



Check Point®

SOFTWARE TECHNOLOGIES LTD.

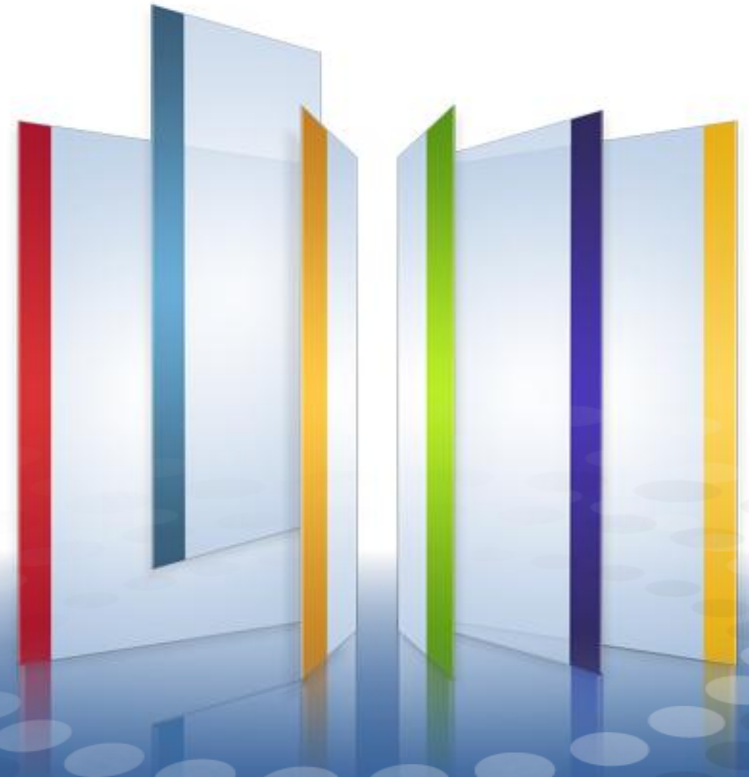
We Secure the Internet.

Mobile Information Protection

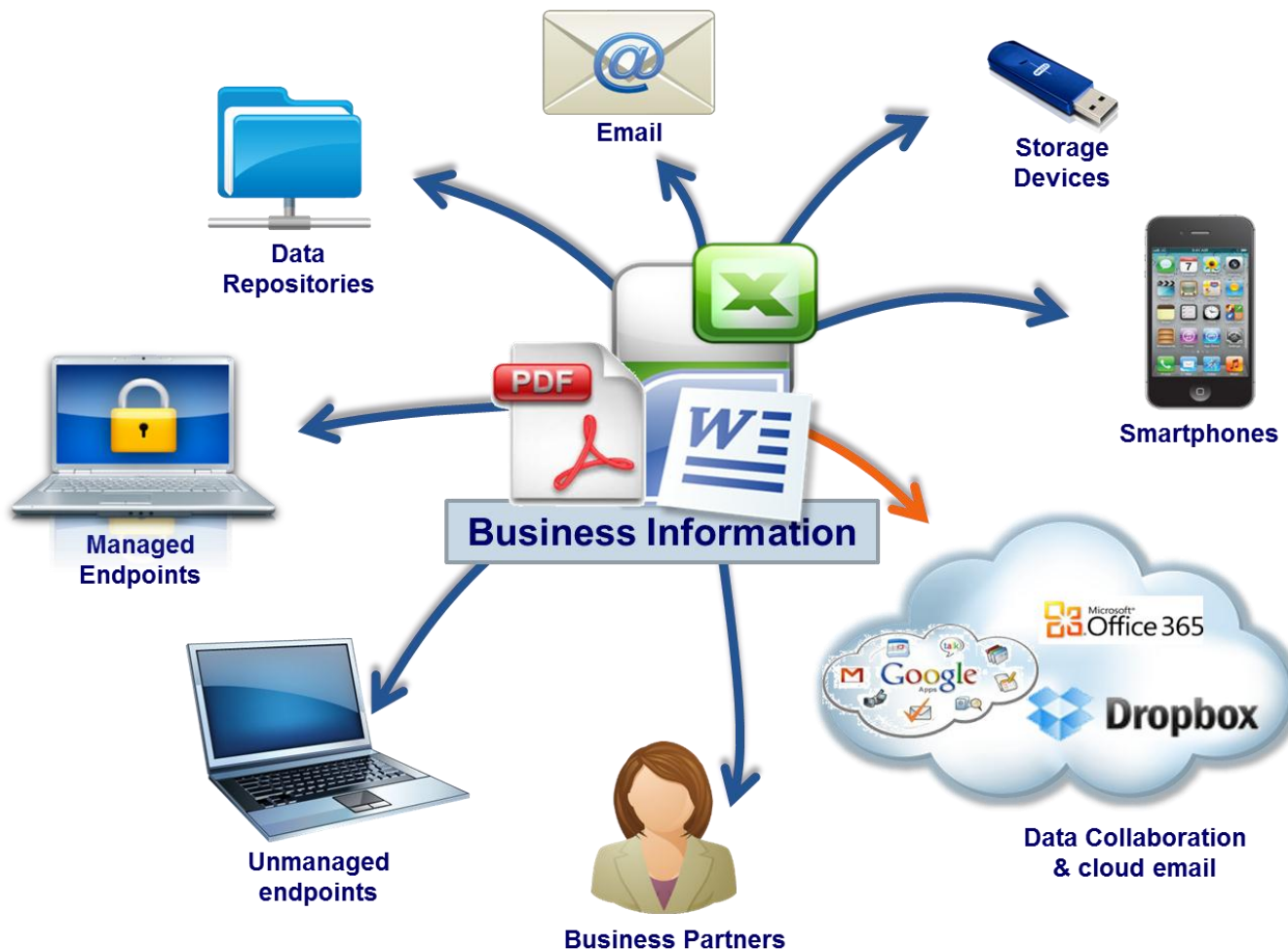
Peter Kovalčík

SE Eastern Europe

pkovalcik@checkpoint.com



Mobile Data Travels Fast, Across All Mobile Devices and Cloud Services



The Risks of Confidential Data Loss are Very High...

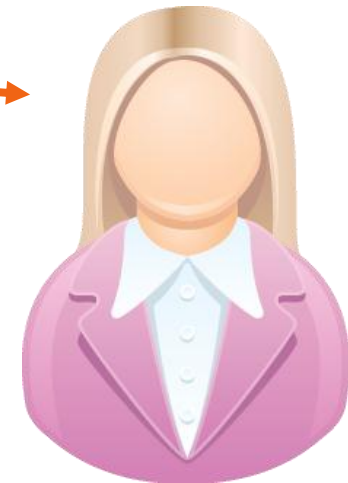
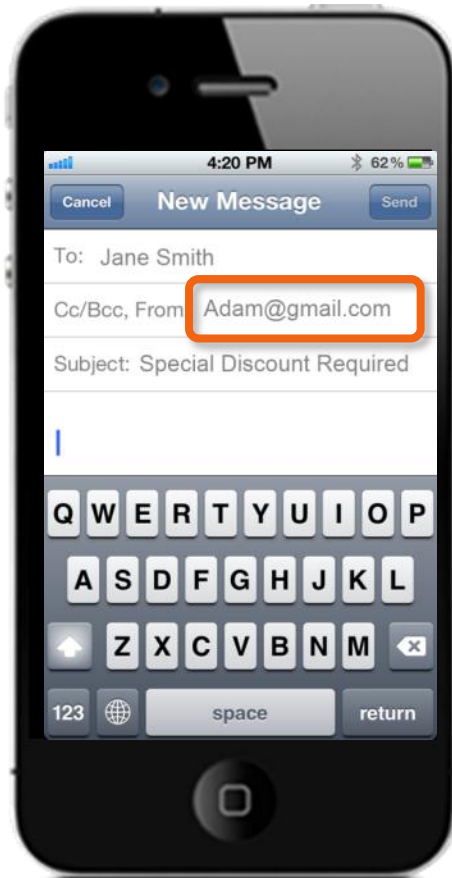


**Lost Portal Media
(USB, SD, etc.)**



**Stolen Corporate
Computers**

Unintentionally initiate business emails from the personal mail box instead of the business one

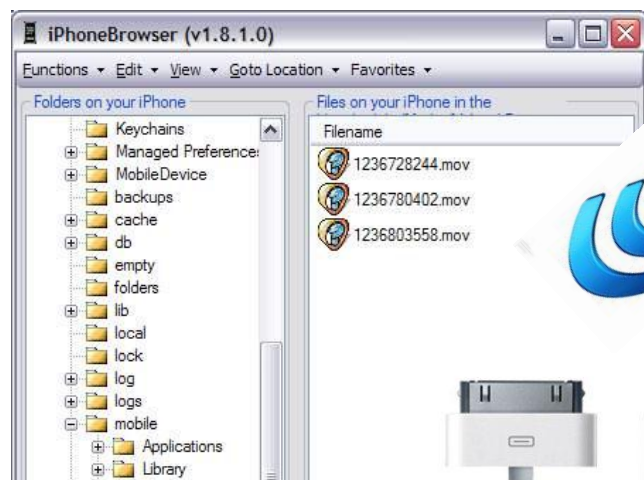


**Jane,
Sales Manager**

Bypass enterprise data protection security layers with just one "tap"



iCloud



When Sharing Data with Partners...



...They May Forward, or Misuse Data

Introducing **MOBILE INFORMATION PROTECTION**

Securing business information
in **Mobile Environments**



MIP Solution

Check Point
Mobile Enterprise
(Mobile Security)

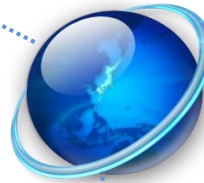


**MIP Mobile Client
Unmanaged**

FDE
MEPP



**MIP Endpoint Client
Managed Asset**



DLP



**MIP Enforcement
Security Gateway**

Unified Central Management
Smart Event



MIP Management



Data Center



Mail Server

Event Analysis tools



MIP Dashboard

Mobile Information Protection Solution



Mobile Security



Data Loss Prevention



Media Encryption



Full Disk Encryption

MIP Mobile Client



Secure business mail, sandbox protection and integrated document security reader

Control Business Data



**Isolate and Encrypt
Business Data**



**Authentication Required
to Access Data**



**Prevent Usage on
Modified Devices**



**Data Expiration and
Remote Wipe**



Is this BYOD ?

- **DEVICE Passlock**
- **DEVICE Encryption**
- **DEVICE Remote Wipe**
- **App BLACKLISTING**
(Block Siri, iCloud, Dropbox, evernote...)
- **Integrating with Mobile Device Management (MDM)**



Overkill to Secure ENTIRE Device

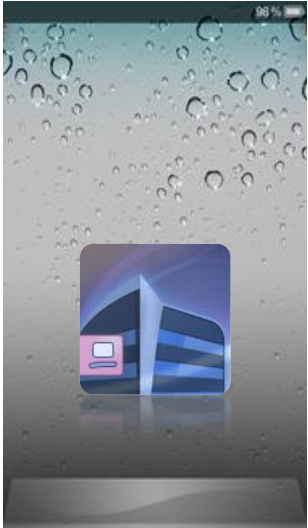
How it works



How it works

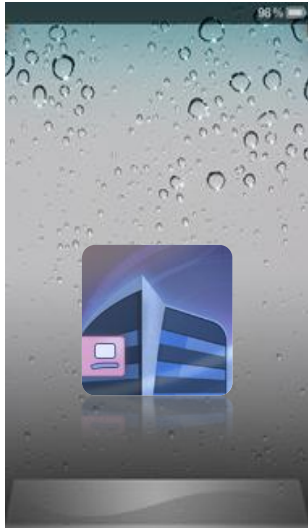
1. Download

Mobile Enterprise



How it works

1. Download Mobile Enterprise



2. Distribute configuration + certificate

Client Certificates

Type to Search 0 items [New...](#) [Edit...](#) [Revoke](#)

CN

Certificate Creation and Distribution [?](#) [X](#)

Certificate Distribution
Select the distribution method for the certificates enrollment keys

Choose how to distribute the certificate enrollment keys to users:

☒ Send emails containing the enrollment keys using the selected email template:

Template: [View...](#)

Site: [Edit...](#)

Mail Server: [Edit...](#)

☒ Generate a file that contains all of the enrollment keys:

Directory: [Browse...](#)

User must enroll within days (key expires at 24/2/2013 18:24)

Comment:

- Use comments to keep track of the newly generated certificates.

[< Back](#) [Next >](#) [Cancel](#)

Email Template

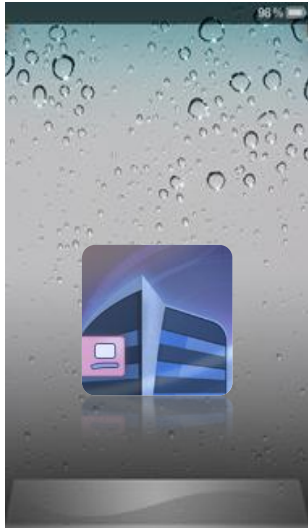
Type to Search

Name

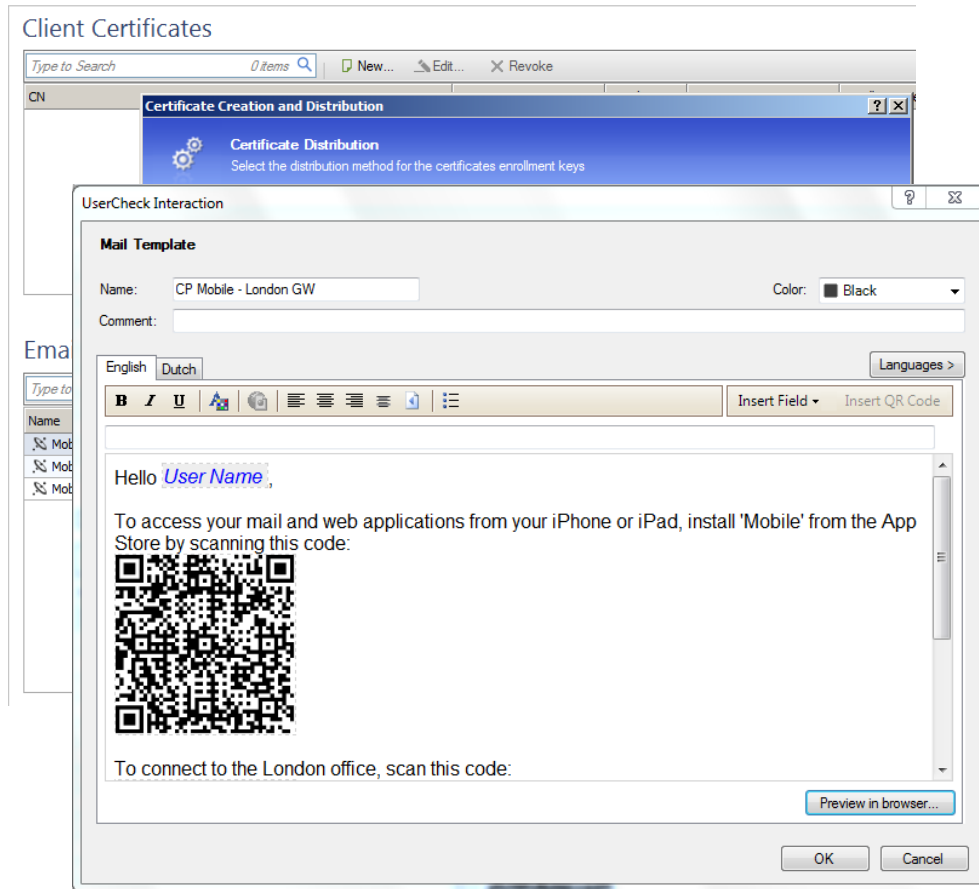
- Mobile VPN iOS
- Mobile Enterprise
- Mobile Enterprise

How it works

1. Download Mobile Enterprise

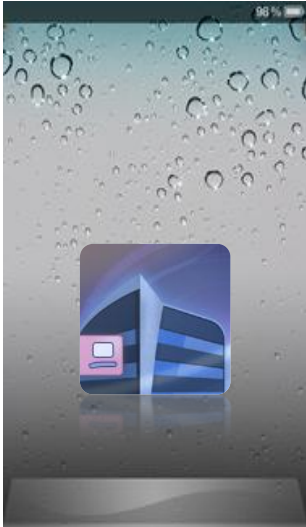


2. Distribute configuration + certificate

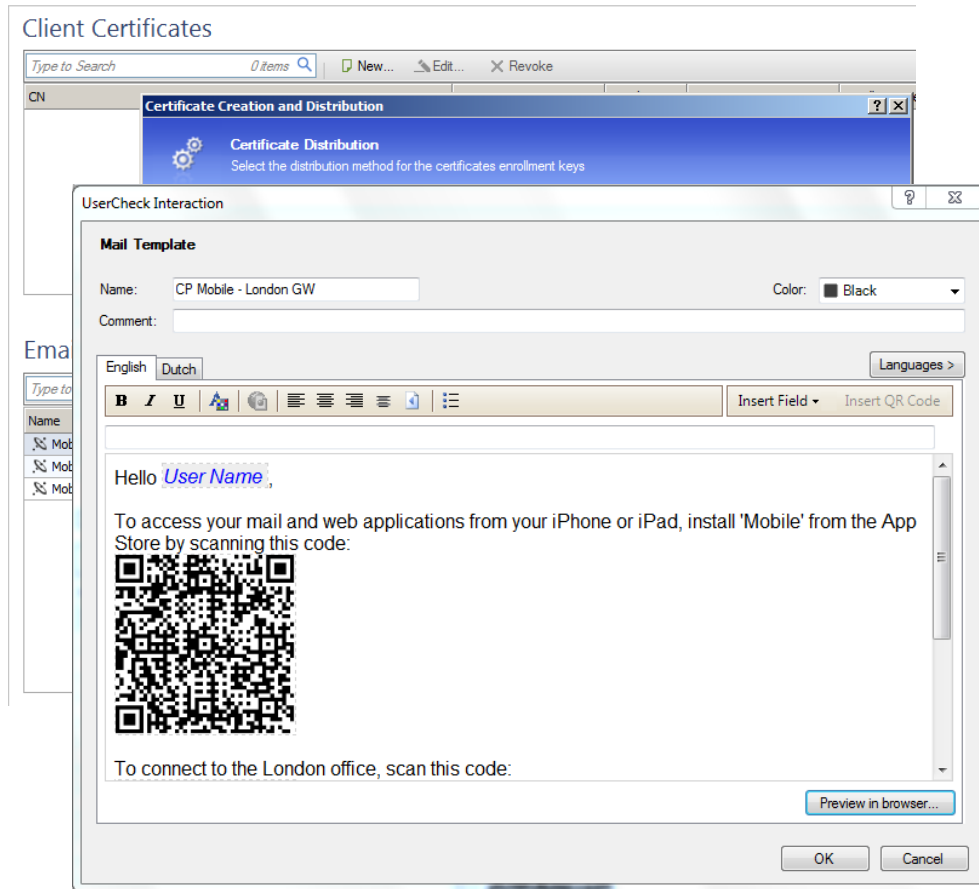


How it works

1. Download Mobile Enterprise



2. Distribute configuration + certificate



3. Connect to site

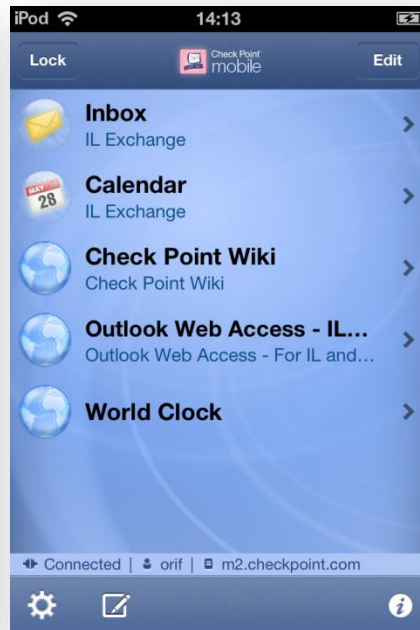


Secure Corporate Mail

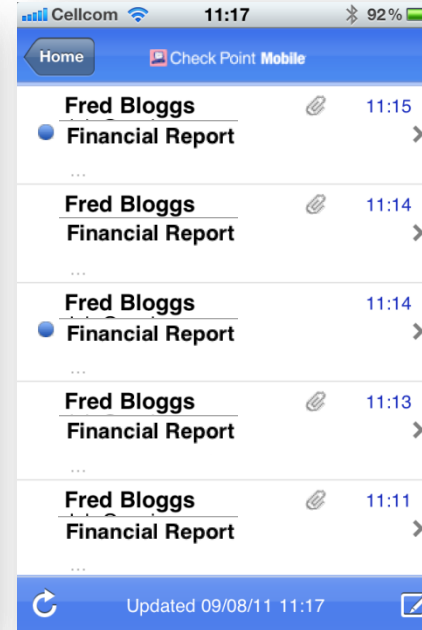
Pin Code



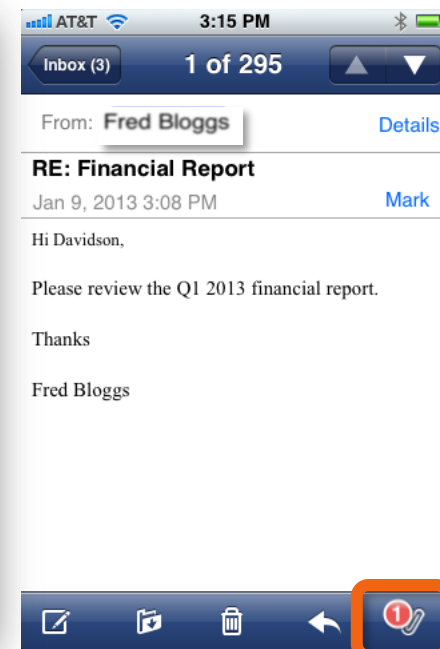
**Secure
Access**



Mail



Sandbox



Protects the app by a pin code

Secure access
to Web portal,
Email and
Calendar items

Native and
easy to use
mail client

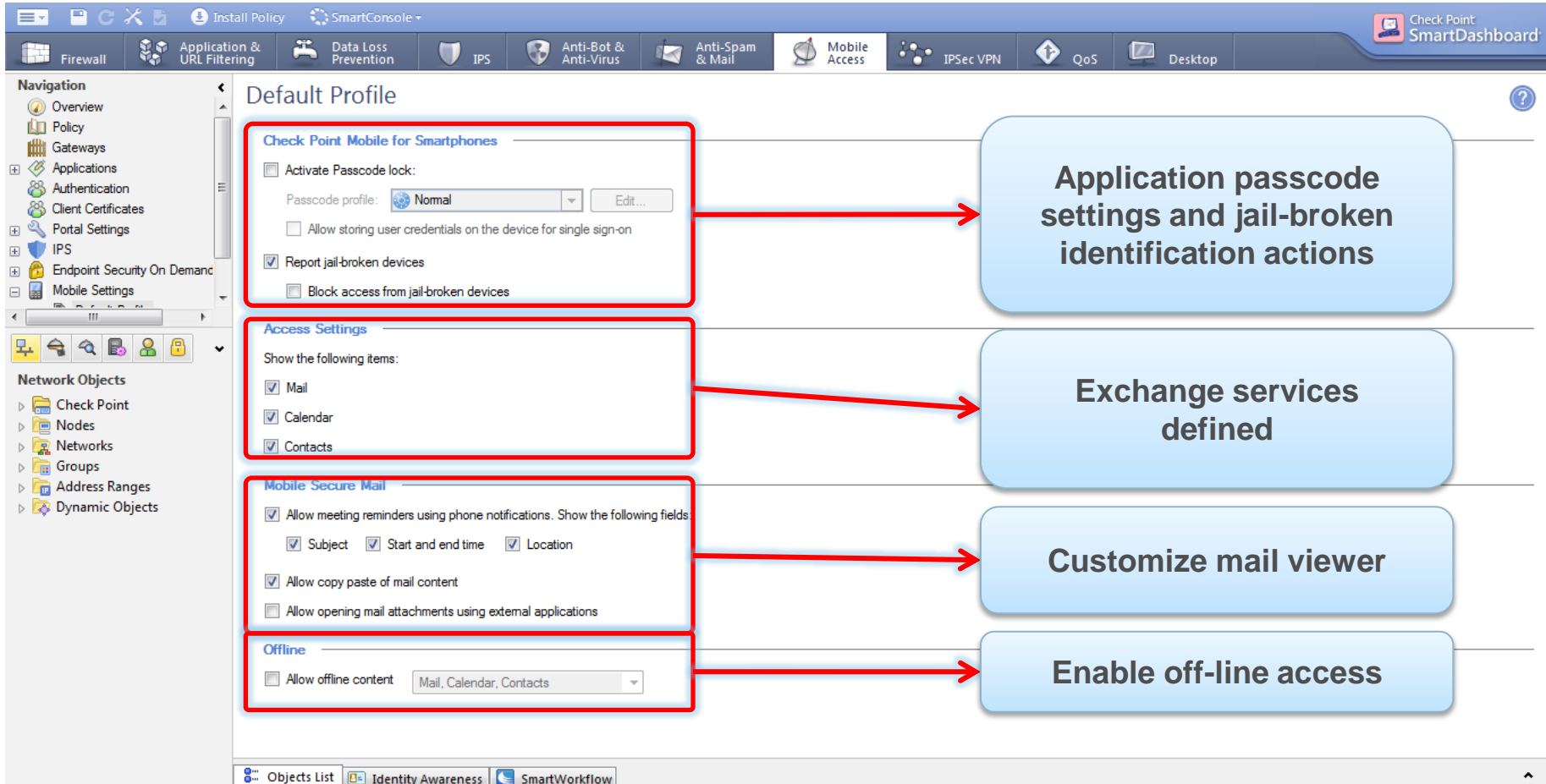
All attached
documents are
opened in the
secure sandbox

Secure Mail Architecture



- Two-factor authentication (usr/pass and certificates)
- Robust performance
- Online and Offline modes
- iOS support Q1/13 , Android Q2/13

■ Mobile client policy enforcement



The screenshot displays the Check Point SmartDashboard interface for Mobile Access configuration. The left sidebar shows the navigation tree with 'Mobile Settings' selected. The main area shows the 'Default Profile' configuration page. Four sections are highlighted with red boxes, and red arrows point from these sections to callout boxes on the right:

- Check Point Mobile for Smartphones:** This section includes settings for 'Activate Passcode lock' (with a 'Normal' passcode profile), 'Allow storing user credentials on the device for single sign-on', 'Report jail-broken devices' (checked), and 'Block access from jail-broken devices'. An arrow points to the callout: **Application passcode settings and jail-broken identification actions**.
- Access Settings:** This section includes 'Show the following items' with checkboxes for 'Mail', 'Calendar', and 'Contacts' (all checked). An arrow points to the callout: **Exchange services defined**.
- Mobile Secure Mail:** This section includes 'Allow meeting reminders using phone notifications. Show the following fields' (with checkboxes for 'Subject', 'Start and end time', and 'Location' all checked), 'Allow copy paste of mail content' (checked), and 'Allow opening mail attachments using external applications' (unchecked). An arrow points to the callout: **Customize mail viewer**.
- Offline:** This section includes 'Allow offline content' (checked) and a dropdown menu showing 'Mail, Calendar, Contacts'. An arrow points to the callout: **Enable off-line access**.

Check Point Mobile Access Gateway

Secure
Access from
PC & Mac



Web Portal
for Business

VPN Client

Secure
Access from
Smartphones



Secure

VPN App



MIP Endpoint Client



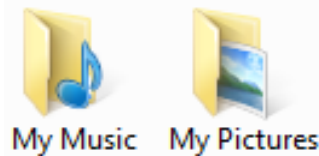
**Secure Data on Computer & External Media, protect from
Malware, Phishing & Network Threats**

Full Disk Encryption

- Industry leading solution – **Over 10 years Leader in Gartner Magic Quadrant**
- Provides a **strong sector encryption** combined with pre-boot authentication to ensure a complete data security
- Flexible pre-boot authentication including strong authentication with more than **90 different smartcard models** supported
- **Full Range of Recovery Options**
 - Remote Help
 - Data Recovery
 - Dynamic Mount Utility
- Best Visibility with SmartEndpoint, SmartLog and SmartEvent



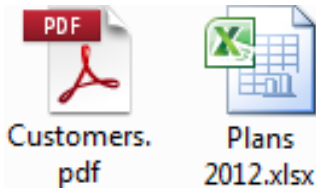
Separate and Protect Business Data from Personal Data on Storage Devices



My Music My Pictures

Personal Data

- ✓ Data is not encrypted
- ✓ Access to any user/device



Customers.
pdf Plans
2012.xlsx

Business Data

- ✓ Data is encrypted
- ✓ Transparent access only to approved users and devices

Media
Encryption



**Check Point
MIP Client**

User Check

 **Check Point**
SOFTWARE TECHNOLOGIES LTD.

Data Must be Encrypted

The company's security policy requires you to encrypt corporate data.

This protects sensitive data from unauthorized disclosure.

You will be able to access your data as follows:

-  **K: Personal (clear) storage.**
-  **L: Corporate (encrypted) storage.**

Password:

Confirm password:

Encrypt & Copy **Don't Copy**

 **Check Point**
SOFTWARE TECHNOLOGIES LTD.

Comprehensive Security on the Endpoint



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



Protect against drive-by-downloads, phishing sites and zero-day attacks

















Stop unwanted traffic, prevent malware and block targeted attacks

The **ONLY** unified Client for PC

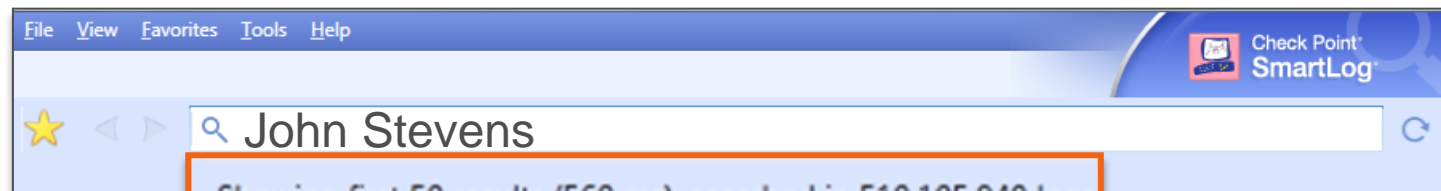
And Now -- **For Mac As Well !**











A Unified, Simple to Understand Endpoint Security Policy

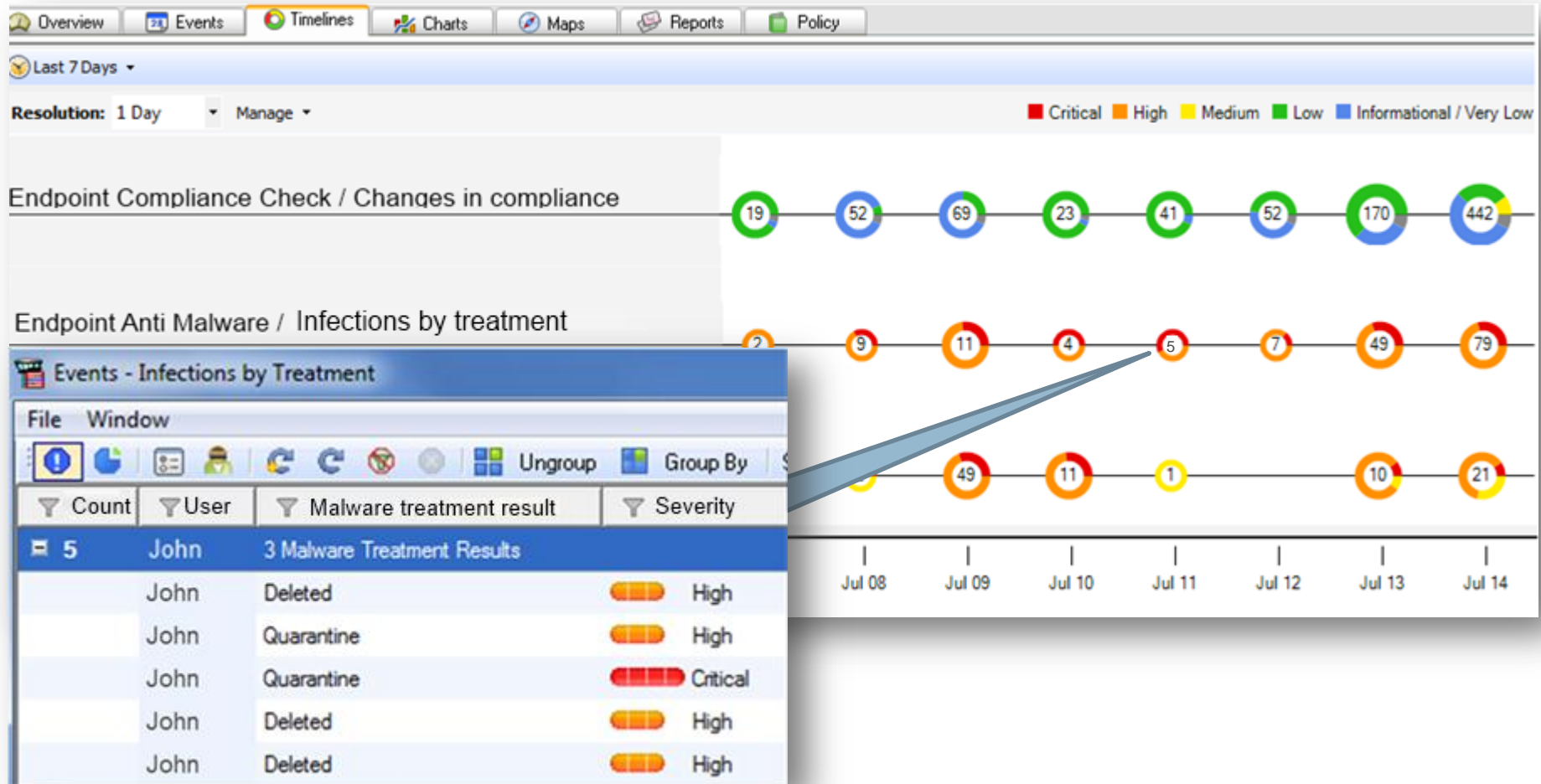
Applies To	Actions
 Full Disk Encryption	
 <i>Entire Organization</i>	 Encrypt all local hard-disks  Do not authenticate user before OS loads (Pre-boot)
 Media Encryption & Port Protection	
 <i>Entire Organization</i>	 Allow reading any data from storage devices  Encrypt business-related data written to storage devices
 Anti-Malware	
 <i>Entire Organization</i>	 Scan all files upon access  Check for malware signature updates every 4 hours
 Firewall	
 <i>Entire Organization</i>	 Allow inbound traffic from trusted zones and connectivity services  Allow any outbound traffic

Visibility to Organizational Security Events Across Network & Endpoint



User Name	Blade	Action	Description
John Stevens	 Application Control	 Allow	Allow application facebook
John Stevens	 DLP	 Ask User	Mail Sent
John Stevens	 Anti Malware	 Control	Anti Malware signatures updated
John Stevens	 Media Encryption	 Allow	Copied AOP2012.docx to encrypted media

Security Forensics & Analysis with Endpoint Security SmartEvent



Prevent Data Loss in Motion



Prevent Data Loss in Motion

File Edit View Manage Rules Policy SmartWorkflow Search Window Help

Firewall NAT IPS Application & URL Filtering Anti-Spam & Mail Mobile Access Anti-Virus Data Loss Prevention IPsec VPN QoS Desktop

Overview Policy Data Types My Organization Gateways Additional Settings

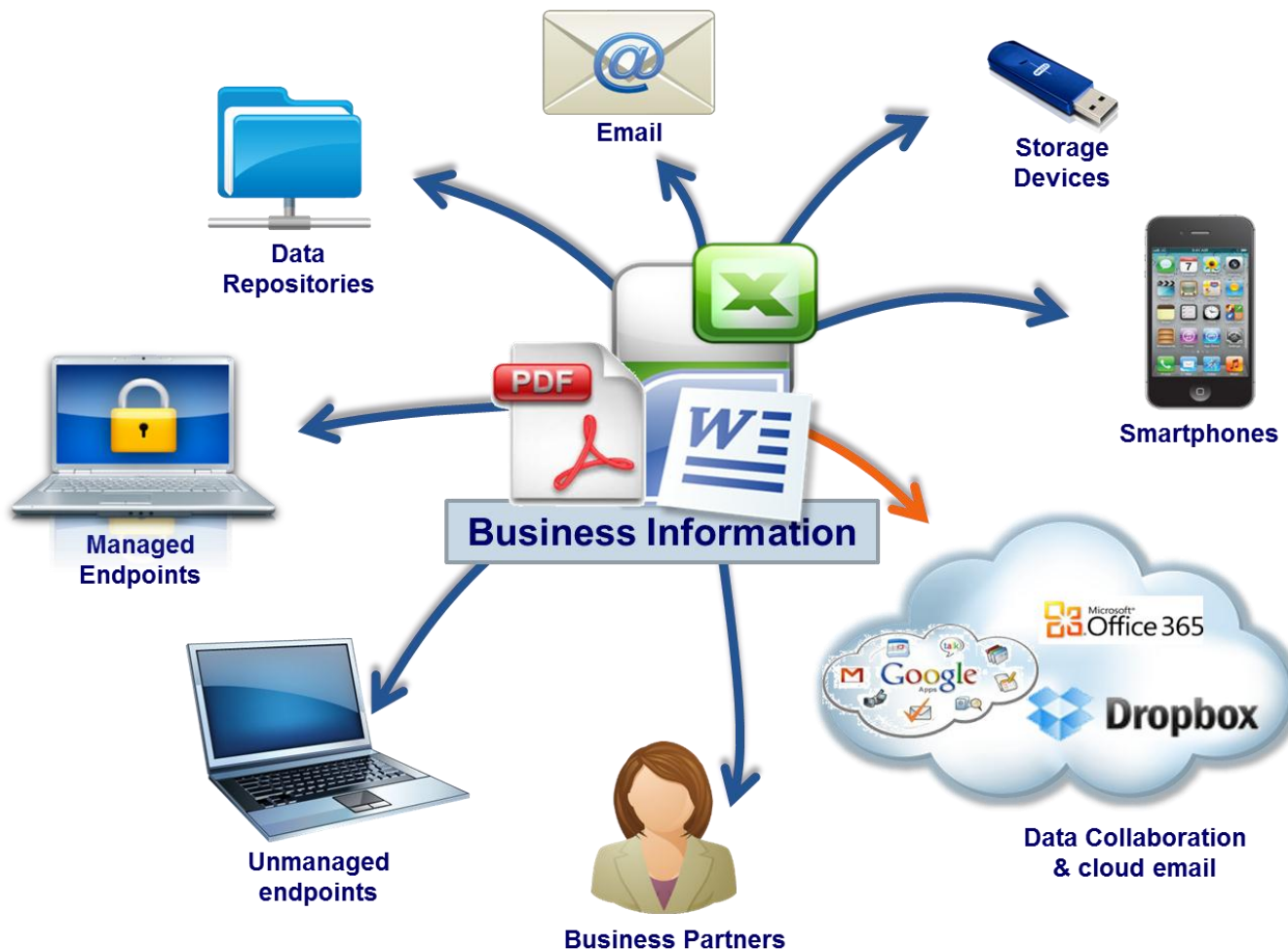
Data Loss Prevention (DLP) Policy

Type to Search [] Grouping: Category []

	Data	Source	Destination	Exceptions	Action	Track	Install On	Category	Comment
Best Practice (6)									
	Database File	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Best Practice	Matches database file types.
	Large File	My Organization	Free Email Dom...	None	Detect	Log	DLP Blades	Best Practice	Matches emails that contain large files and that are sent to a list of private email domains; such emails are considered a common source of data loss.
	External Recipient in BCC	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Best Practice	Matches emails with an external address in BCC, when the To and CC addresses are internal only.
	External Recipient and ...	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Best Practice	Matches emails that appear to be addressed to an external recipient by mistake.
	Inappropriate Language	My Organization	Outside My Org	None	Inform User	Log	DLP Blades	Best Practice	Matches data containing inappropriate words and phrases.
	Password Protected File	My Organization	Outside My Org	None	Ask User	Log	DLP Blades	Best Practice	Matches password protected files.
Business Information (3)									
	Customer Names	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Business Inf...	Matches data containing names of your customers. Replace the placeholder dictionary with your own list.
	Salesforce Reports	My Organization	Outside My Org	None	Ask User	Log	DLP Blades	Business Inf...	Matches reports generated by salesforce.com online Software as a Service.
	Employee Names	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Business Inf...	Matches data containing names of your employees. Replace the placeholder dictionary with your own list.
Compliance (2)									
	PCI - Cardholder Data	My Organization	Outside My Org	None	Prevent	Log	DLP Blades	Compliance	Matches data related to the Payment Card Industry (PCI) Data Security Standard (DSS).
	PCI - Credit Card Num...	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Compliance	Matches data protected by HIPAA.
Financial (1)									
	Confidential Financial R...	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Financial	Matches documents containing confidential financial reports.
Intellectual Property (1)									
	Source Code	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Intellectual ...	Matches data containing Intellectual Property: source code, CAD-CAM designs or graphic design files.
	CAD-CAM Designs	My Organization	Outside My Org	None	Detect	Log	DLP Blades	Intellectual ...	Matches data containing Intellectual Property: source code, CAD-CAM designs or graphic design files.



Mobile Data Travels Fast, Across All Mobile Devices and Cloud Services



Mobile Information Protection Solution



Mobile Security



Data Loss Prevention



Media Encryption



Full Disk Encryption