Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

stallion

Introducing Check Point 3D Security

Jani Ekman

Security Engineer

Users Have Different Needs

Boundaries are disappearing

New environment, new challenges

To secure this new environment,
IT needs to do more

More Security….

…with Less:

Less **Resources**

Less **Time**

Check Point

R75

What’s New in R75

New Blades

- Identity Awareness
- Application Control
- Mobile Access Software Blade

Enhanced Functionality

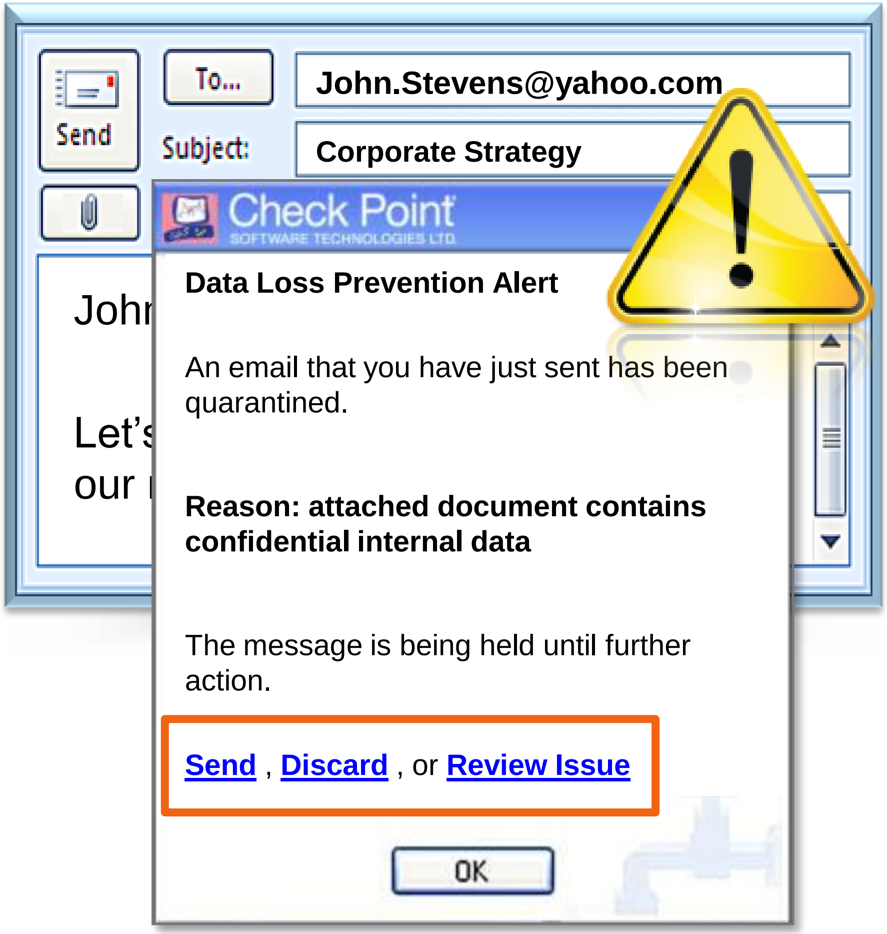
- Integrated DLP Software Blade
- Endpoint Security VPN R75 support
- IPS Signatures - NSS Report
- Multi-Domain Security Management
- Support for SG80

Additional info

- Introduced in Q4/2010

Introducing Check Point Data Loss Prevention

Check Point Combines Technology and Processes to Make DLP Work



John.Stevens@yahoo.com

Corporate Strategy

John

Let's

our

Data Loss Prevention Alert

An email that you have just sent has been quarantined.

Reason: attached document contains confidential internal data

The message is being held until further action.

Send , Discard , or Review Issue

Prevent

Move from detection to prevention

Educate

Users on corporate data policies

Enforce

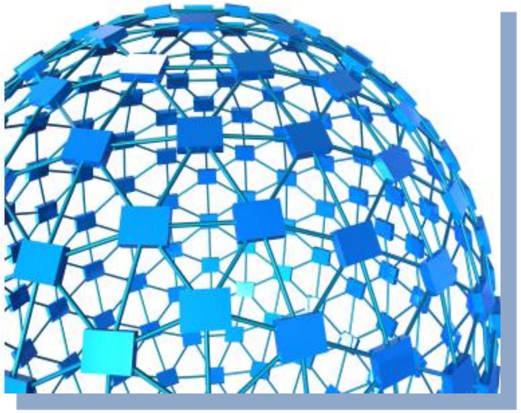
Data loss business processes

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

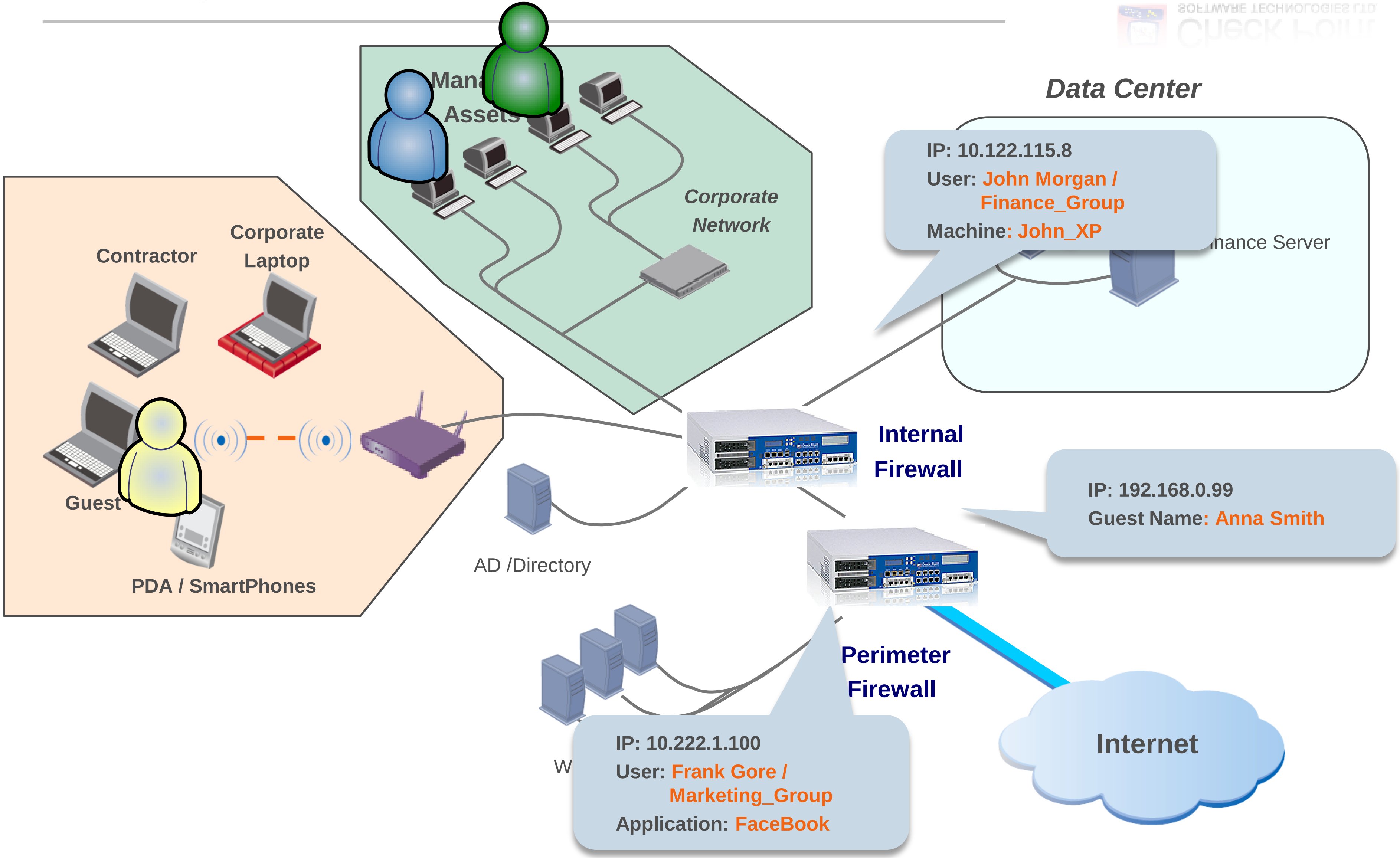
Identity Awareness Software blade

Identity Awareness Software Blade

Granular Security Policy per User, Machine and Location



Example of Identity Awareness



IP: 10.122.115.8
User: John Morgan / Finance_Group
Machine: John_XP

IP: 192.168.0.99
Guest Name: Anna Smith

IP: 10.222.1.100
User: Frank Gore / Marketing_Group
Application: FaceBook

Identity Awareness At-A-Glance

Security Gateway ability to identify users and machines passing through the gateway

Available for multiple Software Blades

- Firewall (R75)
- Application Control (R75)
- *DLP, URLF, IPS (in the future*)

Scalable for up to 25,000 concurrent users on Power-1 series

IA Software Blade

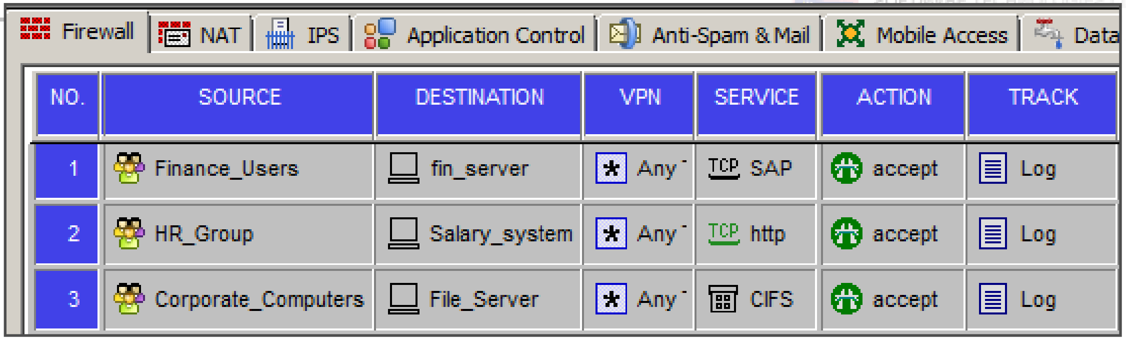
User and Machine Awareness

Across All Software Blades

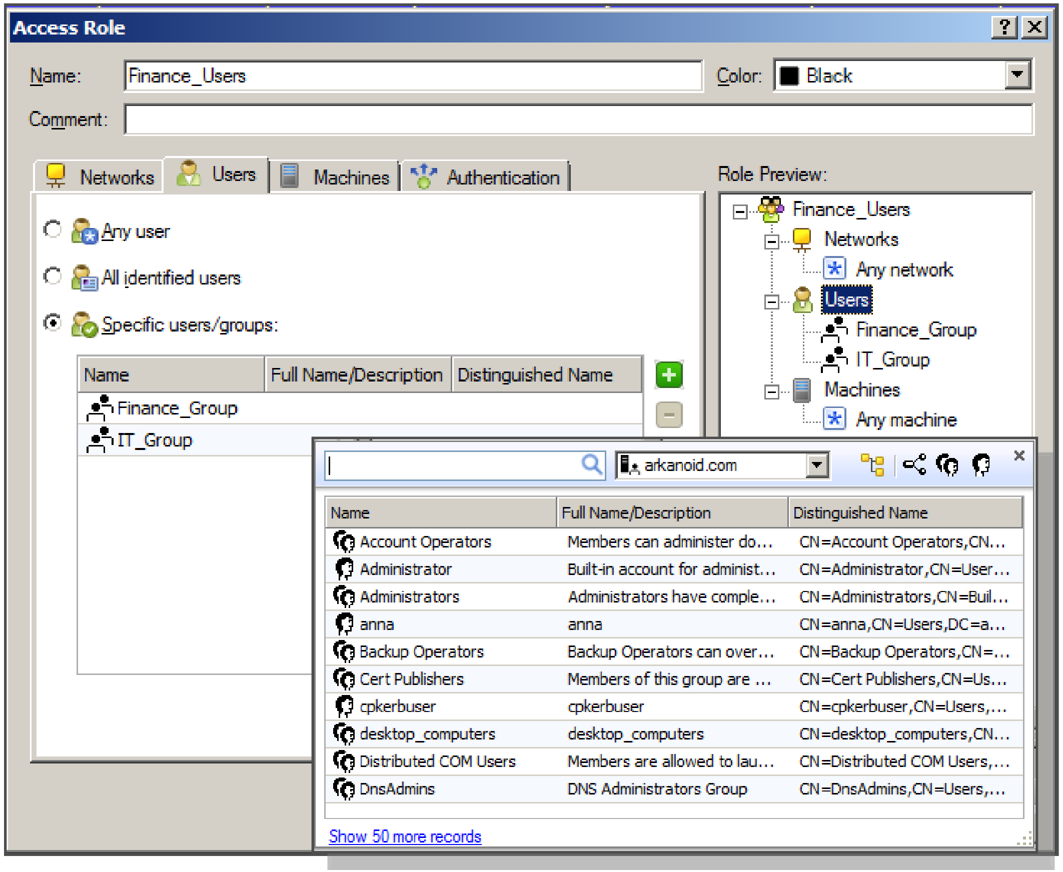
Security Gateways

Access Roles

- Easy to setup
- Users and Groups could be fetched from the AD directly
- Across all blades i.e. Firewall, Application Control



NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1	Finance_Users	fin_server	Any	TCP SAP	accept	Log
2	HR_Group	Salary_system	Any	TCP http	accept	Log
3	Corporate_Computers	File_Server	Any	CIFS	accept	Log



Name: Finance_Users
Color: Black
Comment:

○ Any user
○ All identified users
● Specific users/groups:

Name	Full Name/Description	Distinguished Name
Finance_Group		
IT_Group		

Name	Full Name/Description	Distinguished Name
Account Operators	Members can administer do…	CN=Account Operators,CN…
Administrator	Built-in account for administ…	CN=Administrator,CN=User…
Administrators	Administrators have comple…	CN=Administrators,CN=Buil…
anna	anna	CN=anna,CN=Users,DC=a…
Backup Operators	Backup Operators can over…	CN=Backup Operators,CN=…
Cert Publishers	Members of this group are …	CN=Cert Publishers,CN=Us…
cpkerbuser	cpkerbuser	CN=cpkerbuser,CN=Users,…
desktop_computers	desktop_computers	CN=desktop_computers,CN…
Distributed COM Users	Members are allowed to lau…	CN=Distributed COM Users,…
DnsAdmins	DNS Administrators Group	CN=DnsAdmins,CN=Users,…

Show 50 more records

Identity Sources

Clientless

Captive Portal

Identity Agent

1

2

3

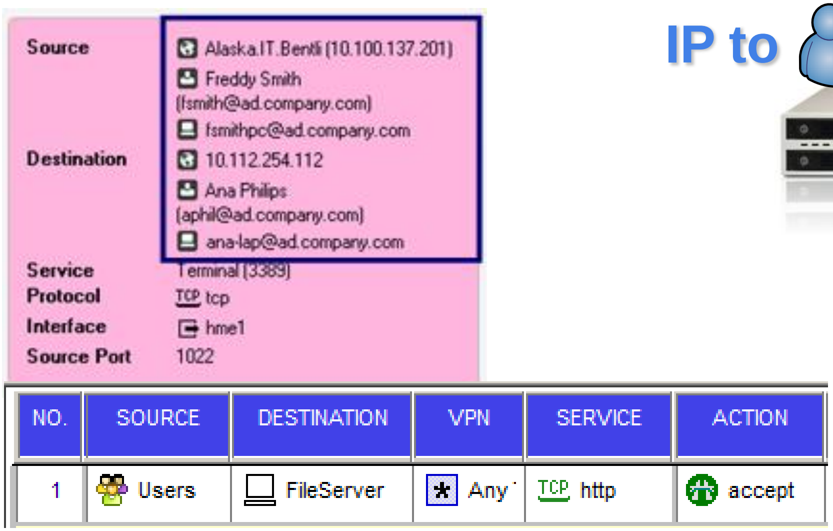
Flexible options to obtain Users' Identity

Identity Sources

Clientless

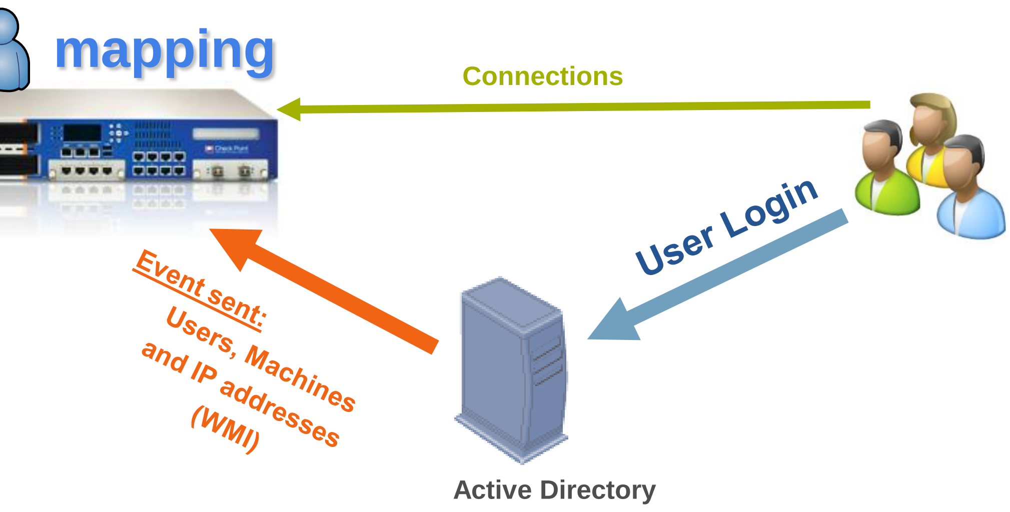
Captive Portal

Identity Agent



Source	Alaska.IT.Bentli (10.100.137.201) Freddy Smith (fsmith@ad.company.com) fsmithpc@ad.company.com
Destination	10.112.254.112 Ana Philips (aphil@ad.company.com) ana-lap@ad.company.com
Service	Terminal (3389)
Protocol	TCP tcp
Interface	hme1
Source Port	1022

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION
1	Users	FileServer	Any	TCP http	accept



Simple and Fast Deployment

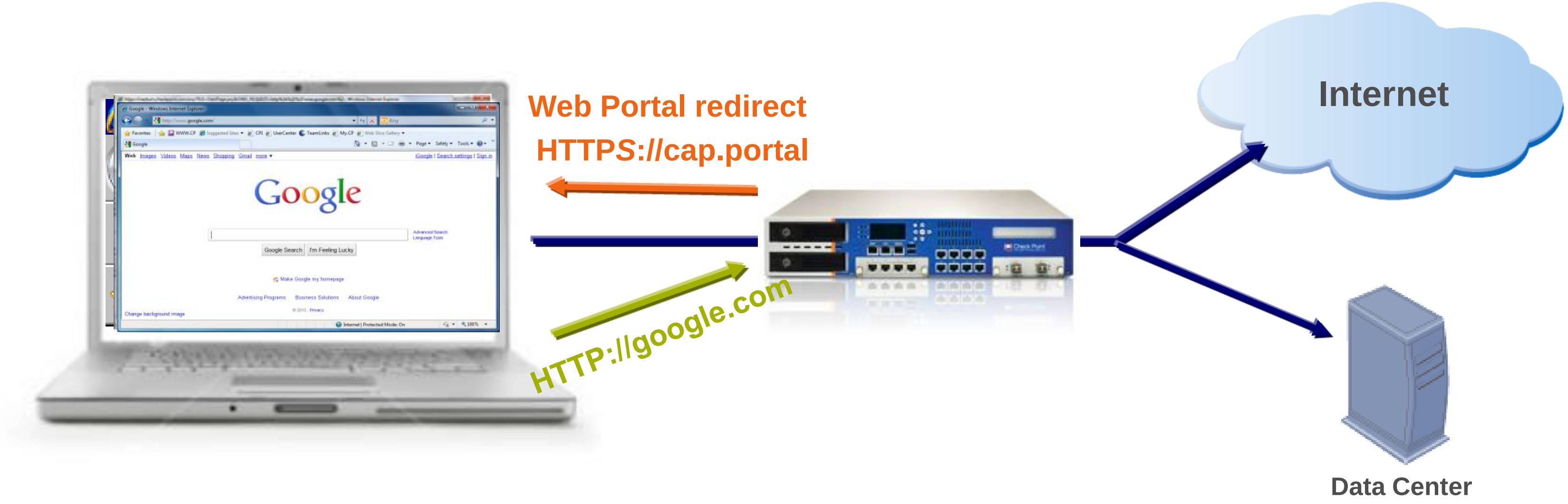
No agent required on endpoint and Active Directory

Identity Sources

Clientless

Captive Portal

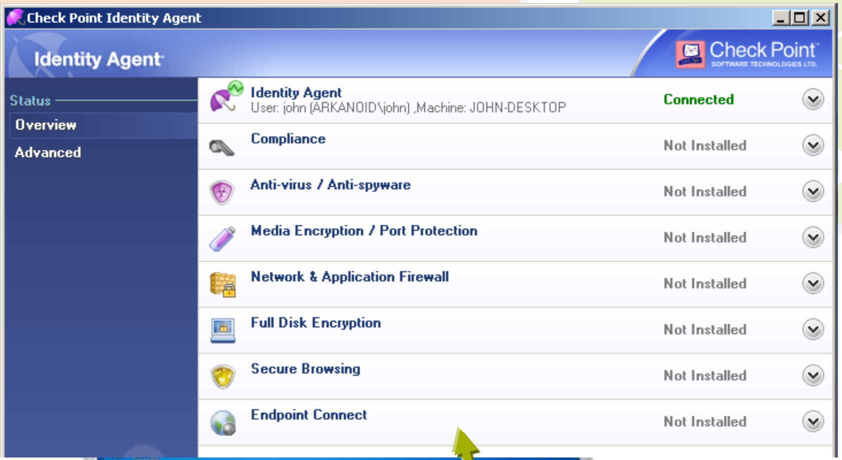
Identity Agent



Restrict Guest access

Provide secure access for non-domain endpoints

Identity Sources



Check Point Identity Agent

Identity Agent

Status

Overview

Advanced

Identity Agent User: john (ARKANOID\john) ,Machine: JOHN-DESKTOP	Connected
Compliance	Not Installed
Anti-virus / Anti-spyware	Not Installed
Media Encryption / Port Protection	Not Installed
Network & Application Firewall	Not Installed
Full Disk Encryption	Not Installed
Secure Browsing	Not Installed
Endpoint Connect	Not Installed

ptive

rtal

Identity Agent

User and Machine Authentication (SSO – Kerberos)

Stronger security with User and Machine Identity SSO and IP spoofing prevention

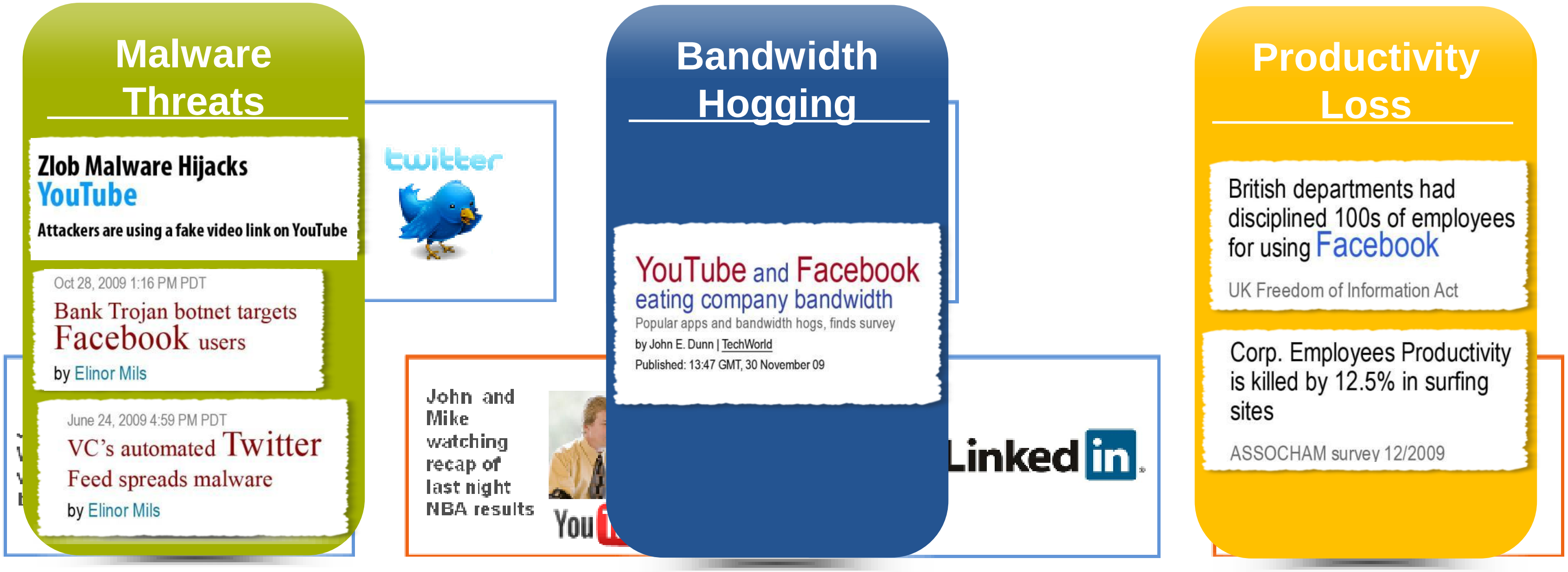
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Check Point Application Control Software Blade

The Need for Application Control

Internet Applications:
An integral part of today's business

IT staff lack strong visibility into this activity



Malware Threats

Zlob Malware Hijacks YouTube

Attackers are using a fake video link on YouTube

Oct 28, 2009 1:16 PM PDT

Bank Trojan botnet targets Facebook users

by Elinor Mils

June 24, 2009 4:59 PM PDT

VC's automated Twitter Feed spreads malware

by Elinor Mils

Bandwidth Hogging

YouTube and Facebook eating company bandwidth

Popular apps and bandwidth hogs, finds survey

by John E. Dunn | TechWorld

Published: 13:47 GMT, 30 November 09

Productivity Loss

British departments had disciplined 100s of employees for using Facebook

UK Freedom of Information Act

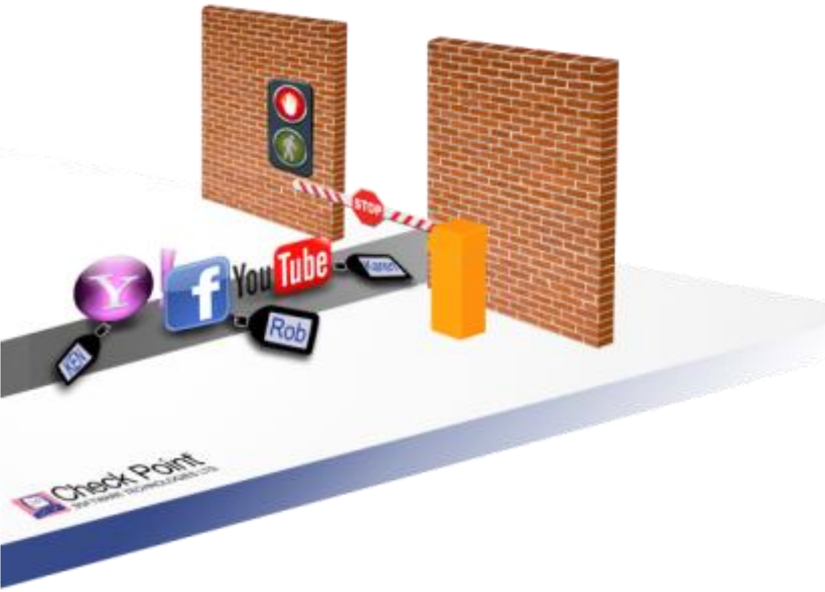
Corp. Employees Productivity is killed by 12.5% in surfing sites

ASSOCHAM survey 12/2009

John and Mike watching recap of last night NBA results

Introducing

Check Point Application Control Software Blade



Detect and control application usage

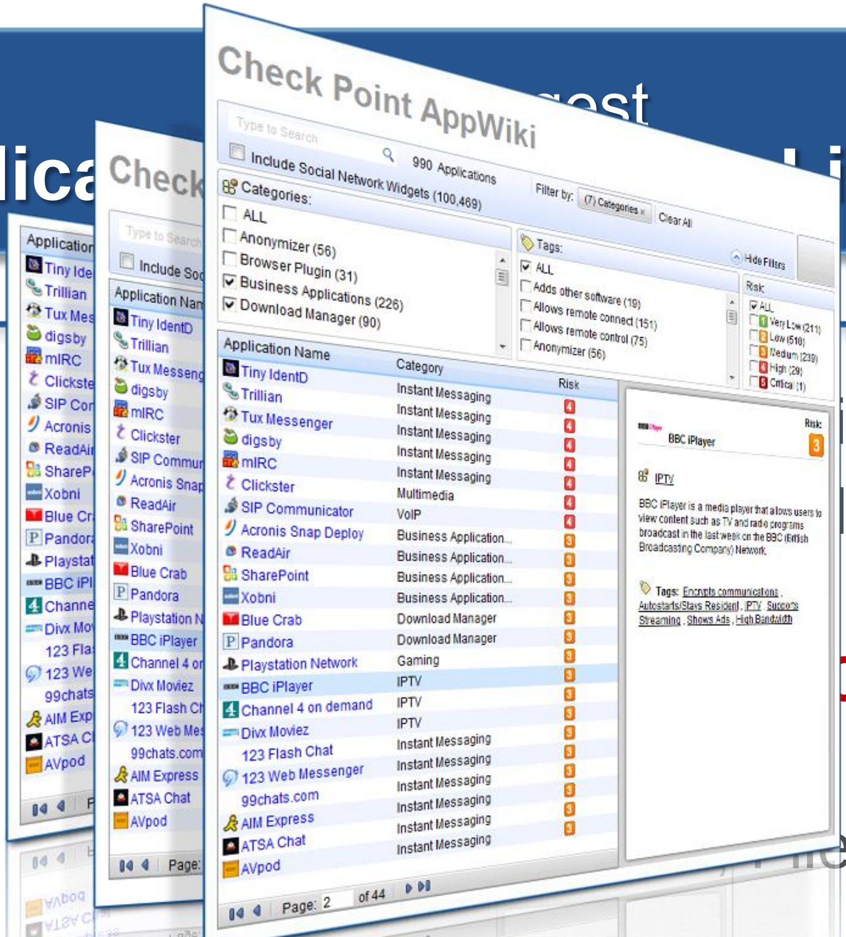
AppWiki—Industry's largest library with over 100,000 applications

Educate users on corporate policies

Available on EVERY gateway

Introducing Check Point AppWiki

Applica… gest … Library



Check Point AppWiki

Type to Search

☐ Include Social Network Widgets (100,469)

990 Applications

Filter by: (7) Categories × Clear All

Categories:
- ☐ ALL
- ☐ Anonymizer (56)
- ☐ Browser Plugin (31)
- ☑ Business Applications (226)
- ☑ Download Manager (90)

Tags:
- ☑ ALL
- ☐ Adds other software (19)
- ☐ Allows remote connect (151)
- ☐ Allows remote control (75)
- ☐ Anonymizer (56)

Hide Filters

Risk:
- ☑ ALL
- ☐ 1 Very Low (211)
- ☐ 2 Low (510)
- ☐ 3 Medium (239)
- ☐ 4 High (29)
- ☐ 5 Critical (1)

Application Name	Category	Risk
Tiny IdentD	Instant Messaging	4
Trillian	Instant Messaging	4
Tux Messenger	Instant Messaging	4
digsby	Instant Messaging	4
mIRC	Instant Messaging	4
Clickster	Multimedia	4
SIP Communicator	VoIP	4
Acronis Snap Deploy	Business Application...	3
ReadAir	Business Application...	3
SharePoint	Business Application...	3
Xobni	Business Application...	3
Blue Crab	Download Manager	3
Pandora	Download Manager	3
Playstation Network	Gaming	3
BBC iPlayer	IPTV	3
Channel 4 on demand	IPTV	3
Divx Moviez	IPTV	3
123 Flash Chat	Instant Messaging	3
123 Web Messenger	Instant Messaging	3
99chats.com	Instant Messaging	3
AIM Express	Instant Messaging	3
ATSA Chat	Instant Messaging	3
AVpod	Instant Messaging	3

Page: 2 of 44

BBC iPlayer Risk: 3

IPTV

BBC iPlayer is a media player that allows users to view content such as TV and radio programs broadcast in the last week on the BBC (British Broadcasting Company) Network.

Tags: Encrypts communications, Autostarts/Stays Resident, IPTV, Supports Streaming, Shows Ads, High Bandwidth

…ions

…l-network

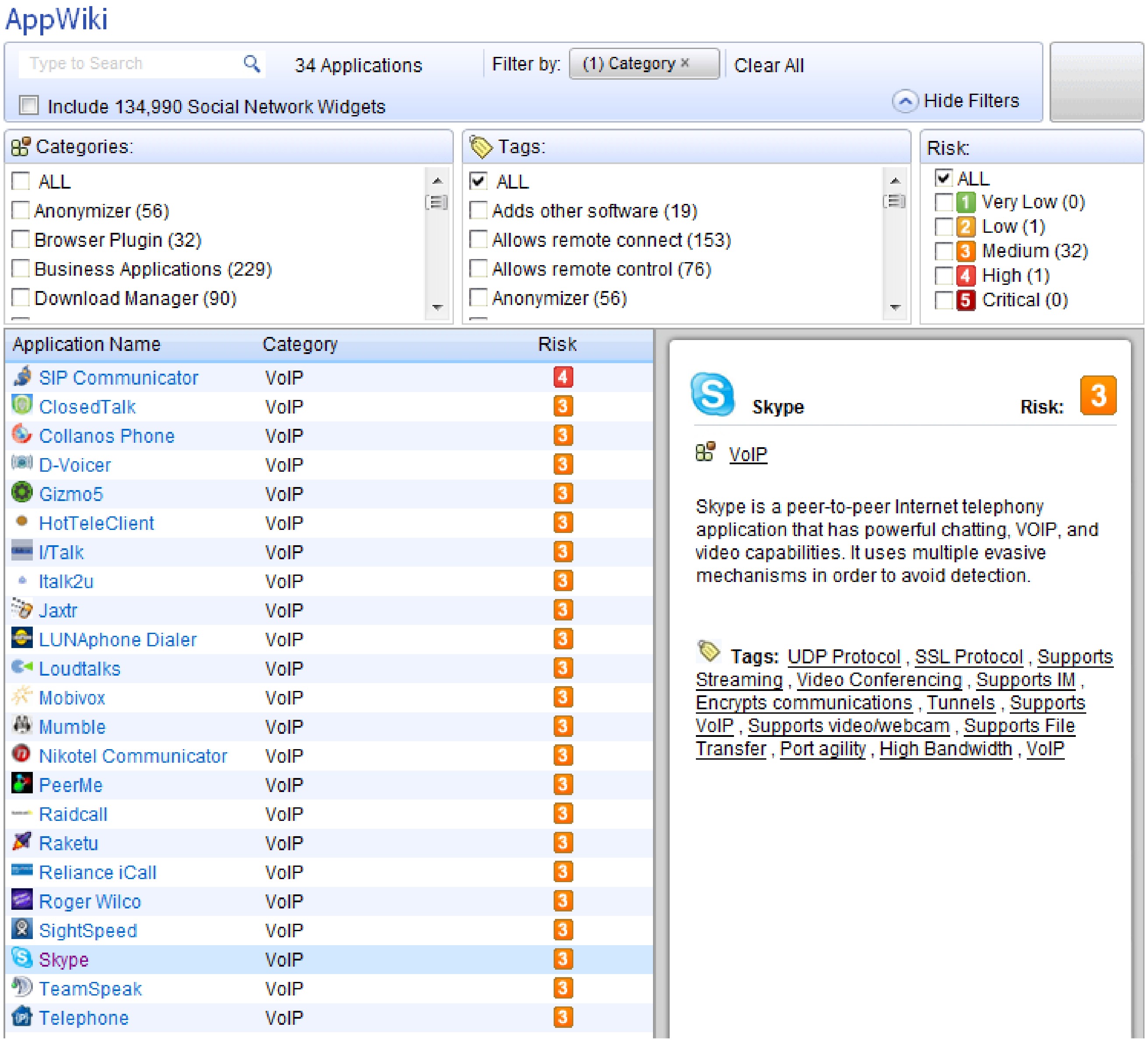
…0 categories

…IM, P2P,

…le Share)

appwiki.checkpoint.com

http://appwiki.checkpoint.com



AppWiki

Type to Search | 34 Applications | Filter by: (1) Category × | Clear All

□ Include 134,990 Social Network Widgets

Hide Filters

Categories:

- □ ALL
- □ Anonymizer (56)
- □ Browser Plugin (32)
- □ Business Applications (229)
- □ Download Manager (90)

Tags:

- ☑ ALL
- □ Adds other software (19)
- □ Allows remote connect (153)
- □ Allows remote control (76)
- □ Anonymizer (56)

Risk:

- ☑ ALL
- □ 1 Very Low (0)
- □ 2 Low (1)
- □ 3 Medium (32)
- □ 4 High (1)
- □ 5 Critical (0)

Application Name	Category	Risk
SIP Communicator	VoIP	4
ClosedTalk	VoIP	3
Collanos Phone	VoIP	3
D-Voicer	VoIP	3
Gizmo5	VoIP	3
HotTeleClient	VoIP	3
I/Talk	VoIP	3
Italk2u	VoIP	3
Jaxtr	VoIP	3
LUNAphone Dialer	VoIP	3
Loudtalks	VoIP	3
Mobivox	VoIP	3
Mumble	VoIP	3
Nikotel Communicator	VoIP	3
PeerMe	VoIP	3
Raidcall	VoIP	3
Raketu	VoIP	3
Reliance iCall	VoIP	3
Roger Wilco	VoIP	3
SightSpeed	VoIP	3
Skype	VoIP	3
TeamSpeak	VoIP	3
Telephone	VoIP	3

Skype **Risk:** 3

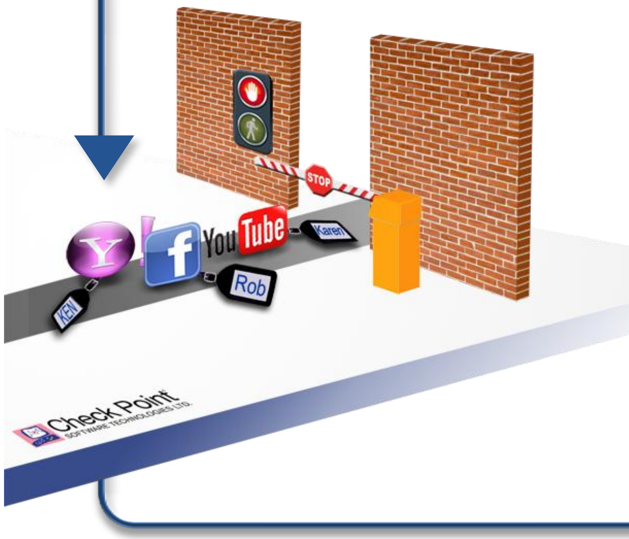
VoIP

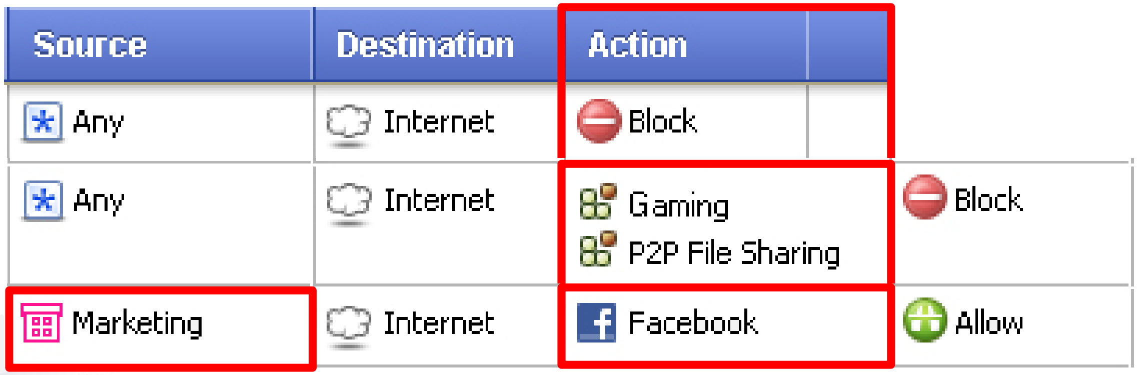
Skype is a peer-to-peer Internet telephony application that has powerful chatting, VOIP, and video capabilities. It uses multiple evasive mechanisms in order to avoid detection.

Tags: UDP Protocol , SSL Protocol , Supports Streaming , Video Conferencing , Supports IM , Encrypts communications , Tunnels , Supports VoIP , Supports video/webcam , Supports File Transfer , Port agility , High Bandwidth , VoIP

Check Point Application Control

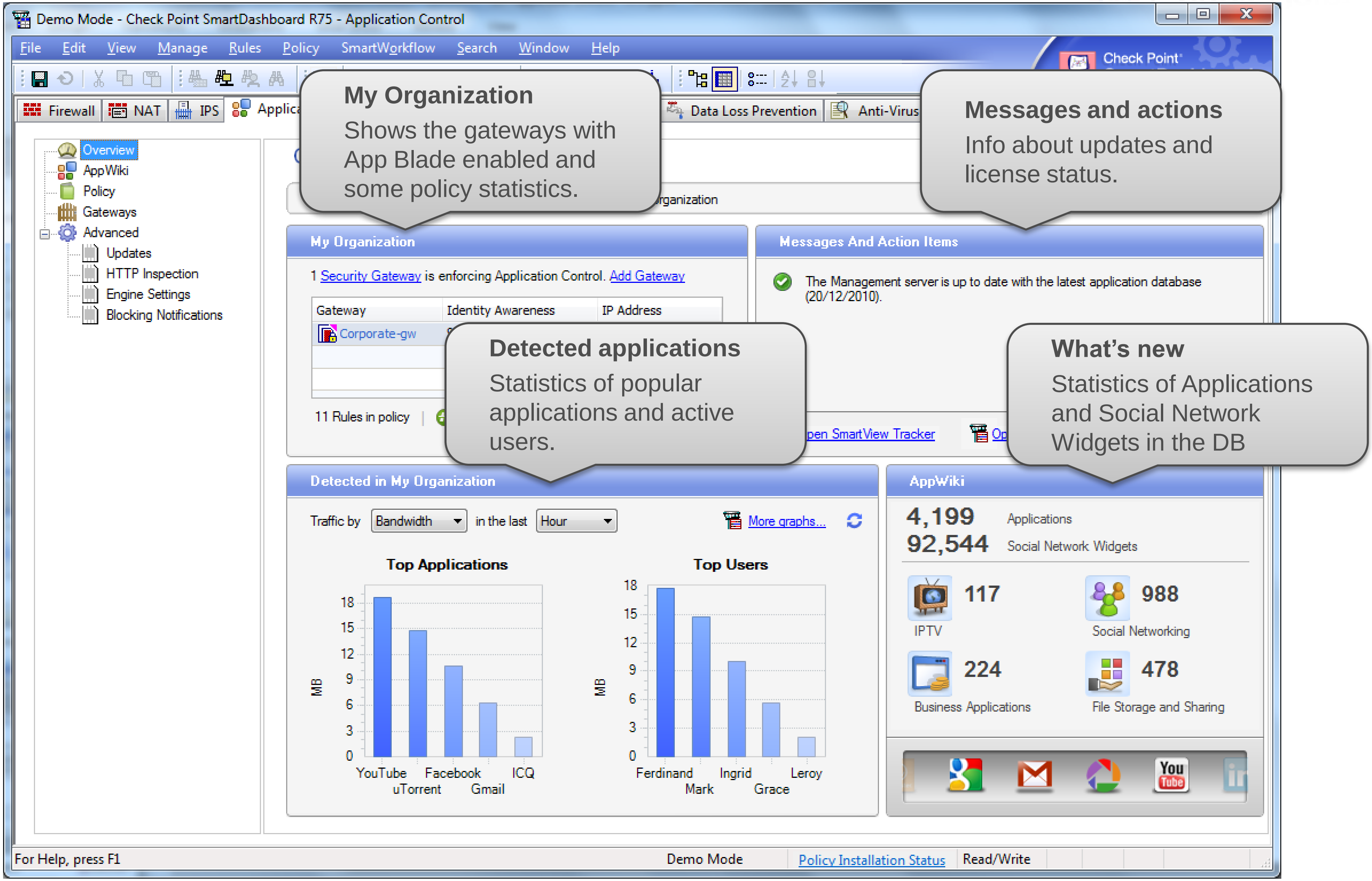
Identify, allow, block or limit usage
of applications at user or group level





Source	Destination	Action	
Any	Internet	Block	
Any	Internet	Gaming P2P File Sharing	Block
Marketing	Internet	Facebook	Allow

Application Control Overview



1 Security Gateway is enforcing Application Control. Add Gateway

11 Rules in policy

The Management server is up to date with the latest application database (20/12/2010).

4,199	Applications
92,544	Social Network Widgets

117	IPTV
988	Social Networking
224	Business Applications
478	File Storage and Sharing

My Organization
Shows the gateways with App Blade enabled and some policy statistics.

Messages and actions
Info about updates and license status.

Detected applications
Statistics of popular applications and active users.

What's new
Statistics of Applications and Social Network Widgets in the DB

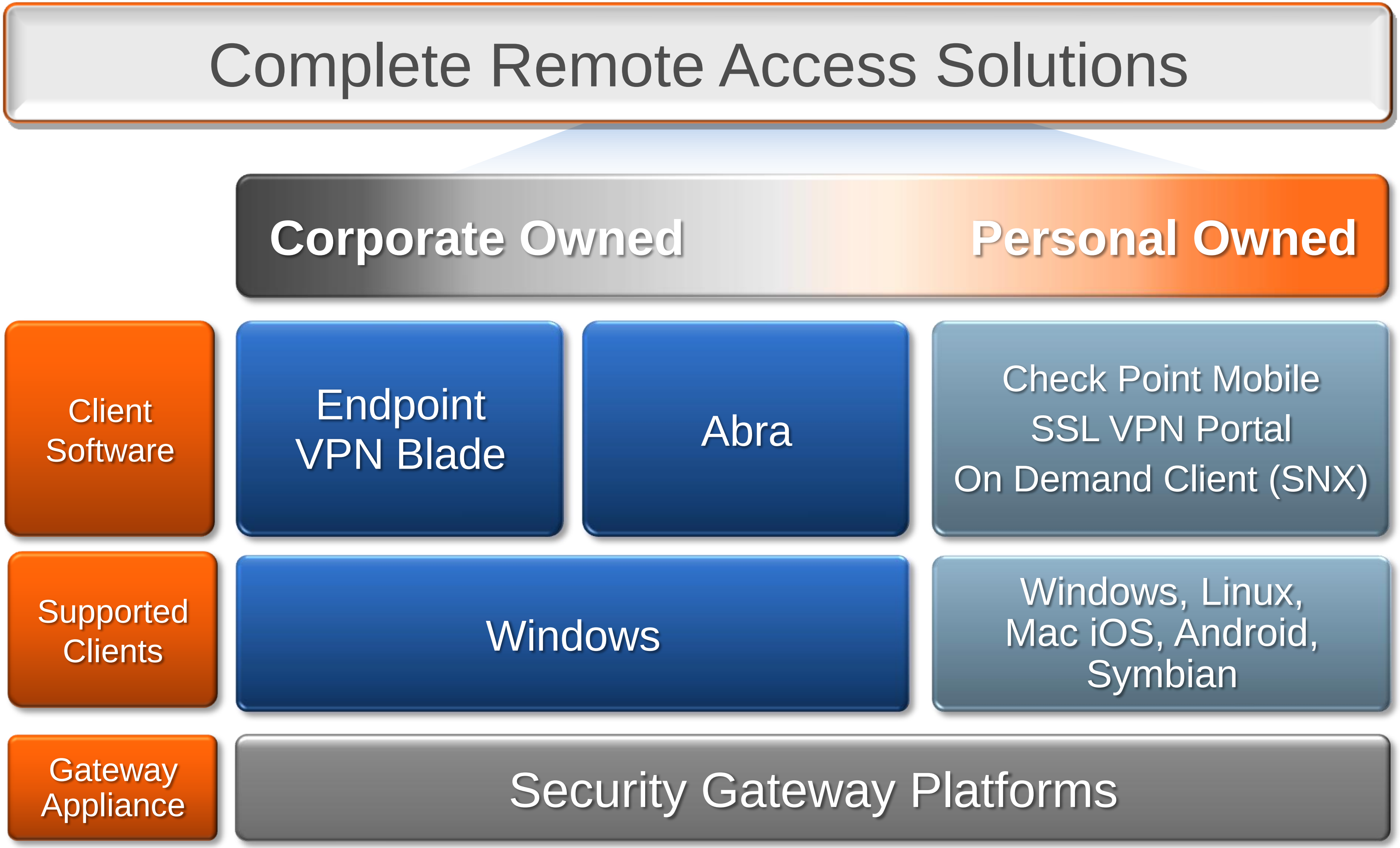
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Mobile Access Software Blade

Jani Ekman

Security Engineer

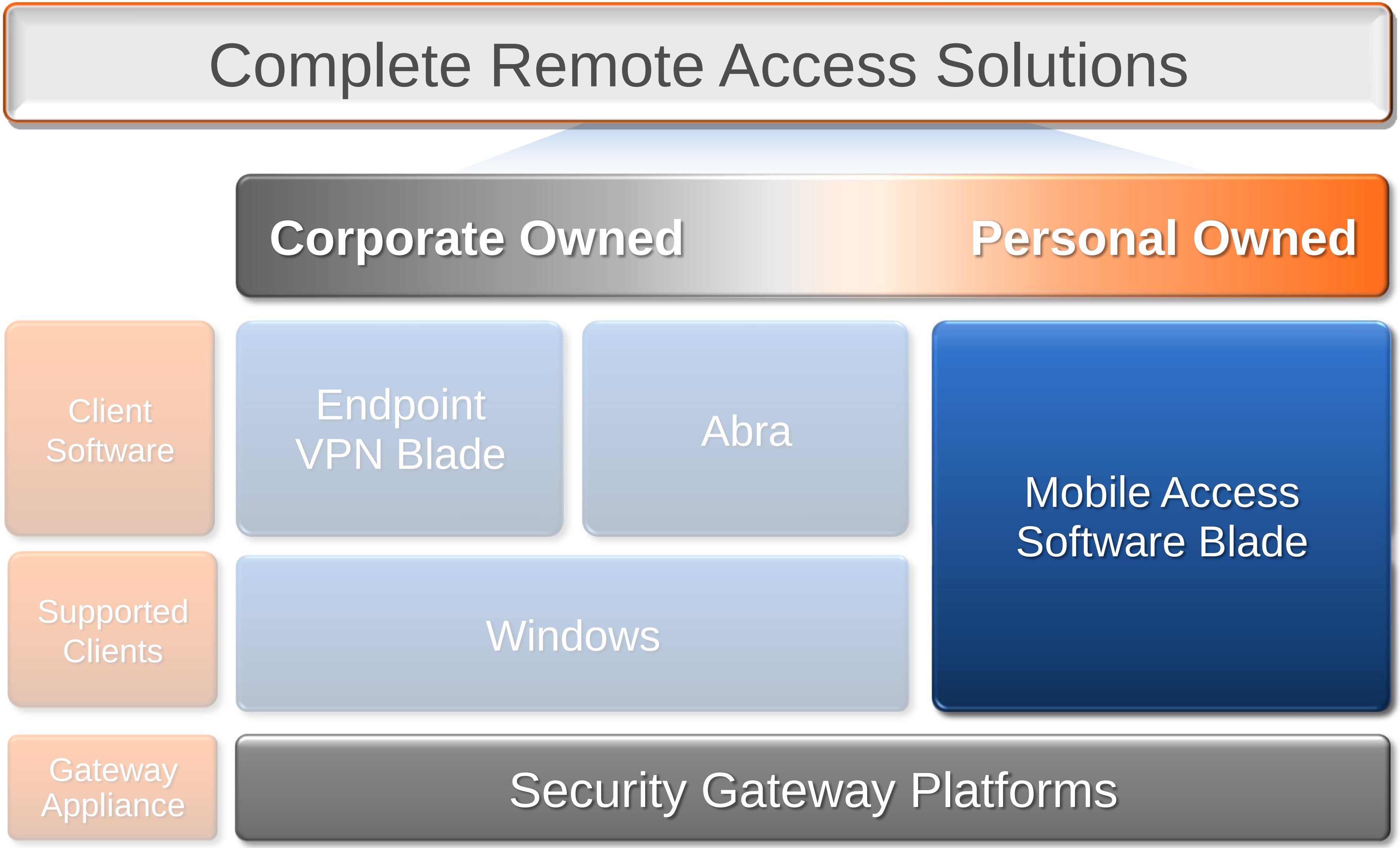
Remote Access Portfolio



Complete Remote Access Solutions

	Corporate Owned		Personal Owned
Client Software	Endpoint VPN Blade	Abra	Check Point Mobile SSL VPN Portal On Demand Client (SNX)
Supported Clients	Windows		Windows, Linux, Mac iOS, Android, Symbian
Gateway Appliance	Security Gateway Platforms		

Remote Access Portfolio



Complete Remote Access Solutions

Corporate Owned

Personal Owned

Client Software

Endpoint VPN Blade

Abra

Mobile Access Software Blade

Supported Clients

Windows

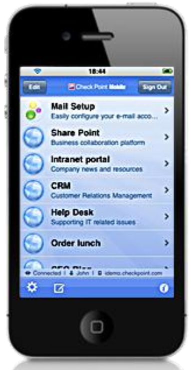
Gateway Appliance

Security Gateway Platforms

Mobile Access Software Blade

Check Point Mobile Access Products

User Experience



Mail Setup
Easily configure your e-mail acco...

Share Point
Business collaboration platform

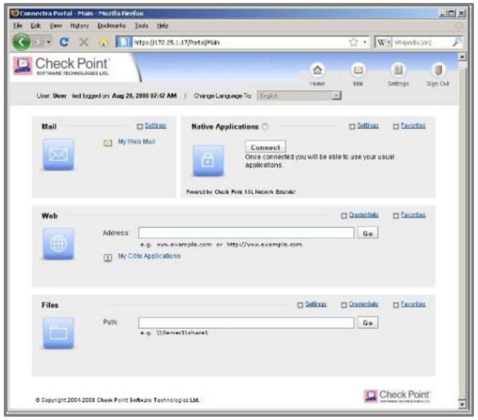
Intranet portal
Company news and resources

CRM
Customer Relations Management

Help Desk
Supporting IT related issues

Order lunch

Connected | John | idemo.checkpoint.com


Connectra Portal - Main - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://172.25.1.17/Portal/Main
Wikipedia (en)
Check Point SOFTWARE TECHNOLOGIES LTD.
Home
Mail
Settings
Sign Out

User: User last logged on: Aug 28, 2008 07:47 AM | Change Language To: English

Mail □ Settings

My Web Mail

Native Applications □ Settings □ Favorites

Connect

Once connected you will be able to use your usual applications.

Powered by Check Point SSL Network Extender

Web □ Credentials □ Favorites

Address: Go

e.g. www.example.com or http://www.example.com

My Citrix Applications

Files □ Settings □ Credentials □ Favorites

Path: Go

e.g. \\Server1\share1

© Copyright 2004-2008 Check Point Software Technologies Ltd.

Security Gateway and Admin

Check Point Clients

- Check Point Mobile
- Clientless Web Portal
- SNX On-Demand

Mobile Access Software Blade

- 50 concurrent connections
- 200 concurrent connections
- Unlimited concurrent connections

Simple for end-user

1

Tap “Check Point Mobile”

2

Enter your password

3

Gain secure access to your data!

Connect Securely from any device

Consistent user experience for all devices

Check point Mobile for iPhone, iPad, Android & Symbian

Check Point Mobile for PC & Mac

SecureConnect
Sign Out
Intranet portal
Company news and resources
Order lunch
SharePoint
Business collaboration platform
CRM
Customer Relations Management
Help Desk
Supporting IT related issues
CEO Blog
Edit

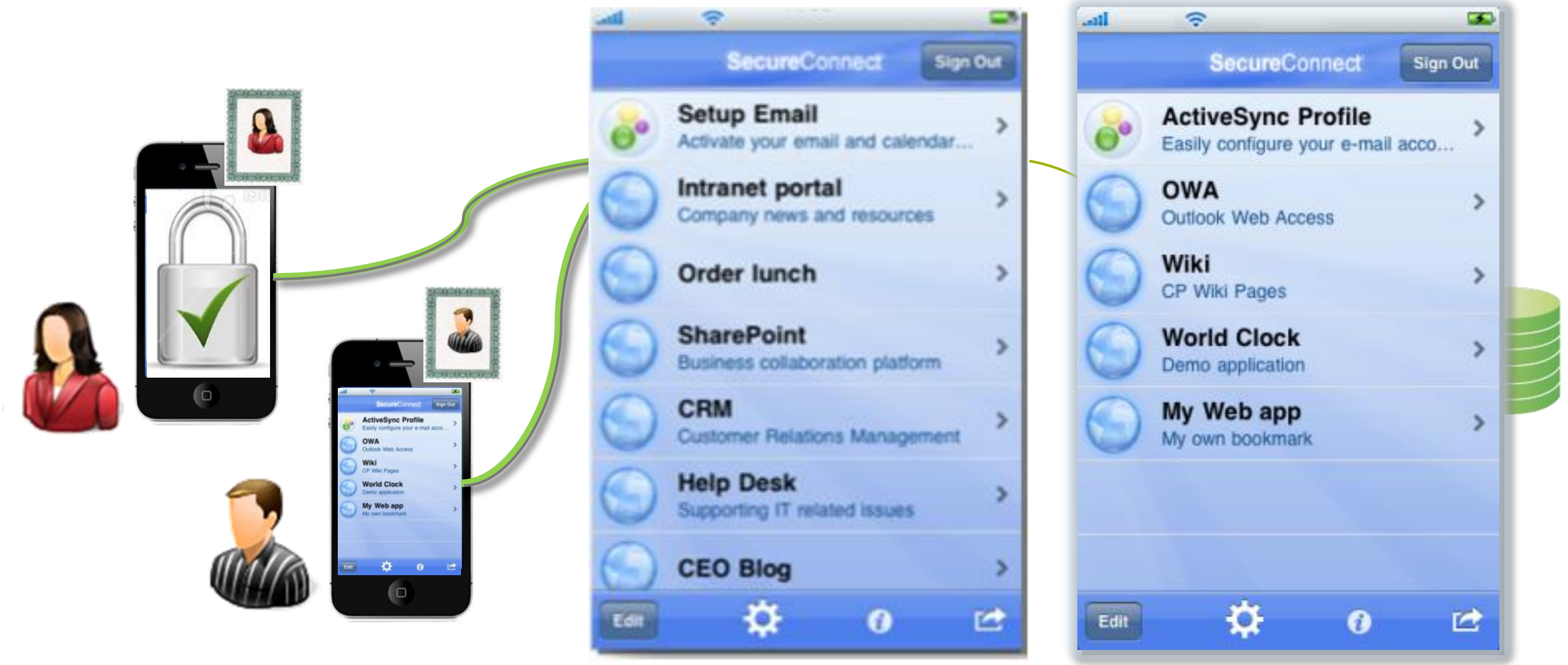
User & Device Access Control

Control data access by user and device settings

Personalized portal, based on identity

Setup device security features

Remote-Wipe device upon loss



SecureConnect Sign Out

- Setup Email – Activate your email and calendar…
- Intranet portal – Company news and resources
- Order lunch
- SharePoint – Business collaboration platform
- CRM – Customer Relations Management
- Help Desk – Supporting IT related issues
- CEO Blog

Edit

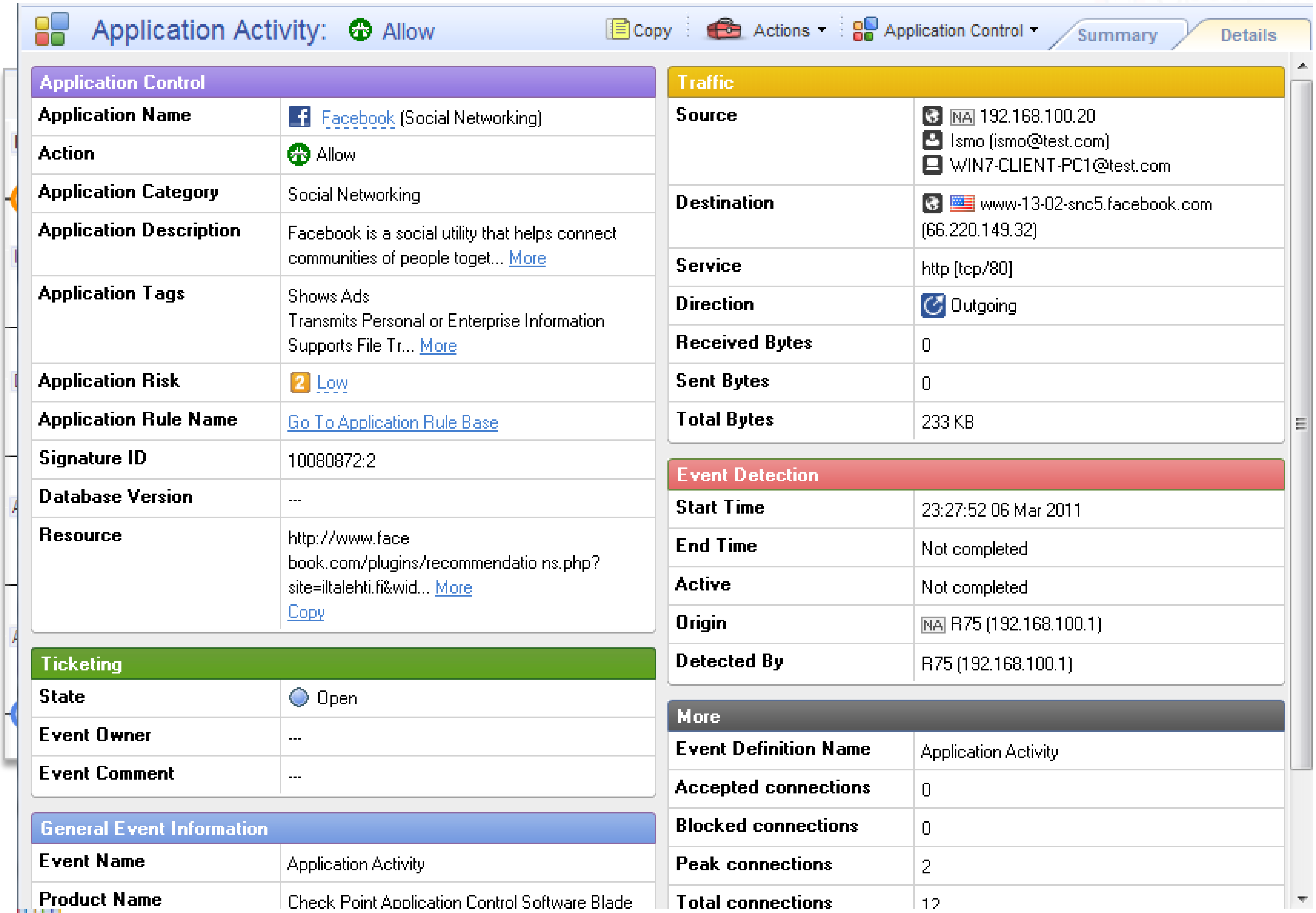
SecureConnect Sign Out

- ActiveSync Profile – Easily configure your e-mail acco…
- OWA – Outlook Web Access
- Wiki – CP Wiki Pages
- World Clock – Demo application
- My Web app – My own bookmark

Edit

There's no Control without Visibility

360º Visibility into All Security Events



Application Control

Application Name	Facebook (Social Networking)
Action	Allow
Application Category	Social Networking
Application Description	Facebook is a social utility that helps connect communities of people toget... More
Application Tags	Shows Ads Transmits Personal or Enterprise Information Supports File Tr... More
Application Risk	2 Low
Application Rule Name	Go To Application Rule Base
Signature ID	10080872:2
Database Version	---
Resource	http://www.facebook.com/plugins/recommendations.php?site=iltalehti.fi&wid... More Copy

Ticketing

State	Open
Event Owner	---
Event Comment	---

General Event Information

Event Name	Application Activity
Product Name	Check Point Application Control Software Blade

Traffic

Source	NA 192.168.100.20 Ismo (ismo@test.com) WIN7-CLIENT-PC1@test.com
Destination	www-13-02-snc5.facebook.com (66.220.149.32)
Service	http [tcp/80]
Direction	Outgoing
Received Bytes	0
Sent Bytes	0
Total Bytes	233 KB

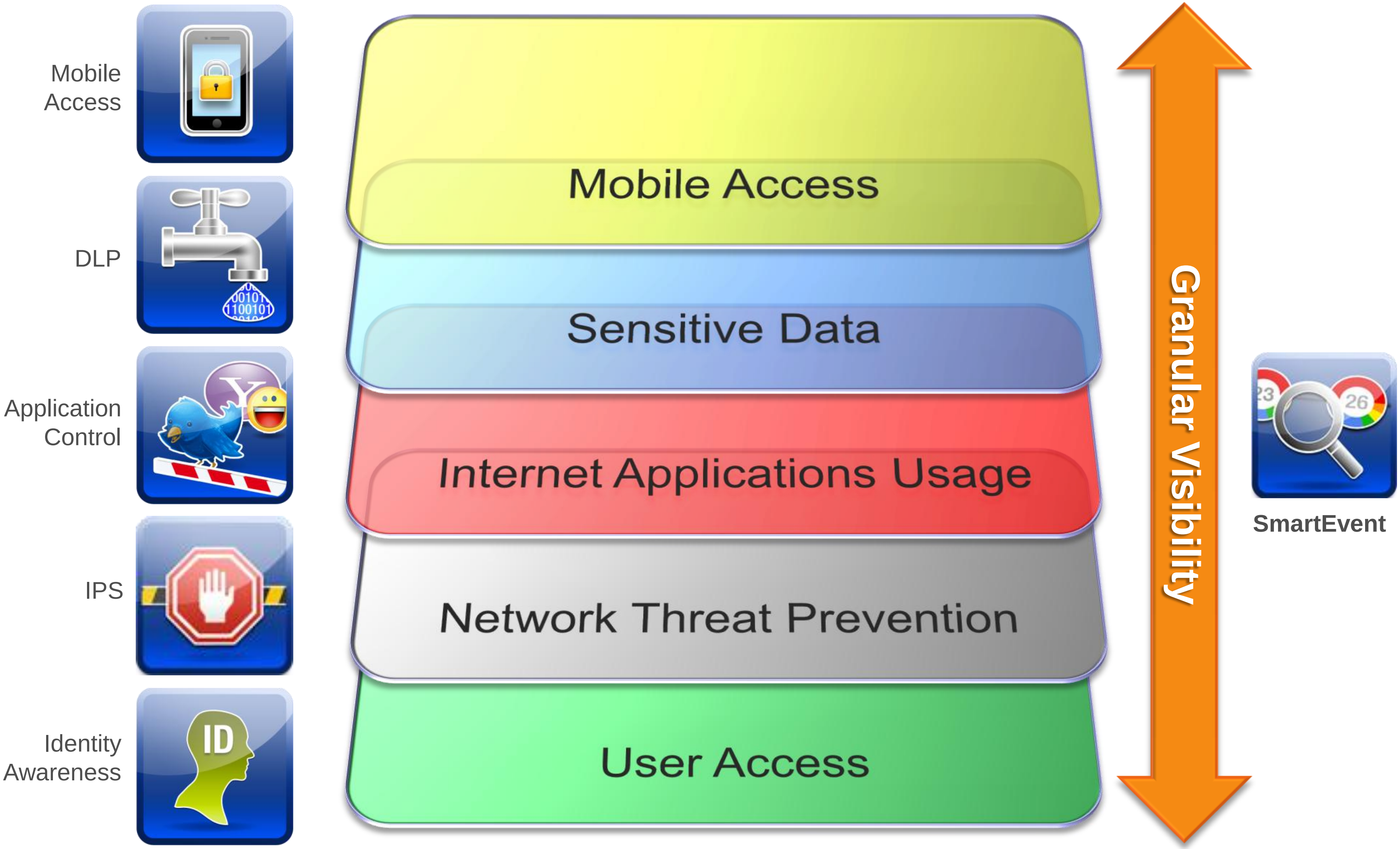
Event Detection

Start Time	23:27:52 06 Mar 2011
End Time	Not completed
Active	Not completed
Origin	NA R75 (192.168.100.1)
Detected By	R75 (192.168.100.1)

More

Event Definition Name	Application Activity
Accepted connections	0
Blocked connections	0
Peak connections	2
Total connections	12

Granular Control of all Security layers



Mobile Access

DLP

Application Control

IPS

Identity Awareness

Mobile Access

Sensitive Data

Internet Applications Usage

Network Threat Prevention

User Access

Granular Visibility

SmartEvent

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Thank You!

janie@checkpoint.com