

# We Secure The Highways



**Safety comes first ....with data availability and data security** 24x7 Highway Monitoring and Control

# About Nea Odos S.A.

ΝέαΟδός

Concession  
period:

- **30** years

Ionia  
Motorway:

- Construction, exploitation  
operation and  
maintenance of **196  
km**

PATHE  
Motorway:

- Reforming, exploitation,  
operation and  
maintenance of **172,5  
km**

Connecting brunch  
Schimatari –  
Halkida:

- Exploitation, operation  
and maintenance of  
**11km**

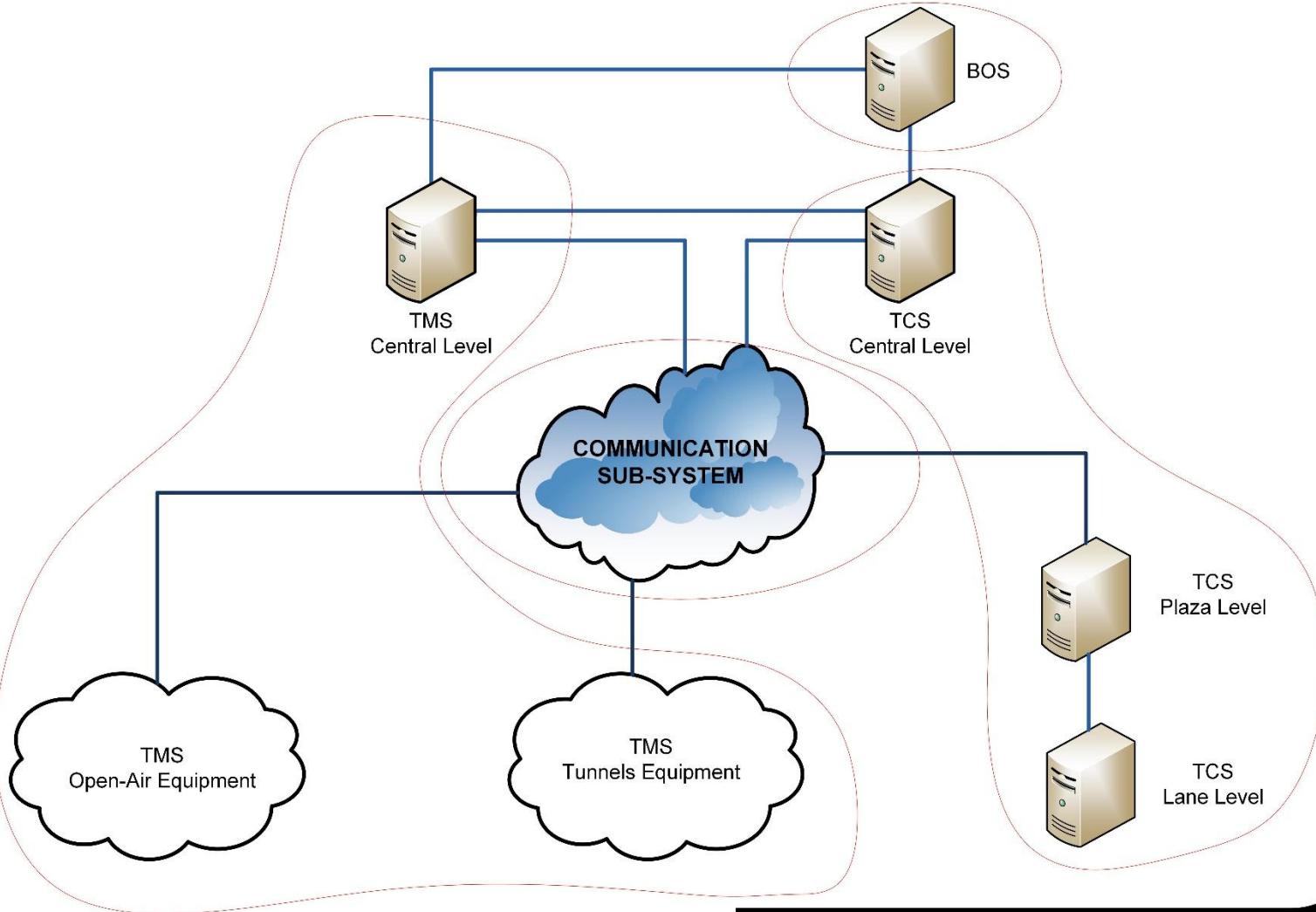


# ITS (Intelligent Transportation System)

- TCS (Toll Collection System)
- TMS (Traffic Management System)
- BOS (Back Office System)

# ITS (Intelligent Transportation System)

## PATHE MOTORWAY – System Schematics

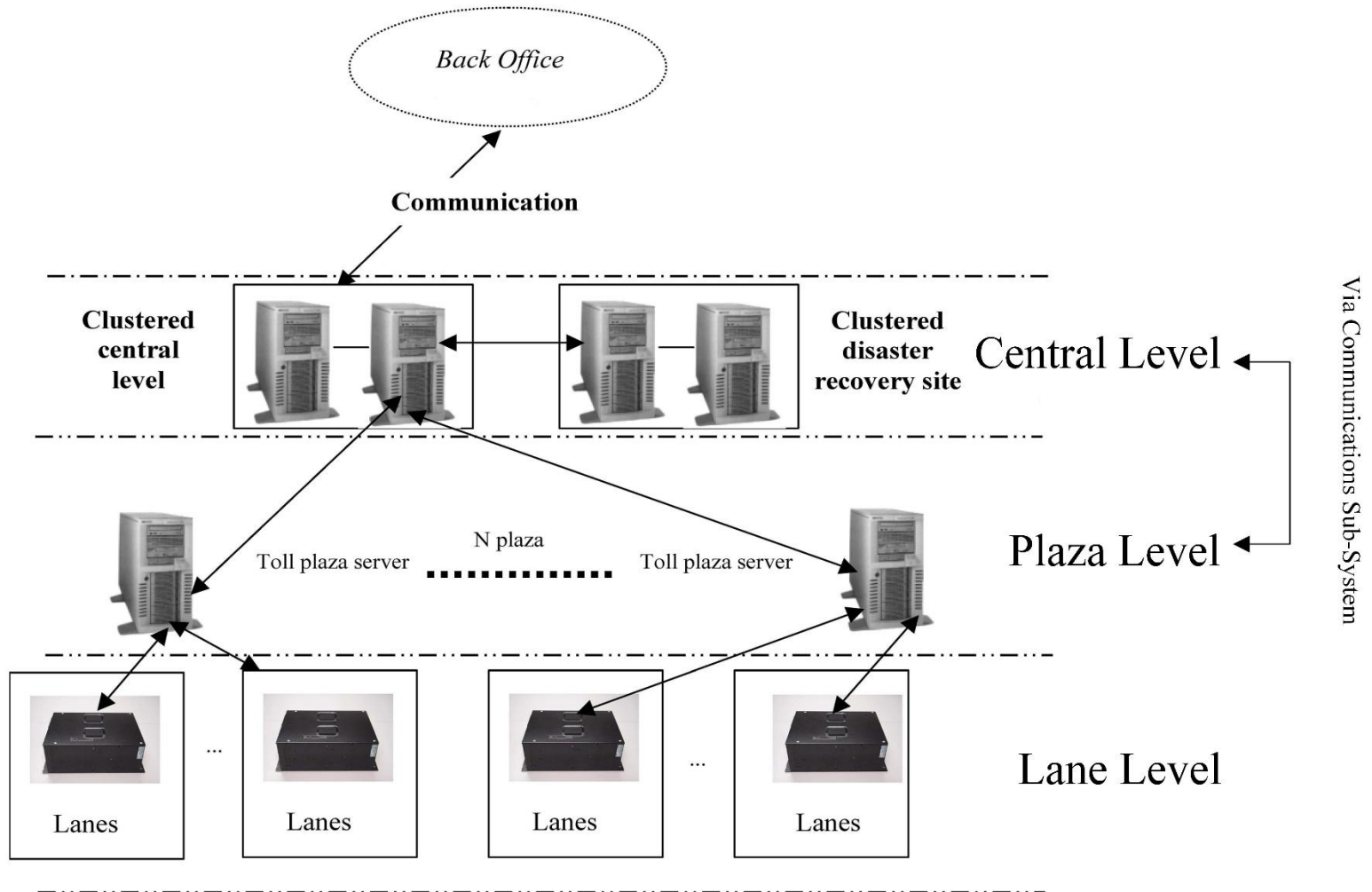


# TCS (Toll Collection System)

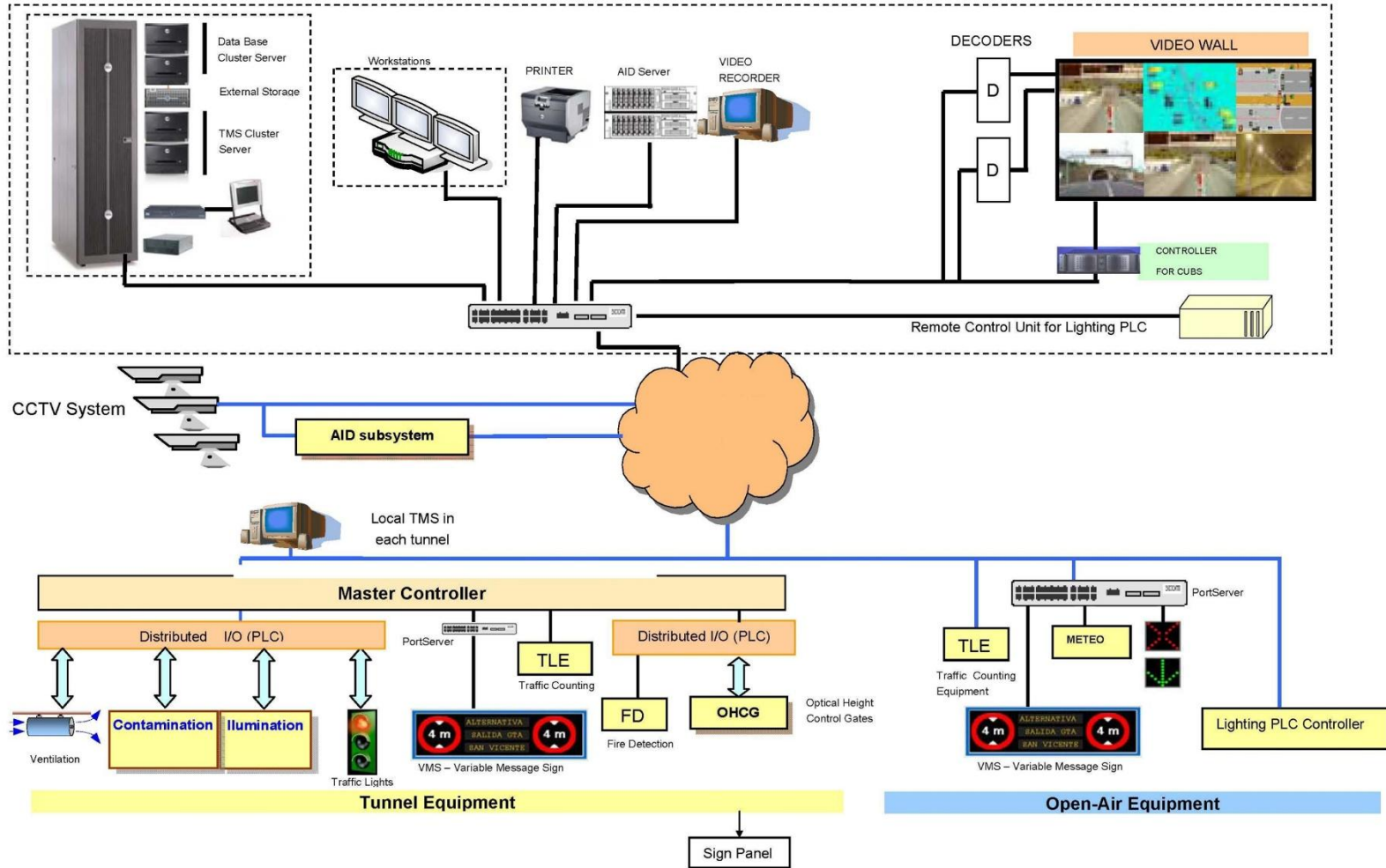
- Lane Level
- Plazas Level
- Central Level

# TCS (Toll Collection System)

## PATHE MOTORWAY – Toll System Architecture



# TMS (Traffic Management System)





# TMS (Traffic Management System)



Fiber Optic backbone network along the motorway



Vehicle Detection System



CCTV PTZ Cameras



Emergency Roadside Telephones

- GSM technology – Solar powered

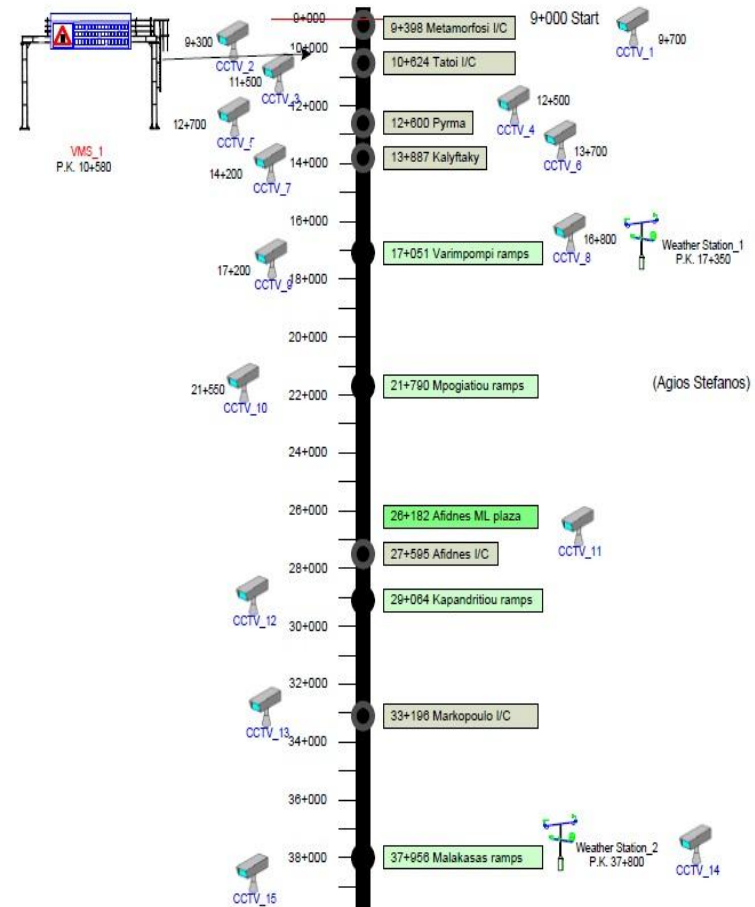


Variable Message Signs

- 1 Graphic zone & 4 lines



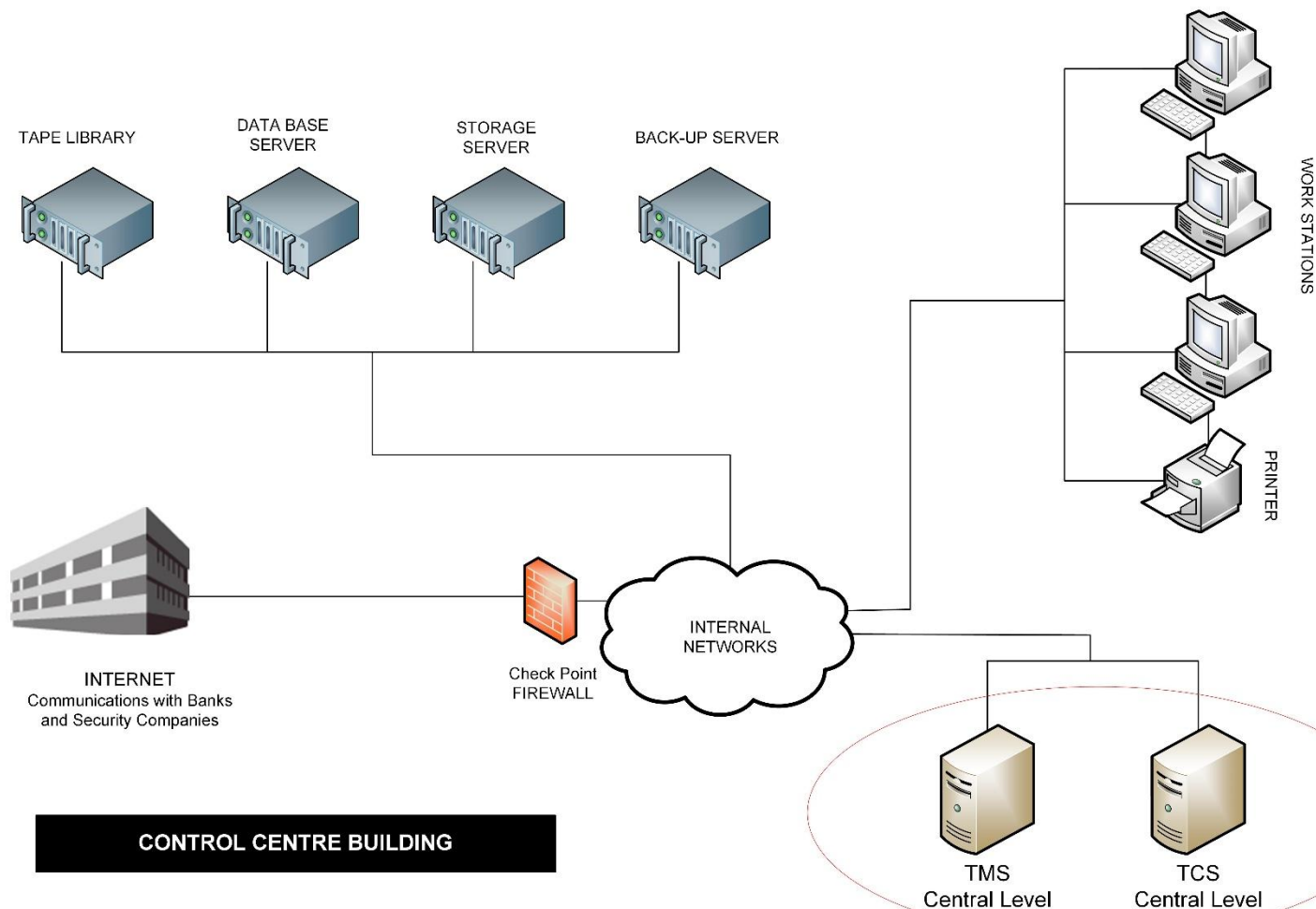
Weather Stations / Pollution Detectors





# BOS (Back Office System)

## PATHE MOTORWAY – Back Office Architecture



# Key Points



**Check Point**<sup>™</sup>  
SOFTWARE TECHNOLOGIES LTD.

**We Secure the Internet.**

**1**

Availability



**2**

Security



**3**

Monitoring



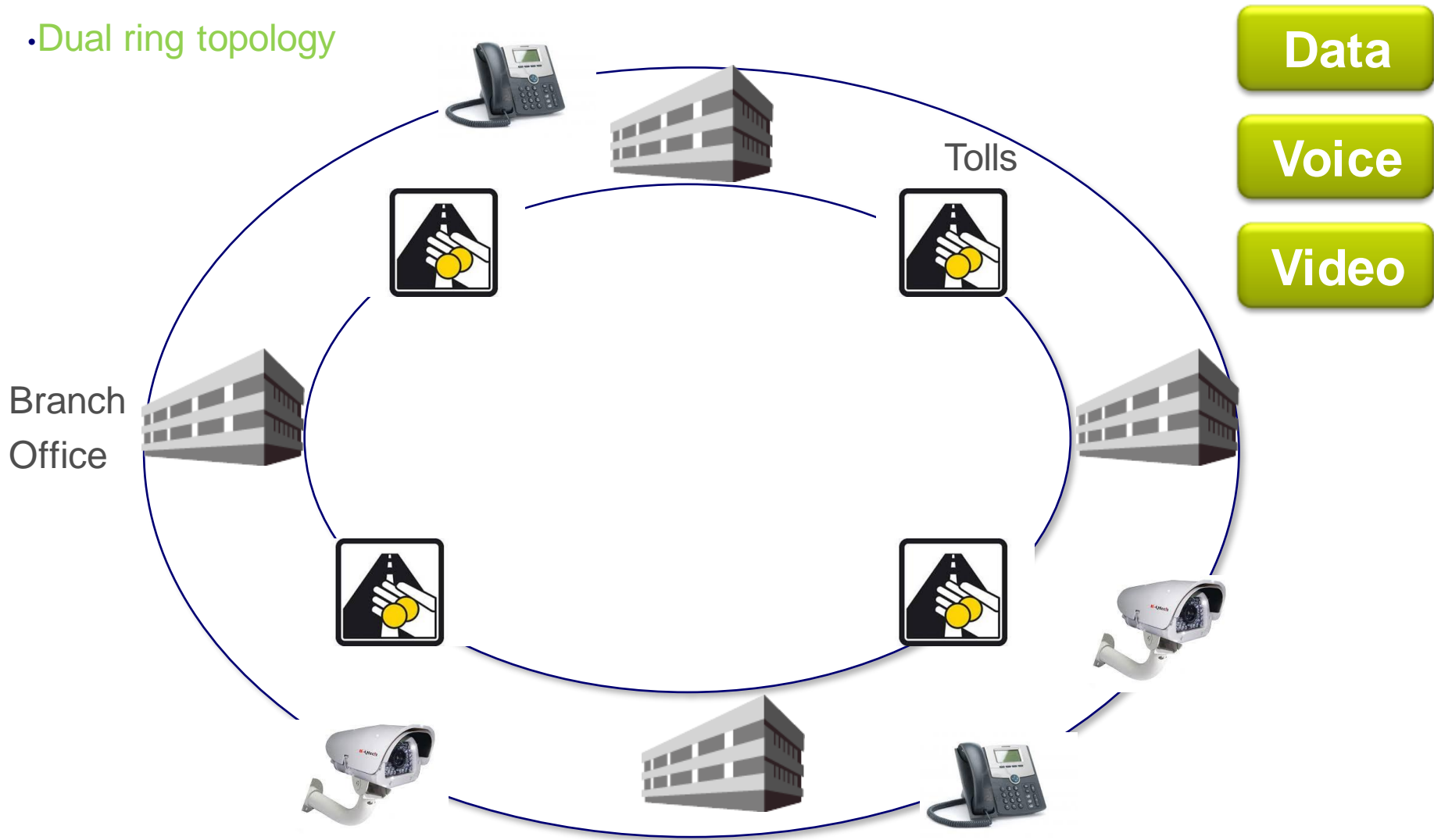
**4**

Access Control



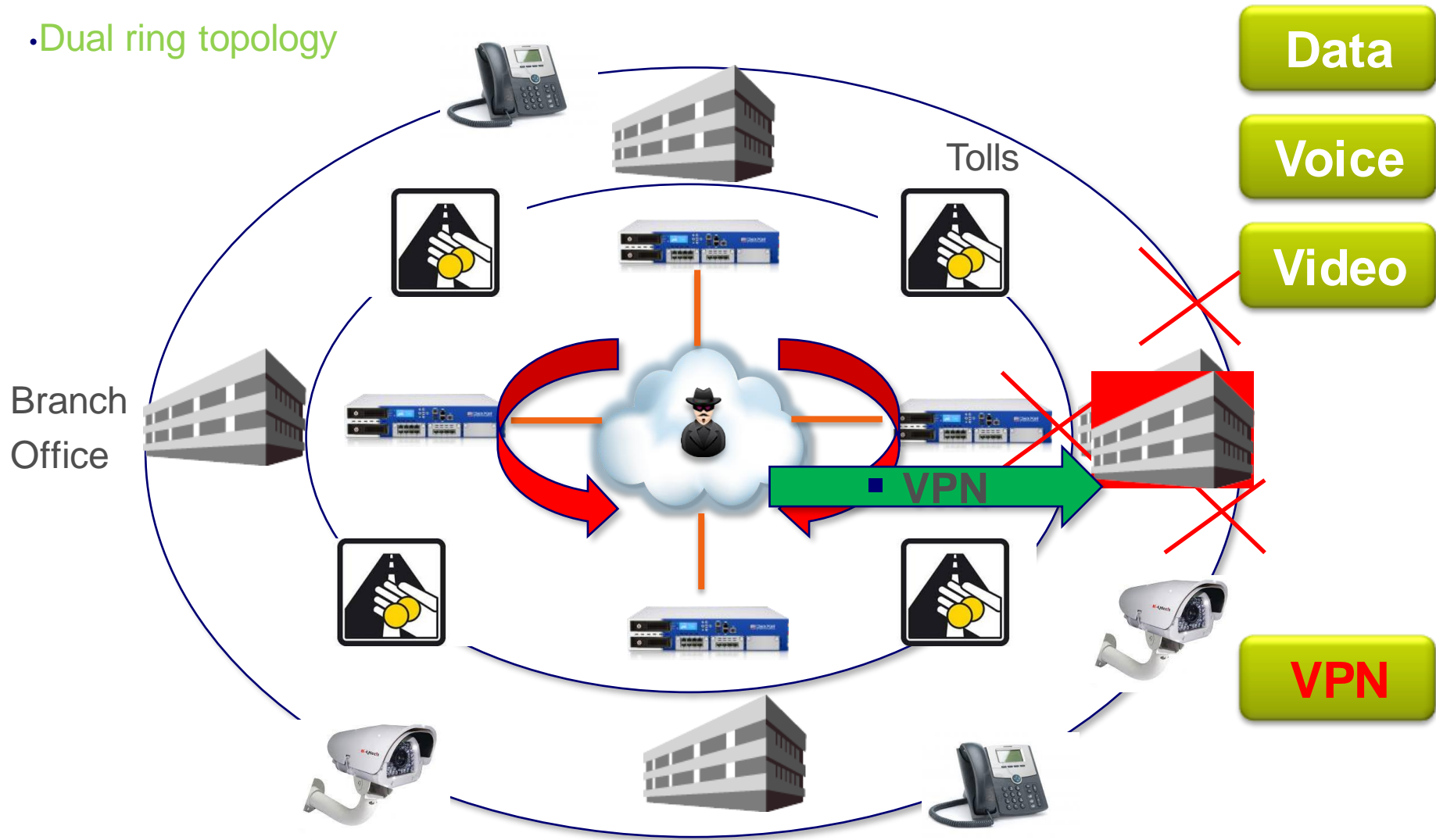
# Network and Security Architecture

- Dual ring topology



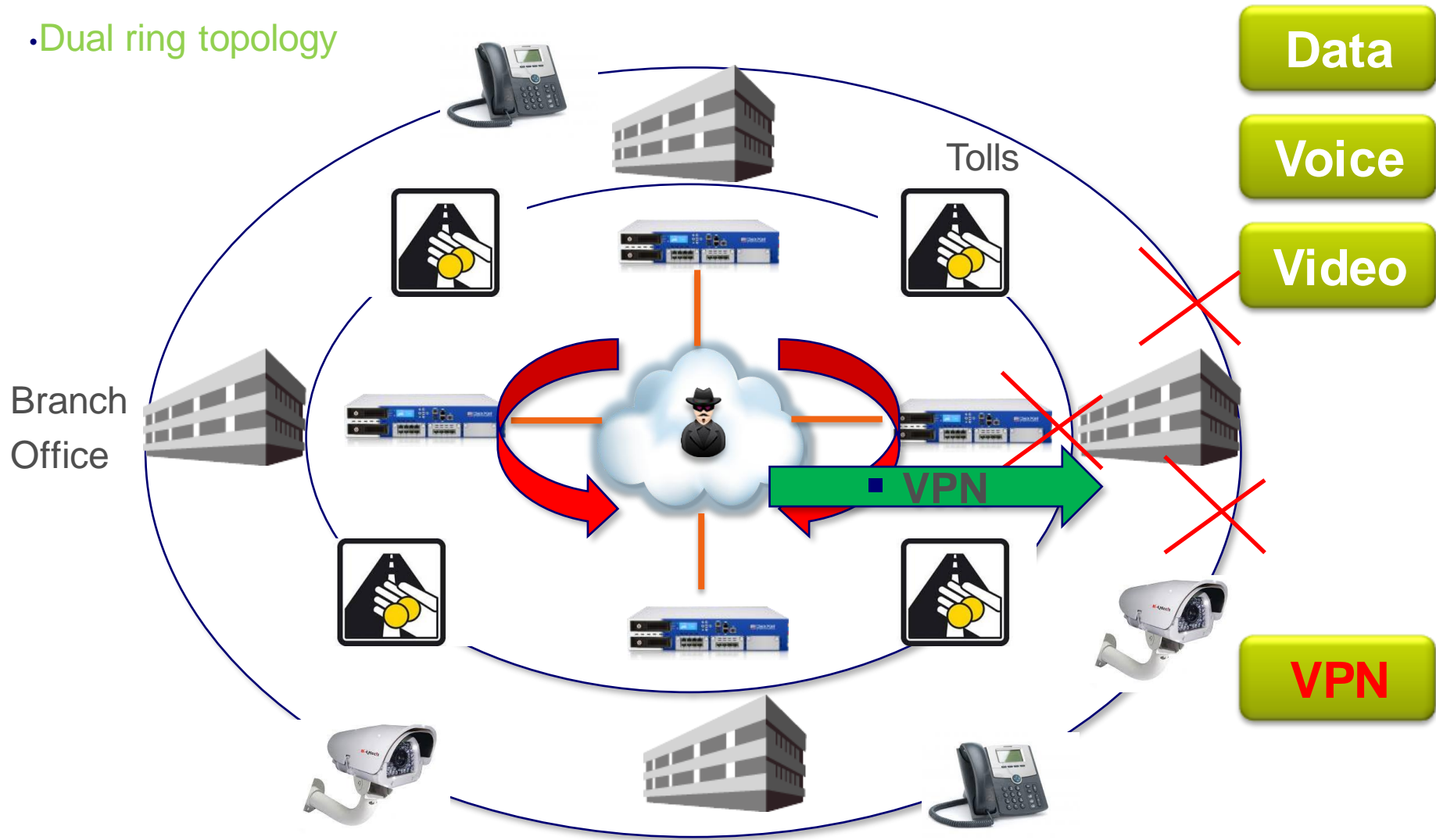
# Network and Security Architecture

- Dual ring topology

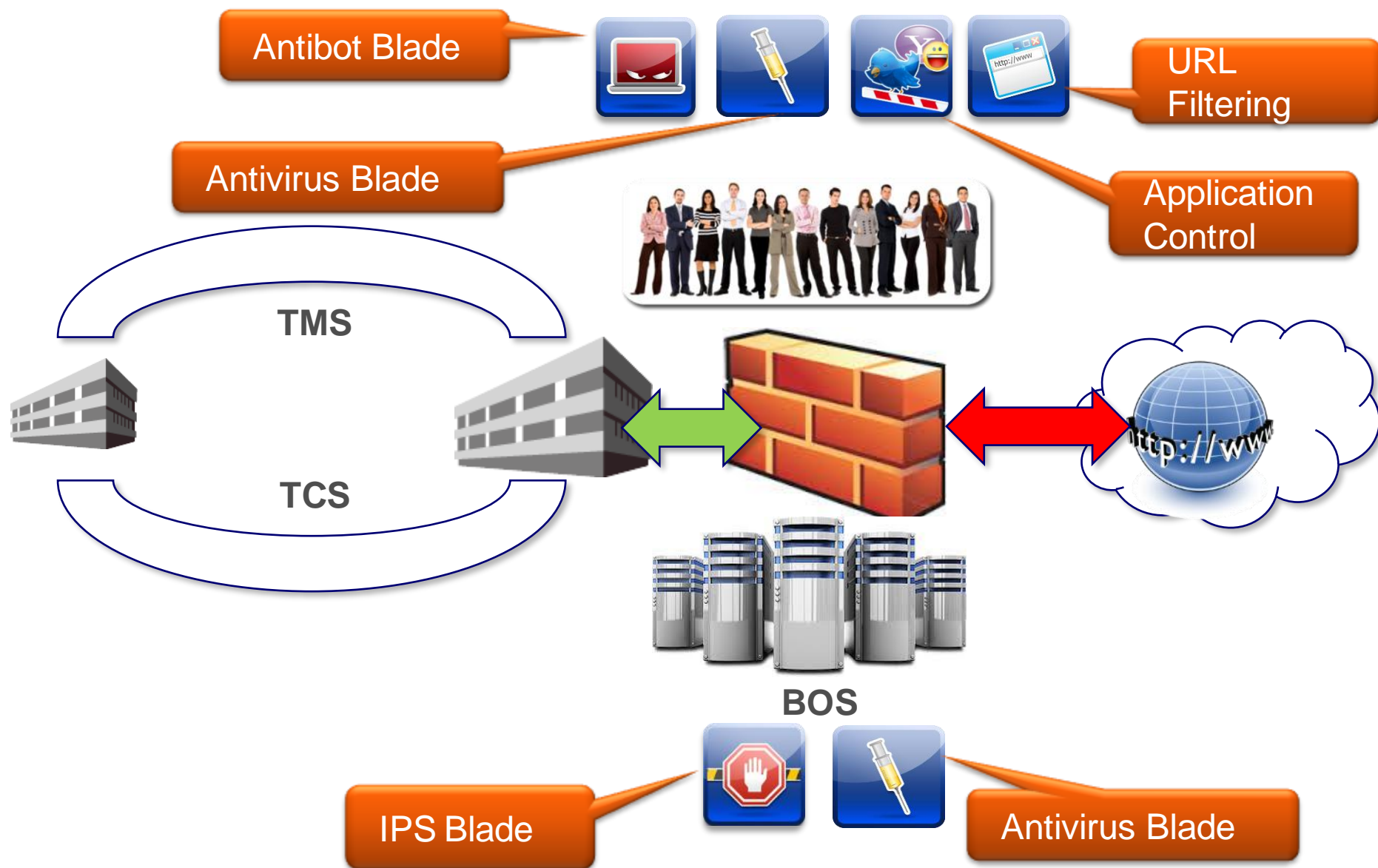


# Network and Security Architecture

- Dual ring topology

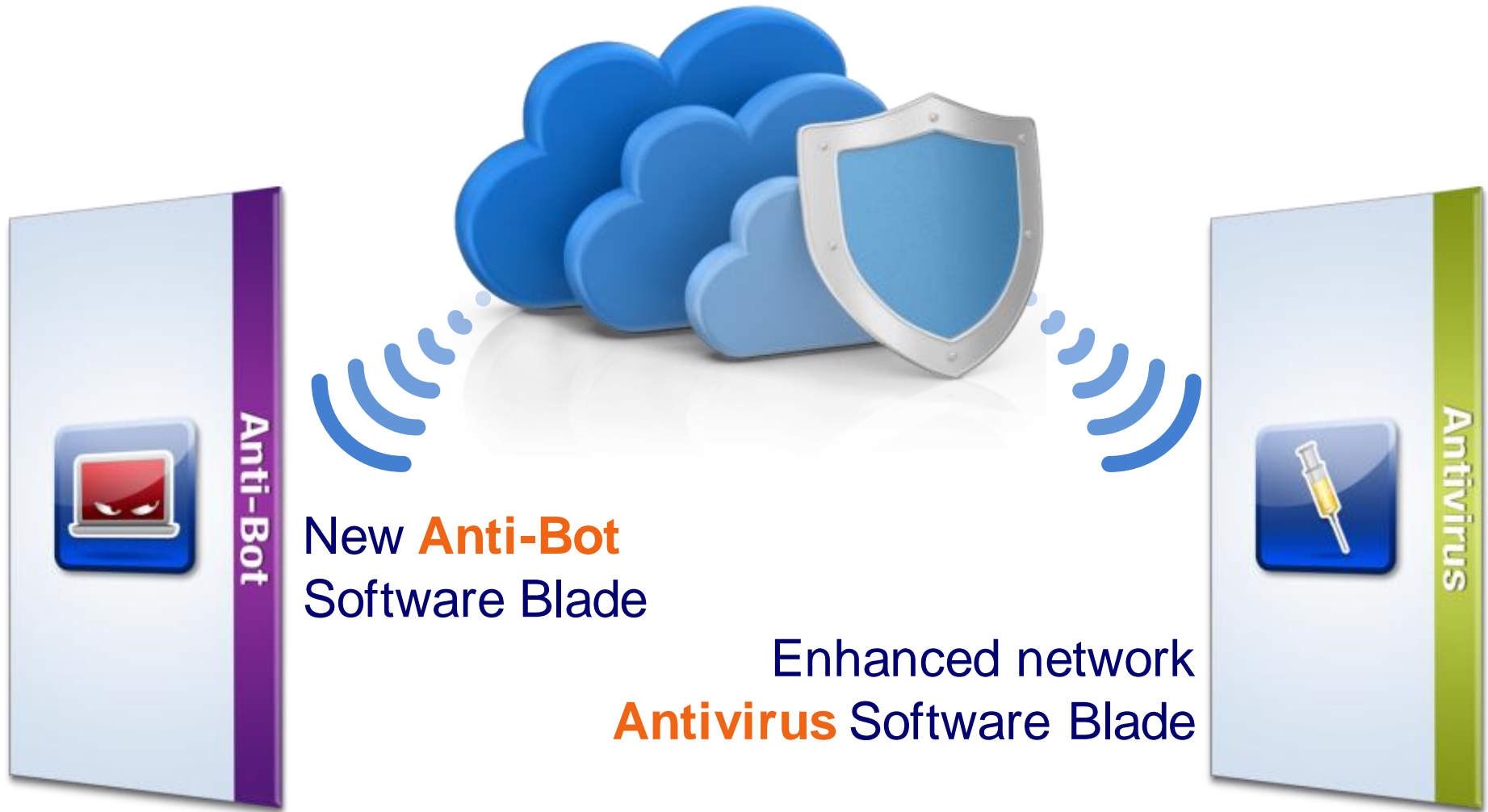


# Branch Anatomy



# Introducing the Most Comprehensive Threat Prevention Powered by ThreatCloud™

Security

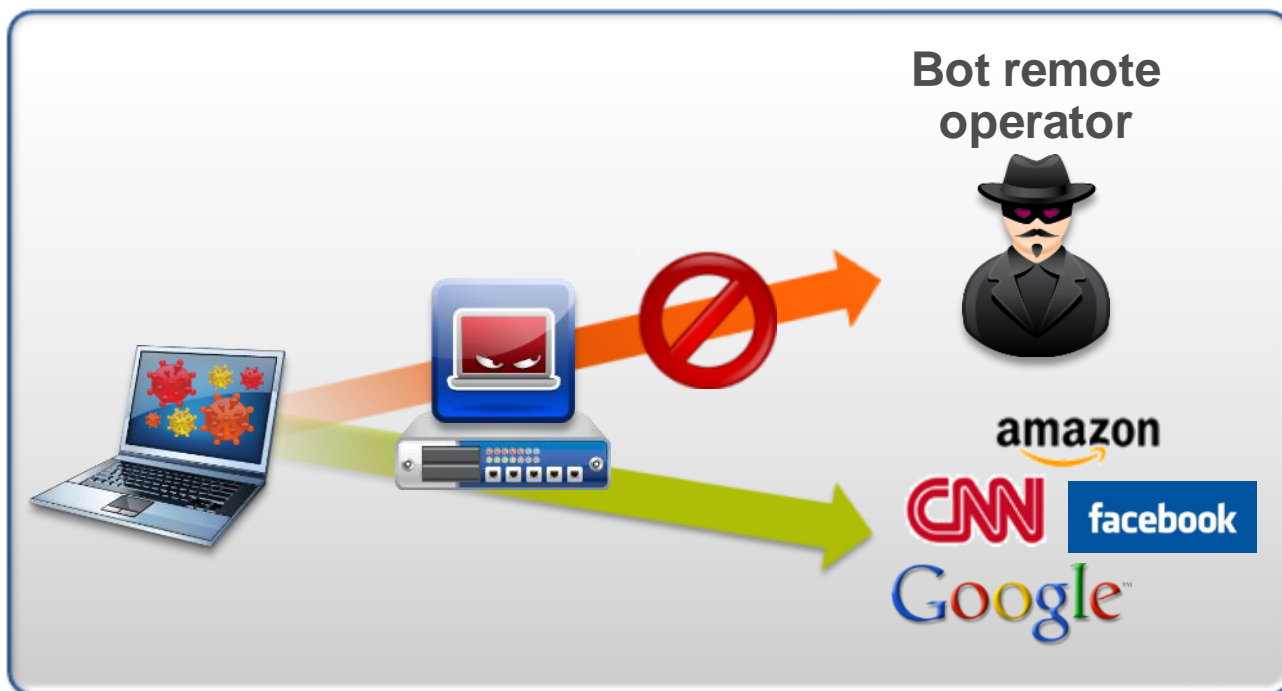




# Bot Damage Prevention



**Stop Traffic between  
Infected Hosts and Remote Operator**



**Stop  
Data Theft**

**Enable User  
Work Continuity**

# Bot Infections Investigation



## Extensive Forensics Tools



**Infected Users  
and Devices**



**Malware  
Type**



**Malware  
Actions**

 **Bot Incident:**  Prevent

 Copy Details  Actions  Anti-Bot Summary Details

 Frances Flash

 [Backdoor.WIN32.IRCBotg](#)  
(Signature)

 Prevented

 Communication with C&C

 High Severity

 High Confidence

 Today at 12:09:43

- Event Description:**

Malware Backdoor.WIN32.IRCBotg on  125.0.0.68 tried to locate its Command and Control server on  203.0.0.210 at 12:09:43 19 Mar 2012.
- Additional Data:**

**Destination:** [203.0.0.210](#)  
**Sent Bytes:** 38 Bytes  
**Received Bytes:** 112 Bytes



# Antivirus Software Blade

## Extended Protection Using ThreatCloud™

**Stop Incoming  
Malware  
Attacks**

**Protect with 300x  
More Signatures  
with ThreatCloud**



**Prevent  
Access to  
Malicious Sites**

**Over 300,000  
Malicious Sites**



**Unified View**

**See the Big  
Malware Picture**



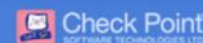
# Unified View of Anti-Malware



## See the BIG Malware Picture

### MALWARE REPORT

Monthly Report | September 1<sup>st</sup> 2011 - September 31<sup>st</sup> 2011 | Origin - London-GW



Anti-Bot Blade: ✔ Active Anti-Virus Blade: ✔ Active

Generated by Check Point SmartEvent<sup>®</sup>, on September 2nd 2011 10:35AM 1



**1290**

Protected Hosts

**70 Hosts**

Involved in Malicious Activity

**12 (2 new)**

Detected Malwares



**Top Hosts**

Involved in Malicious Activity

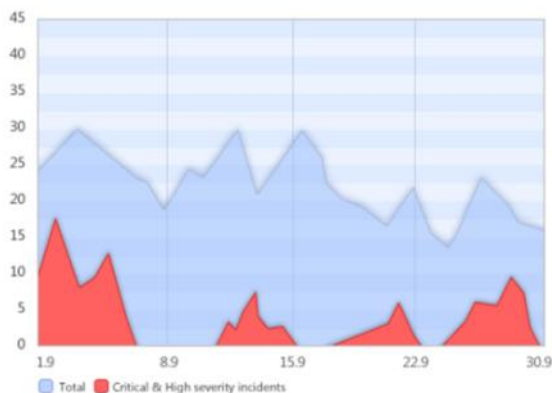
Dan.D-LapTop ..... **55 incidents**  
 John.S-Desk ..... **34 incidents**  
 Jane.P-Lab ..... **32 incidents**  
 Web.Server2 ..... **21 incidents**  
 Web.Proxy3 ..... **19 incidents**



**Top Malwares Found**

14 hosts infected in **Devestator**  
 10 hosts infected in **Welchia Blaster**  
 15 hosts infected in **Trojan.Downloader**  
 5 hosts infected in **Z.bot**  
 5 hosts infected in **SpyEye**

### Incidents in the Last Month



**600**

Malicious Incidents

**400** Prevented

**200** Detected

**135MB** Total Sent

**20MB** Total Received

C&C Communication / Data Leak

71 12 85 ↓ -81

DDOS Attacks

78 42 120 ↑ 24

Self Distribution Attempts

90 90 180 ↑ 35

Click Fraud Hits

42 36 78 ↓ -5

Outgoing Spam Mail

40 95 135 ↑ 90

Legend: ■ Prevent ■ Detect (Policy can be modified to prevent more or all incident types)  
 ↑ ↓ In comparison to previous month

# The Problem with Internet Applications

Security

## 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 Mills

June 24, 2009 4:59 PM PDT

VC's automated **Twitter**  
Feed spreads malware

by Elinor Mills

## 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

# Application Detection and Usage Controls

Security

## Application Detection and Usage Controls



Source	Destination	Action	
 Any	 Internet	 Block	
 Any	 Internet	 Social Networking	 Inform (once a month)
 Support	 Any	 Skype	 Allow



Enable access for support team

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

# Need to Control All Aspects of Web



## Websites



[www.poker.com](http://www.poker.com)



[www.hackthissite.org](http://www.hackthissite.org)



[www.playboy.com](http://www.playboy.com)



[www.fantasyfootball.com](http://www.fantasyfootball.com)

## Applications



Not URL-based



Facebook Chat

Granularity  
beyond URLs

# Unified Control Needed !



# Check Point Unifies URL Filtering and Application Control









Security

Unified Control of All Aspects of Web Security



Websites —  
URL Filtering

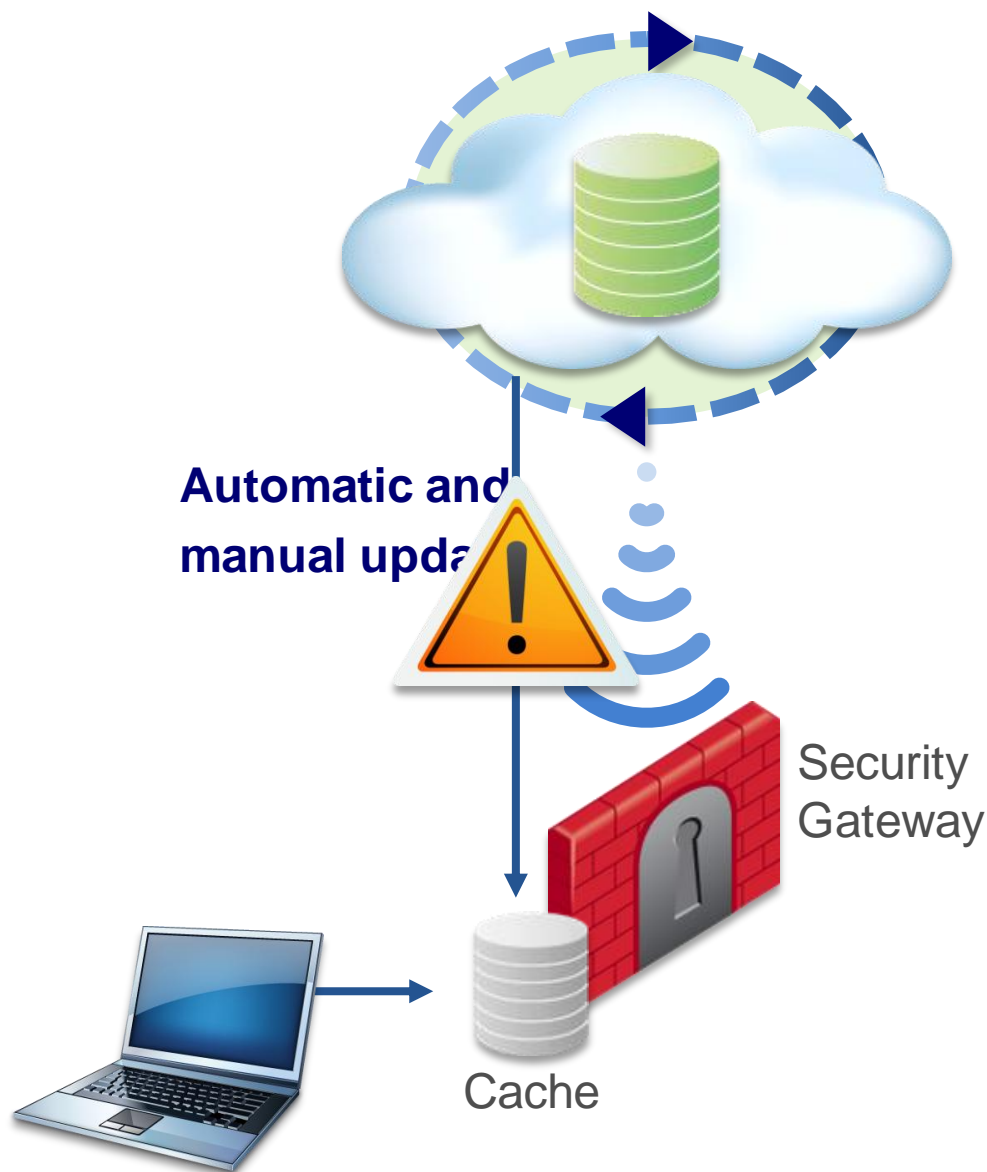
Unified categories —  
URLs and applications

Source	Sites / Applications	Action
 Any	 Violence  Games	 Block
 Marketing	 Media Streaming  Skype	 Allow

User/Group  
Granularity

Applications —  
Application Control

# URL Filtering Dynamic Categorization



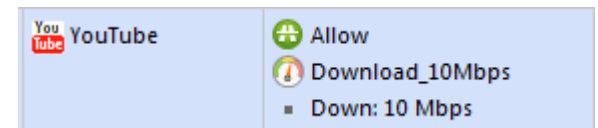
Database constantly updated

**99.2%** of queries are met by cache!

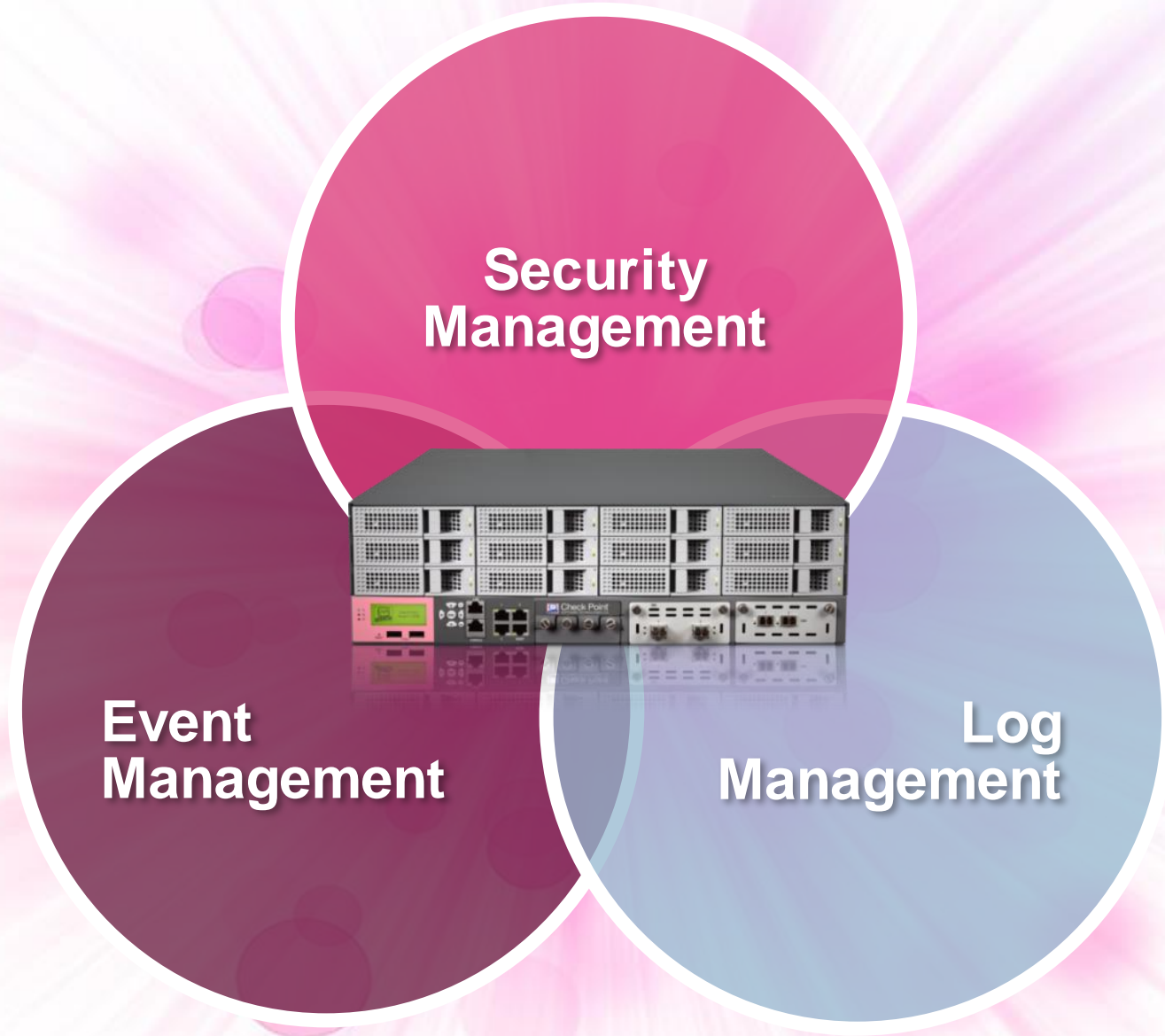
Remove compromised websites from cache

# Qos (Application Layer)

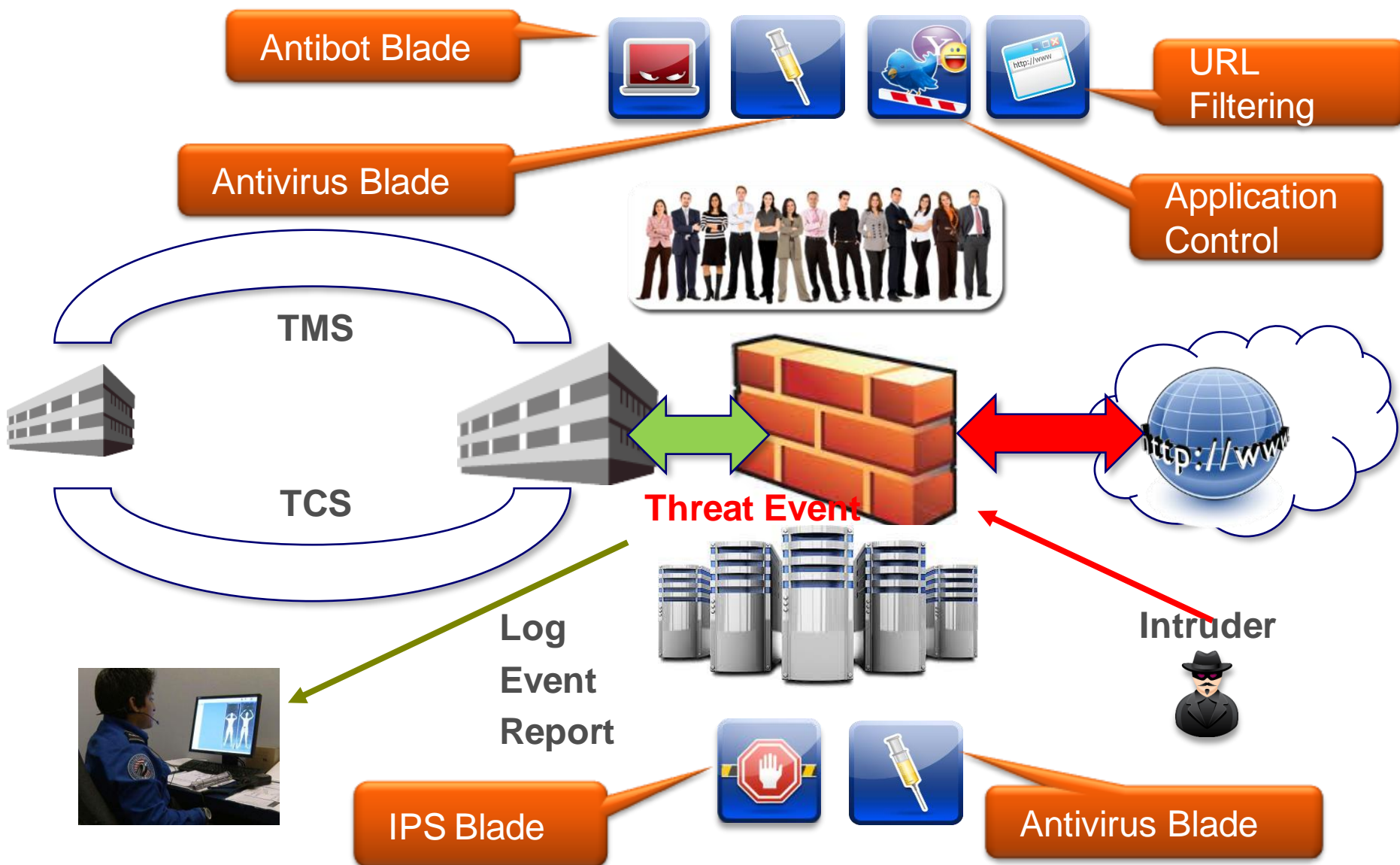
- L3 Quality of Service Rules
  - Limitation
  - Guarantee
  - Prioritization
  
- L4 Quality of Service Rules
  - Limitation
  - Guarantee
  - Prioritization
  
- Application Layer Allow/Block
  - Limit
  - Inform/ask



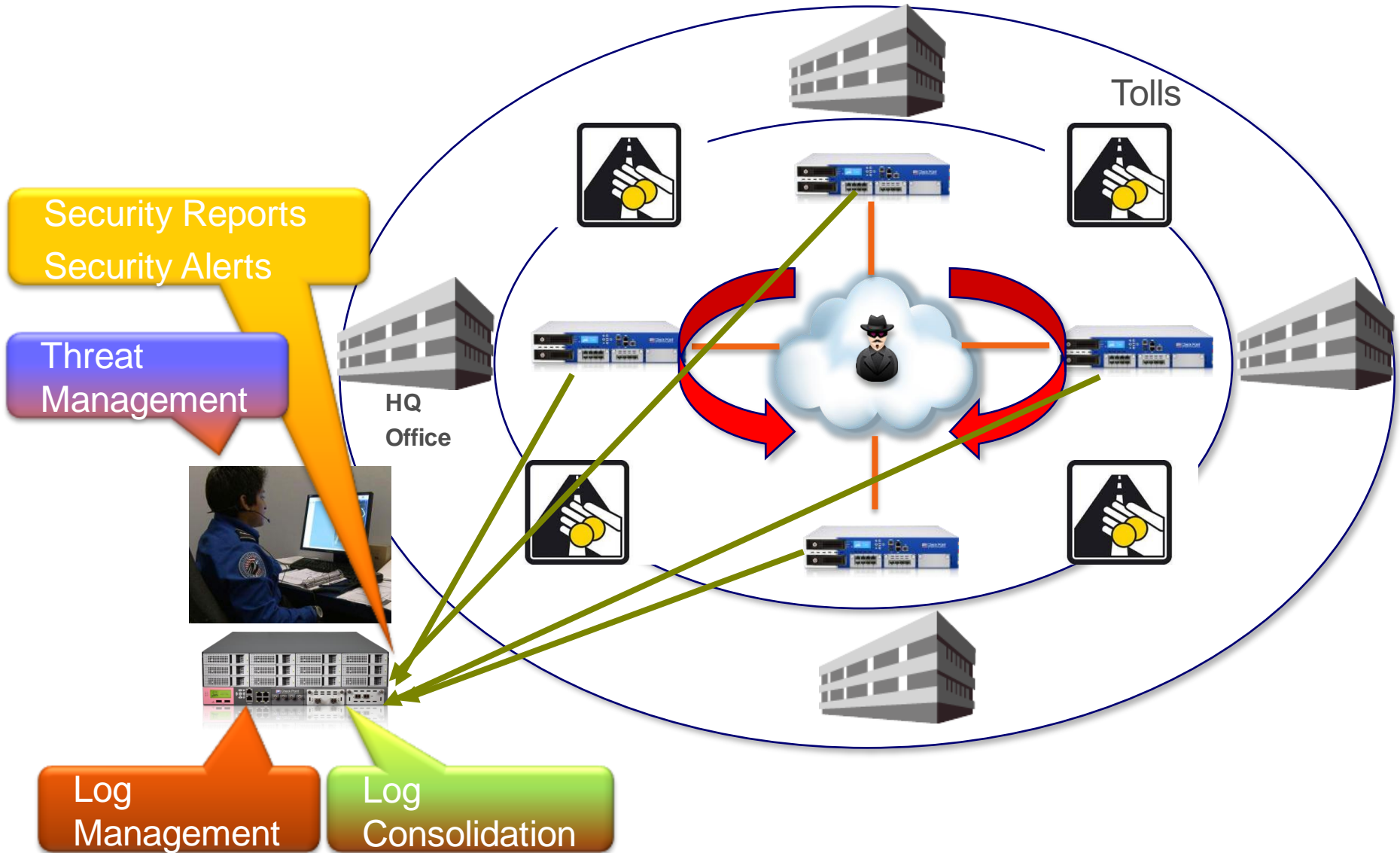
# Consolidated Security Management



# Security Threat Management




# Centralized Management and Monitoring



# Enjoy your results


Record Details



Previous Next Copy Details

URL Filtering:  Block

Administrator (Administrator) was blocked access to galleryofguns.com from Host 172.16.0.2 today at 23:13:33

Details	
Name	* galleryofguns.com (Weapons)
Matched Category	Weapons
All Categories	Weapons, URL Filtering
Risk	Unknown
URL	<a href="http://www.galleryofguns.com/">http://www.galleryofguns.com/</a>

Policy	
Action	 Block
Rule Name	<a href="#">Go to Policy</a>
Policy Name	Standard
Policy Date	Wed Nov 06 22:35:51 2013
Policy Management	gw-r77

More	
User Check	1
Client Type	Microsoft IE 8.0
Server Type	Microsoft-IIS
Product Family	 Network
Log ID	9999
Origin	gw-r77
Number	260310
Type	 Log
Information	---
Time	Nov 6, 2013 at 23:13:33
UserCheck ID	C1453447-72F4-1BD8-C0DF-15979D153D58

User Check	
Message to User	Access to galleryofguns.com is blocked accord... >>
Confirmation Scope	For each application
Frequency	1 days

Traffic	
Source	Host_172.16.0.2 (172.16.0.2) Administrator (Administrator) win2k3@vmware.local
Destination	63-156-49-12.dia.static.qwest.net (63.156.49.12)
Protocol	TCP tcp
Service	http (80)


Check Point UserCheck - Windows Internet Explorer

http://172.31.0.20/UserCheck/PortalMain?IID=C1453447-72F4-1B...


File Edit View Favorites Tools Help

Check Point UserCheck

## Check Point Application Control



### Page Blocked

Access to  galleryofguns.com is blocked according to the organization security policy.

Category: Weapons

Click [here](#) to report wrong category

For more information, please contact your helpdesk.

Done

Internet



# Enjoy your results

Record Details

Previous Next Copy Details

**Application Control:** Inform User

Administrator (Administrator) tried to access Twitter from Host 172.16.0.2 and was asked to approve his access today at 23:14:37

Details	
Name	Twitter (Social Networking)
Matched Category	Social Networking
All Categories	Transmits Information, Instant Chat, Share vi... >>
Description	Twitter is a social networking and microblog... >>
Risk	Low
URL	<a href="http://twitter.com/">http://twitter.com/</a> <a href="#">Copy</a>

User Check	
User Response	Pending
Message to User	Please be reminded that according to the comp... >>
Confirmation Scope	For each application
Frequency	1 days

Traffic	
Source	Host_172.16.0.2 (172.16.0.2) Administrator (Administrator) win2k3@vmware.local
Destination	199.16.156.38
Protocol	TCP tcp
Service	http (80)

Policy	
Action	Inform User
Rule Name	<a href="#">Go to Policy</a>
Policy Name	Standard
Policy Date	Wed Nov 06 22:35:51 2013
Policy Management	gw-r77

More	
User Check	1
Client Type	Microsoft IE 8.0
Server Type	Other: tfe
Primary Category	Social Networking
Signature ID	10005480:1
Product Family	Network
Log ID	9999
Origin	gw-r77
Number	260335
Type	Log
Information	---
Time	Nov 6, 2013 at 23:14:37
UserCheck ID	CF970238-A861-1CF4-DEC7-9C781A425584

Check Point UserCheck - Windows Internet Explorer

http://172.31.0.20/UserCheck/PortalMain?IID=CF970238-A861-1...

File Edit View Favorites Tools Help

Favorites Suggested Sites Free Hotmail Web Slice Gallery

Check Point UserCheck

## Check Point Application Control

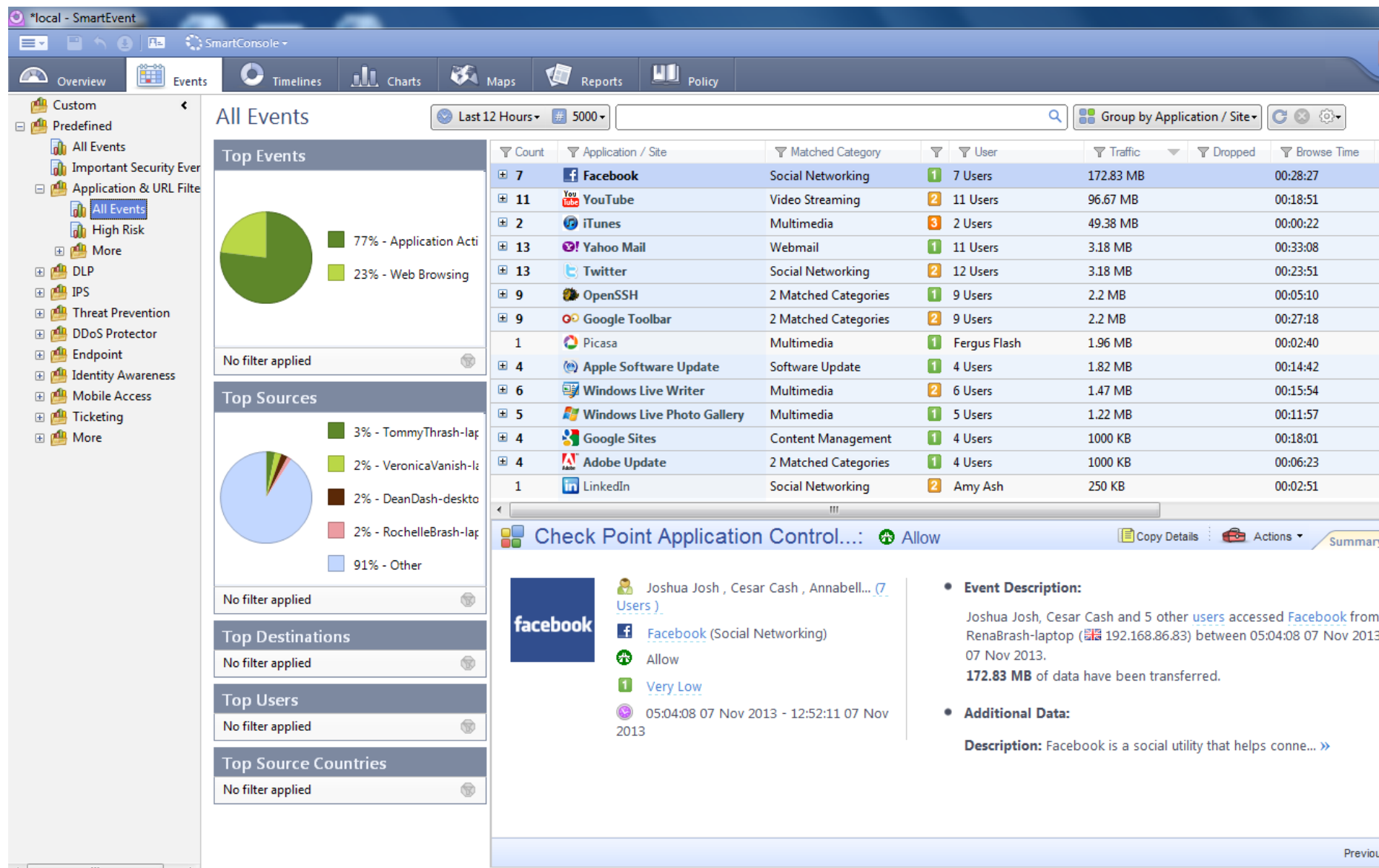
**Access Notification**

Please be reminded that according to the company policy, access to Twitter is intended for work-related use only.

Reference: CF970238-A861-1CF4-DEC7-9C781A425584

Done Internet

# Enjoy your results



# Unified Control and Deployment

## Centralized Management



The diagram illustrates a centralized security management architecture. At the center is a blue circle containing a white padlock icon with two circular arrows around it, signifying a central control or policy engine. Surrounding this central hub are five other circles, each connected to the center by a blue line. These peripheral circles represent different security domains: a blue circle with a white envelope and padlock (top-left), an orange circle with a white hand cursor (top-right), a red circle with a white keyboard (right), a green circle with a white key (bottom), and a yellow circle with a white hand and exclamation mark (bottom-left).

For Unified Control  
Across the Entire  
Security Infrastructure

The background shows a software interface for a security management console. The top navigation bar includes various security modules: Firewall, NAT, IDS, Anti-Spam & Mail, ECD VPM, Data Loss Prevention, Anti-Virus & URL Filtering, IPSec VPN, QoS, and Desktop. The main content area displays a 'Data Loss Prevention (DLP) Policy' configuration page. It features a 'Grouping' dropdown set to 'By Category' and a search bar. Below this is a table listing DLP policies.

Source	Destination	Action	Comments
My Organization	* Outside	Ask user	3
My Organization	* Outside	Detect	2
My Organization	* Outside	Ask user	
My Organization	* Outside	Inform user	
My Organization	* Outside	Detect	
My Organization	* Outside	Detect	2

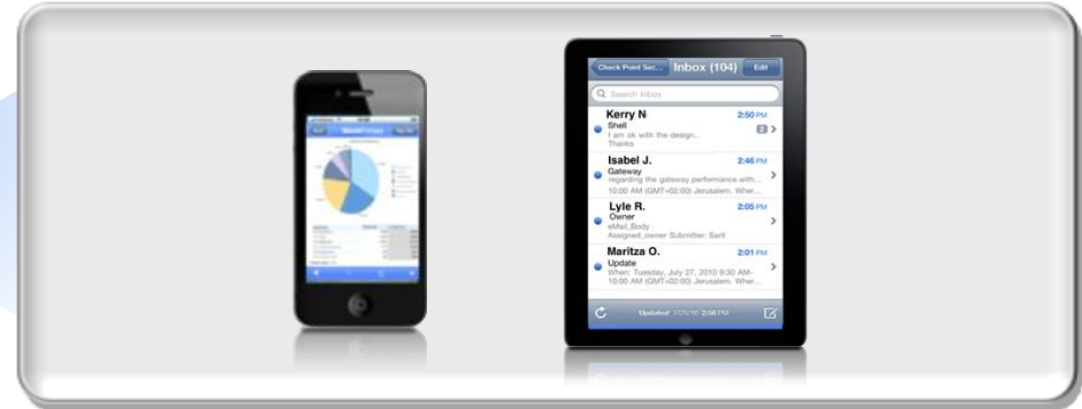
The bottom status bar shows a red flag icon, a bar chart, and a 'HIPAA' label.

## Mobile Platforms Are Becoming an Essential and Standard Business Tool

**Smartphones  
and tablets...**



**...accessing  
email, Web and  
business  
applications**



# Flexible Connectivity from Any Mobile Device

Access Control

Secure access from smartphones and tablets



**Secure Web Portal**

**VPN App**

Secure access from other devices



**Secure Web Portal**



**Mobile Access  
Software Blade on a  
Check Point Gateway**

# Simple to Connect to Business Portal

Access Control

1

Tap  
“Check Point Mobile”



2

Enter your password



3

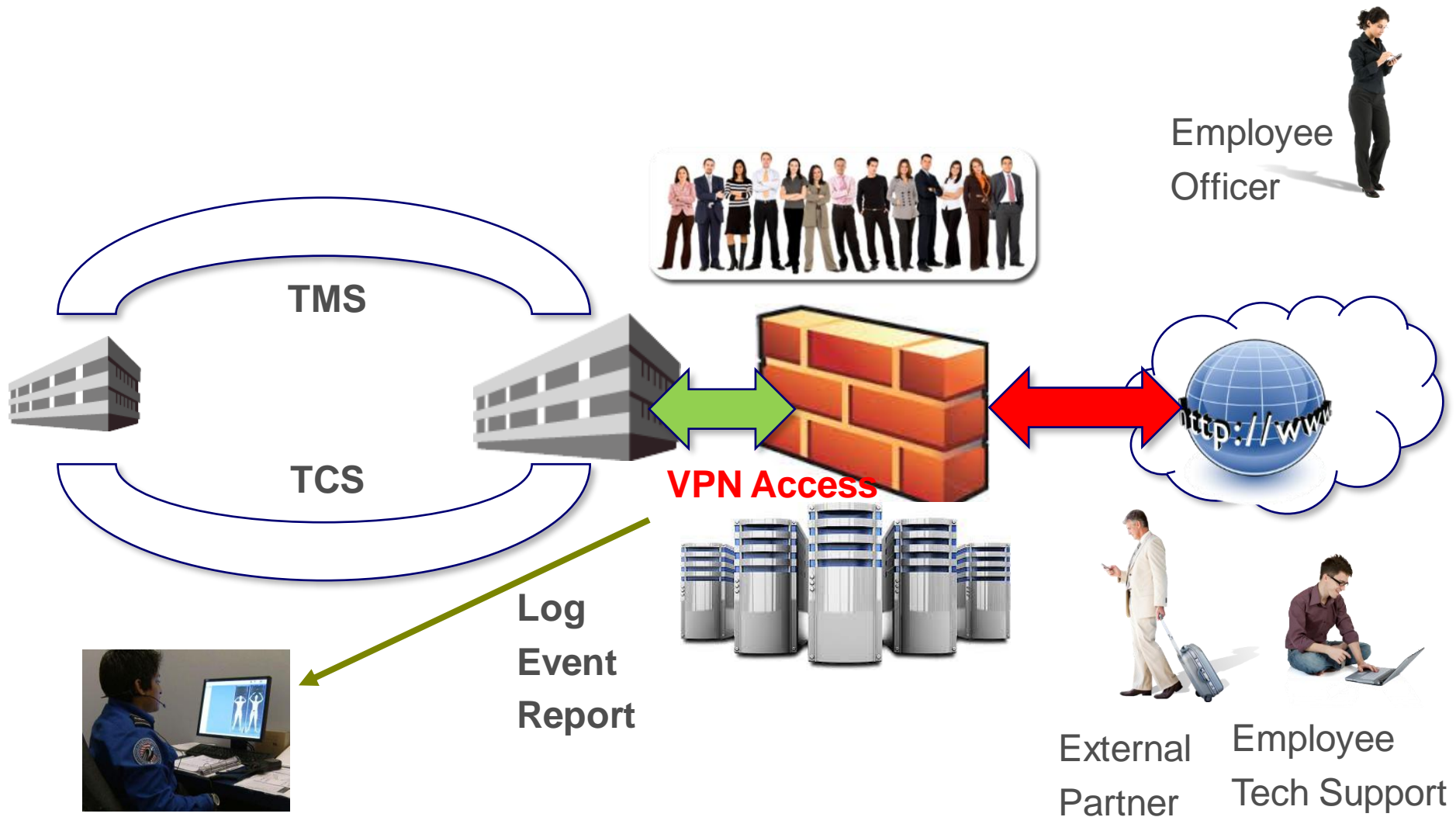
Gain secure access  
to your data  
through portal





# Remote Access Control

Access Control







Tsiairis Konstantinos  
Security Designer



Sakelaridis Theofanis  
IT Manager



Thank You