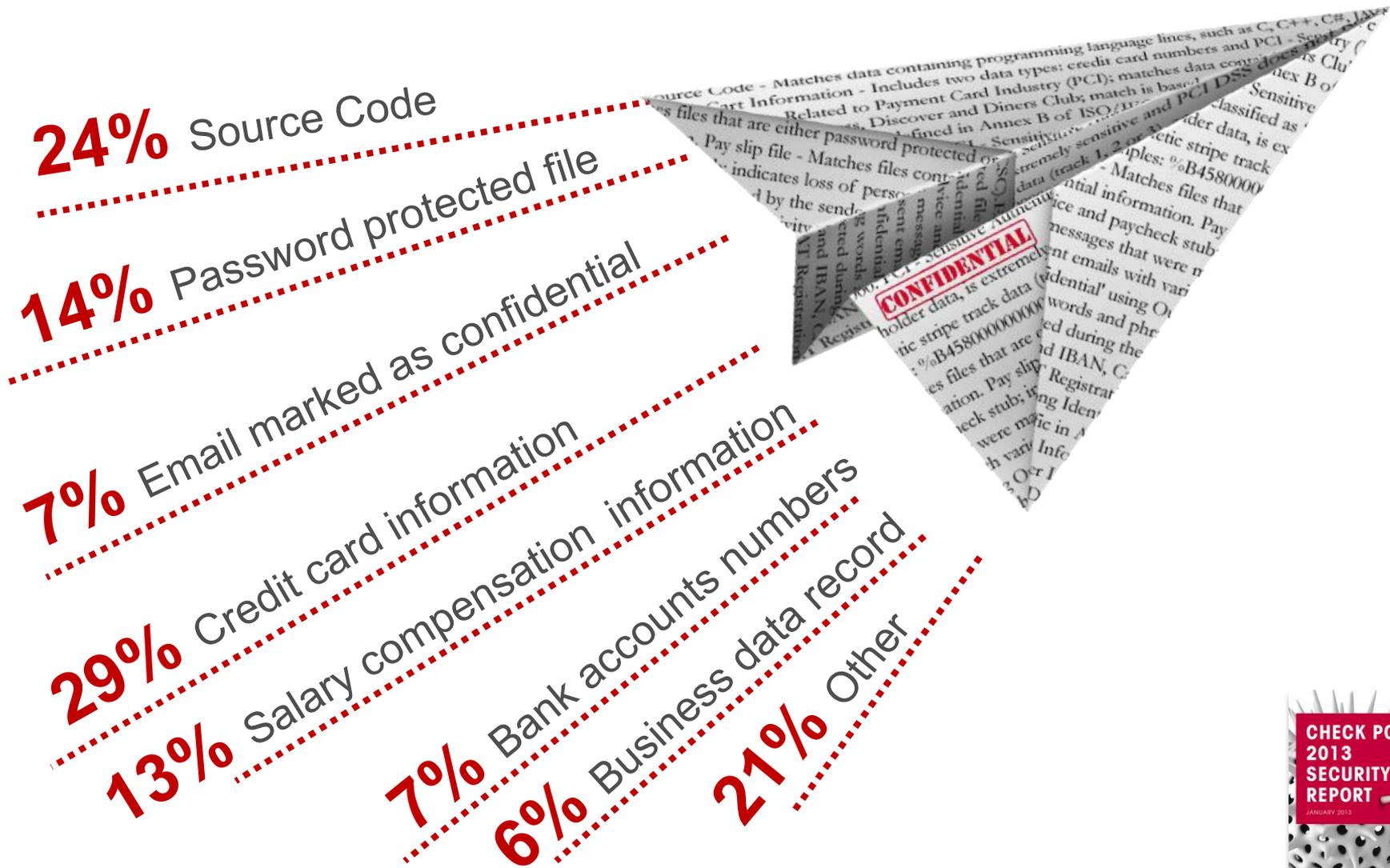


**Of businesses
experience
data loss**

Source: Check Point 2013 Security Report, among 900 organizations



Data Loss Incidents



Source: Check Point 2013 Security Report, among 900 organizations



**Simple to Prevent
Data Loss**

**Engage and Educate
End-Users**

**Unified with Check
Point Architecture**



Best Practices Data Types

File Types



Match more than 800 File formats, Password Protected Files, Large Files, and more.

Messages



Match different types of messages, for example:

- Confidential Outlook Message
- External Recipient in BCC
- Internal Users and a New External Recipient

Inappropriate Language



Match data containing inappropriate behavior such as curses, gambling, and pornographic terms.

Email Typosquatting



Domain typosquatting is an attack commonly used to spread malwares into users' web browser. This attack can also be used to harvest emails by setting up email servers with domains that are very similar to your organization's domains or sub-domains.

Business Information Data Types

Business Numbers



Match sensitive corporate numbers such as:

- International Bank Account Numbers (IBAN) - both electronic and print format.
- Value Added Tax (VAT) identification numbers.
- Corporate and Business identification numbers.
- And many more

Business Plans



Match documents containing a Business Plan – A document that outlines a firm's financial and operational goals and benchmarks.

Corporate Information



Match sensitive corporate information such as:

- Mergers and Acquisitions Data
- Corporate Press Releases
- Shipping Information
- And many more

Personal Information Data Types

National Identity Numbers



Used by governments of many countries as a means of tracking their citizens for the purposes of work, taxation, health care, and other governmentally-related functions.

Names and Surnames



Matches a large amount of common names and surnames from a variety of countries and languages.

Addresses



Matches data containing information such as cities, states, zip codes, etc.

Phone Numbers



Match data containing phone numbers from different countries, which may appear in personal and business records.

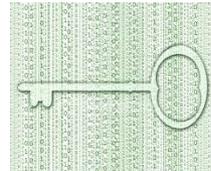
Network and IT Data Types

Internal Network Information



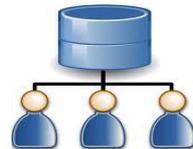
Match data containing IPv4, IPv6, MAC, and employee email addresses, which could reveal details about the organizations internal network.

Certificates and Private Keys



- Matches certificate files, which are usually encrypted, encoded and contain the certificate, including the identity information, public key, expiry date, and signature.
- Matches private key files, which are used to authenticate connections to secure hosts (server, website, webmail, etc.) and to decrypt its data.

Active Directory or LDAP Entries



Matches data containing entries of the Lightweight Directory Access Protocol (LDAP), an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

Intellectual Property Data Types

Source Code



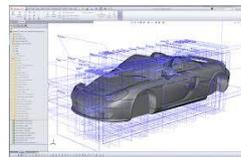
Match data containing programming language lines, such as C, C++, C#, JAVA, Visual Basic, SAP, Python, SQL Queries, and more.

Patents



Matches documents containing U.S. patent related data, forms and applications according to the United States Patent and Trademark Office (USPTO).

Graphic Design Files



Match file types used in graphic design applications such as: Adobe Photoshop, Adobe Illustrator, Solidworks, AutoCAD, Visio, and more.

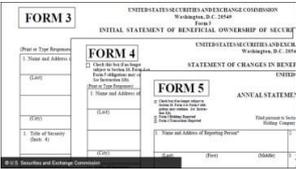
Finance Data Types

SEC Filings



Annual, quarterly and other reports that are filed in the U.S. Securities and Exchange Commission (SEC). Such documents are considered highly restricted according to SEC regulations and the Sarbanes-Oxley (SOX) Act of 2002.

SEC Forms



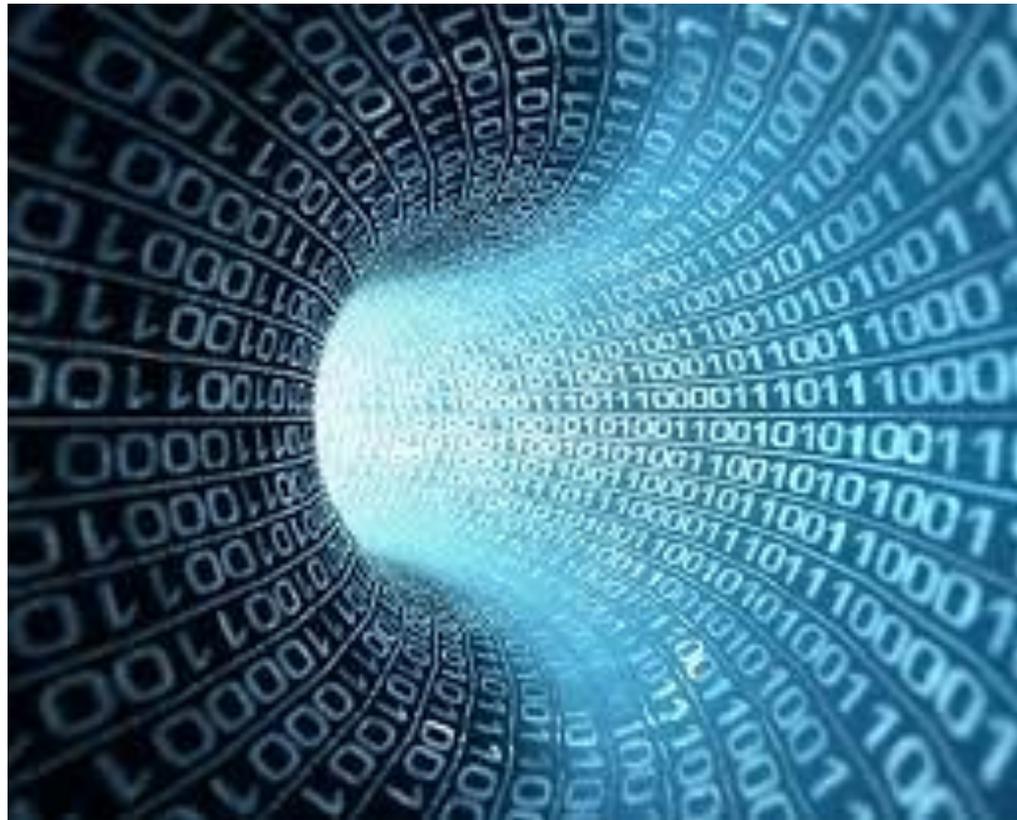
Matched SEC Forms:
10-K, 10-Q, 20-F, 6-K, 8-K.

Finance Reports



Matches documents containing financial reports that are not formatted as reports filed in the Securities and Exchange Commission (SEC).

Want to create your own data types?



Word Data Types

Keywords



Matches a list of keywords.
Example - My Organization Names:
 “Checkpoint” , “Check Point”.

Patterns



Matches a list of Patterns (Regular Expressions).
Example - USA Social Security Numbers:
`\d{9}`
`\d{3}-\d{3}-\d{3}`
 (‘d’ = digit , ‘{ }’ = amount of times it should appear)

Weighted Words and Patterns



Matches a list of Words and Patterns in a weight-sum that you define.
Example - Java Source Code:
 Word: “public static void” , weight: 10
 Pattern: “if(...)” , weight: 1

Dictionary and Templates

Dictionary



Supports a very large number of words and phrases in various languages.
Example - A dictionary of Personal Names.

Templates

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/ID 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 ()

If payment was made to someone other than the

Company Name Here

Address:

Cash Receipt # 1-11-11-11-11 Date: 11/11/11

Cash Received From: of

No.

Total Amount Due	<input type="text"/>
Amount Received	<input type="text"/>
Balance Due	<input type="text"/>

Payment Received in:

Cash

Money

Cheque

Signed By:

Match corporate templates and logos

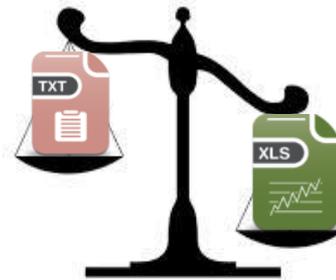


File Attributes

800+
File Formats



File Size

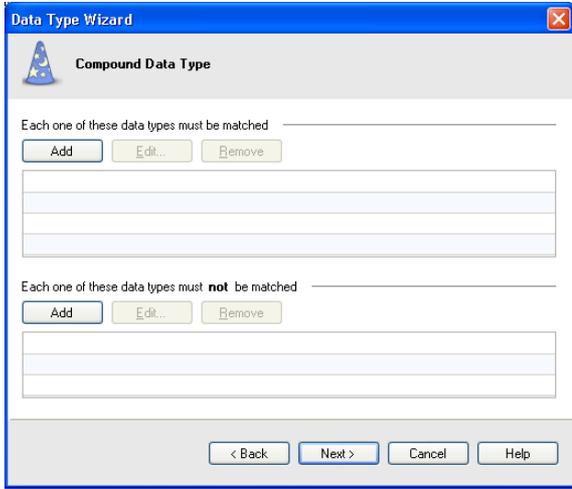


File Name

-  Customer_Orders.xls
-  Finance_Report_Q4.doc
-  admin_guide.pdf

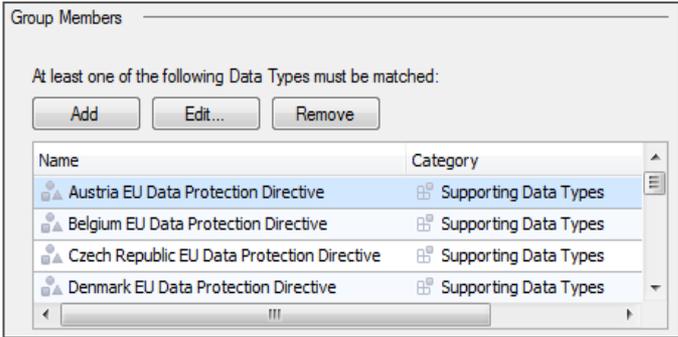
Group Data Types

Compound



A data type that contains multiple data types in an AND or NOT relationship, or both.

Group



A data type that contains multiple data types in an OR relationship.

If data matches any of the data types in the group, it is matched.



CPcode Data Types

CPcode



Open scripting language. Lets you:

- Create completely new data types
- Enhance existing data types

Example



Customer needs to match “Australian Business Numbers”

- Example: 53004085616
- 11 digit number with a validation function

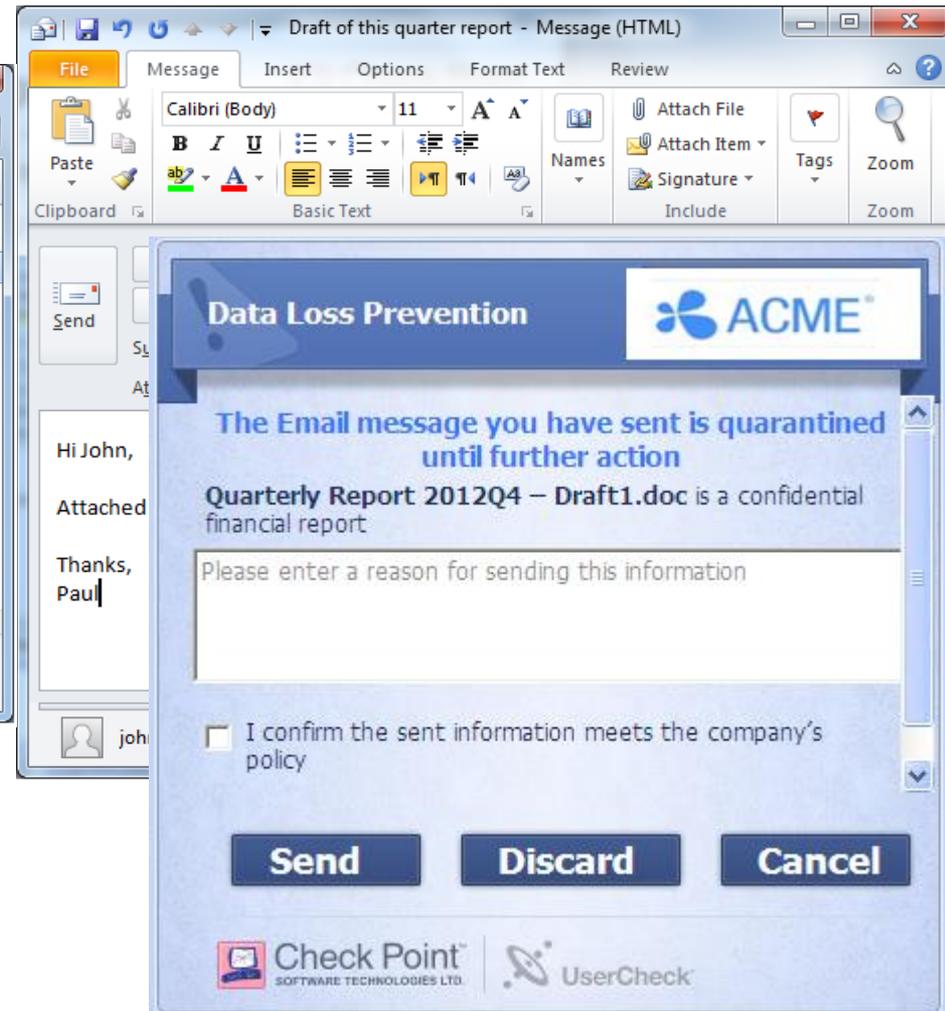
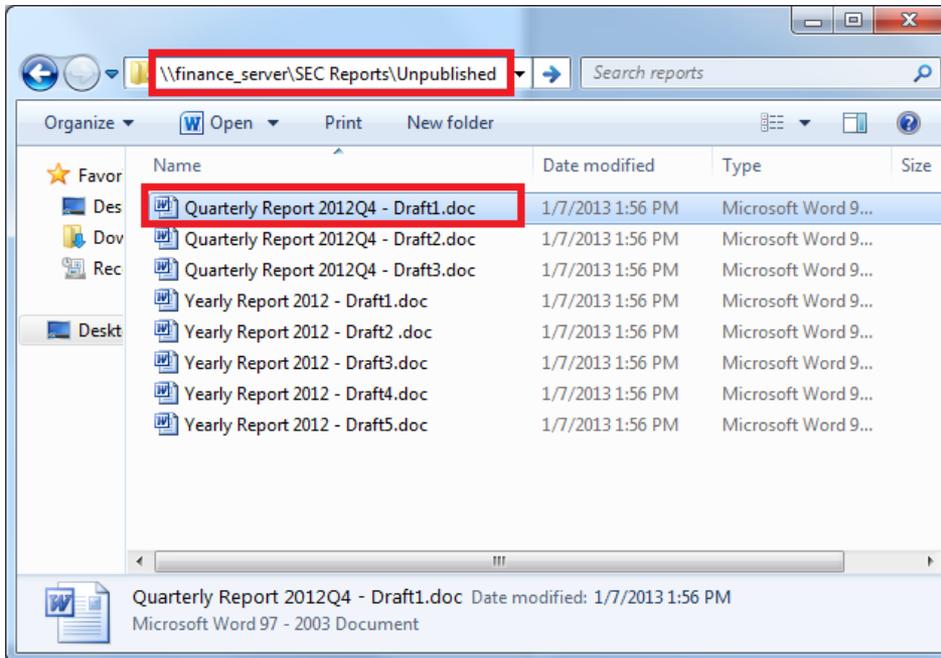
Solution



1. Create pattern data type to match 11 digit numbers
2. CPCODE validation function runs per regular expression match

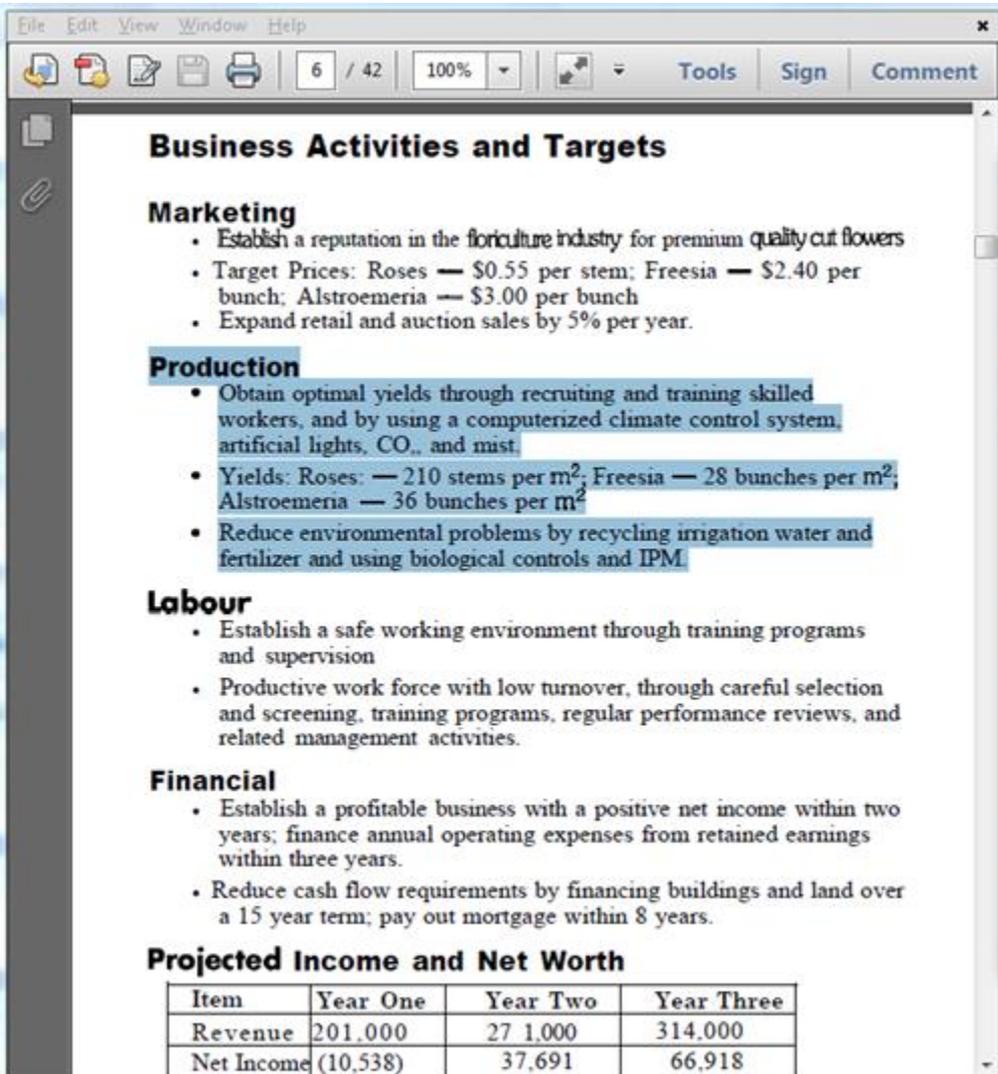
Fingerprint – Exact Match

Exact Match – match the identical file from the repository



Fingerprint – Partial Match

Partial Match - match part of a file from the repository



Business Activities and Targets

Marketing

- Establish a reputation in the floriculture industry for premium quality cut flowers
- Target Prices: Roses — \$0.55 per stem; Freesia — \$2.40 per bunch; Alstroemeria — \$3.00 per bunch
- Expand retail and auction sales by 5% per year.

Production

- Obtain optimal yields through recruiting and training skilled workers, and by using a computerized climate control system, artificial lights, CO₂, and mist.
- Yields: Roses — 210 stems per m²; Freesia — 28 bunches per m²; Alstroemeria — 36 bunches per m²
- Reduce environmental problems by recycling irrigation water and fertilizer and using biological controls and IPM.

Labour

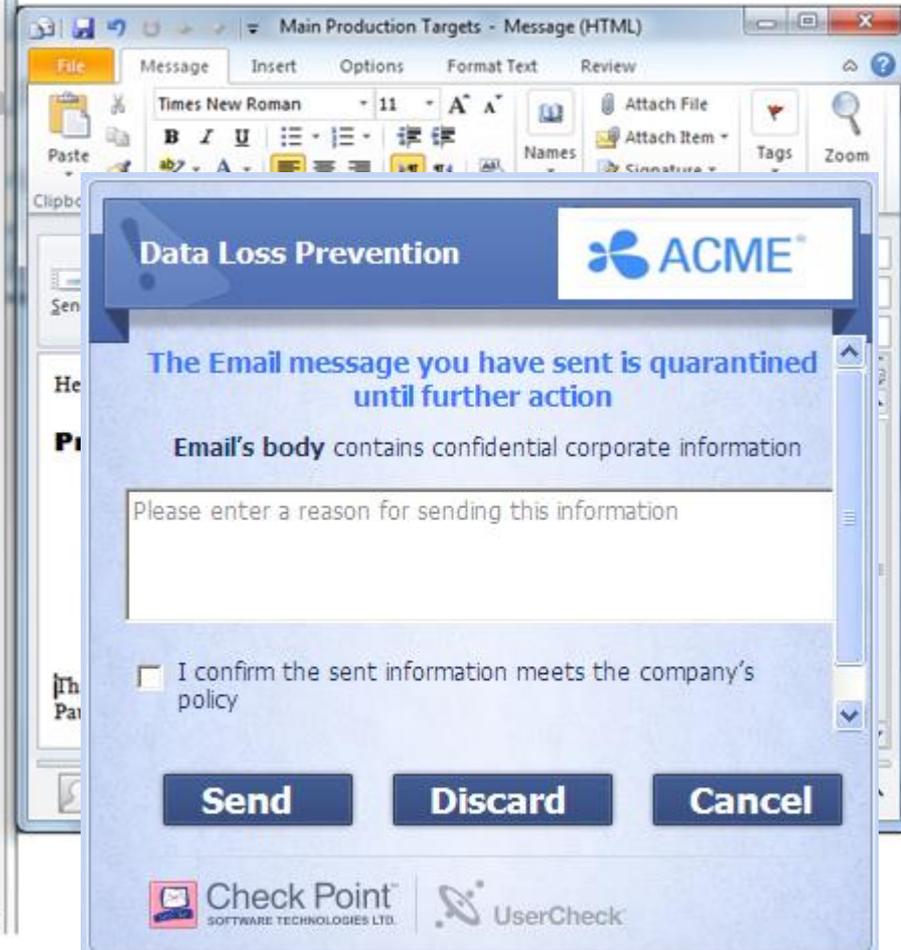
- Establish a safe working environment through training programs and supervision
- Productive work force with low turnover, through careful selection and screening, training programs, regular performance reviews, and related management activities.

Financial

- Establish a profitable business with a positive net income within two years; finance annual operating expenses from retained earnings within three years.
- Reduce cash flow requirements by financing buildings and land over a 15 year term; pay out mortgage within 8 years.

Projected Income and Net Worth

Item	Year One	Year Two	Year Three
Revenue	201,000	271,000	314,000
Net Income	(10,538)	37,691	66,918



Data Loss Prevention 

The Email message you have sent is quarantined until further action

Email's body contains confidential corporate information

Please enter a reason for sending this information

I confirm the sent information meets the company's policy

Send **Discard** **Cancel**

 Check Point SOFTWARE TECHNOLOGIES LTD.  UserCheck



Whitelist Policy

- Whitelist – easily define files that will not be matched by the DLP policy

Whitelist Policy

Whitelist Files

Name	Size	Date added
 Sales Presentation.pptx	166.31 KB	Tuesday, December 11, 2012 5:24:39 PM
 Product Whitepaper.doc	291.5 KB	Monday, January 07, 2013 12:35:24 PM
 user guide.pdf	124.96 KB	Monday, January 07, 2013 12:36:22 PM
 Public Datasheet.doc	291.5 KB	Monday, January 07, 2013 12:37:18 PM
 price catalog.pdf	124.96 KB	Monday, January 07, 2013 12:38:24 PM

Whitelist Repositories

Name	Comments
 Press Releases	Published press releases
 User Manuals	Public user manuals



DLP Actions

Detect



The user gets no notification. A DLP log incident is created, and the actual data is stored.

Inform User



DLP notifies the user that the captured traffic violates DLP rules. The traffic is passed.

Ask User



DLP notifies the user that the message is being held and contains a link to the DLP Portal, where the user decides whether the transmission should go through or be dropped. User decisions, and reasons for sending, are logged for your analysis.

Prevent



The traffic is blocked. The user and the Data Owner may be notified.

Visible and Hidden Watermarks

Add visible and invisible markings to Microsoft Office documents (2007/10) when sent as email attachments:

Visible watermarks alert users to sensitive document content when viewed or printed.

- Add customized text footer to PowerPoint slides: “Highly Restricted, sent by John Smith on 7/7/11”.
- Add a large diagonal “Classified” **visible watermark** at the first page of Word document that match

Exceptions	Action	Track	Install On	Time
None	Detect Classified	Log	DLP Blades	Any
None	Detect	Inform User	DLP Blades	Any
1	Detect	Ask User	DLP Blades	Any
None	Detect	Prevent	DLP Blades	Any
None	Detect	Watermarks	Without Watermark	
None	Inform User	Log	Invisible only	
None	Ask User	Log	Restricted	
None	Ask User	Log	<input checked="" type="checkbox"/> Classified	
None	Ask User	Log	New...	

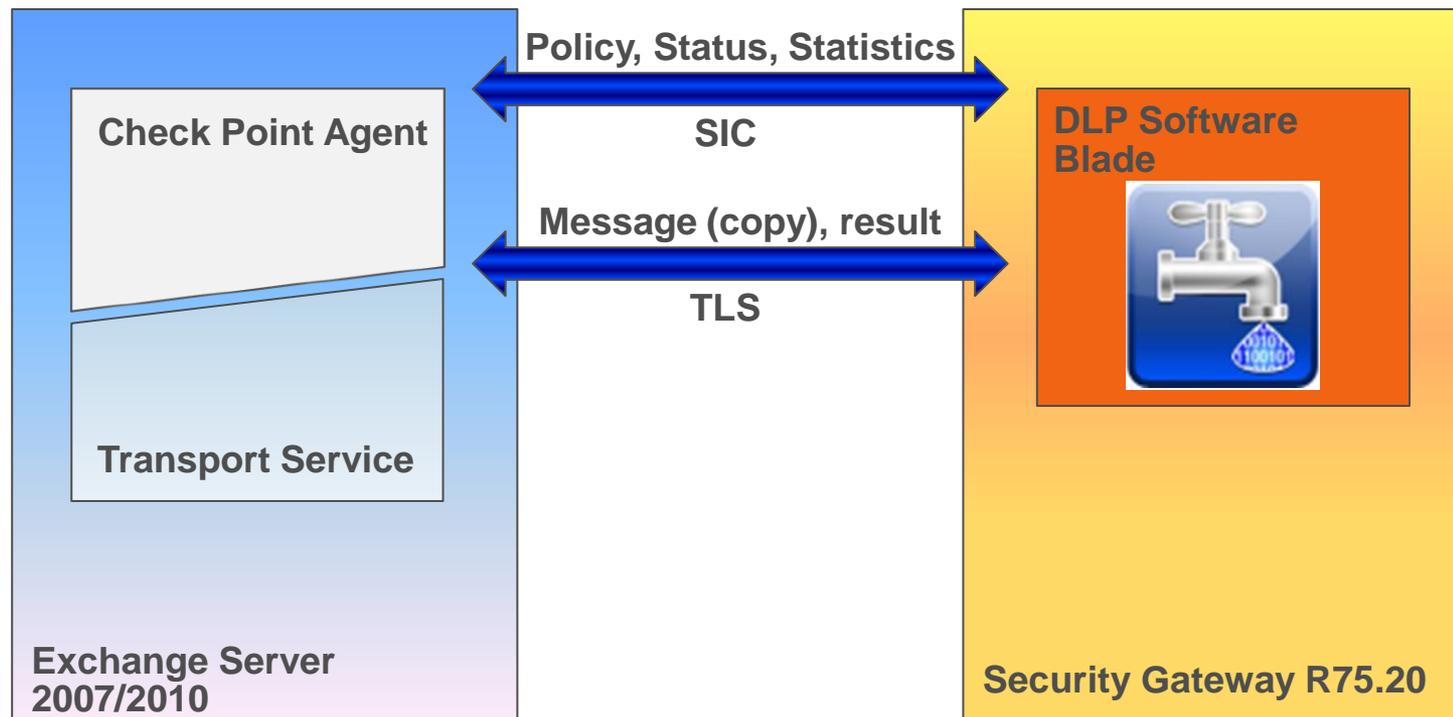


Hidden watermark (encrypted) provide a way to tag documents without impacting formatting.

- Does not impact visible document formatting
- Can be used for forensic analysis to track leaked documents

DLP Exchange Agent

The Exchange Security Agent is a Check Point agent on the organization's Exchange Server. It enables inspection of internal and outgoing emails.



Identity Awareness

When Identity Awareness and DLP blades are enabled on the same gateway:



- Access role objects can be used in the Source or Destination column of a DLP rule.
- SmartEvent, SmartLog and SmartView Tracker logs identify users that violate the DLP policy.
- Email notifications can be sent when DLP violations occur using the FTP or HTTP protocols.
- The DLP can redirect HTTP traffic of unknown user to “Identity Captive Portal” for authentication.

Privacy

The admin can choose not to store original message in the DLP log. There are 4 options:

Yes: saves the original incident as before.

Only as text: Saves the incident in an HTML format.

Don't Store: If only this rule is matched, don't store the incident.

Delete: Don't store the incident, even if other rules are marked as Yes.

Data Loss Prevention (DLP) Policy

Type to Search		Grouping: Category					
Data	Source	Destination	Exceptions	Action	Track	Install On	Time
Best Practice (7)							
Outlook Message - Con...	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Any
Database File	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Any
Large File	My Organization	Free Email Dom...	None	Detect	Log	DLP Blades	Any
External Recipient in BCC	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Any
External Recipient and ...	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Any
Inappropriate Language	My Organization	Outside My Org	None	Inform User	Log	DLP Blades	Any
Password Protected File	My Organization	Outside My Org	None	Ask User	Log	DLP Blades	Any
Business Information (3)							
Customer Names	My Organization	Outside My Org	None	Detect Classified	Log	DLP Blades	Any

Email...

Log

Alert

SNMP Trap

User Defined

User Defined 2

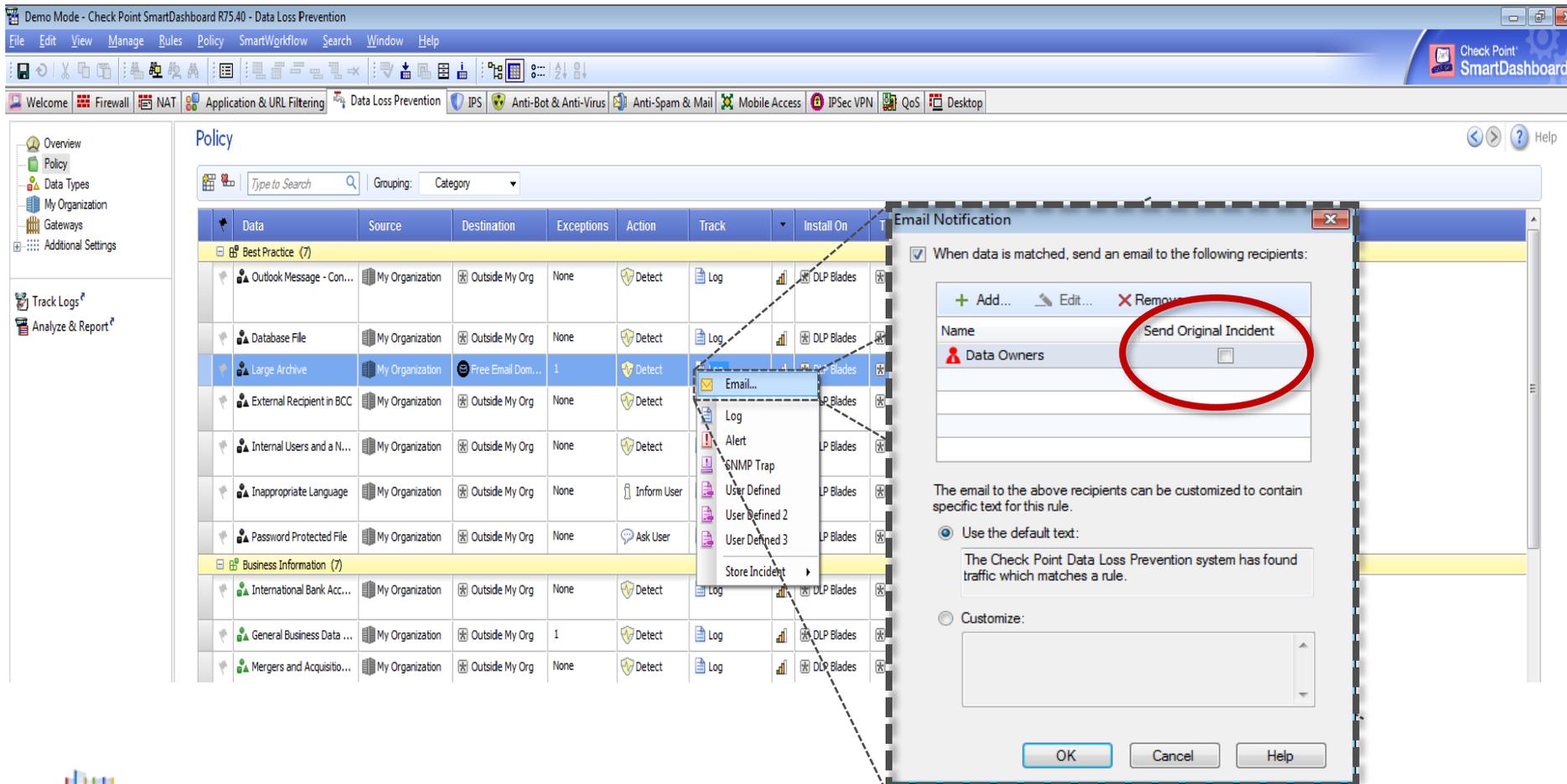
User Defined 3

Store Incident

- Yes
- Only as Text
- Don't Store
- Delete

Data Owners

Send the original message (email) to data owner



The screenshot shows the Check Point SmartDashboard interface. A table lists various data types and their associated policies. The 'Email...' option is selected for the 'Large Archive' policy, opening the 'Email Notification' dialog box. In this dialog, the 'Data Owners' recipient is selected, and the 'Send Original Incident' checkbox is checked and circled in red.

Data	Source	Destination	Exceptions	Action	Track	Install On
Best Practice (7)						
Outlook Message - Con...	My Organization	Outside My Org	None	Detect	Log	DLP Blades
Database File	My Organization	Outside My Org	None	Detect	Log	DLP Blades
Large Archive	My Organization	Free Email Dom...	1	Detect	Log	DLP Blades
External Recipient in BCC	My Organization	Outside My Org	None	Detect	Log	DLP Blades
Internal Users and a N...	My Organization	Outside My Org	None	Detect	Log	DLP Blades
Inappropriate Language	My Organization	Outside My Org	None	Inform User	Log	DLP Blades
Password Protected File	My Organization	Outside My Org	None	Ask User	Log	DLP Blades
Business Information (7)						
International Bank Acc...	My Organization	Outside My Org	None	Detect	Log	DLP Blades
General Business Data ...	My Organization	Outside My Org	1	Detect	Log	DLP Blades
Mergers and Acquisitio...	My Organization	Outside My Org	None	Detect	Log	DLP Blades

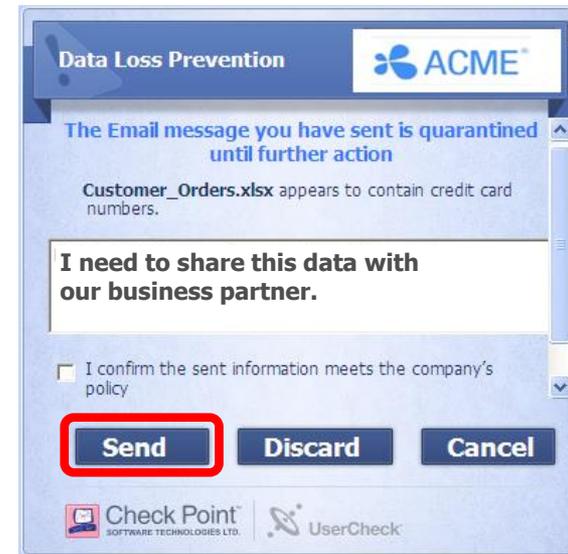
Engage and Educate end users with Check Point UserCheck™



Users UNDERSTAND the security policy

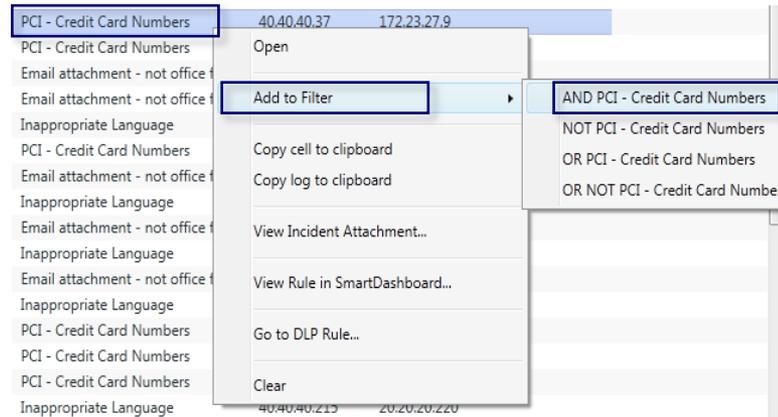


Switch from Detection to PREVENTION



SmartLog

Easy and fast filtering - Check Point SmartLog transforms data into security intelligence. split-second searches that provide instant visibility into billions of log Records.



action:Detect AND "PCI - Credit Card Numbers"

Found 8 results (5 ms)

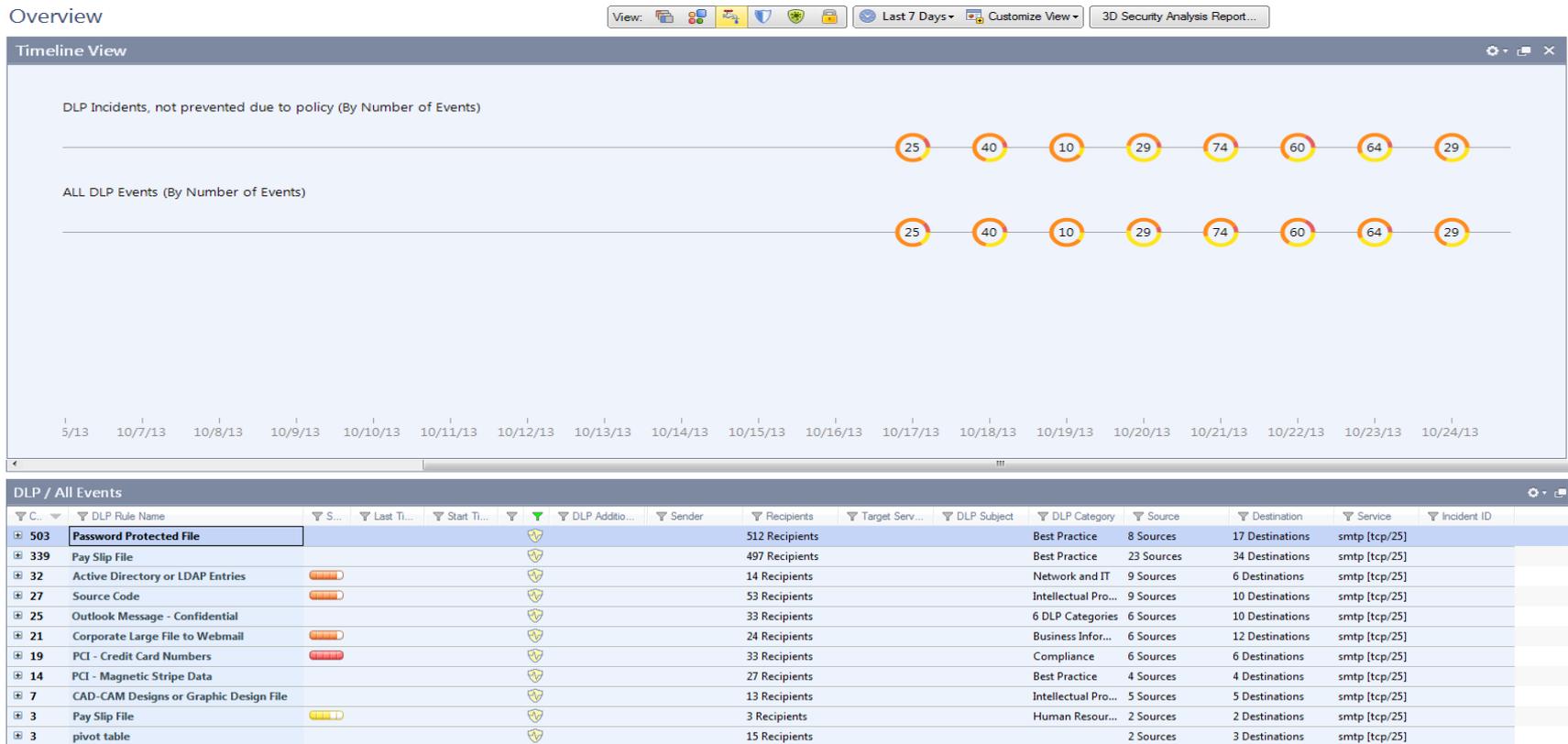
Time	Blade	Type	DLP Incident U...	Severity	Action	Sender	DLP Recipients	DLP Rule Name	Source	Destination
Today 13:25:30	DLP	Log	{FB615F58-EB7...	Medium	Detect	adir@checkpoi...	adi_ext@extern...	PCI - Credit Card Numbers	40.40.40.37	172.23.27.9
Today 13:25:14	DLP	Log	{FE3D059A-470...	Medium	Detect	adir@checkpoi...	adi_ext@extern...	PCI - Credit Card Numbers	40.40.40.37	172.23.27.9
Today 13:25:08	DLP	Log	{55422A87-OCE...	Medium	Detect	adir@checkpoi...	adi_ext@extern...	PCI - Credit Card Numbers	40.40.40.37	172.23.27.9
Today 13:24:07	DLP	Log	{562CE849-703...	Medium	Detect	adir@checkpoi...	adi_ext@extern...	PCI - Credit Card Numbers	40.40.40.37	172.23.27.9
Today 11:56:09	DLP	Log	{5F4FF832-108...	Medium	Detect	adir@checkpoi...	adi_ext@extern...	PCI - Credit Card Numbers	40.40.40.37	172.23.27.9
Today 11:55:58	DLP	Log	{7D1667A1-DC...	Medium	Detect	adir@checkpoi...	adi_ext@extern...	PCI - Credit Card Numbers	40.40.40.37	172.23.27.9
Today 11:23:30	DLP	Log	{4D0A3BDA-33...	Medium	Detect	adir@checkpoi...	adi_ext@extern...	PCI - Credit Card Numbers	40.40.40.37	172.23.27.9



SmartEvent

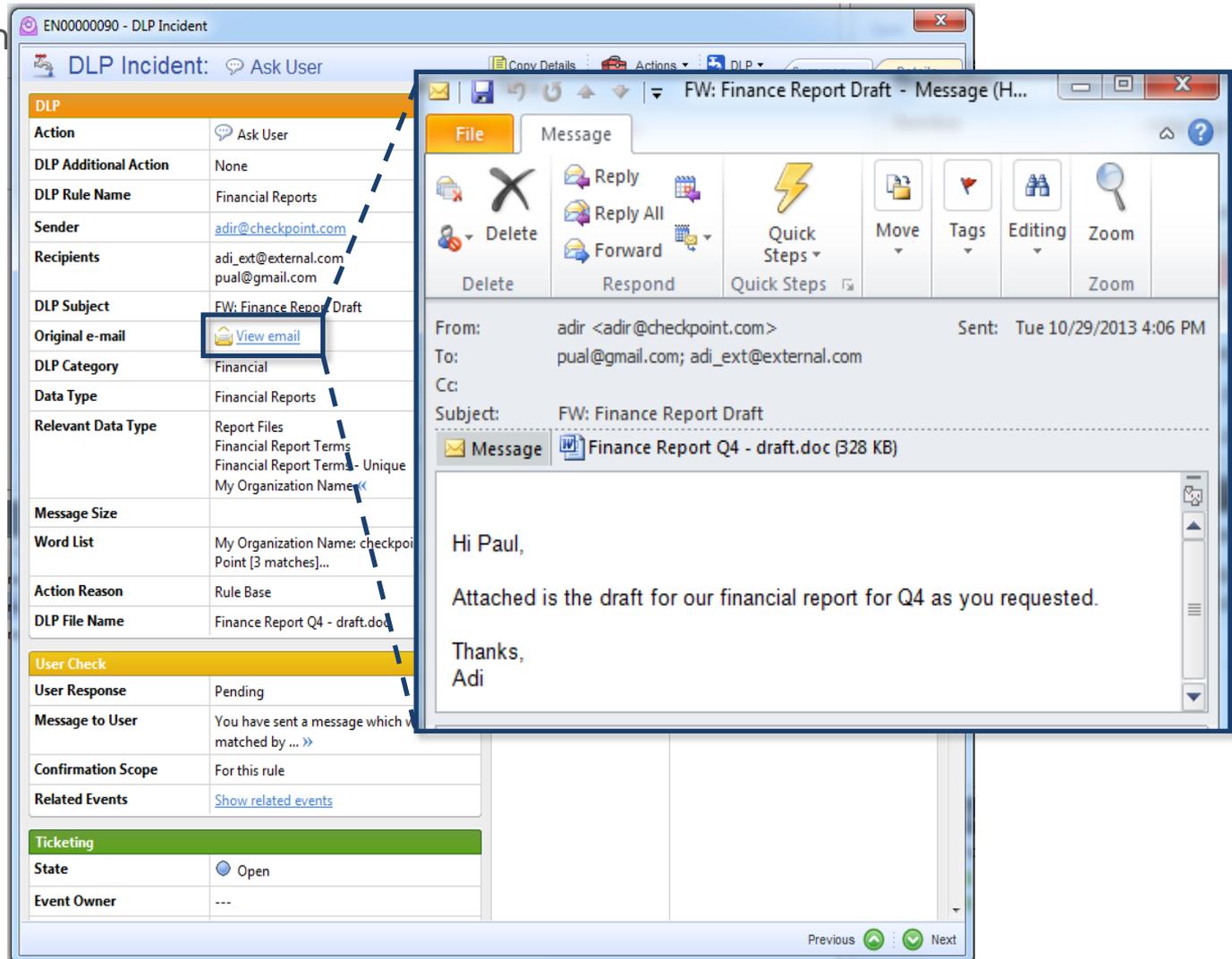
The SmartEvent is a Check Point blade designed for analyzing Check Point and third-party devices logs and creating events based on these logs.

Overview



SmartEvent

Example of a DLP event



The screenshot displays a SmartEvent window titled "EN00000090 - DLP Incident" with a sub-header "DLP Incident: Ask User". The main content is a table of incident details:

DLP	
Action	Ask User
DLP Additional Action	None
DLP Rule Name	Financial Reports
Sender	adir@checkpoint.com
Recipients	adi_ext@external.com pual@gmail.com
DLP Subject	FW: Finance Report Draft
Original e-mail	View email
DLP Category	Financial
Data Type	Financial Reports
Relevant Data Type	Report Files Financial Report Terms Financial Report Terms - Unique My Organization Name
Message Size	
Word List	My Organization Name: checkpoi Point [3 matches]...
Action Reason	Rule Base
DLP File Name	Finance Report Q4 - draft.doc
User Check	
User Response	Pending
Message to User	You have sent a message which w matched by ... >>
Confirmation Scope	For this rule
Related Events	Show related events
Ticketing	
State	Open
Event Owner	---

Overlaid on the right is a Microsoft Outlook message window titled "FW: Finance Report Draft - Message (H...". The message content is:

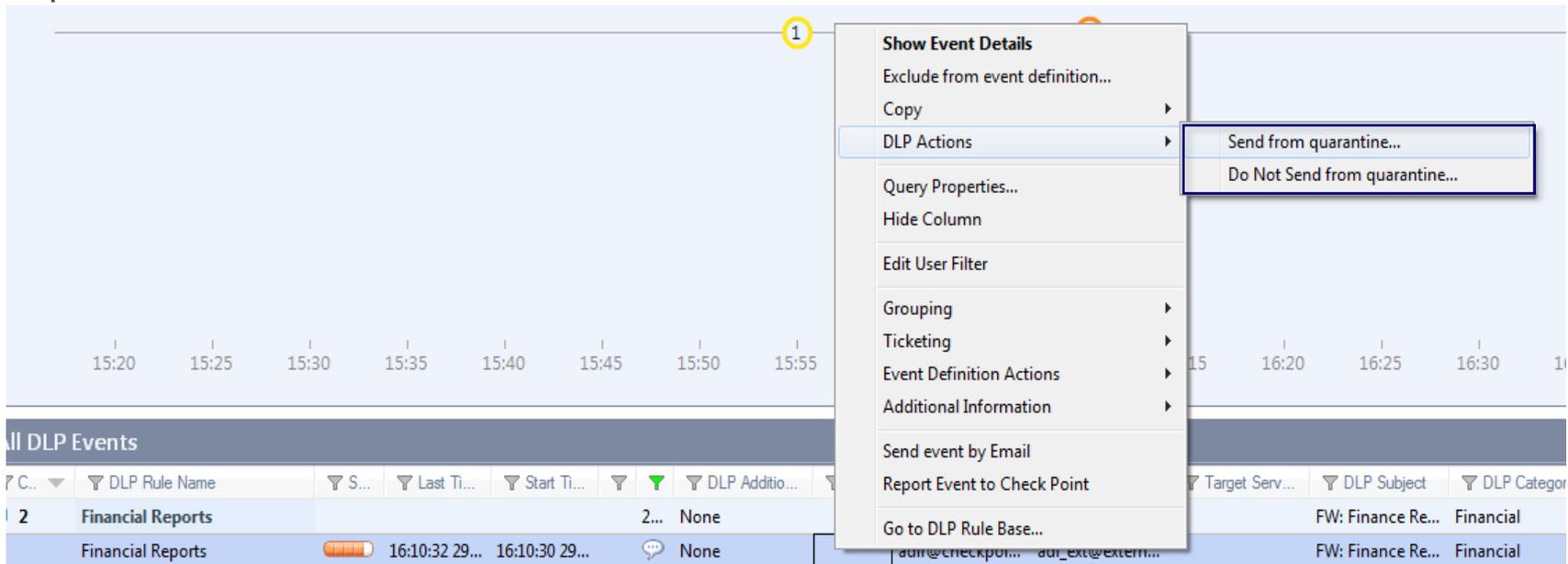
From: adir <adir@checkpoint.com> Sent: Tue 10/29/2013 4:06 PM
 To: pual@gmail.com; adi_ext@external.com
 Cc:
 Subject: FW: Finance Report Draft

Attachments: Message, Finance Report Q4 - draft.doc (328 KB)

Hi Paul,
 Attached is the draft for our financial report for Q4 as you requested.
 Thanks,
 Adi

SmartEvent

From the SmartEvent GUI, the admin can decide to release emails from quarantine:



The screenshot shows the SmartEvent GUI interface. A context menu is open over a table of DLP events. The menu items are:

- Show Event Details
- Exclude from event definition...
- Copy
- DLP Actions (highlighted)
- Query Properties...
- Hide Column
- Edit User Filter
- Grouping
- Ticketing
- Event Definition Actions
- Additional Information
- Send event by Email
- Report Event to Check Point
- Go to DLP Rule Base...

The 'DLP Actions' sub-menu is open, showing two options:

- Send from quarantine...
- Do Not Send from quarantine...

A yellow circle with the number '1' is positioned above the context menu trigger. A blue rectangular box highlights the 'Send from quarantine...' option in the sub-menu.

C...	DLP Rule Name	S...	Last Ti...	Start Ti...	DLP Additio...	Target Serv...	DLP Subject	DLP Categor...
2	Financial Reports	2...	None				FW: Finance Re...	Financial
	Financial Reports	16:10:32 29...	16:10:30 29...		None	adm@checkpoi...	adm_ext@extern...	FW: Finance Re...



**Simple to Prevent
Data Loss**

**Engage and Educate
End-Users**

**Unified with Check
Point Architecture**





Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Thank You

