Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point R76 Update

Rami Rauanmaa
Sr. Security Engineer
Check Point Software Technologies

Agenda

1. R76 Software version
2. Threat Emulation Blade
3. Document Security
4. Compliance Blade

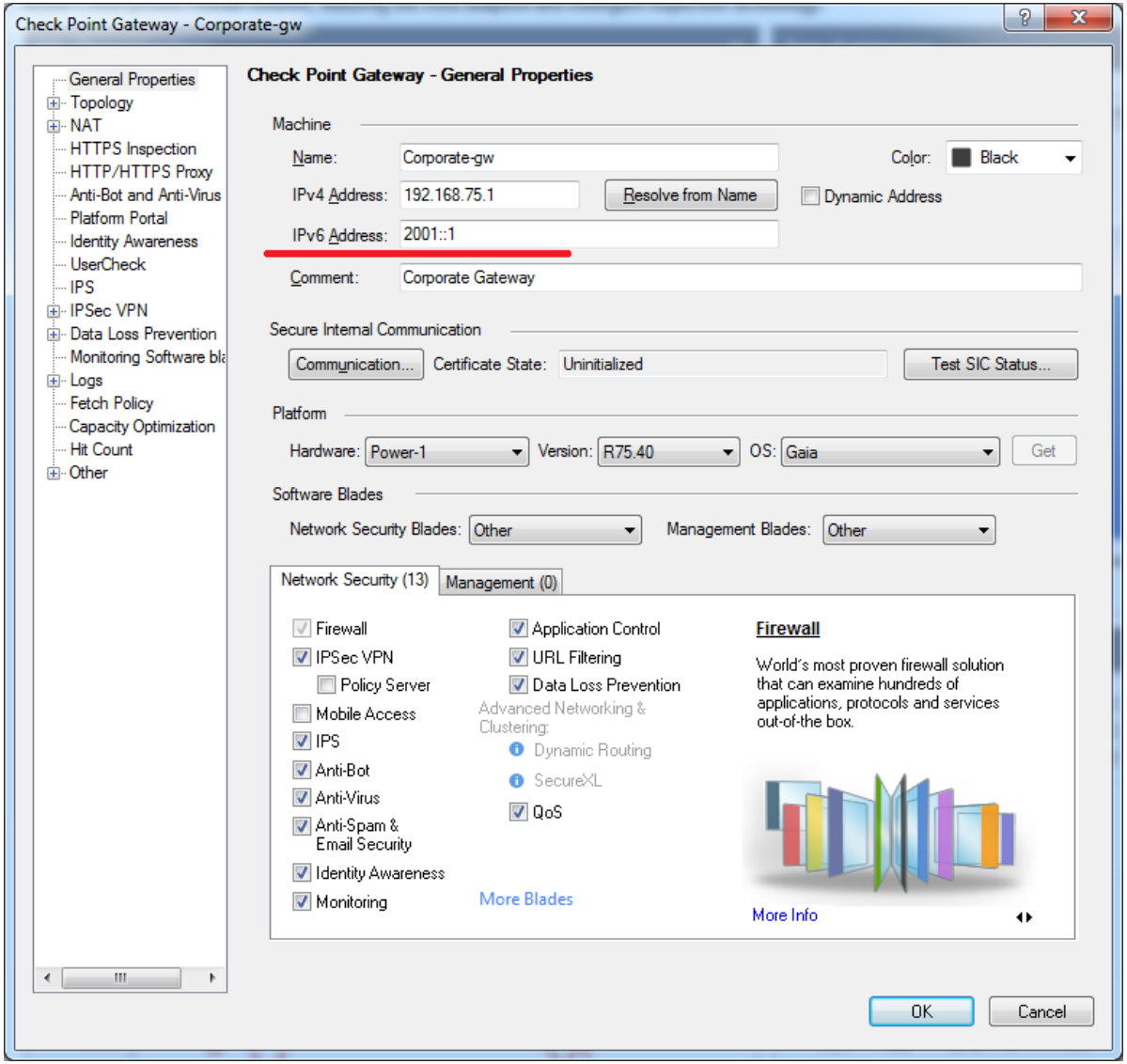
Support for IPv6 - Features description

- Access Policy
  - Complete Firewall support, including dynamic objects and time objects.
  - Full stateful inspection for IPv6 connections.
  - NAT66 and NAT64
- URL filtering and Application control
- Identity awareness and Authentication
- User Check
- Anti Bot and Anti Malware
- Advanced Networking and OS
- Dynamic Routing: OSPF and BGP
- HA: Clustering and VRRP
- IPS
- VPN Site-to-Site

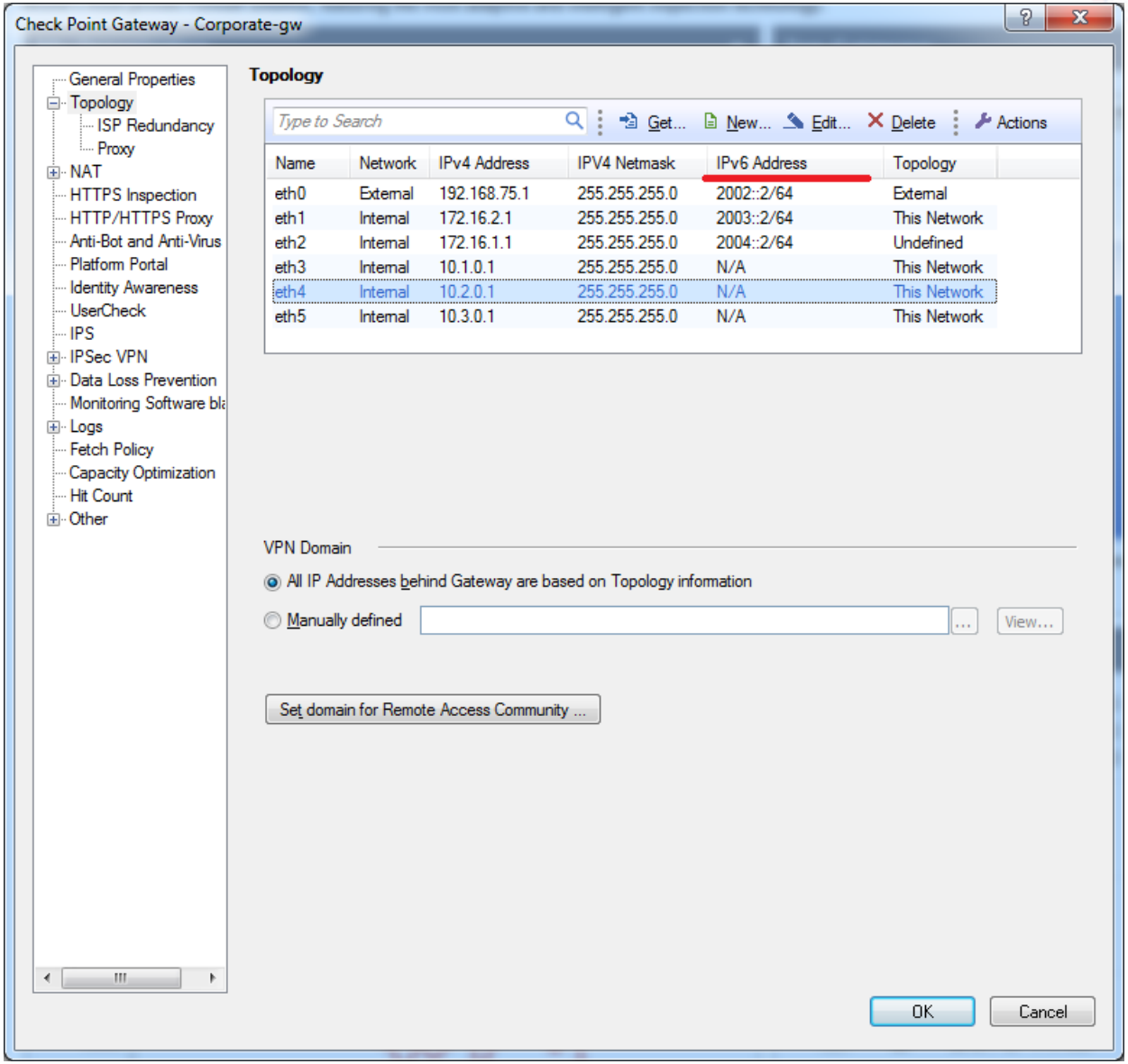
Features description (cont.)

- Central Management
  - Support IPv6 for all communications between gateway and management
  - SmartDashboard
    - Ability to connect to Management with IPv6 address
    - Support dual-stack definition for all network objects
    - Support IPv6 addresses in all IP containers
    - Support for multiple IPv6 ranges on the same object
    - Get topology covers IPv4 and IPv6
- SmartLog and SmartEvent
- SmartView Monitor (except traffic counters)
- Support IPv6-only Security Gateway and IPv6-only Security Management server

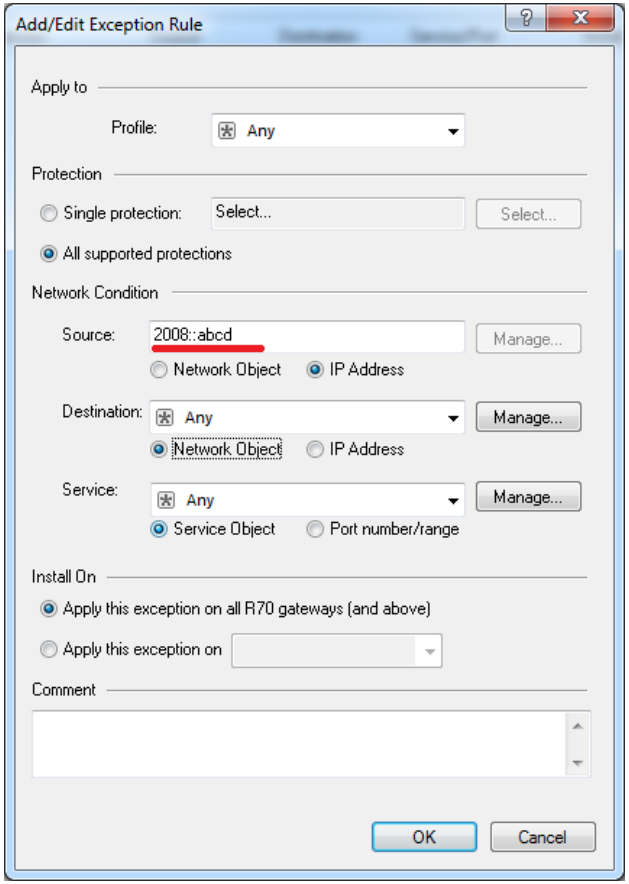
IPv6 - Gateway Configuration

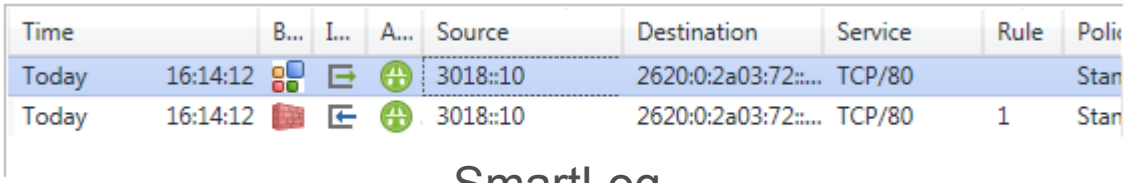


IPv6 - Topology



IPv6 - Additional Screenshots

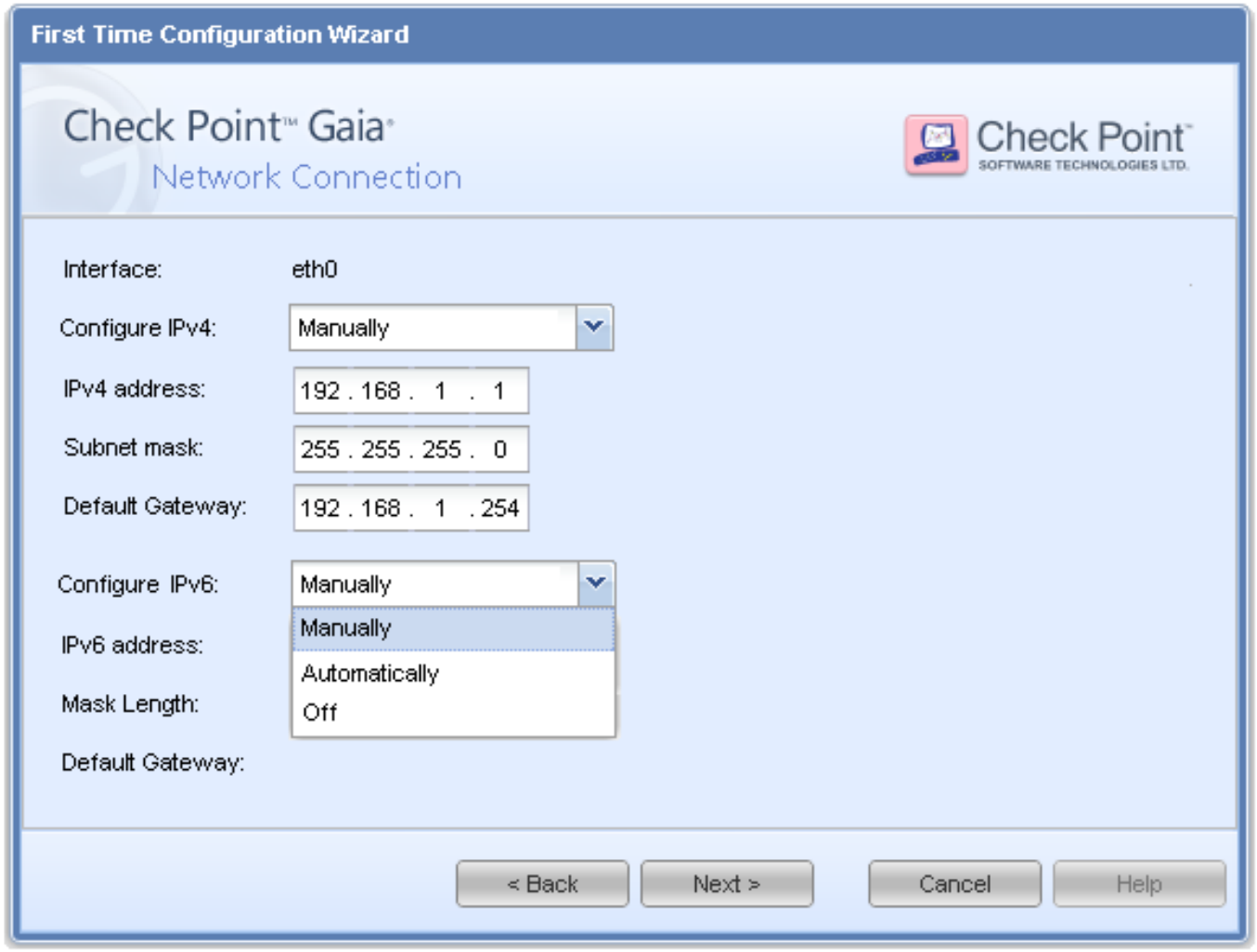




SmartLog

IPS exceptions

Full IPv6 Support in Gaia WebUI – including FTW



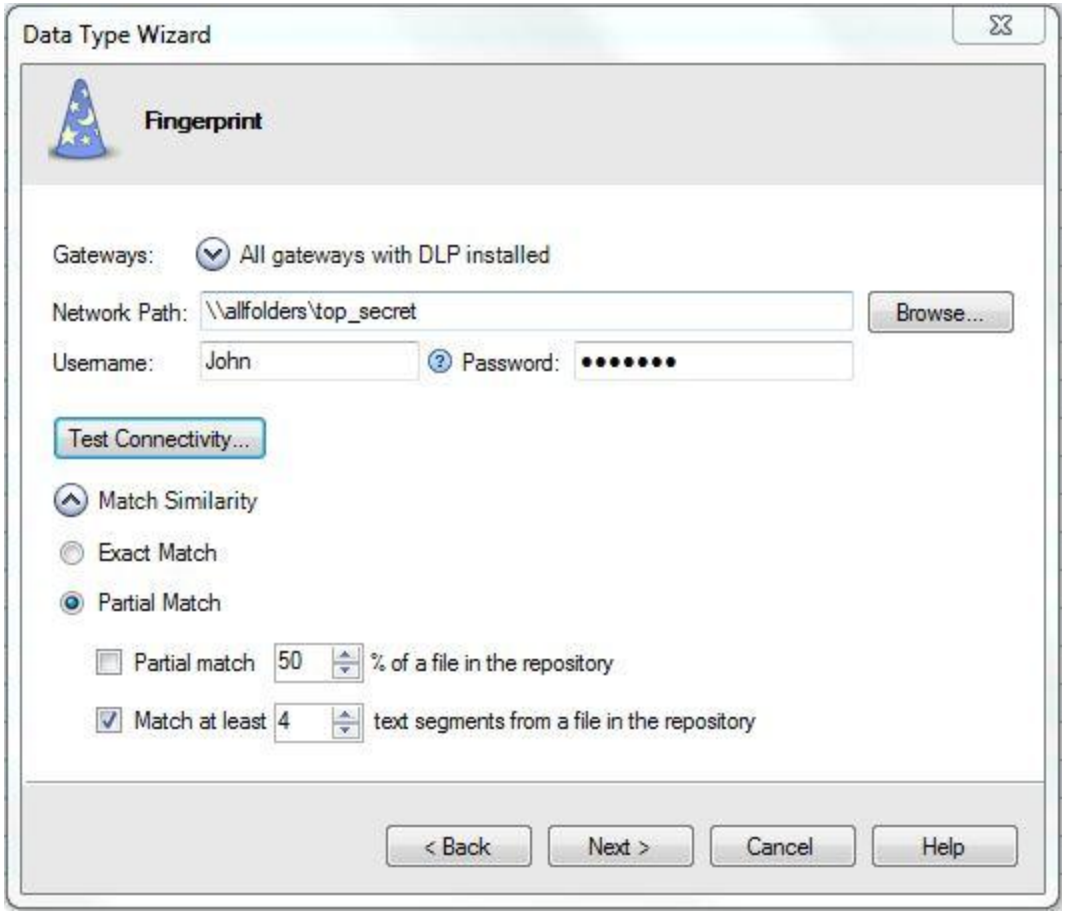
–[Restricted] ONLY for designated groups and individuals

DLP enhancements

- Define DLP policies in user and user-group granularity
  - Integration with Identity Awareness
- Fingerprinting – DLP scans file repositories of sensitive files and match when a file from this repository (or part of it) leaves the organization.
- Whitelist – define a repository of white listed files for DLP engine to exempt.
- Enhancements to User Engagement
  - DLP email notifications to end-user for all protocols
  - UserCheck notifications configuration and multi-language support

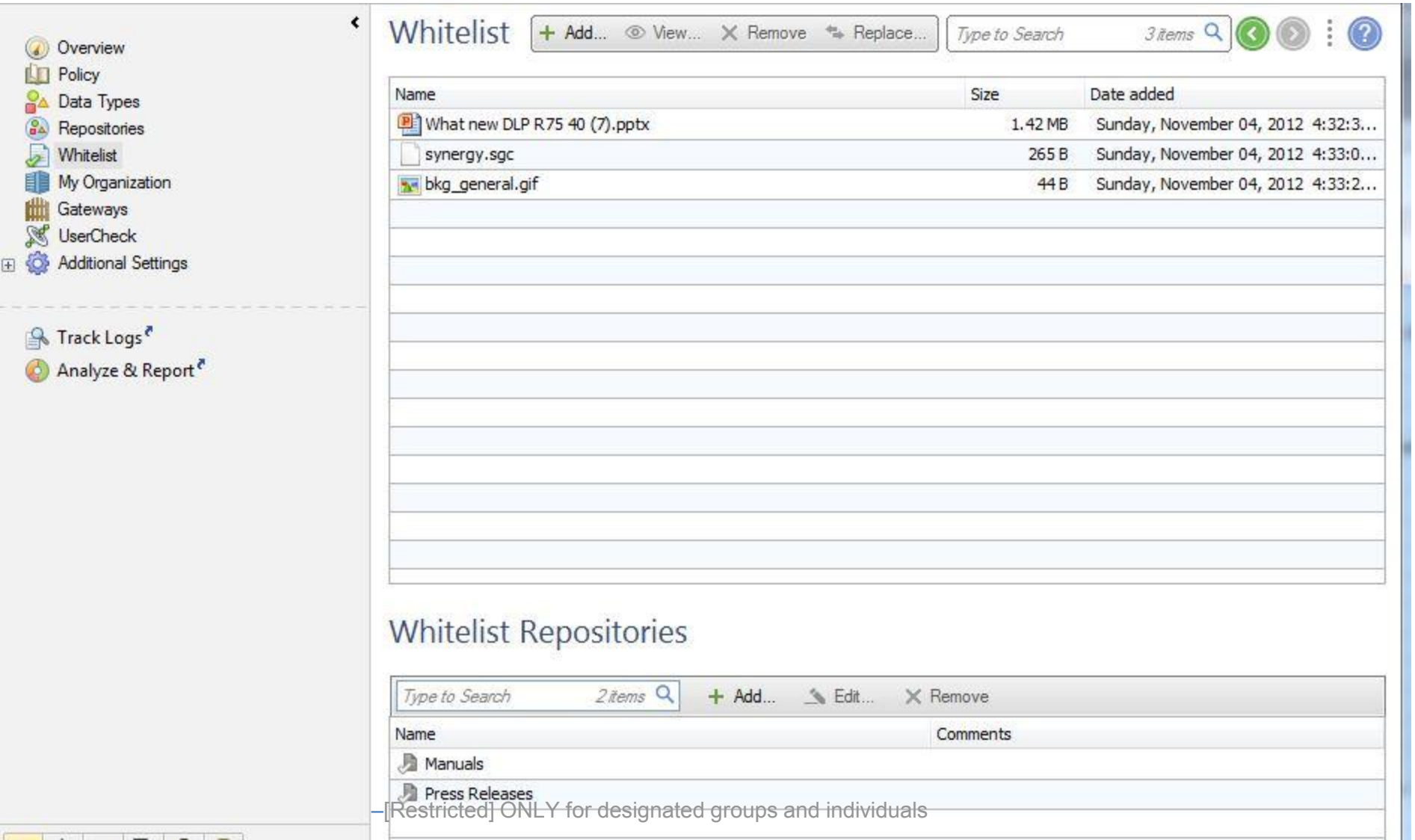
DLP Enhancements - Fingerprint

- DLP scans file repositories of sensitive files and match when a file from this repository (or part of it) leaves the organization.



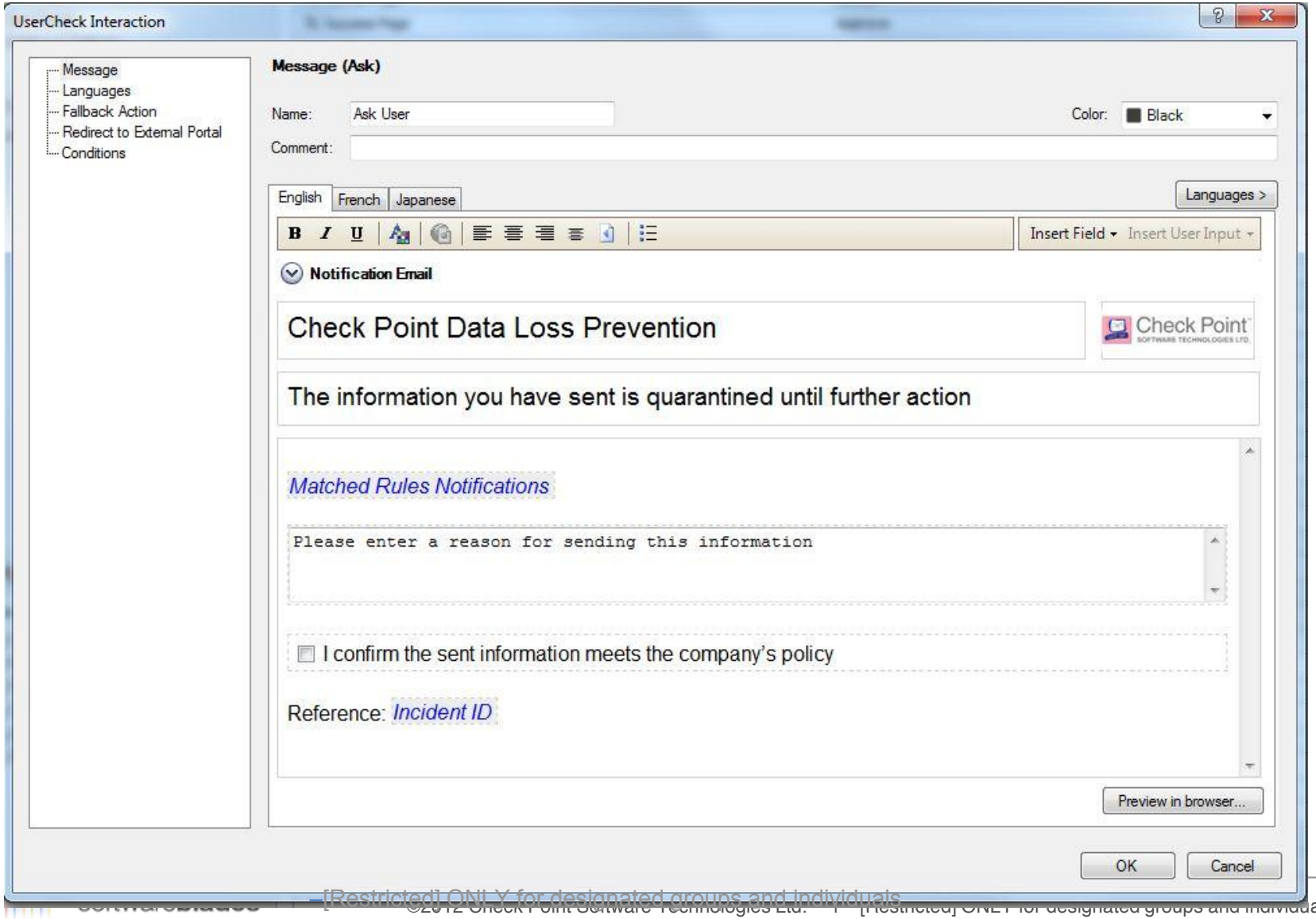
DLP enhancements – White List

- Whitelist – define a repository of white listed files for DLP engine to exempt.



DLP enhancements - UserCheck

- UserCheck notifications configuration and multi-language support



New Hardware support

- New 21600 appliance

- Support for DDoS Protector appliance

DDoS and Gateway durability

- A new set of features is being introduced to the Check Gateways to improve its durability under DoS and DDoS conditions
- These include:
  - A Penalty Box mechanism
  - Improved SYN Attack mitigation
  - Drop templates
  - DDoS enforcement

URLF and Application control enhancements

- Enhanced Filtering Options
  - "Lite" HTTPS filtering – filter HTTPS traffic without SSL inspection
  - Enforce Safe Search in Search Engines – filter explicit content in search engines results
  - Filter cached and translated pages in search engines
- Enhanced Reporting
  - User detailed activity report
  - Browse Time – show time spent in web browsing in logs, events and reports
  - Allow non-admin access to reports with dedicated permission
- Support for more protocols

URLF/APCL – User Detailed Activity

Application and URL User Activity - John Smith

November 13, 2011 12:00 AM - January 12, 2012 11:59 PM

Check Point SOFTWARE TECHNOLOGIES LTD.

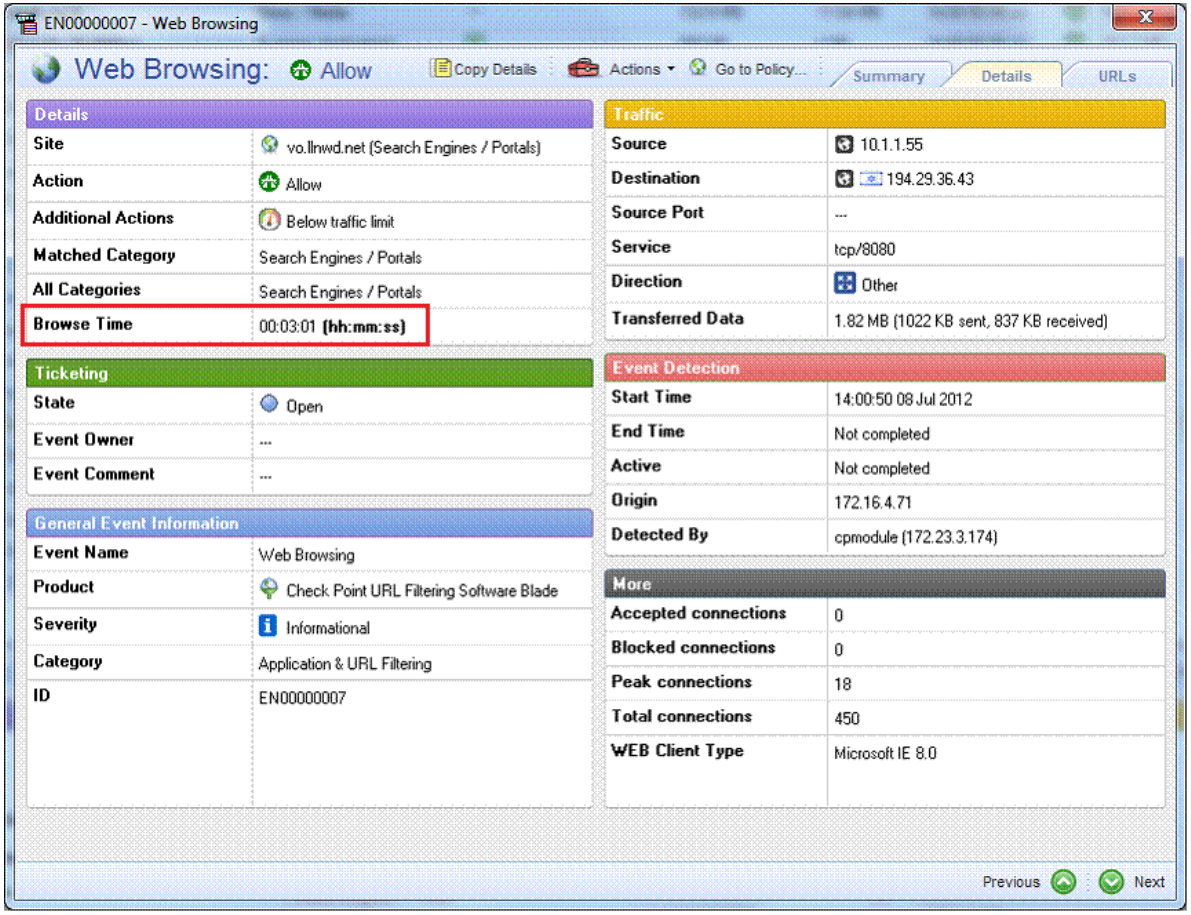
Detailed User Activity (1 out of 2)

2

Start Time	Application / Site	Risk	Category	Action	Traffic
28-Mar-2012 04:32:15 PM	MAPI Protocol	Very Low	Network Protocols	Allow	20B
28-Mar-2012 04:32:14 PM	http://www.ynet.co.il/home/0,7340,L-8,00.html	Unknown	Web Browsing	Allow	1.2KB
28-Mar-2012 04:32:13 PM	mIRC	High	Instant Messaging	Block	0B
28-Mar-2012 04:32:13 PM	YouTube	Low	Media Sharing	Allow	4.4KB
28-Mar-2012 04:32:12 PM	DNS Protocol	Very Low	Network Protocols	Allow	154B
28-Mar-2012 04:32:11 PM	Paypal	Very Low	Business Applications	Allow	382B
28-Mar-2012 04:32:11 PM	Gmail	Medium	Email	Allow	5.5KB
28-Mar-2012 04:32:10 PM	DNS Protocol	Very Low	Network Protocols	Allow	123B
28-Mar-2012 04:32:10 PM	mIRC	High	Instant Messaging	Block	0B
28-Mar-2012 04:32:10 PM	PPTP Protocol	High	Network Protocols	Block	0B
28-Mar-2012 04:32:10 PM	Kerberos Protocol	High	Network Protocols	Block	0B
28-Mar-2012 04:32:09 PM	DCE-RPC Protocol	Low	Network Protocols	Allow	848B
28-Mar-2012 04:32:09 PM	YouTube	Low	Media Sharing	Allow	3.9KB
28-Mar-2012 04:32:06 PM	Paypal	Very Low	Business Applications	Allow	920B
28-Mar-2012 04:32:01 PM	DNS Protocol	Very Low	Network Protocols	Allow	152B
28-Mar-2012 04:31:57 PM	PPTP Protocol	High	Network Protocols	Block	0B
28-Mar-2012 04:31:56 PM	Telnet Protocol	High	Network Protocols	Block	0B
28-Mar-2012 04:31:55 PM	DNS Protocol	Very Low	Network Protocols	Allow	120B
28-Mar-2012 04:31:48 PM	YouTube	Low	Media Sharing	Allow	24.5KB
28-Mar-2012 04:31:48 PM	Windows Update	Very Low	Business Applications	Allow	7.1KB
28-Mar-2012 04:31:47 PM	Telnet Protocol	High	Network Protocols	Block	0B
28-Mar-2012 04:31:45 PM	mIRC	High	Instant Messaging	Block	0B
28-Mar-2012 04:31:45 PM	Windows Update	Very Low	Business Applications	Allow	4.1KB
28-Mar-2012 04:31:40 PM	Paypal	Very Low	Business Applications	Allow	120B
28-Mar-2012 04:31:37 PM	Gmail	Medium	Email	Allow	9.9KB
28-Mar-2012 04:31:30 PM	DNS Protocol	Very Low	Network Protocols	Allow	120B
28-Mar-2012 04:31:21 PM	http://www.cplusplus.com/forum/general/	Unknown	Web Browsing	Allow	1.9KB
28-Mar-2012 04:31:16 PM	DNS Protocol	Very Low	Network Protocols	Allow	120B
28-Mar-2012 04:31:13 PM	DNS Protocol	Very Low	Network Protocols	Allow	120B
28-Mar-2012 04:31:08 PM	mIRC	High	Instant Messaging	Block	0B

URLF – Browse Time

- Browse Time – show time spent in web browsing in logs, events and reports



Various Software Blades enhancements

- **UserCheck**
  - UserCheck client single sign on.
  - Improved performance and usability.
- **Identity Awareness**
  - New, rich login logs (similar to Remote Access login logs)
- **Anti-Bot and Anti-Virus**
  - Improved scanning and recognition of bots and viruses.
  - User Check support
  - Support for URLs in rulebase exceptions
- **VPN**
  - AES performance enhancements for high end appliances - 12400, 12600 & 21000 series: Increased Site to Site VPN , Remote Access and HTTPS Inspection throughput.
  - HTTPS Inspection blacklist automatic updates
  - Increased session rate for Identity Awareness Captive Portal.
- **IPS**
  - Aggregation of logs of the IPS Non Compliant HTTP and Non Compliant DNS protections.
- **General (Monitoring)**
  - Netflow services can be used to collect information about network traffic patterns and volume.

Control Business Data

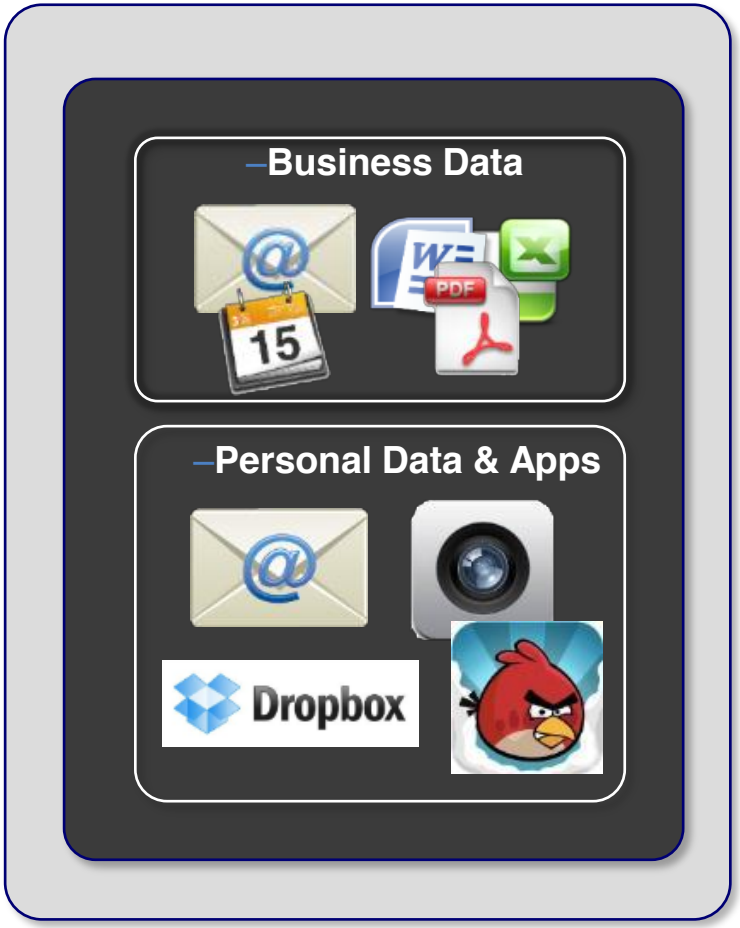
Check Point SOFTWARE TECHNOLOGIES LTD.

Isolate and Encrypt Business Data

Authentication Required to Access Data

Prevent Usage on Modified Devices

Data Expiration and Remote Wipe



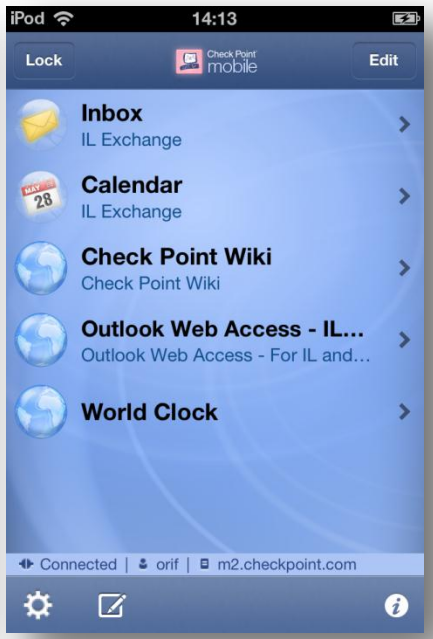
Mobile Enterprise for iOS

Check Point SOFTWARE TECHNOLOGIES LTD.

Passcode

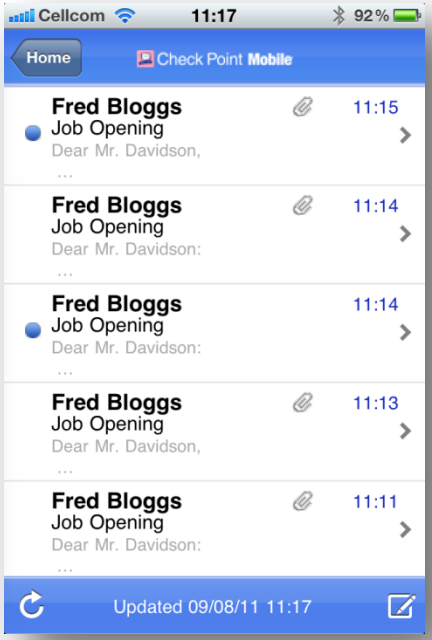
Protect access to the application by a passcode

Secure Access



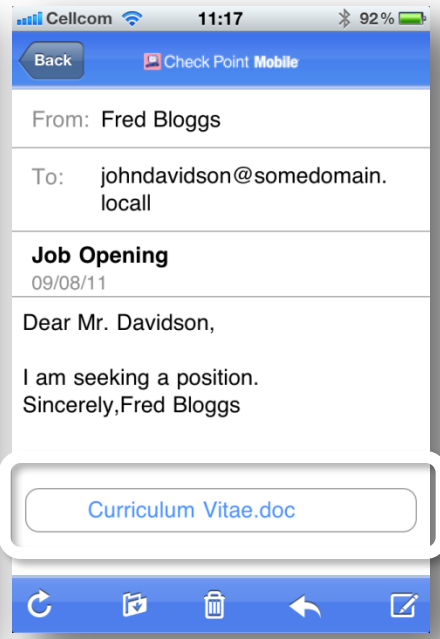
Secure access to Web portal, Email and Calendar items

Mail



Native and easy to use mail client

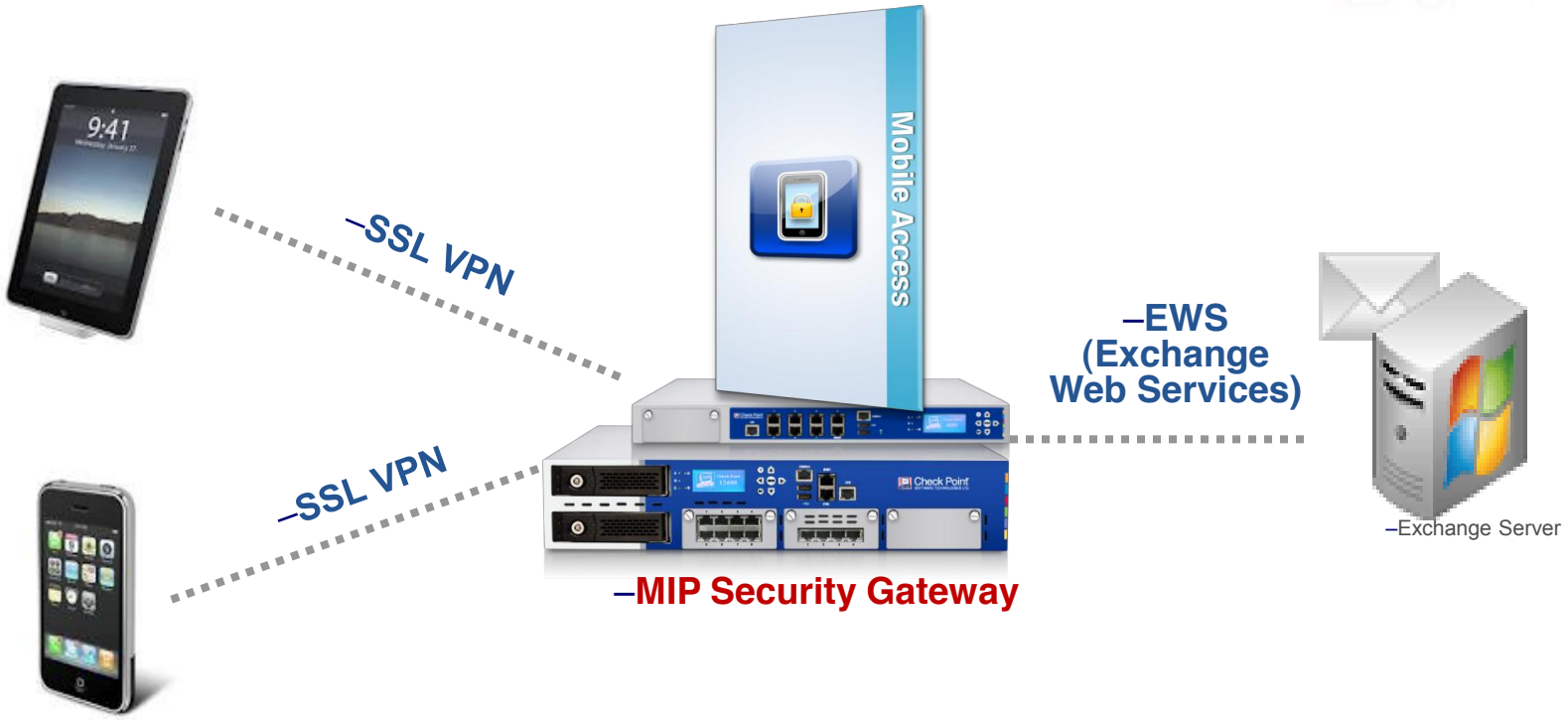
Sandbox



All attached documents are opened in the secure sandbox

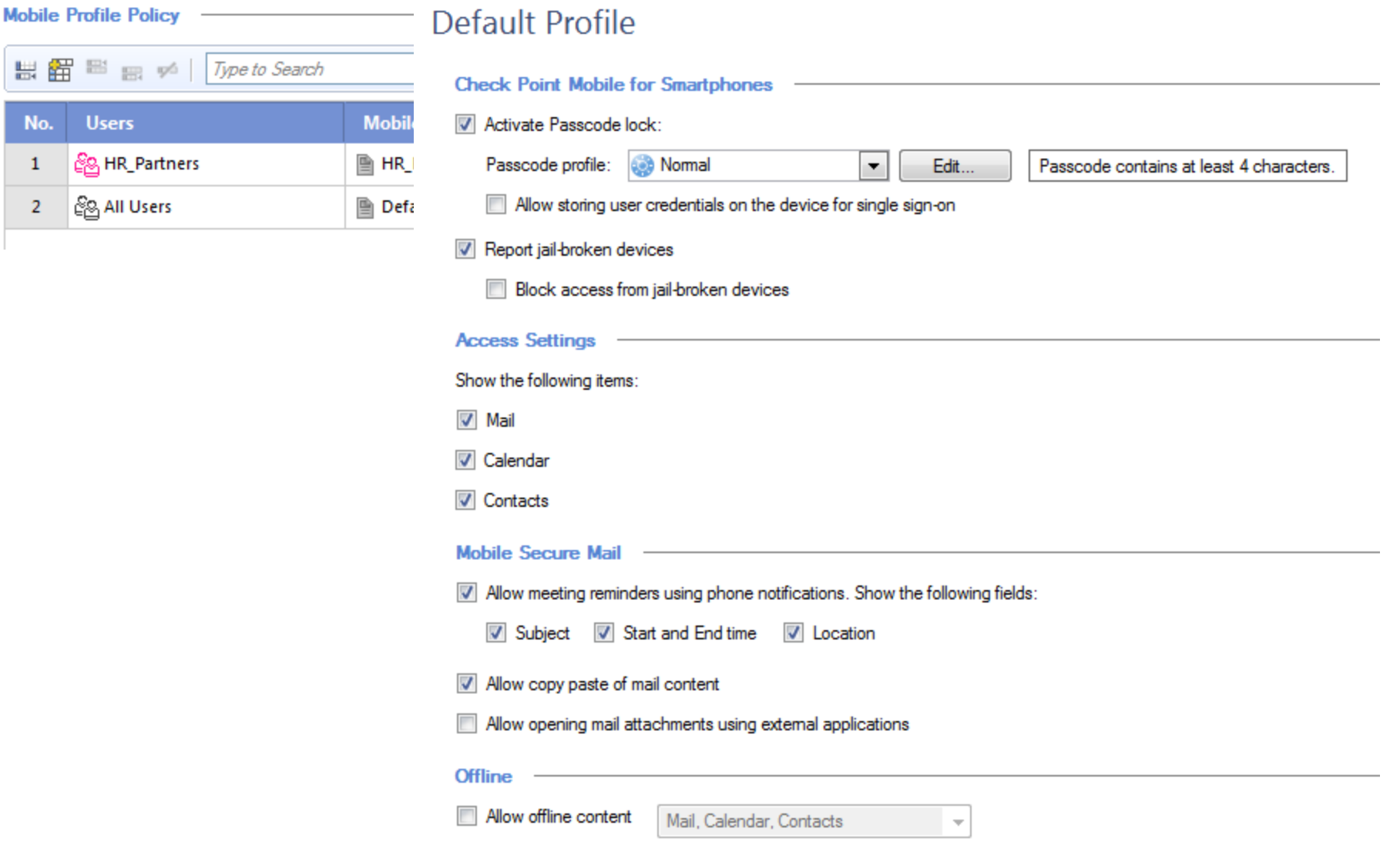
–[Restricted] ONLY for designated groups and individuals

Secure Mail Architecture



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

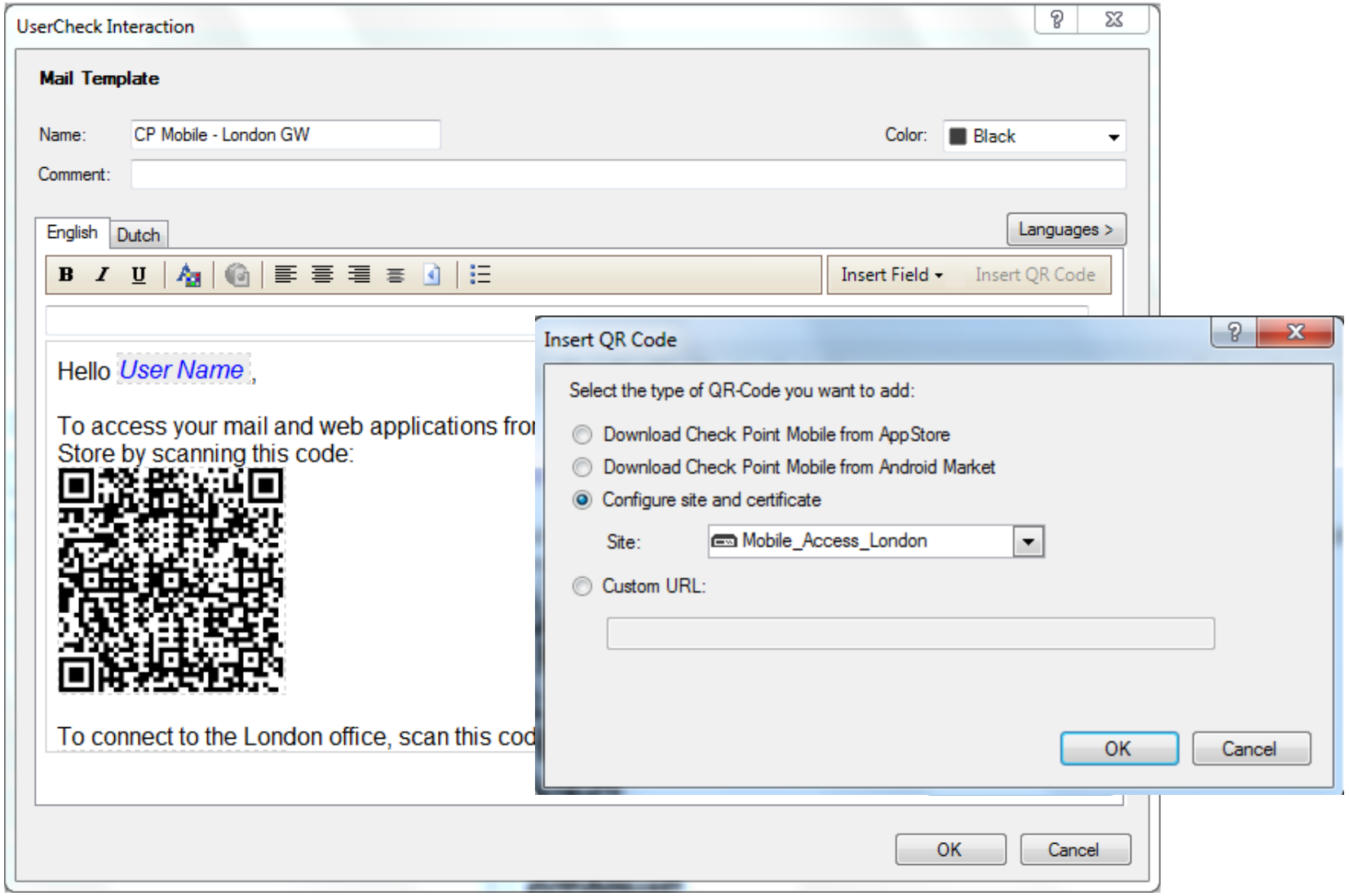
Mobile Profiles



Mobile Access Enhancements

- New SmartDashboard GUI for internal certificate management
  - Easier searching
  - Batch generation of keys for groups, OUs
- Mass distribution of clients to users with UserCheck Email templates
- Unified, rich remote access login logs
- Mobile Access Wizard allows easy connection to Exchange server

Email Distribution Templates



Batch deployment

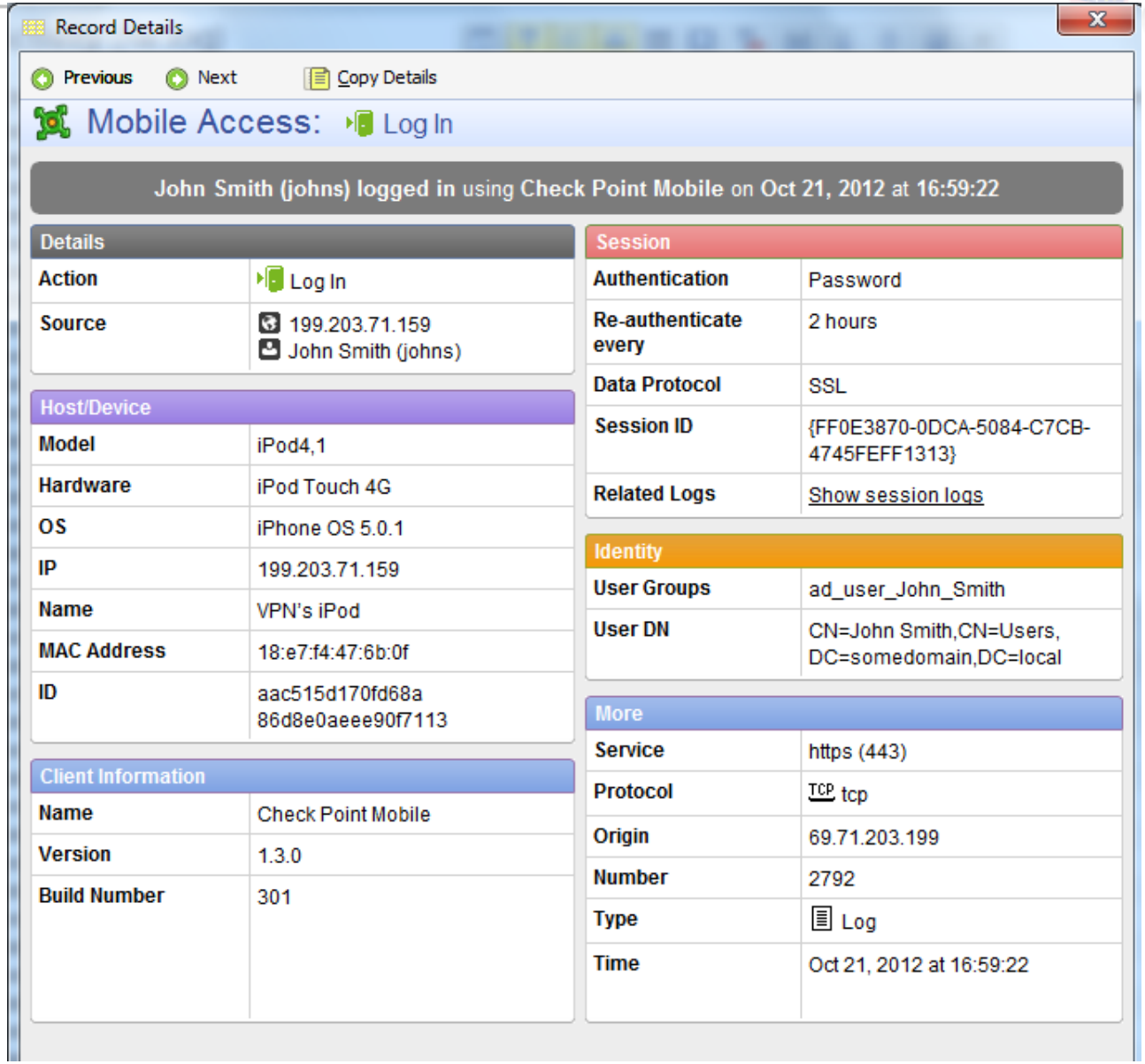
Hello John Smith,

To access your mail and web applications from your iPhone or iPad, install 'Mobile' from the App Store by scanning this code:

To connect to the London office, scan this code:

For questions or assistance please contact IT helpdesk at +972-3-467890.

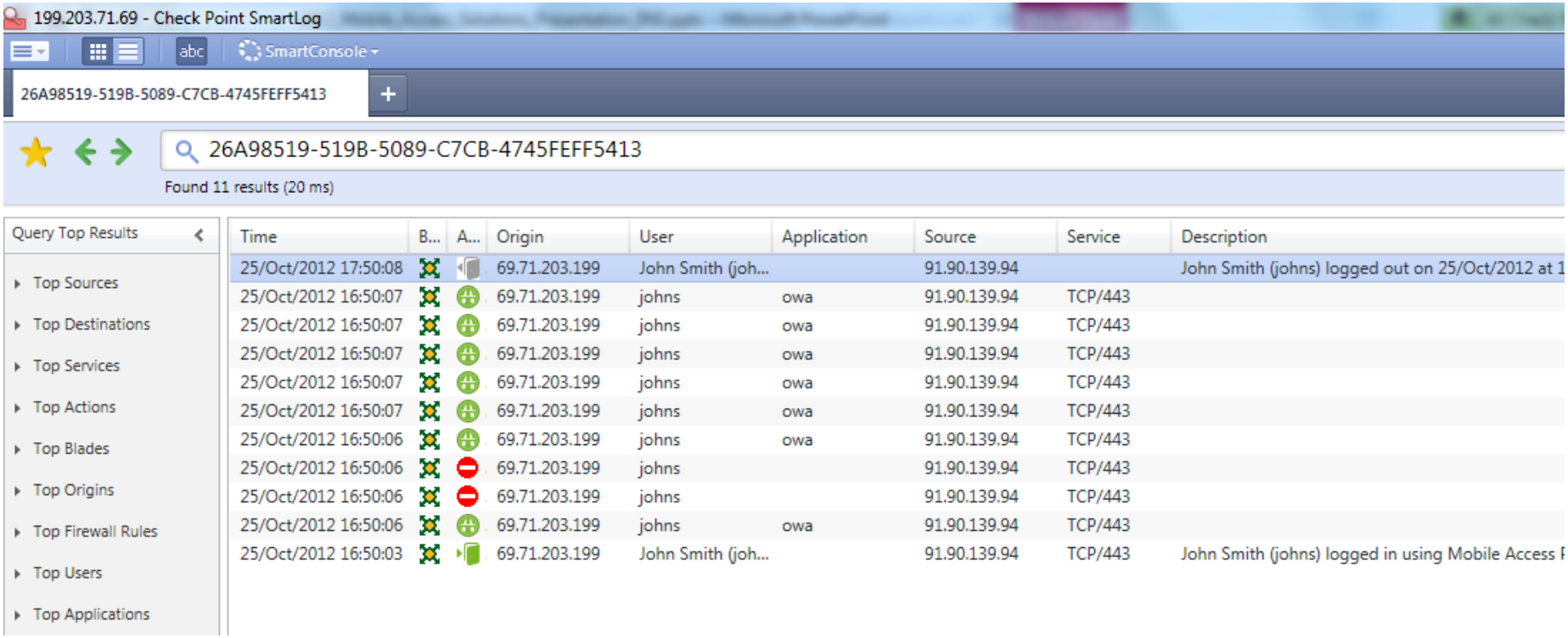
Unified, rich remote access login logs



–[Restricted] ONLY for designated groups and individuals

Unified, rich remote access login logs

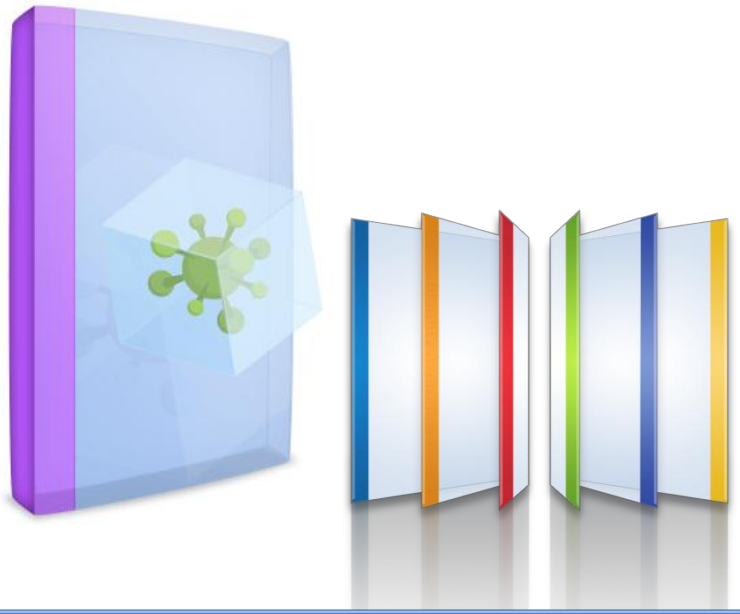
Follow session trail:



Zero-day Threat Discovery

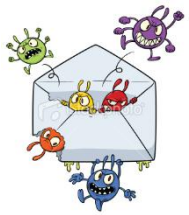
Check Point SOFTWARE TECHNOLOGIES LTD.

Introducing Check Point Threat Emulation Software Blade



Instant protection against unknown threats

Threat Emulation – Malicious Attachment Example



Email with malicious attachment

Intercepted by Threat Emulation Software Blade

Extracting attachments

Emulation

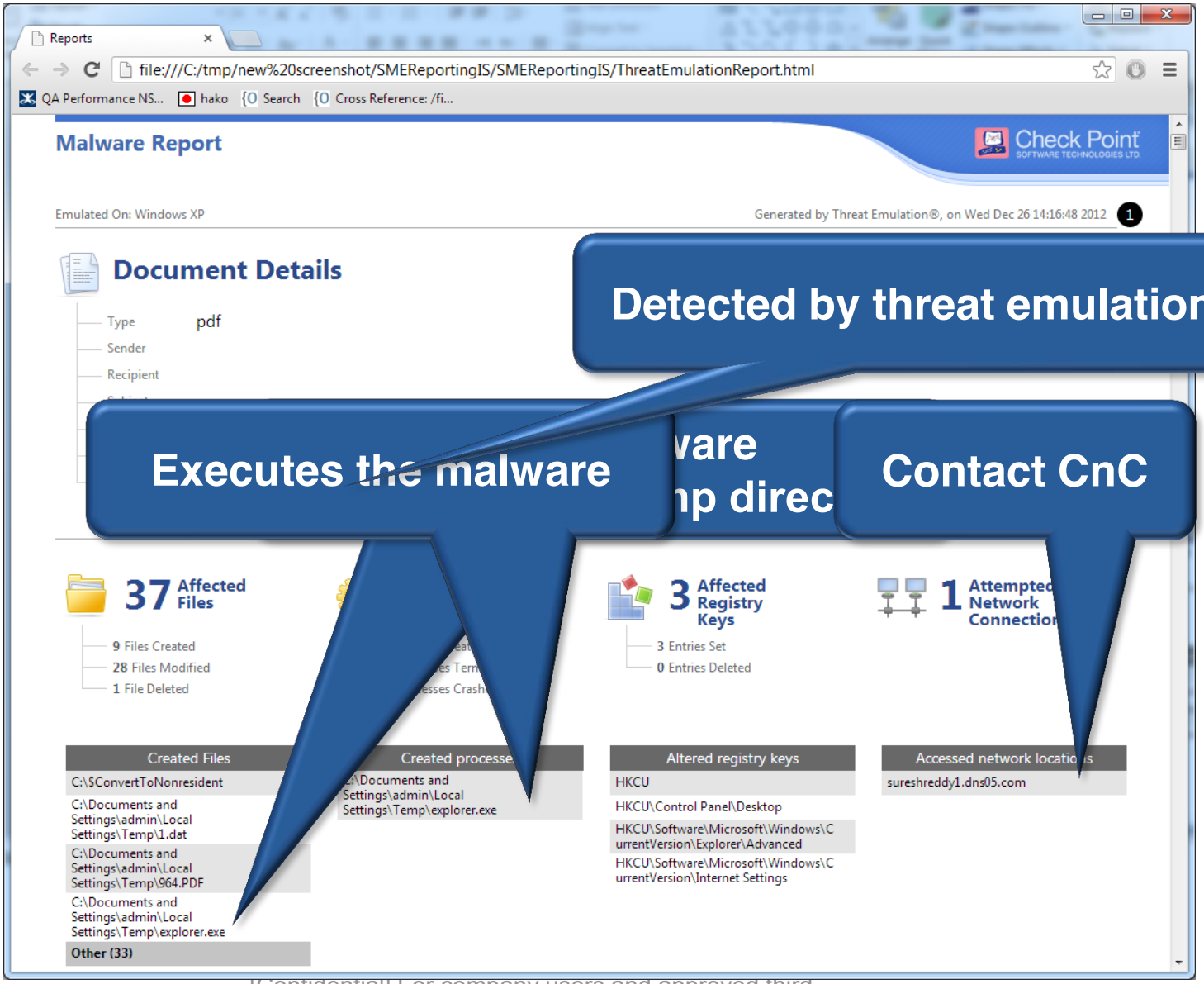
Clean

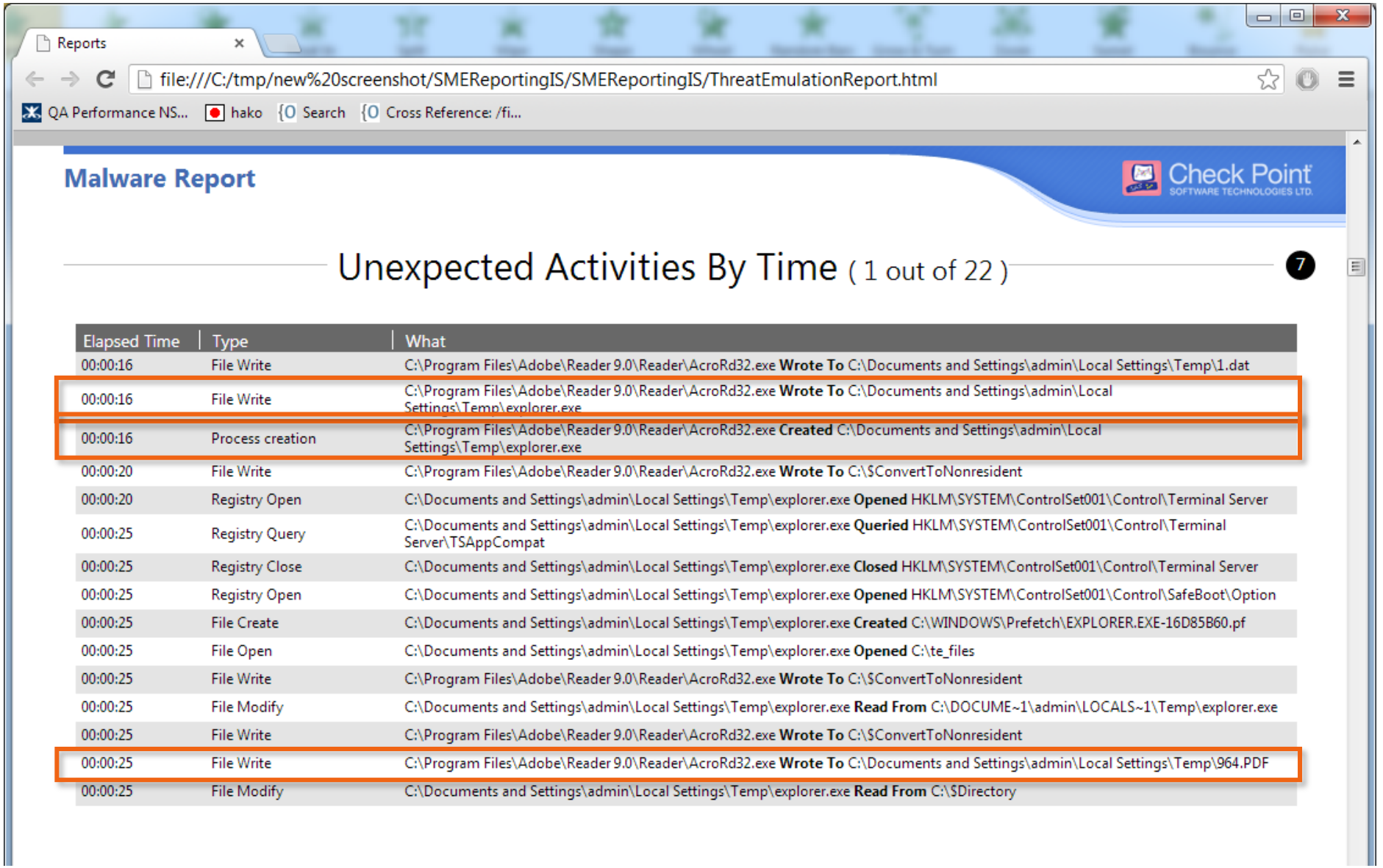
Malware detected

We know what should happen when opening a legitimate document ('White List')

Any document which causes abnormal behavior can be safely consider as malicious

Real Detection of the Syrian Attack, Fed to the Threat Emulation





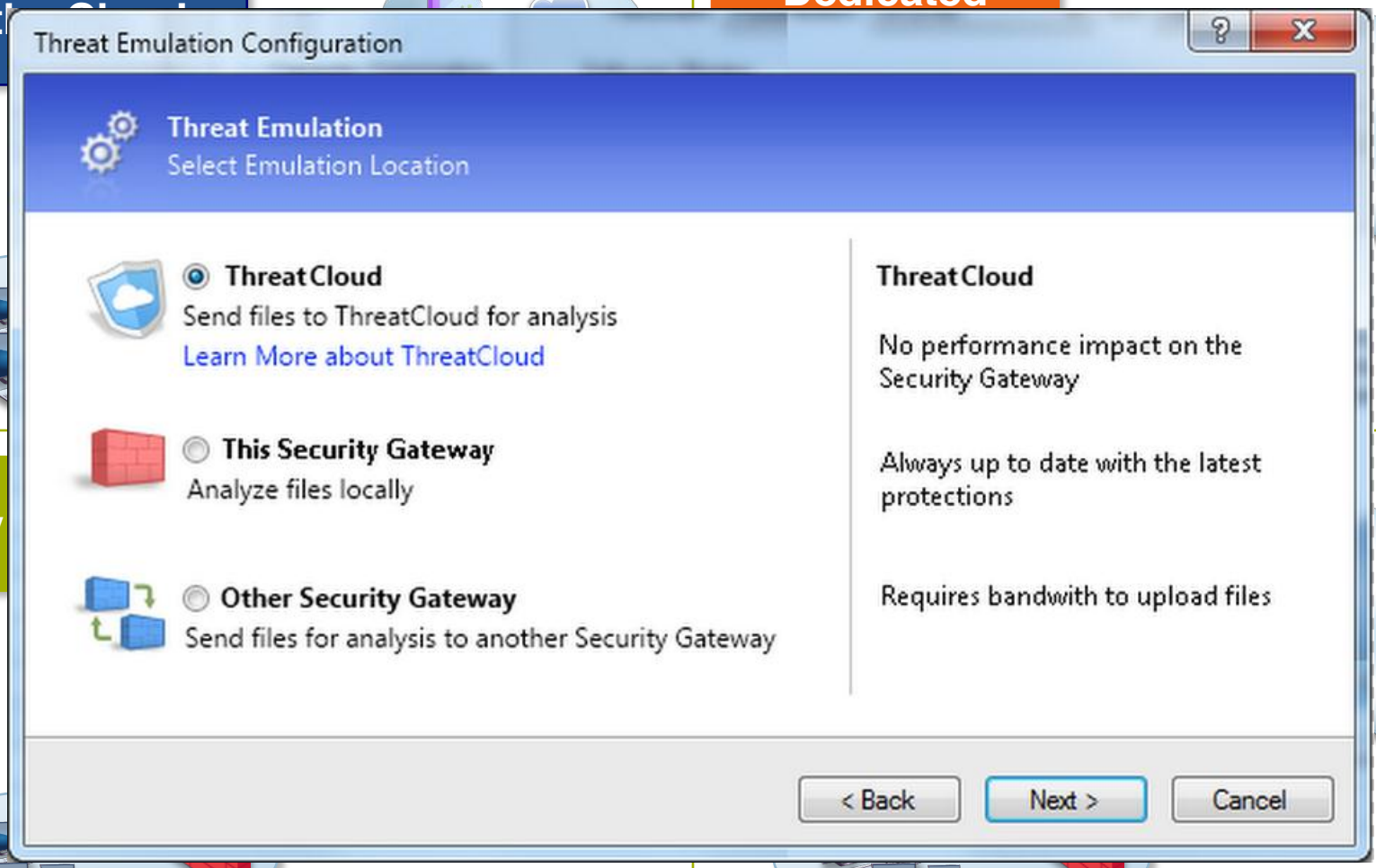
Elapsed Time	Type	What
00:00:16	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe **Wrote To** C:\Documents and Settings\admin\Local Settings\Temp\1.dat
00:00:16	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe **Wrote To** C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe
00:00:16	Process creation	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe **Created** C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe
00:00:20	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe **Wrote To** C:\$ConvertToNonresident
00:00:20	Registry Open	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Opened** HKLM\SYSTEM\ControlSet001\Control\Terminal Server
00:00:25	Registry Query	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSAppCompat
00:00:25	Registry Close	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Terminal Server
00:00:25	Registry Open	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Opened** HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Option
00:00:25	File Create	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Created** C:\WINDOWS\Prefetch\EXPLORER.EXE-16D85B60.pf
00:00:25	File Open	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Opened** C:\te_files
00:00:25	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe **Wrote To** C:\$ConvertToNonresident
00:00:25	File Modify	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Read From** C:\DOCUME~1\admin\LOCALS~1\Temp\explorer.exe
00:00:25	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe **Wrote To** C:\$ConvertToNonresident
00:00:25	File Write	C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe **Wrote To** C:\Documents and Settings\admin\Local Settings\Temp\964.PDF
00:00:25	File Modify	C:\Documents and Settings\admin\Local Settings\Temp\explorer.exe **Read From** C:\$Directory

Flexible Deployment Options

Check Point SOFTWARE TECHNOLOGIES LTD.

In t

Dedicated

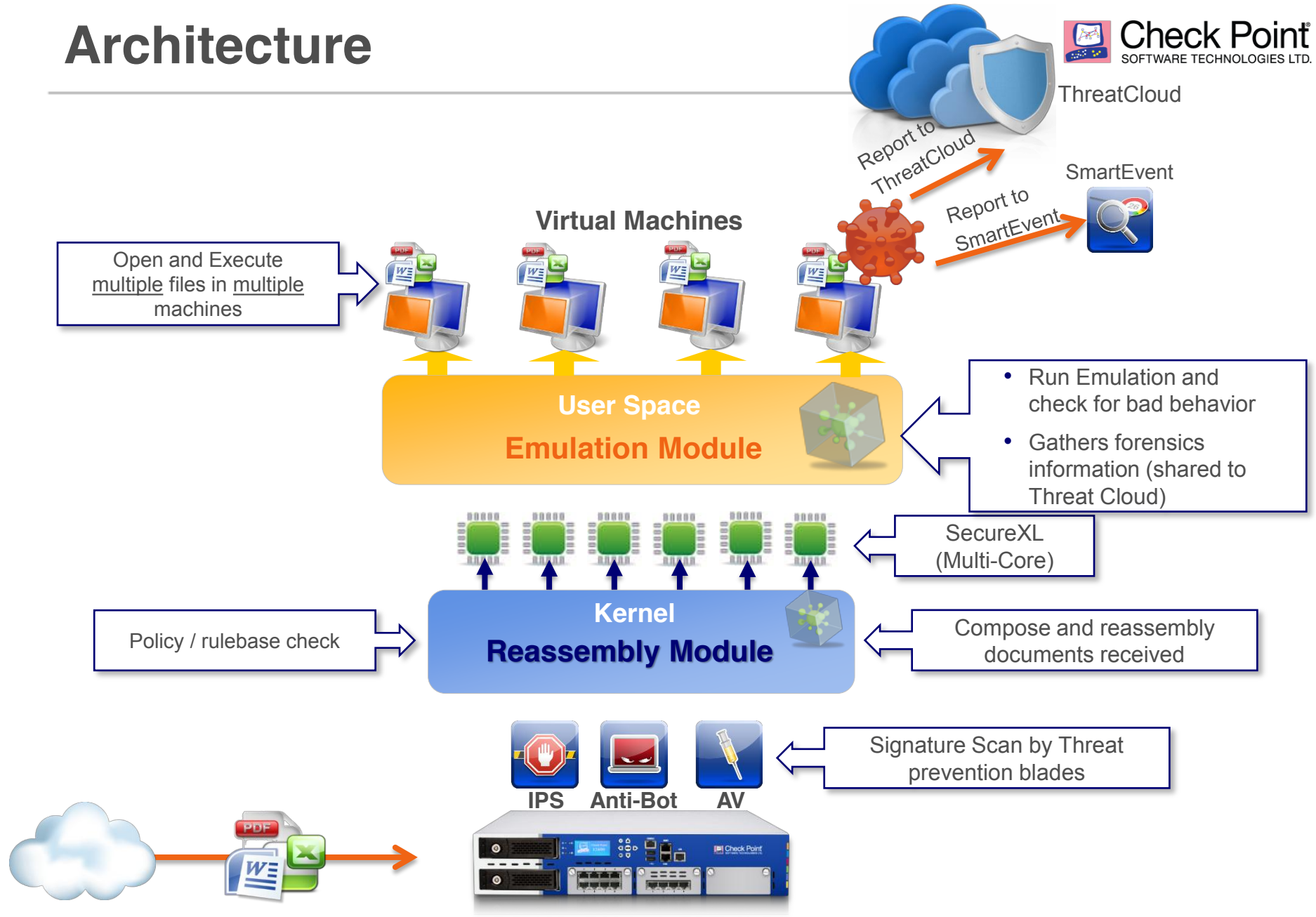


Fully

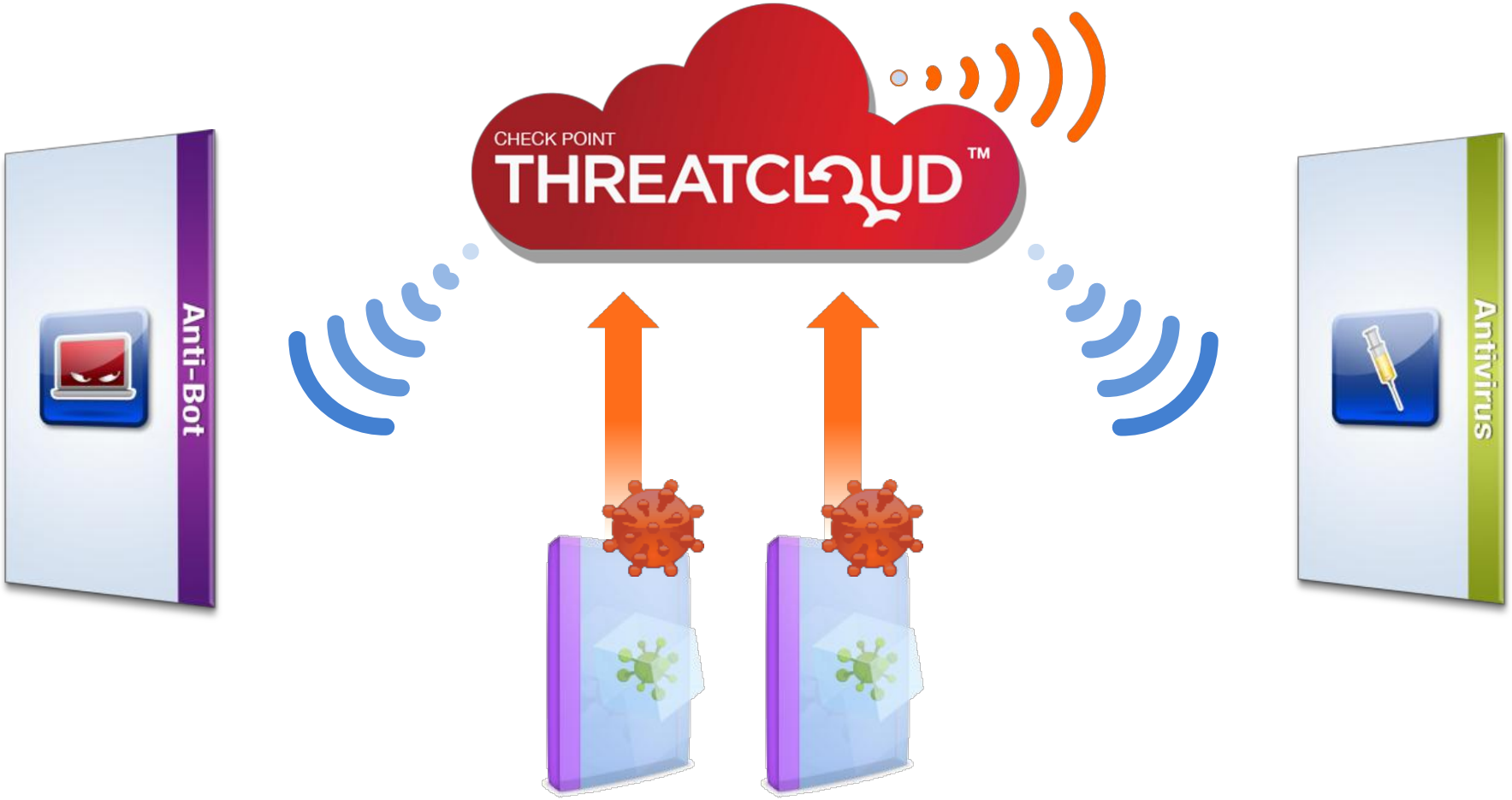
Enterprise

Enterprise

Architecture



Boosting Collaboration Power of ThreatCloud



Dynamic Signatures Updated by Network of Threat Emulation Servers in Threat Cloud

Document Security

Protect data at rest, in motion, in use and in the cloud by classifying and encrypting documents

What Is Document Security?

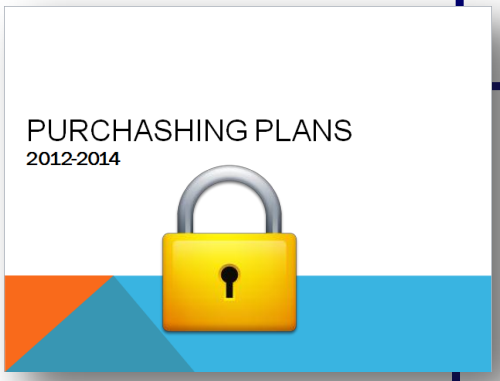
Check Point SOFTWARE TECHNOLOGIES LTD.

A new, simple way to protect and share business documents

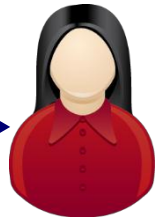
- **Encrypt**
- **Set Access Rights**
- **Classify**

Document Security Example

Tammy,
Purchasing Manager



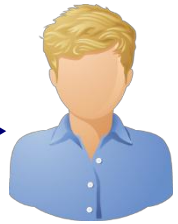
File Share



Dana,
Co-worker

Full Access

Web Mail



John,
Business Partner

Read Only

Cloud Based
Web App

Suzan,
Not in this project

No Access

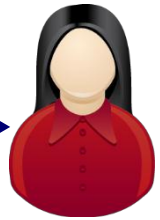
Document Security Example

Check Point SOFTWARE TECHNOLOGIES LTD.

Tammy,

✓ **Control who can internally access data**

File Share



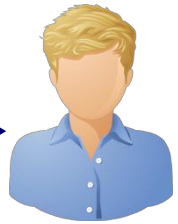
Dana,
Co-worker

Full Access

✓ **Assure proper document usage e.g. prevent forwarding to others**

2012-2014

Web Mail



John,
Business Partner

Read Only

✓ **Protect data stored on untrusted services and devices**

Cloud Based
Web App

Suzan,
Not in this project

No Access

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point's New Compliance Blade

Mati Ram
Head of GRC Business
January 2013

Compliance Blade – Main Features

Check Point SOFTWARE TECHNOLOGIES LTD.

New Management Blade

Fully integrated into Check Point's architecture

Real Time Compliance Monitoring

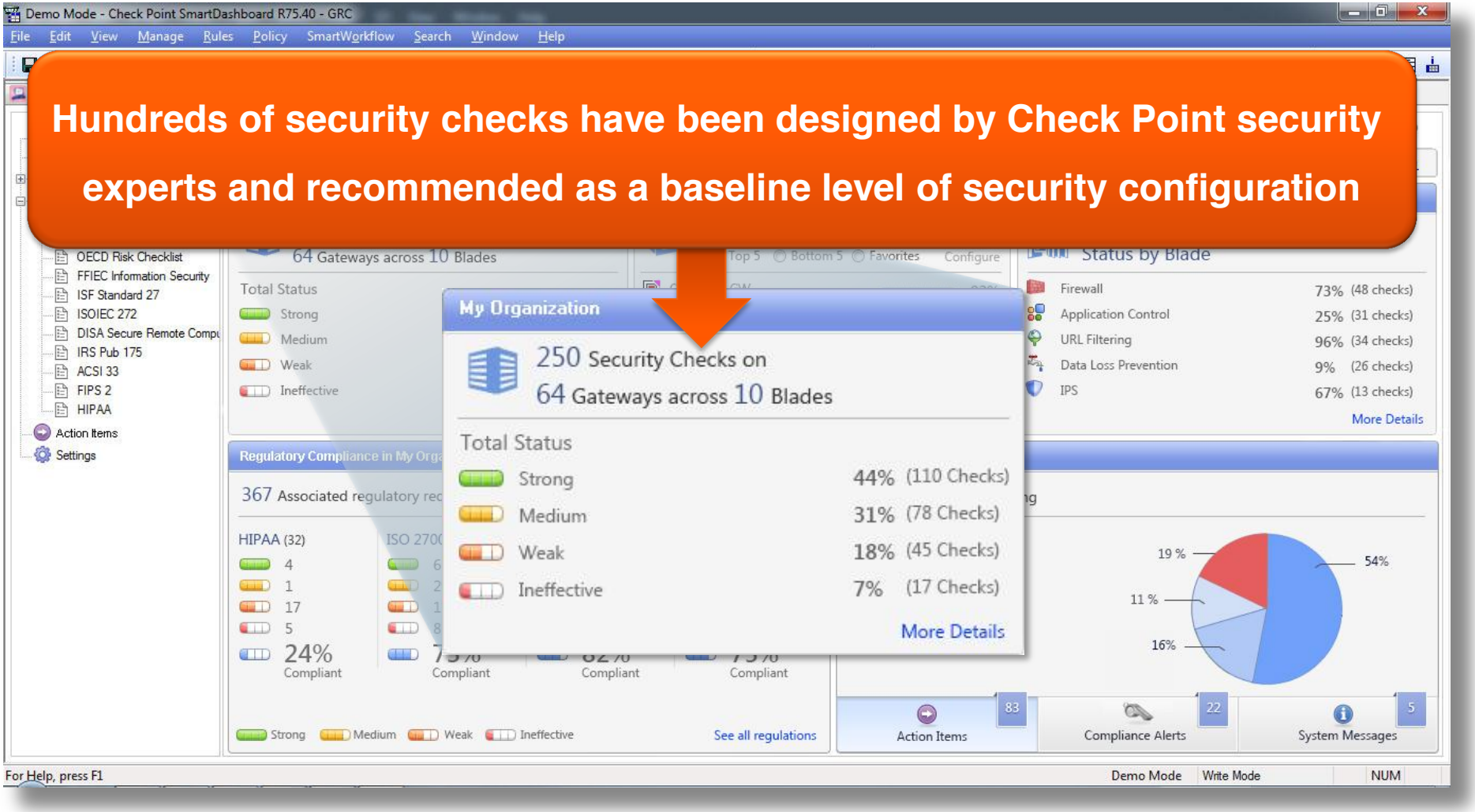
More than 250 Security Checks across Check Point's Blades

Continuous Policy Optimization Process

Provides practical guidance on how to improve Security Policy

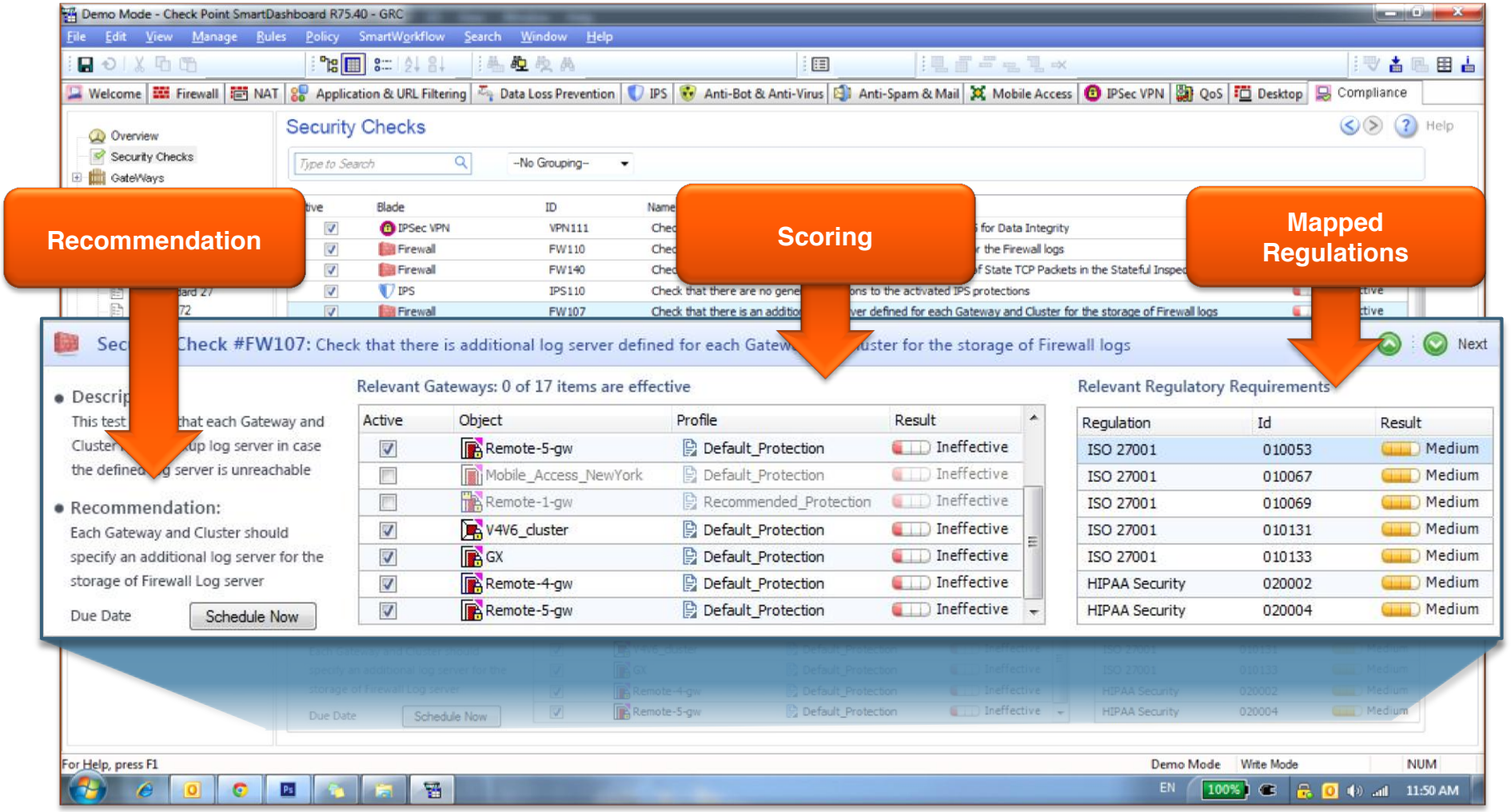
Overview Screen

Check Point SOFTWARE TECHNOLOGIES LTD.



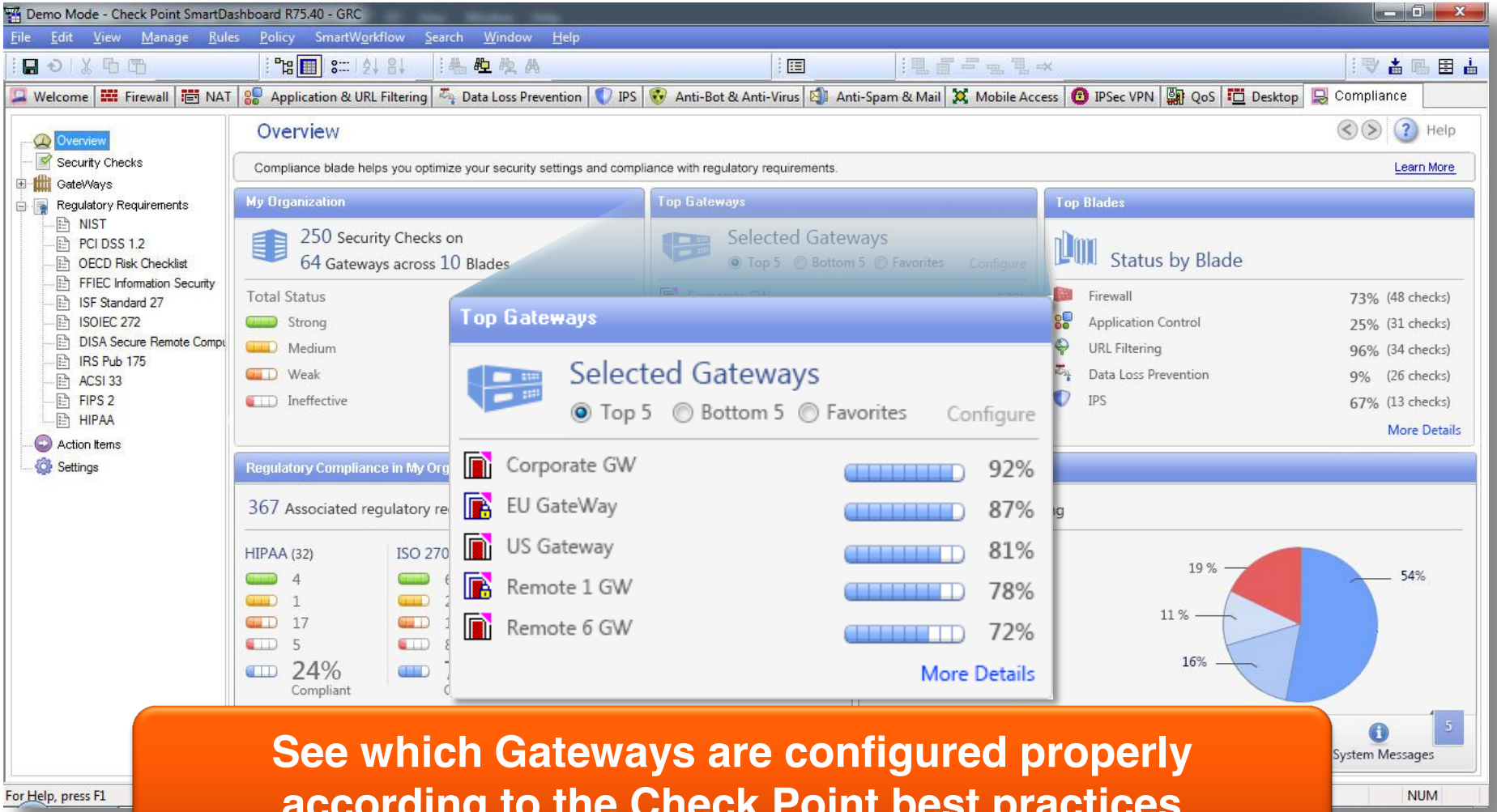
View Plan Act

Security Check Detailed Information



View Plan Act

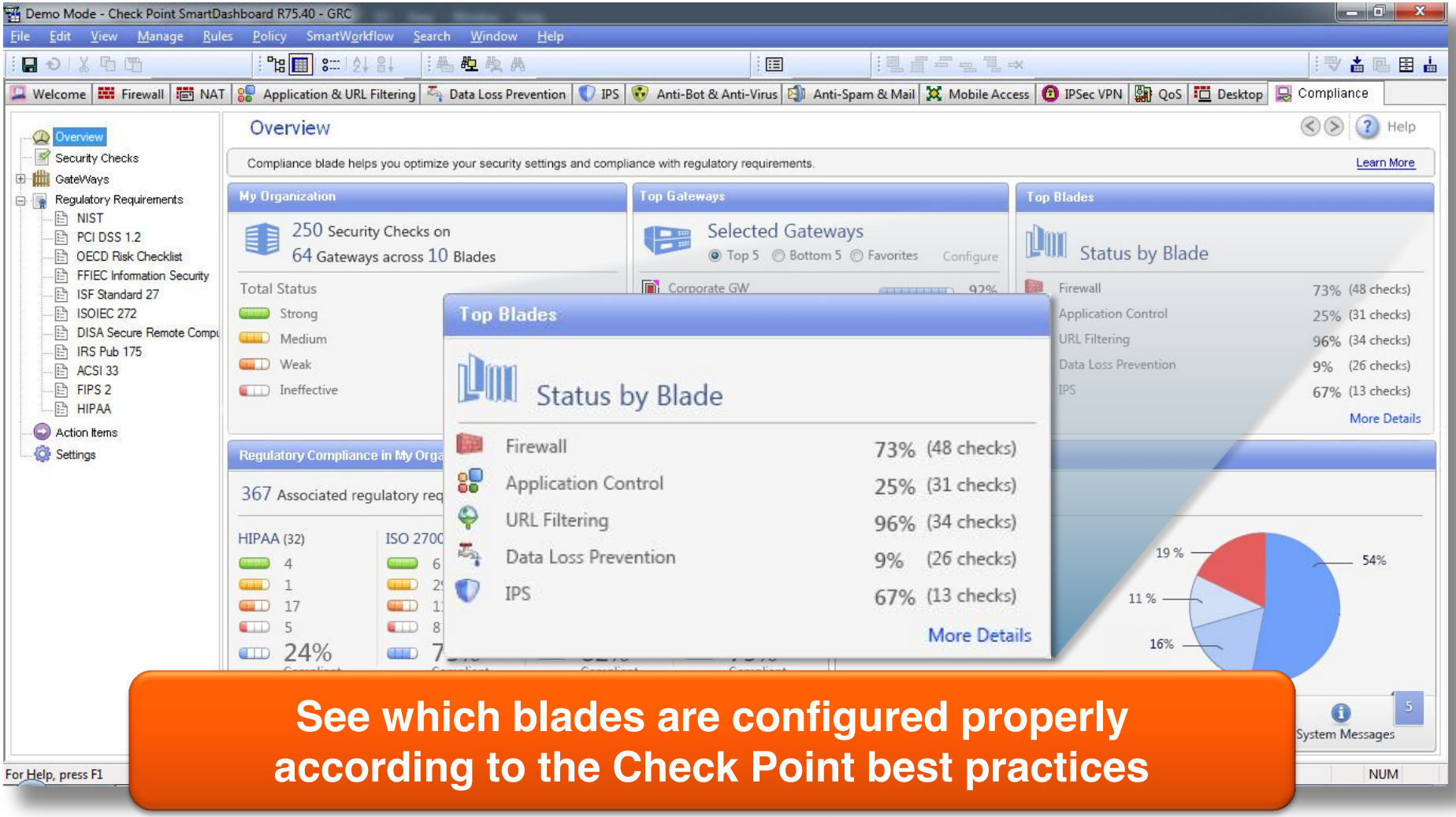
Status By Gateway



See which Gateways are configured properly according to the Check Point best practices

View Plan Act

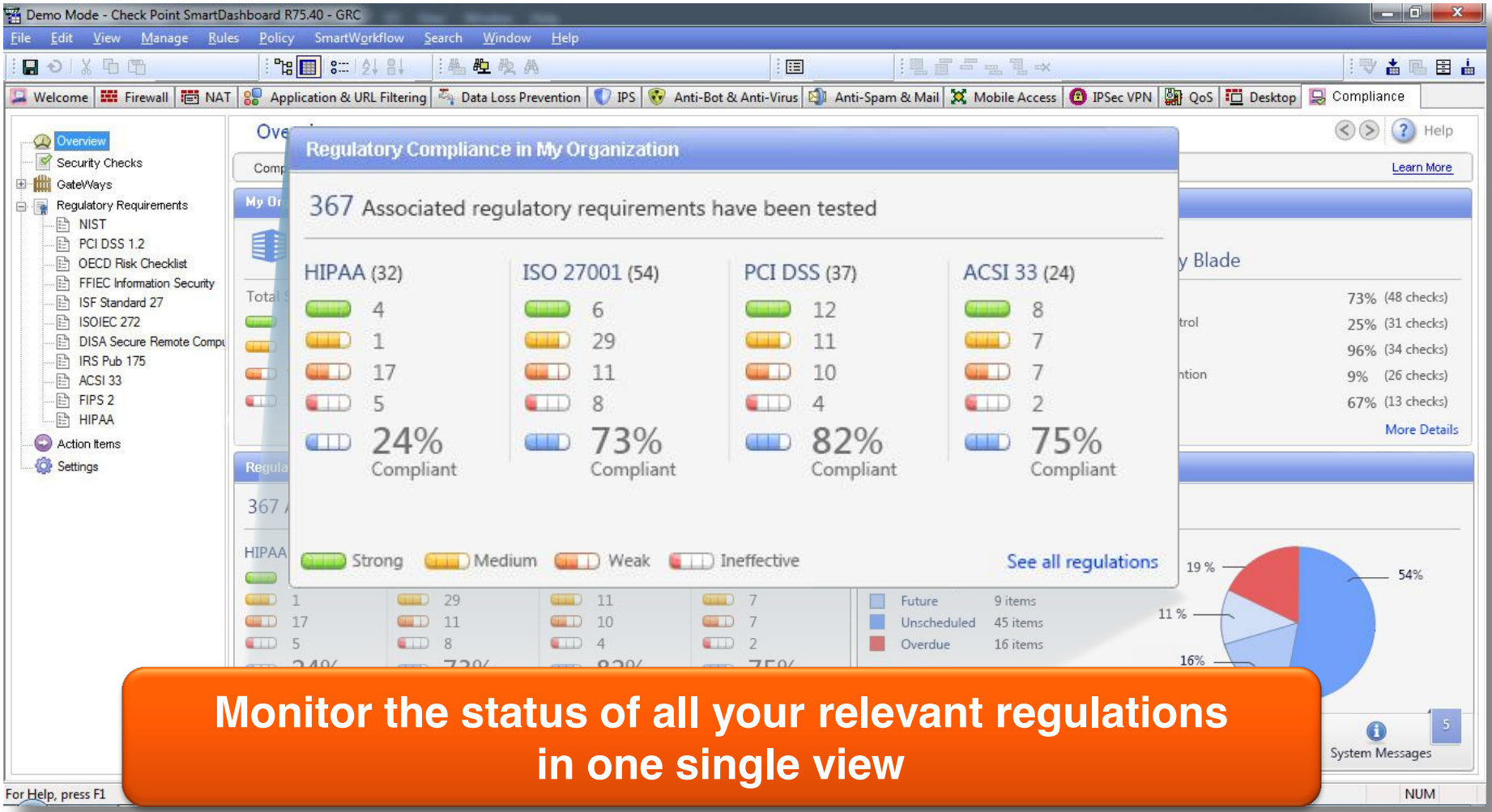
Status By Blade



See which blades are configured properly according to the Check Point best practices

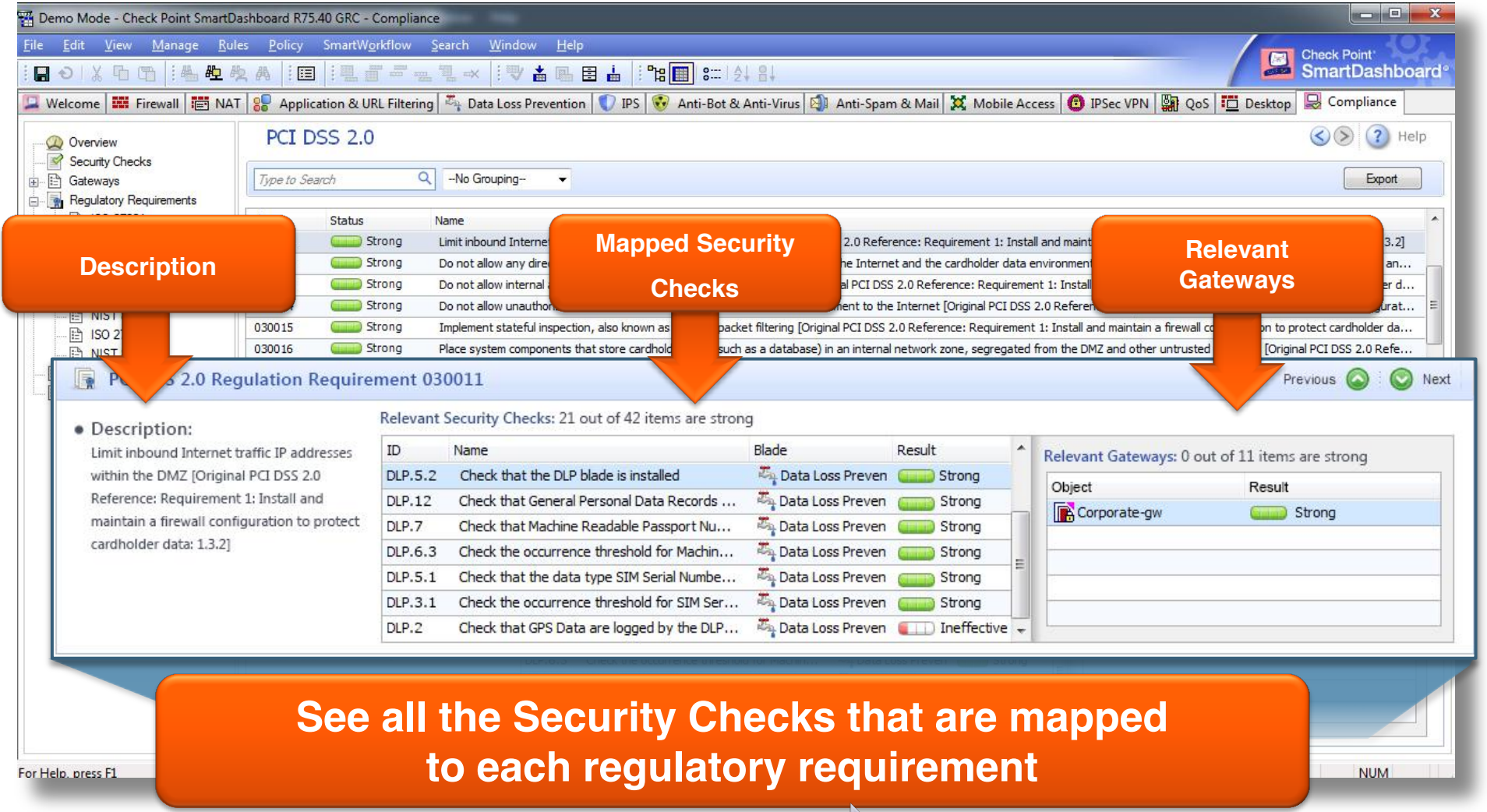
View Plan Act

Status By Regulation

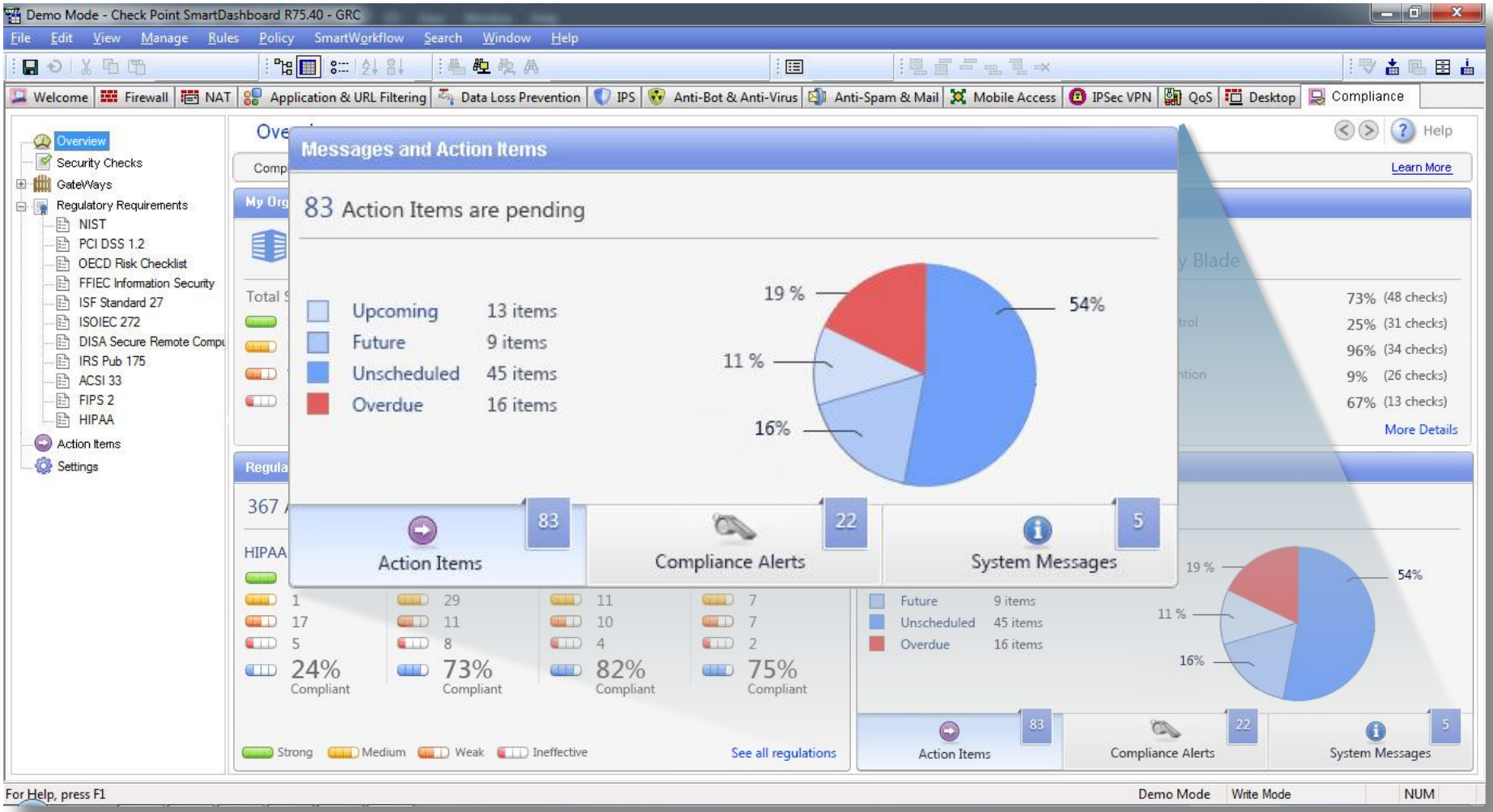


View Plan Act

Status By Regulation



Action Items



View Plan Act

Security Check Sample

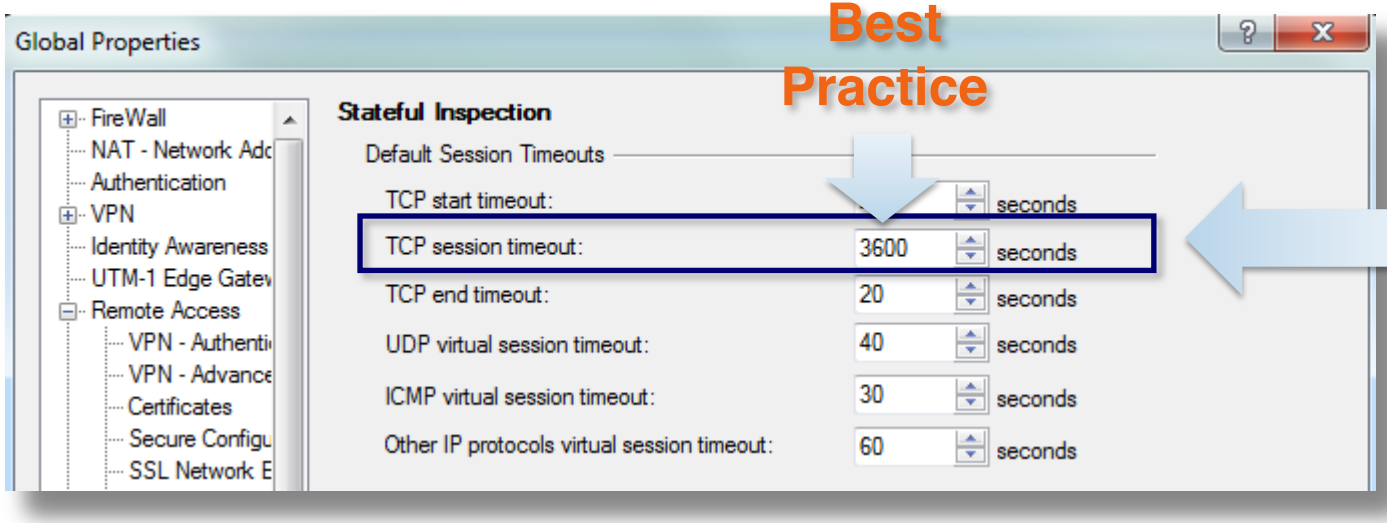
Check Point SOFTWARE TECHNOLOGIES LTD.

Ensure that Firewalls are configured to drop idle connections

Security Control

Security Check 1 out of 8

Best Practice



Security Check

Compliance Alerts

Check Point SOFTWARE TECHNOLOGIES LTD.

Real Time Compliance Monitoring

On-screen alerts when configuration changes impact Compliance

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

Questions?