



**Check Point®**  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

---

# Defining Your Security Blueprint



**Daniel Phuan**

**Technical Manager, Southeast Asia**

# Dynamic Environment, New Challenges



**We live in a VERY dynamic environment,  
IT needs to enable & support it**





# Security Modular Packages

# Check Point Global Presence

## LOCATIONS



## AUDIENCES

## APPLICATIONS



 **More than 70 offices**



# Check Point Global Presence





## LOCATIONS



## AUDIENCES

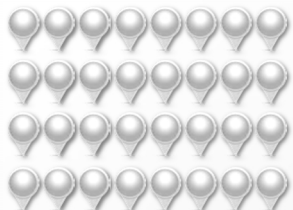
## APPLICATIONS



-  4 major offices
-  2 co-location sites
-  6 development sites
-  12 medium offices, 38 small offices

# Check Point Global Audiences

## LOCATIONS



## AUDIENCES

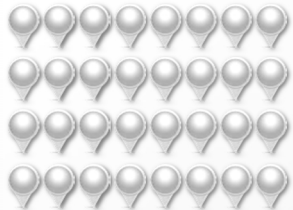


## APPLICATIONS



# Check Point Global Audiences

## LOCATIONS



## AUDIENCES



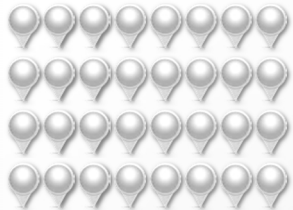
## APPLICATIONS





# Check Point Global Audiences

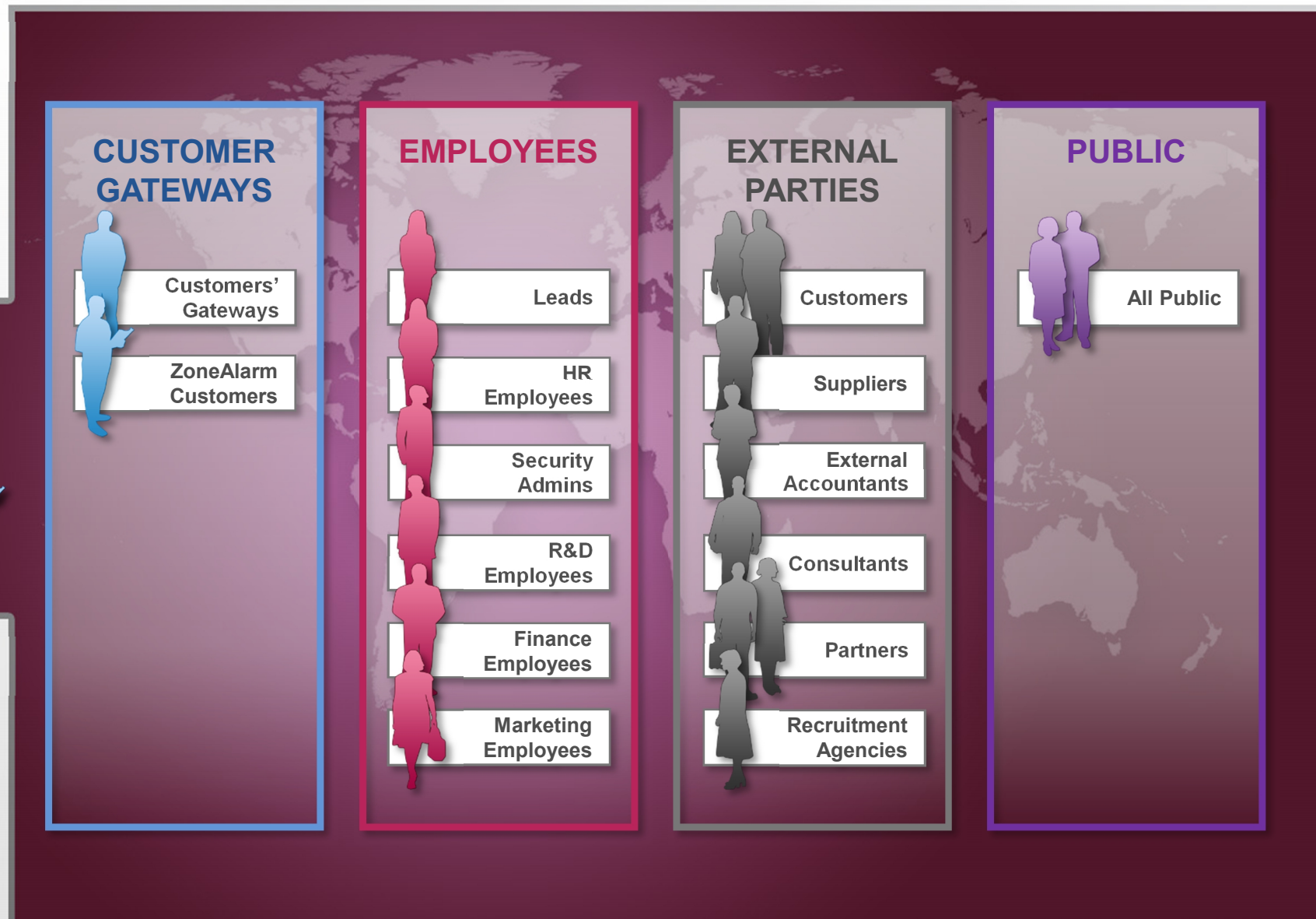
## LOCATIONS



## AUDIENCES

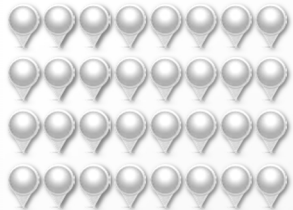


## APPLICATIONS

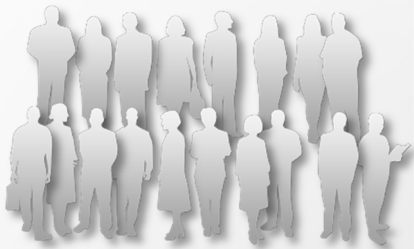


# Check Point Global Applications

## LOCATIONS



## AUDIENCES

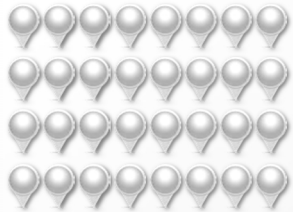


## APPLICATIONS

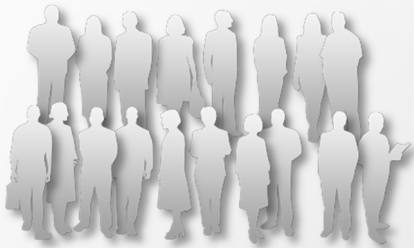


# Check Point Global Applications

## LOCATIONS



## AUDIENCES



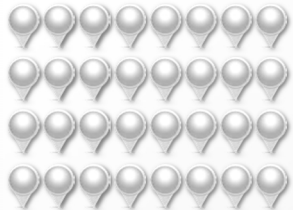
## APPLICATIONS



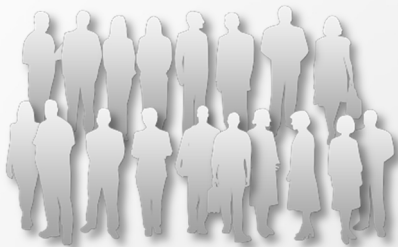


# Check Point Global Applications

## LOCATIONS







## AUDIENCES







## APPLICATIONS



### CUSTOMERS AND PUBLIC

-  Public Site
-  ZoneAlarm Store
-  Customer Portal
-  Support Center


### EMPLOYEES *from anywhere*

-  Wiki
-  Call Center
-  Sales Systems
-  Exchange

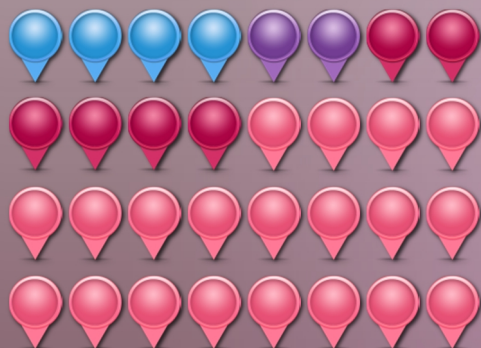
### EMPLOYEES *at the office*

-  Performance Review
-  Business Warehouse
-  Time Attendance

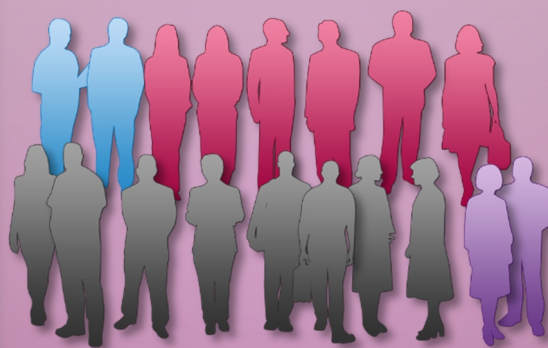
### DESIGNATED EMPLOYEES *only*

-  R&D Source Code
-  Salary
-  HR System
-  R&D Project Management

## LOCATIONS



## AUDIENCES

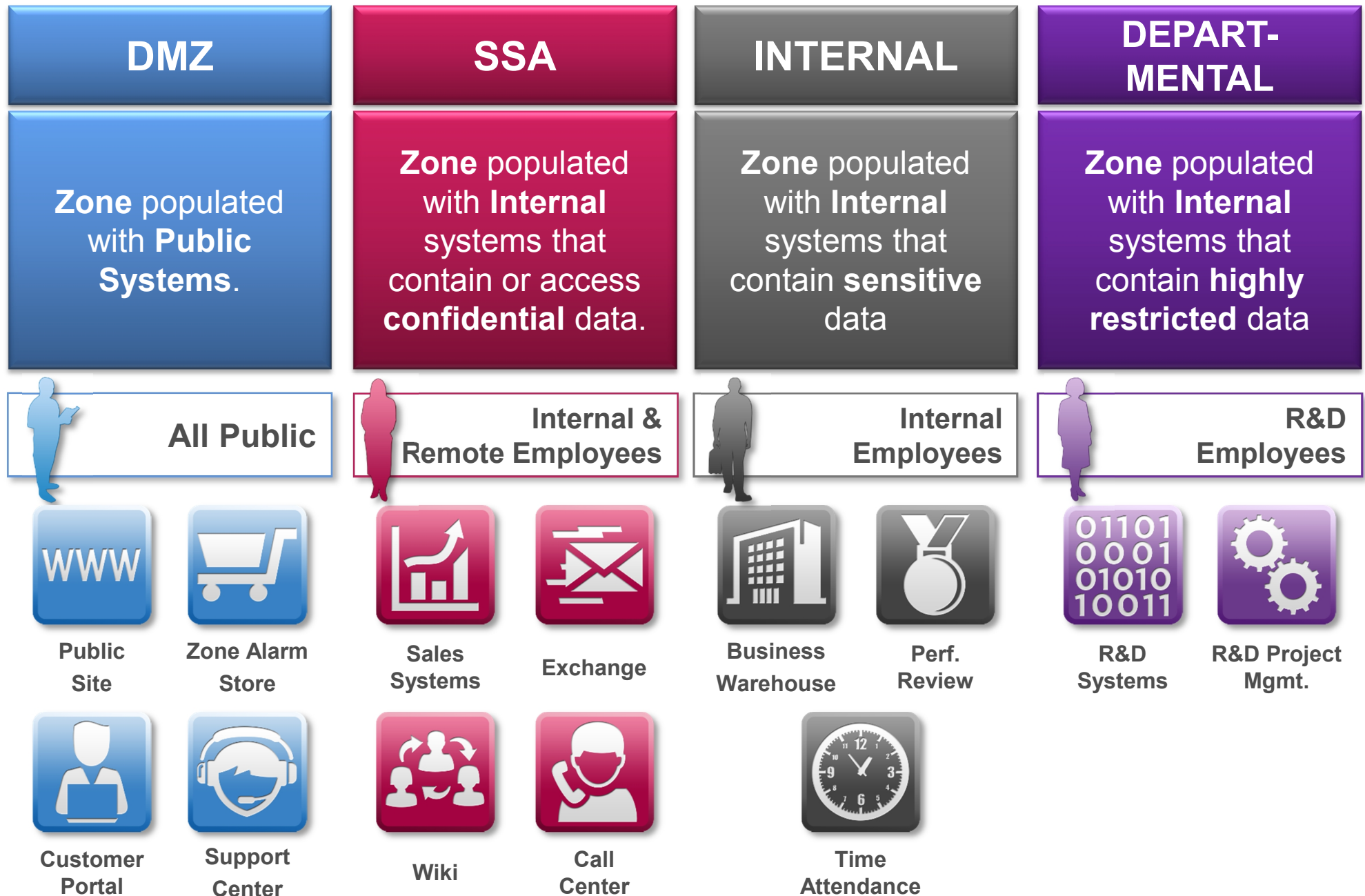


## APPLICATIONS





# Define Network Zones & Policy



# Define Network Zones & Policy

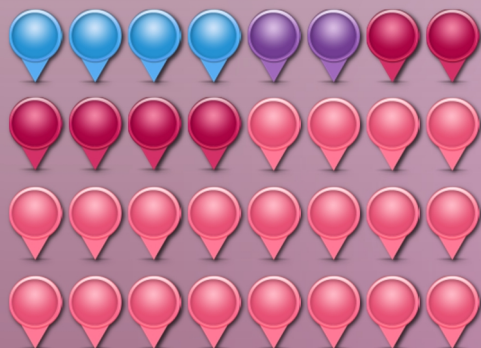
DMZ	SSA	INTERNAL	DEPARTMENT- MENTAL
Zone populated with <b>Public Systems</b> .	Zone populated with <b>Internal</b> systems that contain or access <b>confidential</b> data.	Zone populated with <b>Internal</b> systems that contain <b>sensitive</b> data	Zone populated with <b>Internal</b> systems that contain <b>highly restricted</b> data

- Any User can reach the **DMZ** zone
- Only corporate users can reach the **SSA** zone from internal networks or through VPN
- Only corporate users can reach the **Internal** zone from internal networks only
- Only specific users can reach the corresponding **Departmental** zone

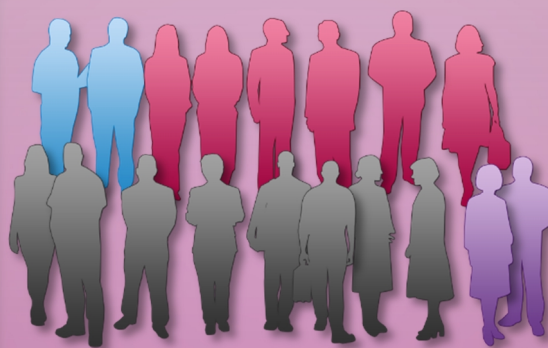


**Any other access is considered an exception and must be approved**

## LOCATIONS



## AUDIENCES



## APPLICATIONS



# Define Modular Packages



# We Will Focus on the 3 Main Risks



Threats to the organization

**63%**

infected with bots



Addressing external threats

Risky enterprise applications

**47%**

used anonymizers



Enable secure application use

Data loss incidents

**54%**

had a data loss event



Preventing Data Loss



# Adopt a multi-layer protection

Firewall	DLP	Logging & Status
VPN	URLF	Full Disk Encryption
IPS	Application control	Policy Management
Mobile	Anti-Spam	Anti-Bot
Compliance	Anti-Virus	Media Encryption



**Addressing  
external threats**



**Enable secure  
application use**



**Preventing  
Data Loss**

[Restricted] ONLY for designated groups and individuals

# Adopt a multi-layer protection

Firewall	DLP	Logging & Status
VPN	URLF	Full Disk Encryption
IPS	Application control	Policy Management
Mobile	Anti-Spam	Anti-Bot
Compliance	Anti-Virus	Media Encryption



**Addressing  
external threats**



**Enable secure  
application use**



**Preventing  
Data Loss**

[Restricted] ONLY for designated groups and individuals

# Adopt a multi-layer protection

Firewall	DLP	Logging & Status
VPN	URLF	Full Disk Encryption
IPS	Application control	Policy Management
Mobile	Anti-Spam	Anti-Bot
Compliance	Anti-Virus	Media Encryption



**Addressing  
external threats**



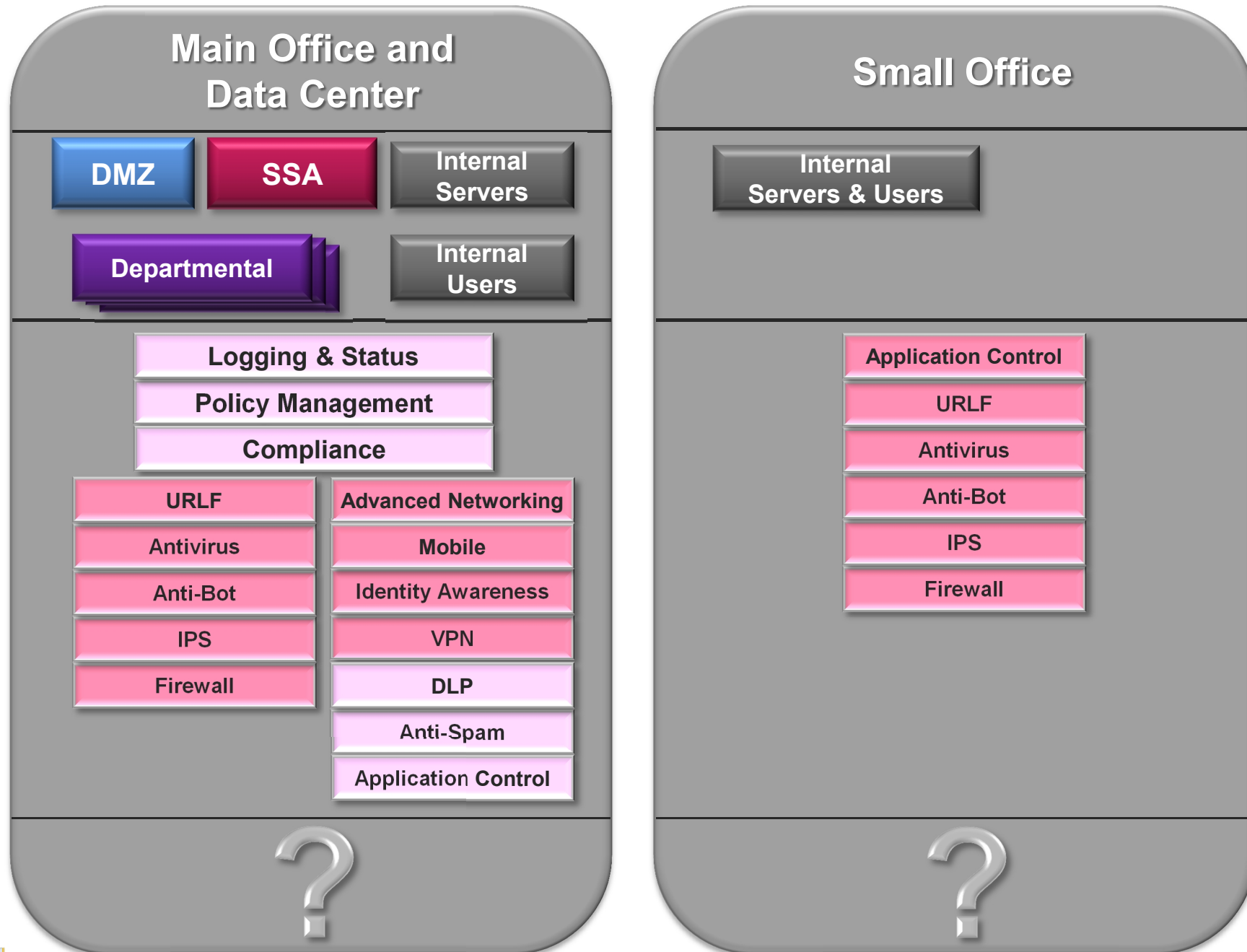
**Enable secure  
application use**



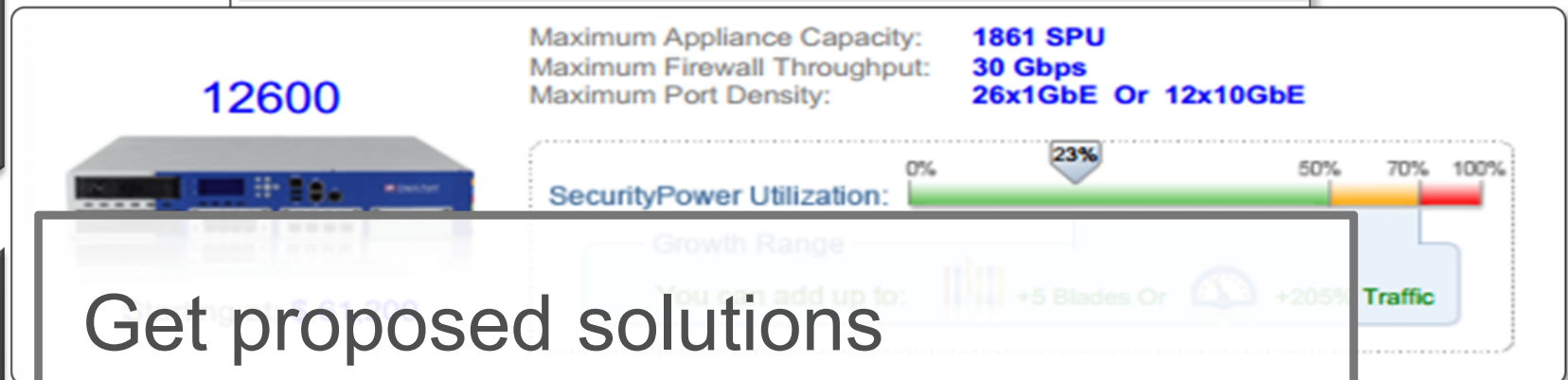
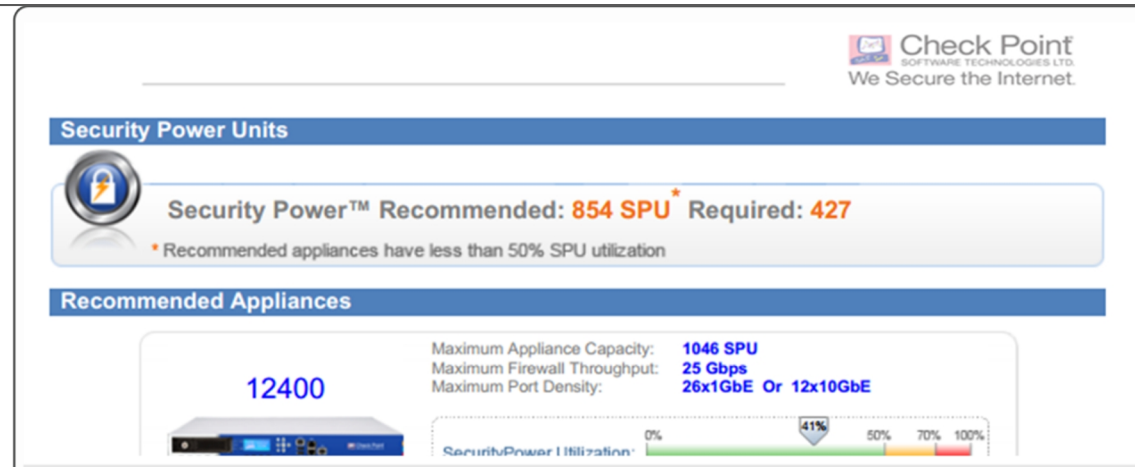
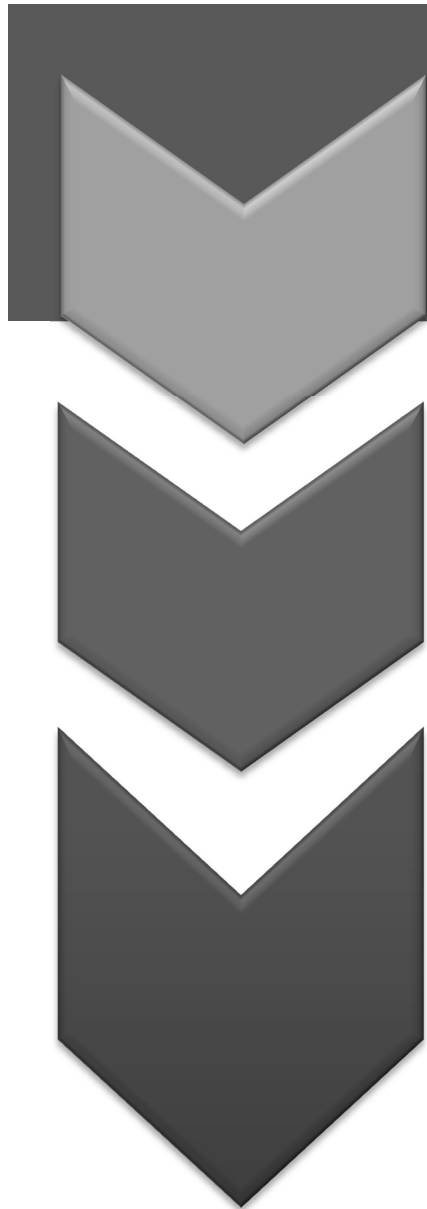
**Preventing  
Data Loss**

[Restricted] ONLY for designated groups and individuals

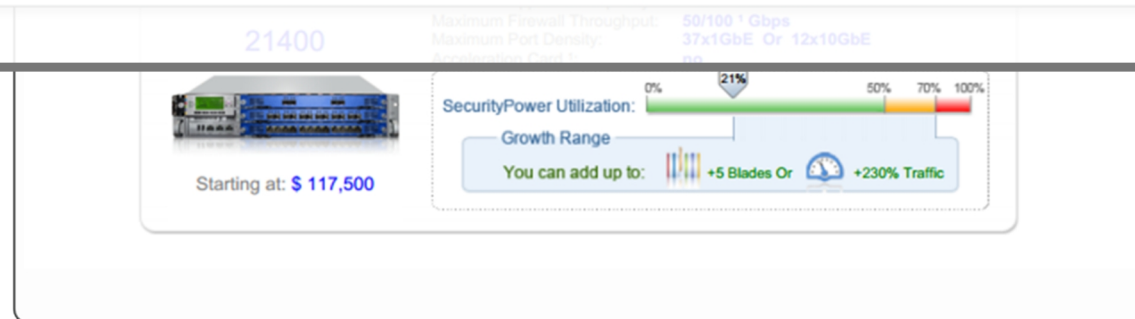
# Define Modular Packages



# Analyze Performance Requirements



Get proposed solutions



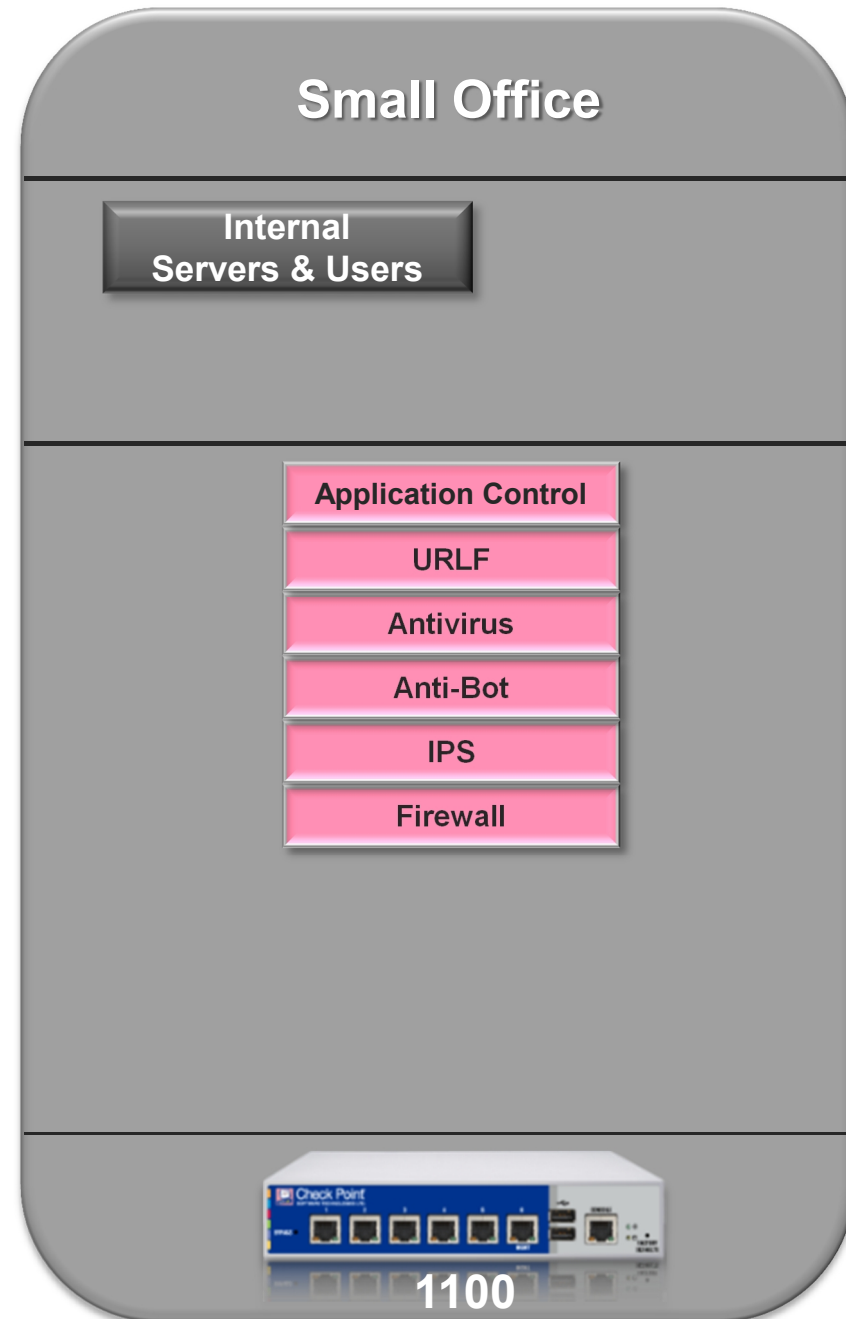
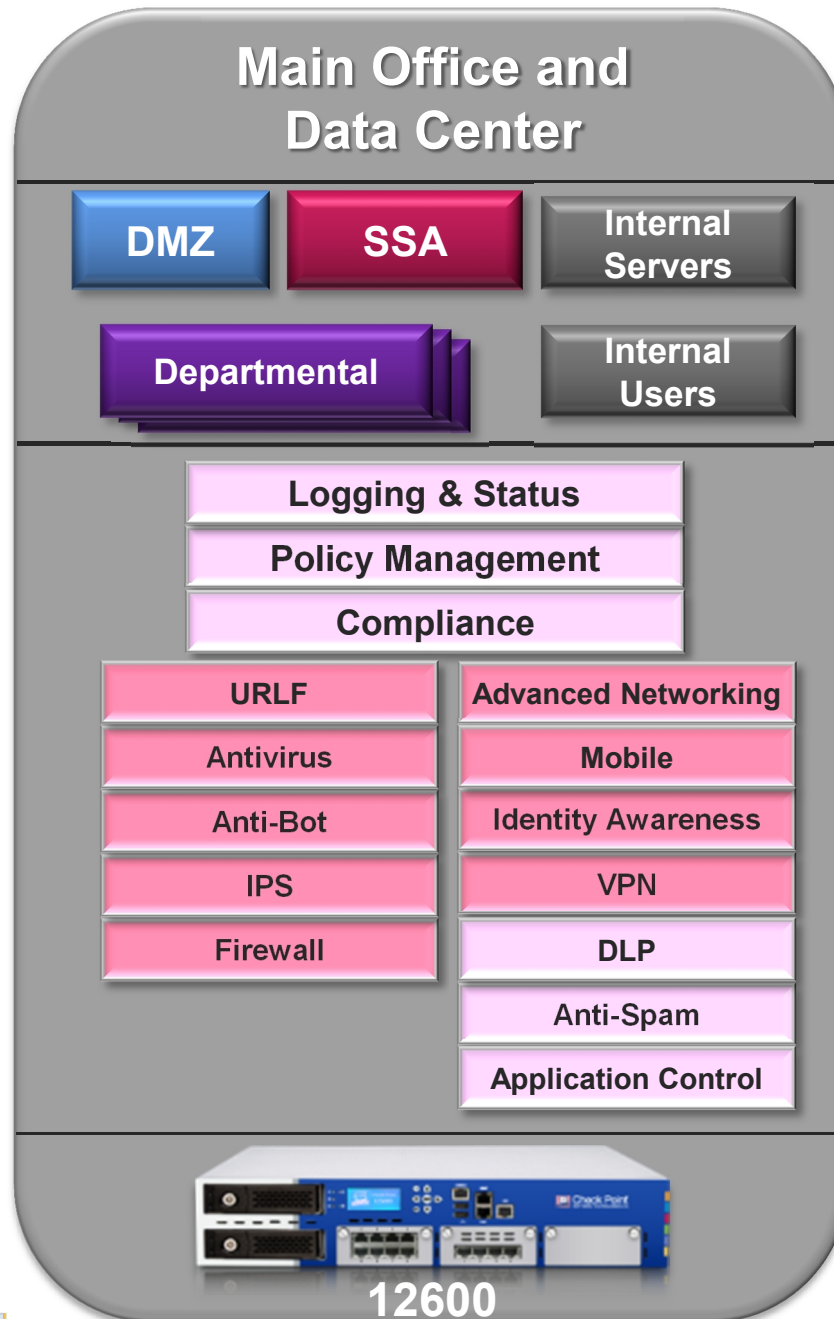
Total Users: 3000

URL Filtering





# Define Modular Packages



# Apply Policy for Your Main Risks



**Addressing  
external threats**



**Enable secure  
application use**



**Preventing  
Data Loss**

# Case 1: Provoked Leakage

## Singapore

November 28<sup>th</sup>, 2012


14:00 hrs. local time







# Case 1: Leakage Prevention

Daniel gets a notification from the DLP system

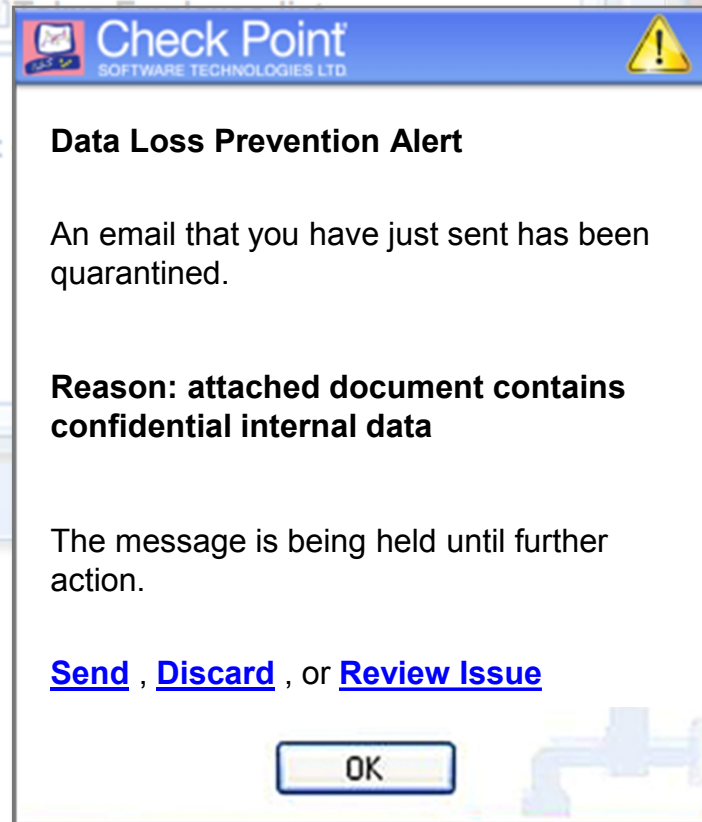
 **To...**

**Subject:**







 **Attached:** 

Hi,  
Attached is the list  
Have a good flight

Daniel



**Contacts**

	Ariens, Candice (262) 555-5874	
	Bancroft, Billy (414) 555-1234	
	Black, Ian (262) 555-5874	
	Bradley, Jim jim@developerone.com	



**DLP  
Enforcement**

# DLP Policy Definition

Personal \ Public	Confidential	Restricted \ Highly Restricted
Non confidential or personal information that has non or positive effect on the company	Important information that has limited impact on the company	Sensitive or highly sensitive information that may compromise the company

- Sending **out** data classified as **Personal or Public** is allowed.
- Sending **out** data classified as **Restricted, Highly Restricted** or **Confidential** is not allowed.



**Exceptions are approved by the employee using User Check.**

# DLP Policy Implementation



Data Type	Action
Our business information: Customers, contracts, etc	ASK USER
Source code	ASK USER
Financial data, Intellectual property	ASK USER
Personal employee data	ASK USER
Special documents	BLOCK



# DLP Incident Statistics

Average  
monthly  
events

- ASK USER: ~**2,700**
- BLOCK: ~7

ASK USER  
per  
employee

~**1**

ASK USER  
feedback  
distribution

- Sent: 85%
- **Don't send: 15%**

# Case 2: Unintended Exposure

## Minsk, Belarus

Oct 22nd, 2012

13:30 hrs. local time

## Tel-Aviv, Israel

Oct 22nd, 2012

13:45 hrs. local time



# Case 2: Exposure Prevention

BitTorrent detected on one of the lab machines which was connected to the internal network



EN99778029 - Application Activity

**Application Activity: Block**

Details	
Application	Bittorrent.Biz
Action	Block
Matched Category	High Risk
All Categories	Autostarts/Stays Resident, High Bandwidth, Tr... >>
Description	Bittorrent.biz is a French-language torrent do... >>
Risk	4 High



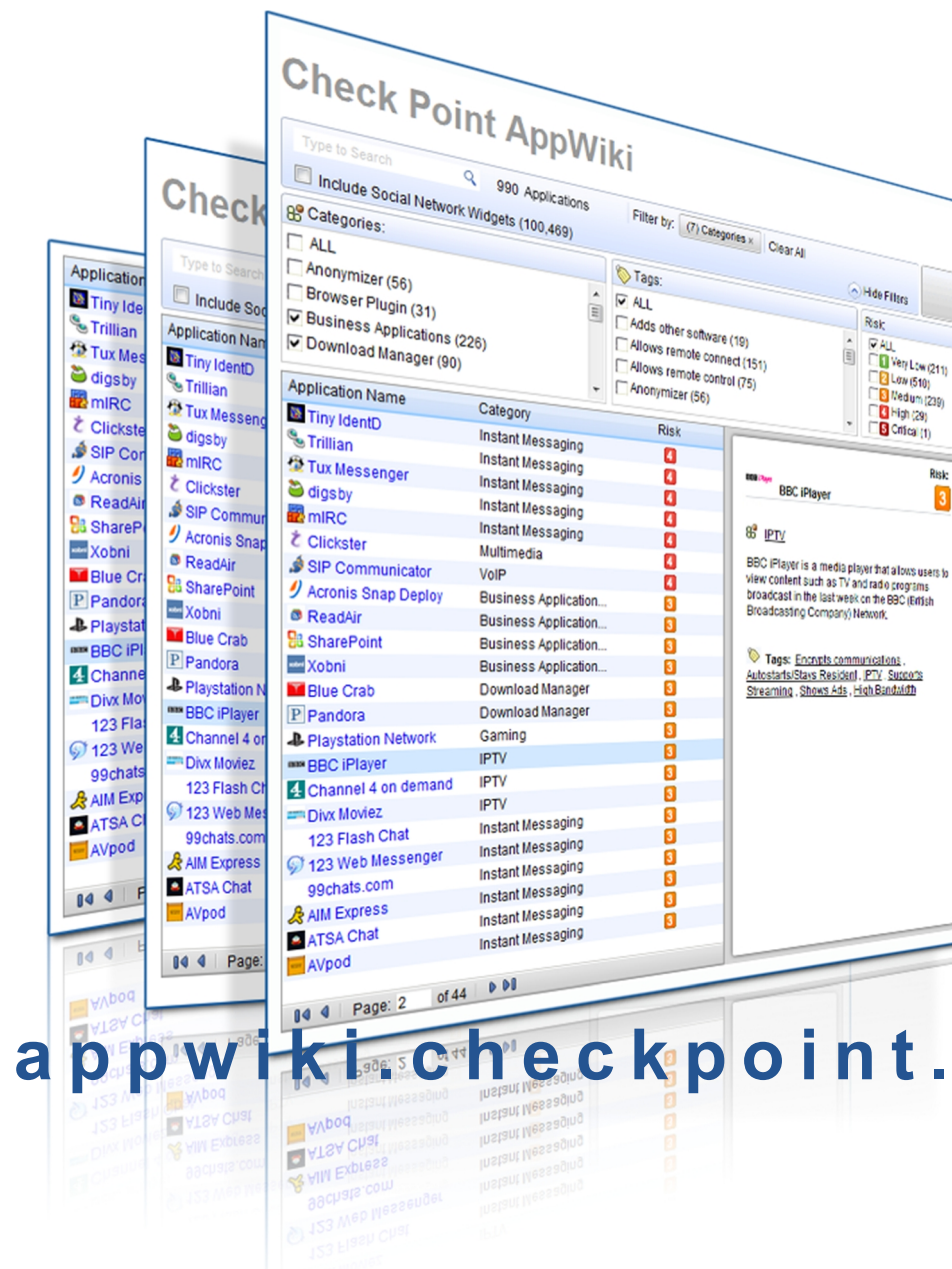
**App  
Name**

**Action**

**Risk**



# App Wiki—Applications Library



Applications  
social-network

80 categories  
M, P2P,  
Share)

[appwiki.checkpoint.com](http://appwiki.checkpoint.com)



# Application Control Policy Definition

## Low Risk

Applications from the following categories:  
Business applications, Mobile software, Social networking,...

## Medium Risk

Application from the following categories:  
Browser plugins, Personal mail, VoIP,...

## High Risk

Application from the following categories:  
File storage & sharing, P2P file Sharing, Remote administration,...

- Usage of **Low Risk** and **Medium Risk** applications is **allowed**
- Usage of **High Risk** applications is **not allowed**



**Exceptions are approved by the employee using User Check.**

# Application Control Implementation



Application Type	Action
Critical or high risk	Block
Anonymizer, P2P file sharing, botnets, etc.	Block
Department special need (e.g., hacker sites)	Ask User
Medium risk	Monitor



**Monthly  
events:  
20,000**

**Number of  
users: 600**

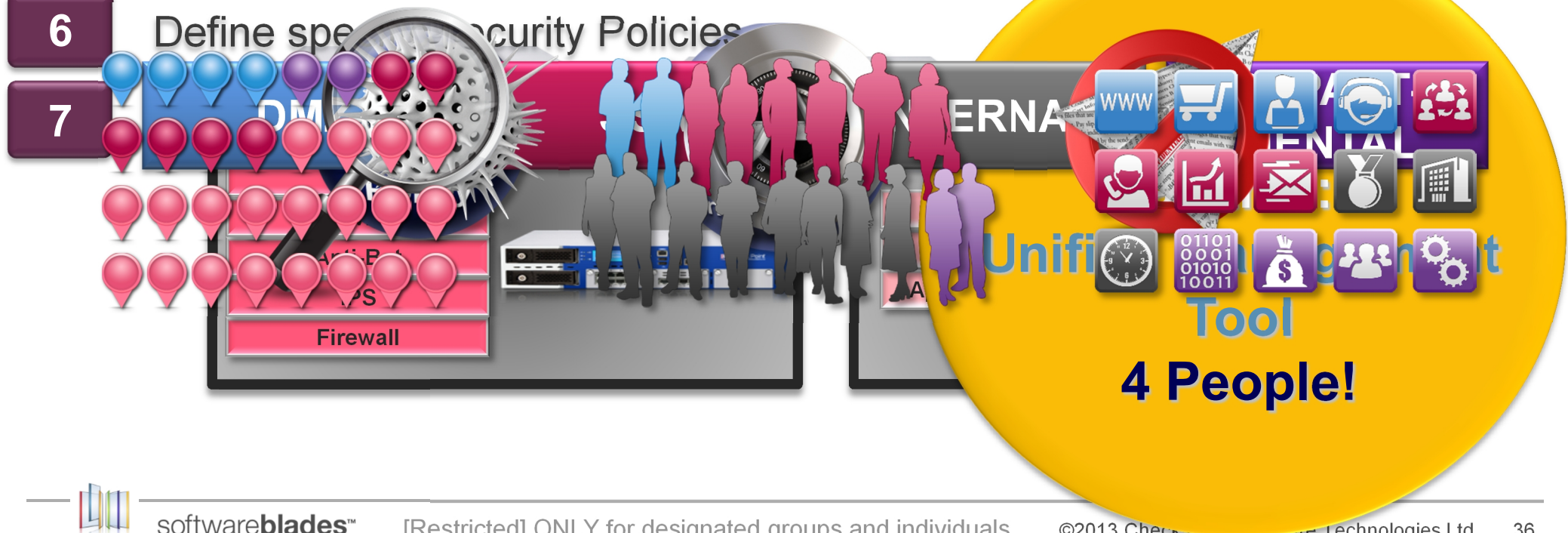
## Top block applications \ protocols

- Dropbox — 52%
- Sugarsync. — 43%
- BitTorrent — 2%
- Lync (Microsoft Chat tool) — 2%

Top 4 covers ~90% of the cases

# Defining Your Security Blueprint

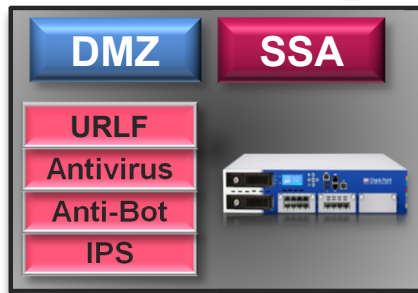
- 1 Identify your environment
- 2 Define your security zones
- 3 Identify main threats & protections
- 4 Analyze performance requirements
- 5 Define modular packages
- 6 Define specific Security Policies
- 7







My needs are **customers' needs**;  
my security solutions are **customers' solutions**



Build security modular packages,  
adopting a **multi-layer** protection:  
- Be a business enabler



**Analyze** your data to **improve** your security



**Easy to manage** with Software Blades





**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

---

**Thank You**

