



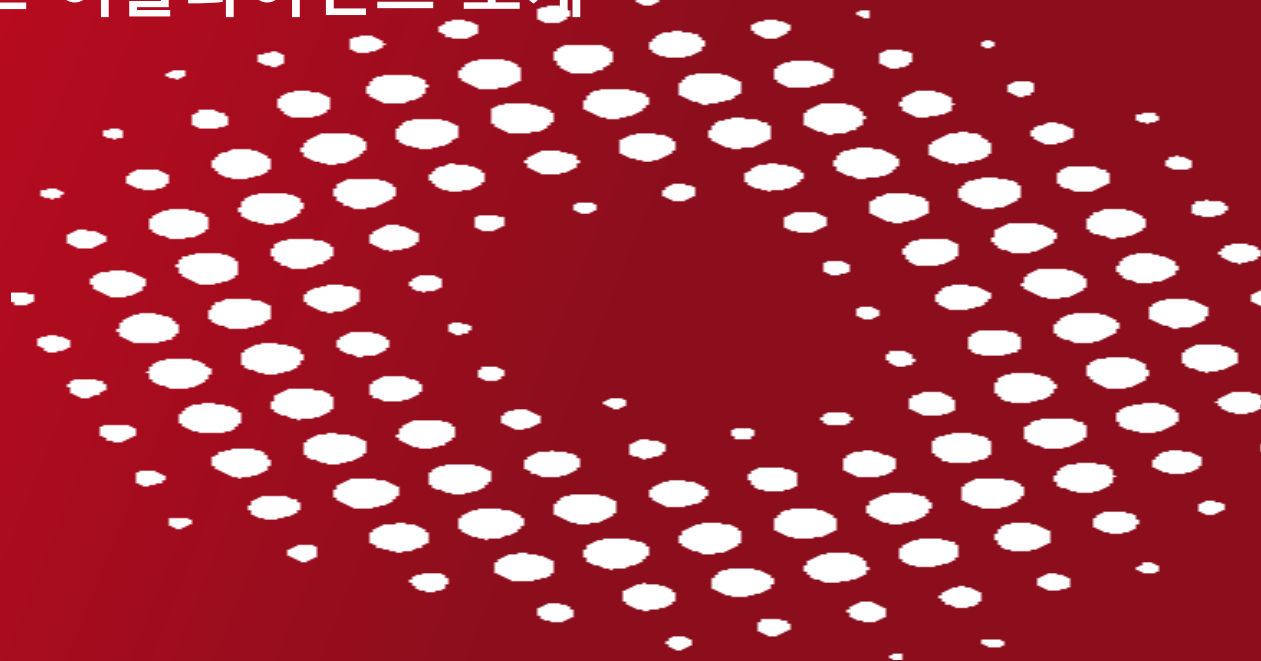
# 체크포인트 차세대 통합보안솔루션



(주)Innerinfo

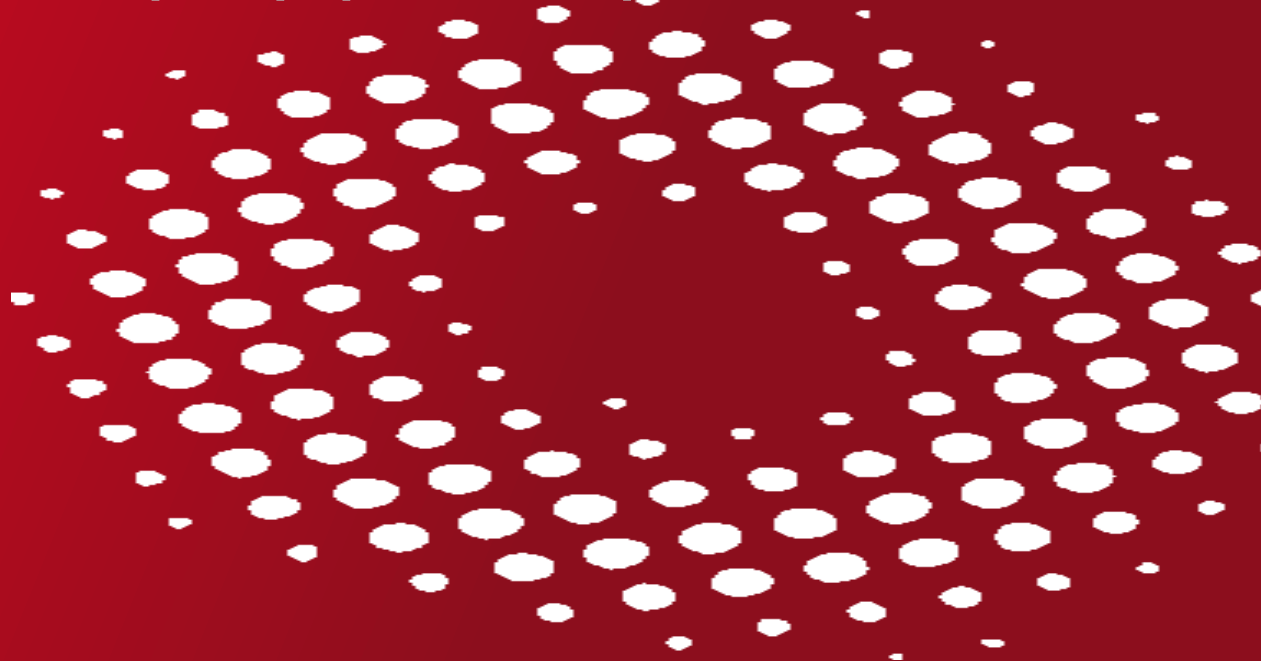
# Contents

1. 체크포인트 회사 소개
2. 체크포인트 제품 소개
3. 체크포인트 어플라이언스 소개



# Contents

1. 체크포인트 회사 소개
2. 체크포인트 제품 소개
3. 체크포인트 어플라이언스 소개



## Leader

- ▶ 세계적인 방화벽, VPN, 데이터 암호화의 리더
- ▶ 170,000개 이상의 프로젝트 수행
- ▶ 6천만 명의 사용자
- ▶ Fortune紙 선정 500대 모든 기업이 고객

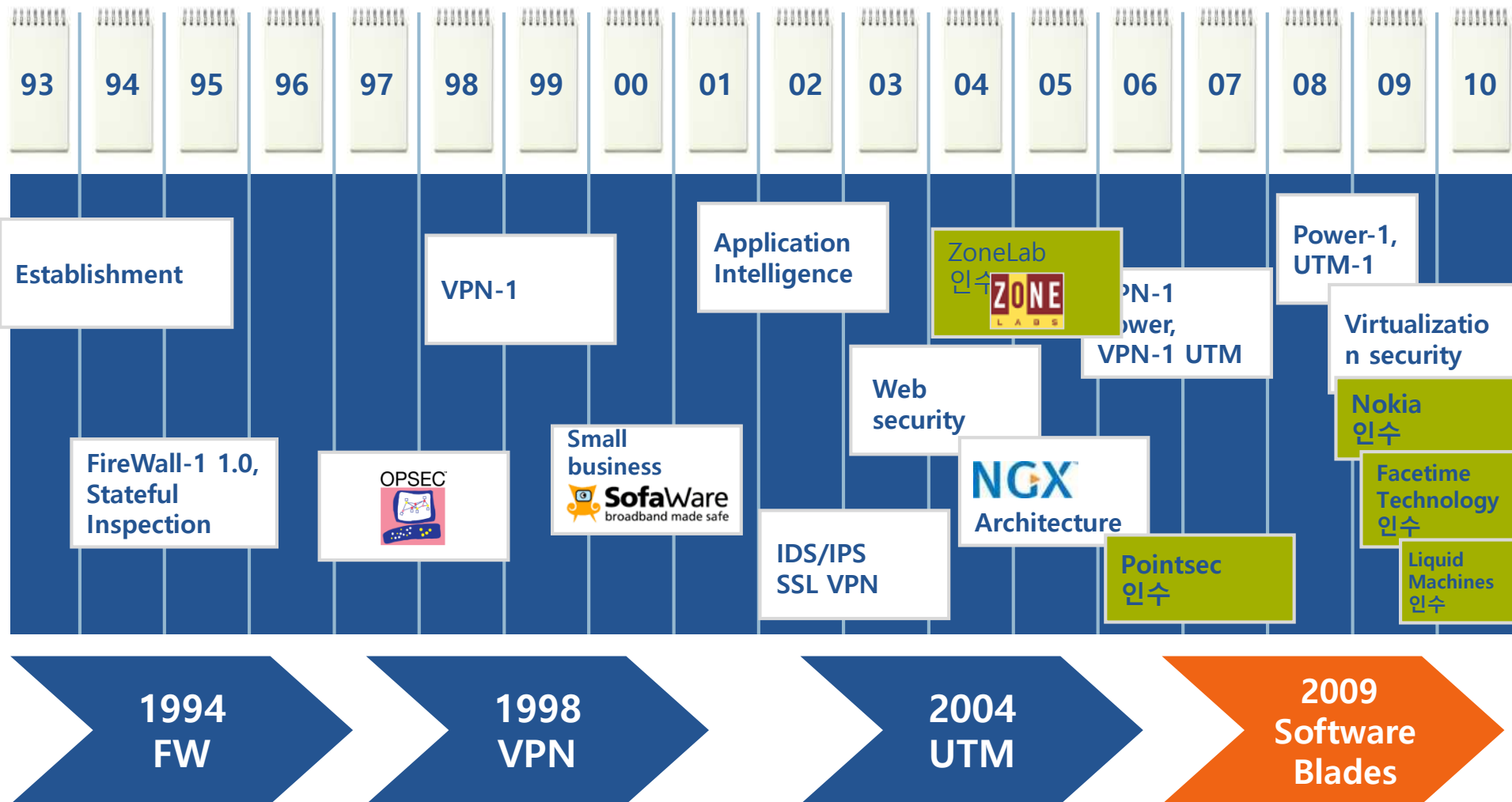
## 100% Security

- ▶ 100%, 회사의 모든 역량을 보안에만 집중
- ▶ 1,500 이상의 보안 전문가
- ▶ 전 세계 66,000명의 Check Point 공인전문가 보유
- ▶ Firewall-1 에서 software blade 까지

## Global Footprint

- ▶ 직원 수 2,300명, 이스라엘과 미국에 본사를 두고 30개국 80개의 지사 보유
- ▶ 88개국 3,000 partners 보유
- ▶ 전 세계 250개 지역의 물류 창고 보유
- ▶ 120개의 공인 training centers

# 혁신의 역사



## \$1.25 Billion (Revenue)

2011 revenue, 17% CAGR 2006-2011  
Software Blades fueling growth

## 100% (Security)

Pure focus on security  
All of Fortune 500 are Check Point customers

## #1 (Threat Coverage)

Best coverage for Microsoft and Adobe vulnerabilities  
Largest Web 2.0 application control library

**당신의 비즈니스를 보안하기 위해 어떤 벤더를  
신뢰하시겠습니까?**

# 보안제품 수상 경력

**Best IPS/IDS Product  
Reader Trust  
Award**



**2012**

**Leader, Magic  
Quadrant Enterprise  
Network Firewall**

**Gartner**

**2004–2011**

**Leader, Magic  
Quadrant Mobile  
Data Protection**

**Gartner**

**2001–2011**

**Leader, Magic  
Quadrant - UTM**

**Gartner**

**2010–2011**

**Network Security  
Vendor of the Year**



**2011**

**Computing Security  
Awards Encryption  
Product of the Year**



**2011**

**NGFW Earns  
"Recommend"  
Rating from NSS**



**2011**

**IPS Earns  
"Recommend"  
Rating from NSS**



**2011**

**Best Buy,  
Endpoint Security**



**2011**

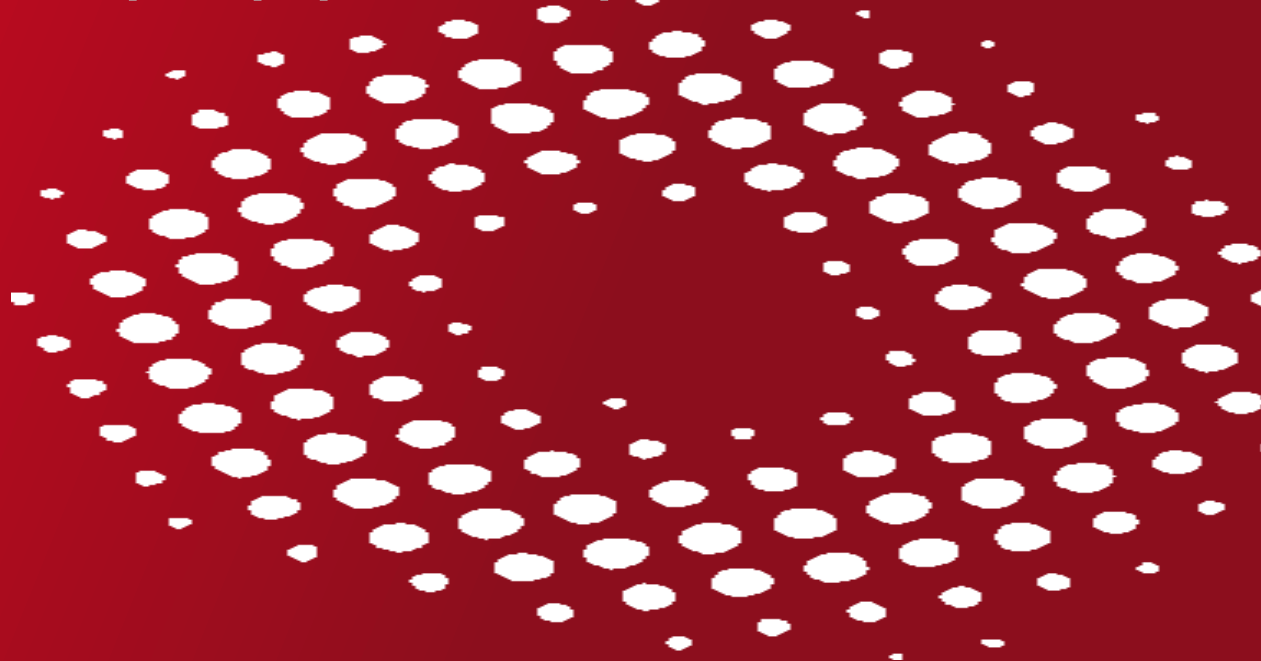
**IT Product of the  
Year – DLP  
Computerworld  
Czech Republic**



**2010**

# Contents

1. 체크포인트 회사 소개
2. 체크포인트 솔루션 소개
3. 체크포인트 어플라이언스 소개



# 체크포인트 - 모든 네트워크 환경을 보호

Network  
Perimeter



Branch Office  
Solution



Internal  
Networks



Data Center &  
Cloud Security



## 보안 소프트웨어 블레이드 아키텍처 개요

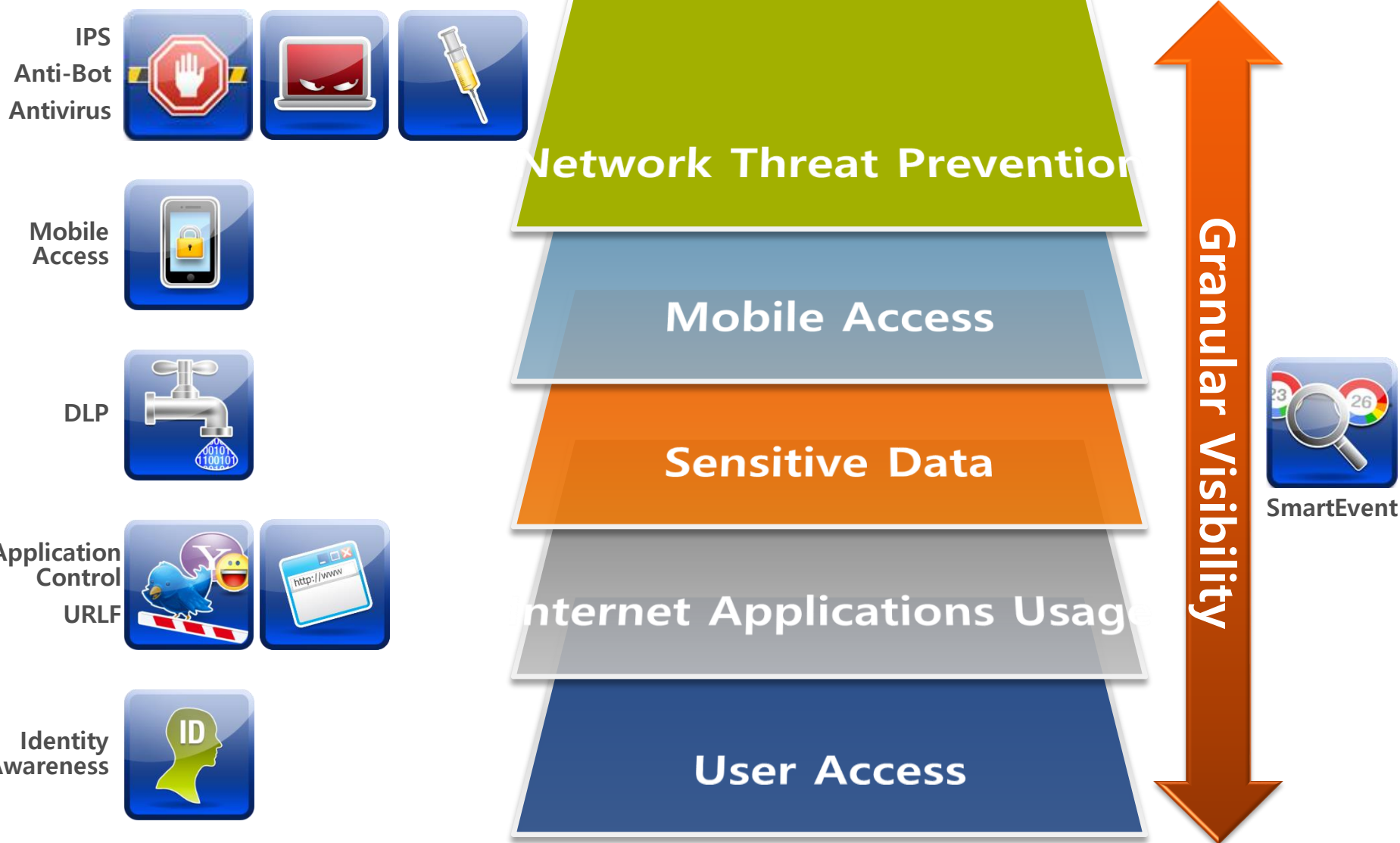


- 소프트웨어 블레이드 : 보안 기능을 수행하는 독립된 소프트웨어 모듈
- 소프트웨어 블레이드 종류 : 방화벽, VPN, IPS, 어플리케이션 컨트롤, URL 필터링, 안티바이러스&멀웨어, 안티스팸, 모바일 액세스, DLP, 안티봇 등

### 소프트웨어 블레이드의 특징

- 유연성 : 비즈니스 요구에 따라 블레이드를 선택적 확장
- 단순함 : 한 개의 벤더, 한 개의 OS, 통합로그, 통합관리
- 보안성 : 다양한 보안기능을 통해 높은 보안수준 달성

# 모든 보안 계층을 통제



# 진정한 차세대 방화벽

## UTM + Package



URL Filtering



Antivirus &  
Anti-Malware



Anti-Spam  
and Email  
Security



Anti Bot  
Software Blade

## DLP + Package



DLP

## On Every New Appliance...



Firewall



IPsec VPN



Identity  
Awareness



IPS



Application  
Control



Advanced  
Networking &  
Acceleration



Mobile  
Access  
(5 Users)



Network  
Policy  
Management



Logging &  
Status

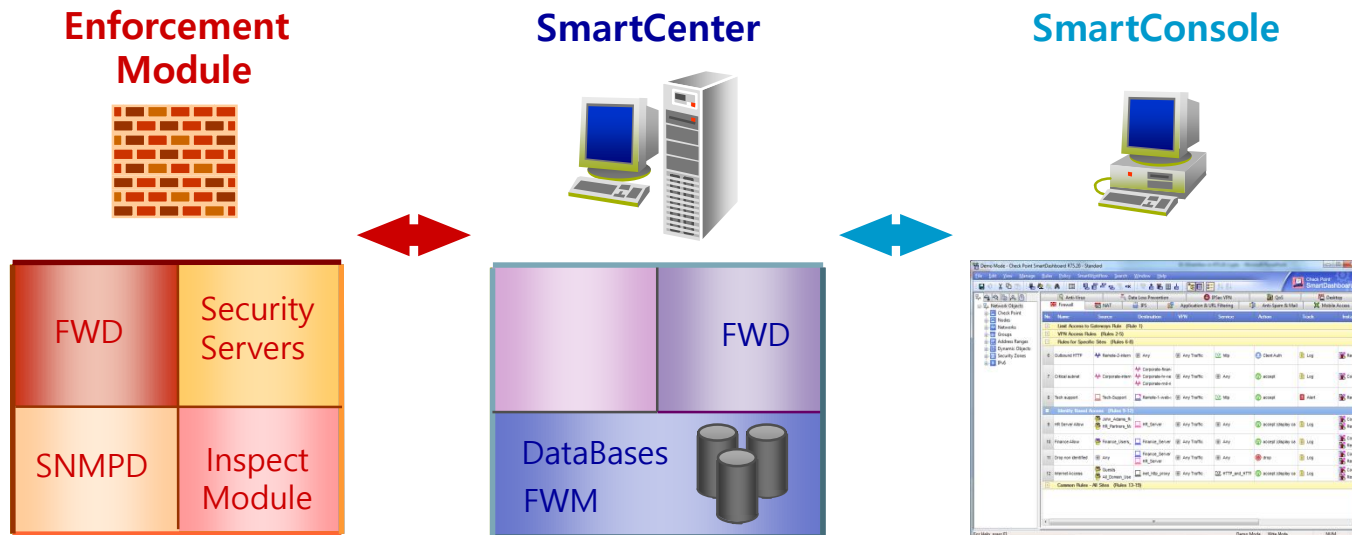


고객이 필요하는 소프트웨어 블레이드를 통합

# 체크포인트 보안시스템 아키텍처

## 보안 시스템 구성 모듈

- **Enforcement Module** – 실제 보안 기능을 수행하는 소프트웨어 모듈
- **SmartCenter** – 여러 개의 Enforcement Module을 동시에 통합 관리를 하는 Management Server로 Enforcement Module과 독립적으로 설치운영 할 수 있으며 보안정책, Log 관리, 상태 모니터링 등의 기능을 통합적으로 수행
- **SmartConsole** – SmartCenter를 제어하는 관리자를 위한 Check Point 전용 GUI Client Software. 이 툴을 통해 Check Point 침입차단 시스템을 비롯한 모든 보안 모듈을 통합 관리



Check Point Firewall 3-tier architecture

# 체크포인트 보안시스템 아키텍처

## 운영자 중심의 직관적인 통합관리 화면

Demo Mode - Check Point SmartDashboard R77.30 - Standard

Install Policy SmartConsole

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

Overview Policy Gateways NAT Track Logs Analyze & Report

### Policy

Search for IP, object, action, ... Query Syntax

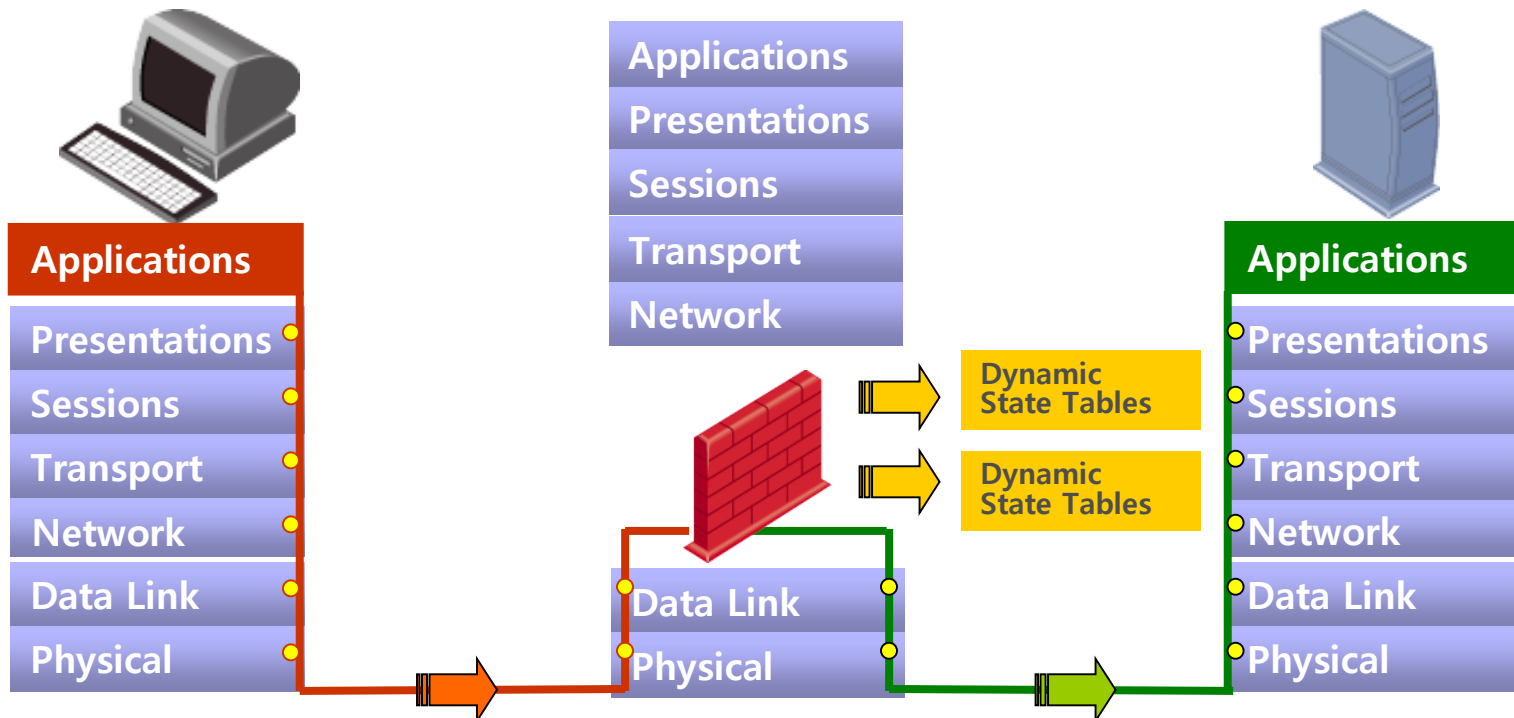
| No.                                    | Hits | Name             | Source                                   | Destination                                                    | VPN          | Service                                   | Action            | Track | Install On                  | Time |
|----------------------------------------|------|------------------|------------------------------------------|----------------------------------------------------------------|--------------|-------------------------------------------|-------------------|-------|-----------------------------|------|
| Limit Access to Gateways Rule (Rule 1) |      |                  |                                          |                                                                |              |                                           |                   |       |                             |      |
| 1                                      | 111K | Stealth          | Corporate-internal-net                   | GW-group                                                       | Any Traffic  | Any                                       | drop              | Alert | Policy Targets              | Any  |
| VPN Access Rules (Rules 2-5)           |      |                  |                                          |                                                                |              |                                           |                   |       |                             |      |
| 2                                      | 325K | Site to site VPN | Any                                      | Any                                                            | All_GwToGw   | CIFS<br>ftp-port<br>http<br>https<br>smtp | accept            | Log   | Policy Targets              | Any  |
| 3                                      | 2M   | Remote access    | Mobile-vpn-user@Any                      | Any                                                            | RemoteAccess | CIFS<br>http<br>https<br>imap             | accept            | Log   | Policy Targets              | Any  |
| 4                                      | 201K | Clientless VPN   | Clientless-vpn-user@Any                  | Corporate-WA-proxy-server                                      | Any Traffic  | https                                     | User Auth         | Log   | Policy Targets              | Any  |
| 5                                      | 1M   | Web server       | L2TP-vpn-user@Any<br>Customers@Any       | Remote-1-web-server                                            | Any Traffic  | http                                      | accept            | Log   | Policy Targets              | Any  |
| Rules for Specific Sites (Rules 6-8)   |      |                  |                                          |                                                                |              |                                           |                   |       |                             |      |
| 6                                      | 55K  | Outbound HTTP    | Remote-2-internal                        | Any                                                            | Any Traffic  | http                                      | Client Auth       | Log   | Remote-2-gw                 | Any  |
| 7                                      | 3M   | Critical subnet  | Corporate-internal-net                   | Corporate-finance-net<br>Corporate-hr-net<br>Corporate-rnd-net | Any Traffic  | Any                                       | accept            | Log   | Corporate-gw                | Any  |
| 8                                      | 310K | Tech support     | Tech-Support                             | Remote-1-web-server                                            | Any Traffic  | http                                      | accept            | Alert | Remote-1-gw                 | Any  |
| Identity Based Access (Rules 9-12)     |      |                  |                                          |                                                                |              |                                           |                   |       |                             |      |
| 9                                      | 433K | HR Server Allow  | John_Adams_Role<br>HR_Partners_Managed_I | HR_Server                                                      | Any Traffic  | Any                                       | accept (display c | Log   | Corporate-gw<br>Remote-1-gw | Any  |
| 10                                     | 78K  | Finance Allow    | Finance_Users_Role                       | Finance_Server                                                 | Any Traffic  | Any                                       | accept (display c | Log   | Corporate-gw<br>Remote-1-gw | Any  |

Objects List Parent Tasks Identity Awareness SmartWorkflow

Demo Mode Write Mode

## Strong Stateful Inspection

- INSPECT VM(virtual machine)에 의한 유연하고 신속한 보안 검사 수행
  - INSPECT code를 통해 높은 수준의 포괄적인 보안 검사를 수행하는 강력한 엔진 생성
- Full Application Layer Awareness
  - Dynamic 상태에서 table을 저장하고 Context를 연결하며 나가는 connection을 검사 후 돌아오는 connection을 해당된 OSI 7 layer를 통해 검사



## 1. 접근제어 (Access Control)

- 기업의 정보보안 정책에 의거하여 인트라넷 및 내부의 네트워크 자산을 보호하기 위한 접근제어 정책 설정
- 서비스별, IP Address 별, 사용자별, 시간별 접근제어

## 2. 사용자 인증

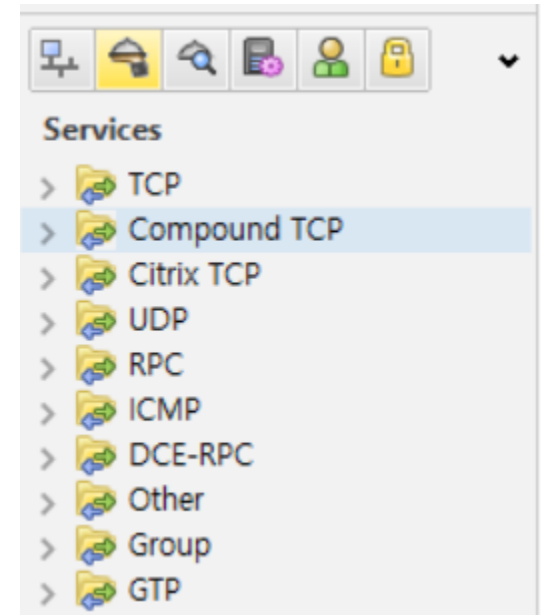
- 인증 방식 : User 인증, Session 인증, Client 인증
- 강력한 인증방안 지원
  - User ID, Password, ICA에 의해 생성된 PKCS#12 인증서
  - RSA SecureID, RADIUS, TACACS

## 3. NAT(Network Address Translation)

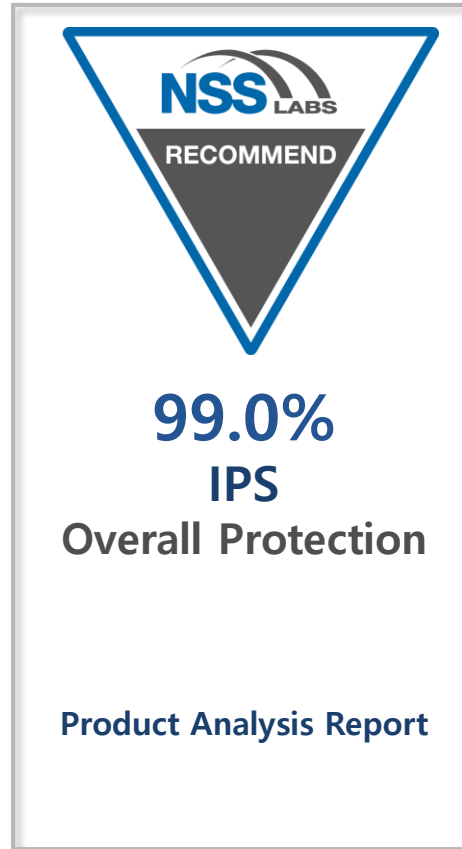
- 1:n (Hide NAT), 1:1 or n:n (Static NAT), VPN의 IP Pool

## 4. TCP/UDP외 다양한 Protocol의 보안성 검사 기능

- 복잡한 프로토콜, 서비스 보안
  - 업계 최고의 250여 개 이상의 서비스 보안검사 기본 정의
- TCP, UDP 이외에도 다양한 프로토콜을 미리 정의하여 지원
  - ICMP, DCE-RPC, RPC, GTP, Citrix TCP 등
- 이외에도 Protocol Number가 할당된 다양한 프로토콜 지원
  - GRE, AH, ESP, SKIP 등
- 업계 최초로 IPv6 체계의 방화벽 기능 지원



## 최고등급의 공인인증기관 평가 – NSS Labs



## IPSec VPN Blade 주요 기능

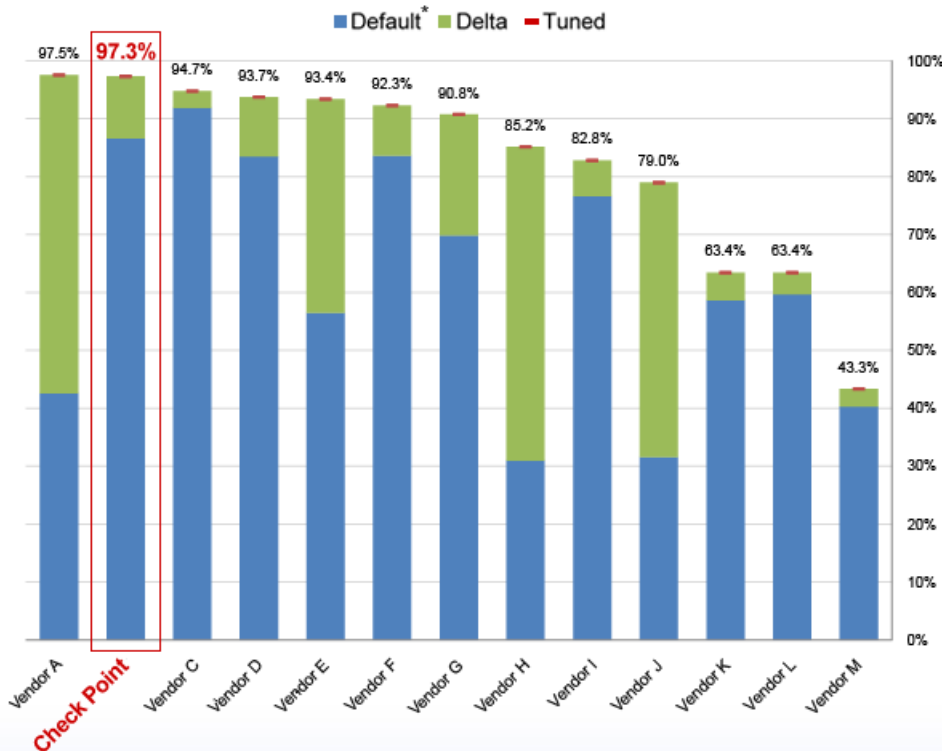
- IPSEC 표준을 지원하여 타 VPN 장비와의 호환성을 세계적으로 검증 받음
- 다양한 형태의 VPN 기능을 지원
  - VPN Community : 여러 곳에 동시 VPN 장비를 설치, 연결하는 경우 Visual 한 Community Graphic 설정환경을 제공하여 One Click 방식으로 VPN 설정을 매우 용이하게 지원
  - Extranet Management : 고객 및 파트너와 VPN 연동 시 상대 네트워크 구성의 변경에 따른 자동적인 VPN 설정을 변경 및 관리함
- 강력한 VPN Client 프로그램 제공 또는 Clientless VPN 지원

| <div> <div>Firewall</div> <div>Application &amp; URL Filtering</div> <div>Data Loss Prevention</div> <div>IPS</div> <div>Threat Prevention</div> <div>Anti-Spam &amp; Mail</div> <div>Mobile Access</div> <div>IPSec VPN</div> <div>Compliance</div> <div>QoS</div> <div>Desktop</div> </div> |      |                                                                                                      |                                    |                           |              |                                           |             |       |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------------------------------------------------------------------------------------------------|------------------------------------|---------------------------|--------------|-------------------------------------------|-------------|-------|--|
| <div> <div>Overview</div> <div>Policy</div> <div>Gateways</div> <div>NAT</div> </div>                                                                                                                                                                                                         |      | <div> <div>Policy</div> <div>Search for IP, object, action, ...</div> <div>Query Syntax</div> </div> |                                    |                           |              |                                           |             |       |  |
| <div> <div>Track Logs</div> <div>Analyze &amp; Report</div> </div>                                                                                                                                                                                                                            |      |                                                                                                      |                                    |                           |              |                                           |             |       |  |
| <div> <div>Services</div> <div>TCP</div> <div>Compound TCP</div> <div>Citrix TCP</div> <div>UDP</div> </div>                                                                                                                                                                                  |      |                                                                                                      |                                    |                           |              |                                           |             |       |  |
| No.                                                                                                                                                                                                                                                                                           | Hits | Name                                                                                                 | Source                             | Destination               | VPN          | Service                                   | Action      | Track |  |
| Limit Access to Gateways Rule (Rule 1)                                                                                                                                                                                                                                                        |      |                                                                                                      |                                    |                           |              |                                           |             |       |  |
| 1                                                                                                                                                                                                                                                                                             | 111K | Stealth                                                                                              | Corporate-internal-net             | GW-group                  | Any Traffic  | Any                                       | drop        | Alert |  |
| VPN Access Rules (Rules 2-5)                                                                                                                                                                                                                                                                  |      |                                                                                                      |                                    |                           |              |                                           |             |       |  |
| 2                                                                                                                                                                                                                                                                                             | 325K | Site to site VPN                                                                                     | Any                                | Any                       | All_GwToGw   | CIFS<br>ftp-port<br>http<br>https<br>smtp | accept      | Log   |  |
| 3                                                                                                                                                                                                                                                                                             | 2M   | Remote access                                                                                        | Mobile-vpn-user@Any                | Any                       | RemoteAccess | CIFS<br>http<br>https<br>imap             | accept      | Log   |  |
| 4                                                                                                                                                                                                                                                                                             | 201K | Clientless VPN                                                                                       | Clientless-vpn-user@Any            | Corporate-WA-proxy-server | Any Traffic  | https                                     | User Auth   | Log   |  |
| 5                                                                                                                                                                                                                                                                                             | 1M   | Web server                                                                                           | L2TP-vpn-user@Any<br>Customers@Any | Remote-1-web-server       | Any Traffic  | http                                      | accept      | Log   |  |
| Rules for Specific Sites (Rules 6-8)                                                                                                                                                                                                                                                          |      |                                                                                                      |                                    |                           |              |                                           |             |       |  |
| 6                                                                                                                                                                                                                                                                                             | 55K  | Outbound HTTP                                                                                        | Remote-2-internal                  | Any                       | Any Traffic  | http                                      | Client Auth | Log   |  |

## Check Point Sets a New Standard in Latest NSS Group IPS Test



Overall Achievable Block Rate



\* 'Default' in legend above represents Check Point 'Recommended' profile

업계를 선도하는 IPS 기술

검증된 정확도 및 차단 능력

- 97.3% Security Effectiveness
- 2.4Gbps IPS Throughput
- 100% anti-evasion coverage

## 최고등급의 공인인증기관 평가 – NSS Labs



**#1 in**  
마이크로소프트 Threat 커버리지  
2008, 2009, 2010 and 2011

**Check Point 620**

Sourcefire 590

HP Tipping Point 498

Cisco 483

Juniper 344

McAfee 342

**#1 in**  
어도비 리더, 아크로뱃 Threat  
커버리지 2009, 2010, 2011

**Check Point 185**

Sourcefire 148

Juniper 90

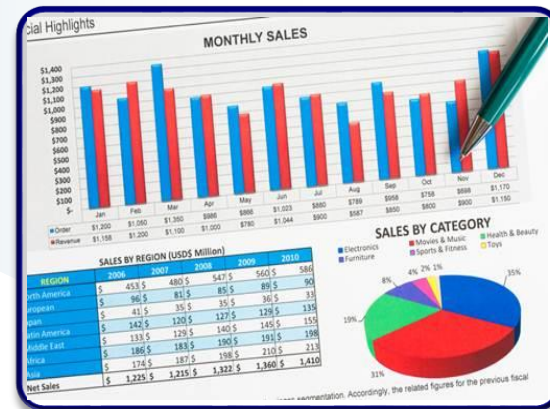
Tipping 70

Cisco 41

McAfee 28

Signature counts attained from vendor public web sites.

모바일 기기 및 PC에서 SSL VPN 접속으로  
이메일과 Application에 접근하여 업무 처리



사용자, 사용자 그룹 및 컴퓨터를  
인지하여 통제하는 보안 정책 구현

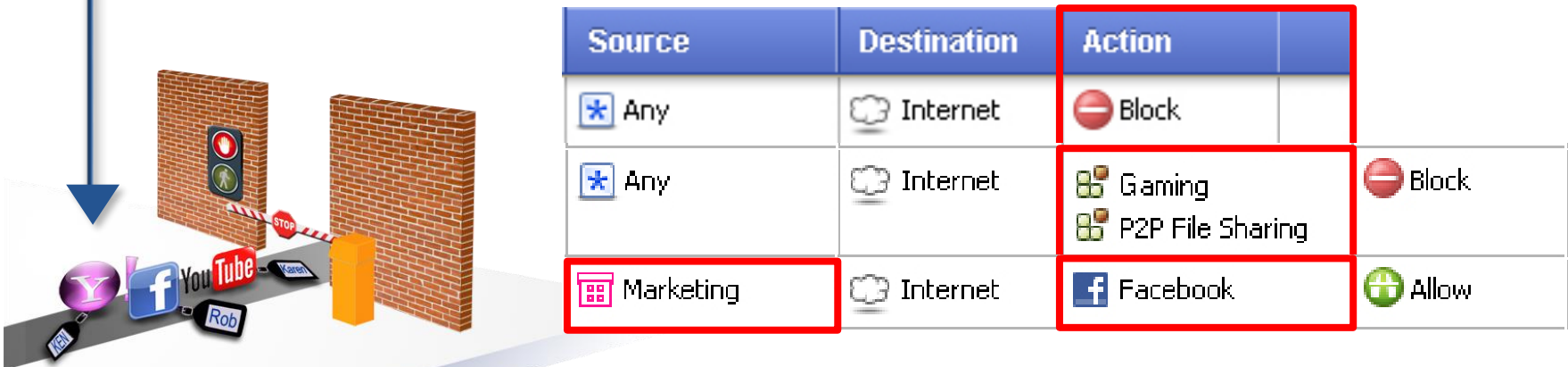


Active  
Directory  
통합

사용자 및  
그룹 식별

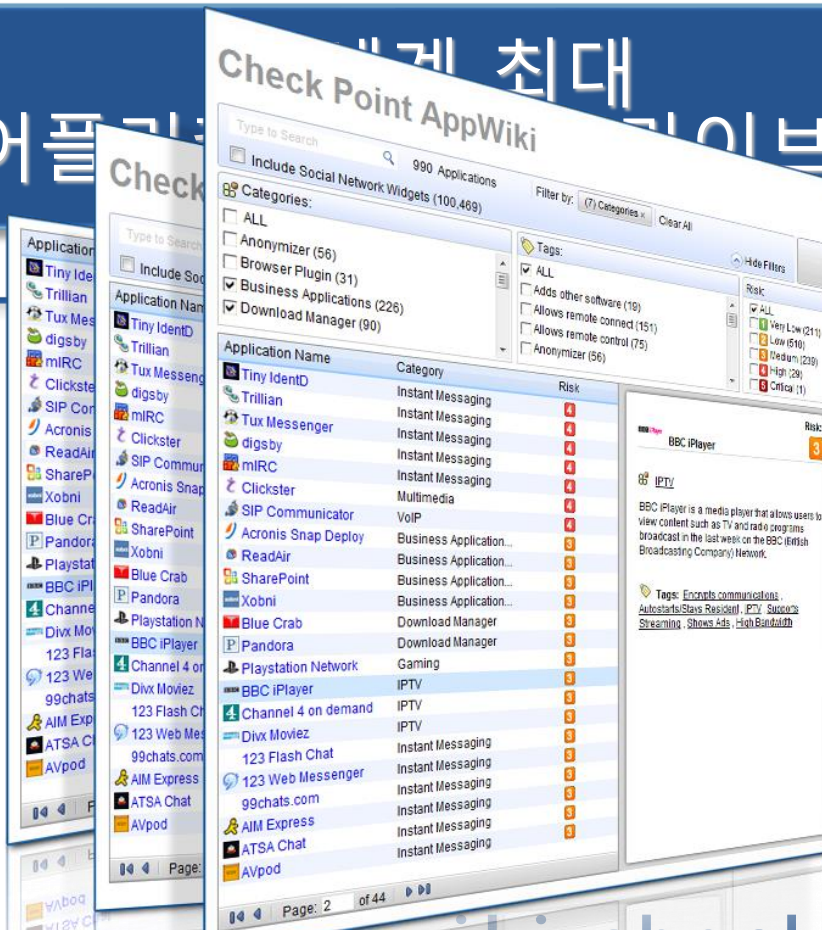
기존 보안과  
통합

사용자 또는 그룹레벨에서 어플리케이션 사용을  
식별, 허가, 차단 또는 제한



# Application Control 블레이드

어플리케이션 제어 최대 라이브러리

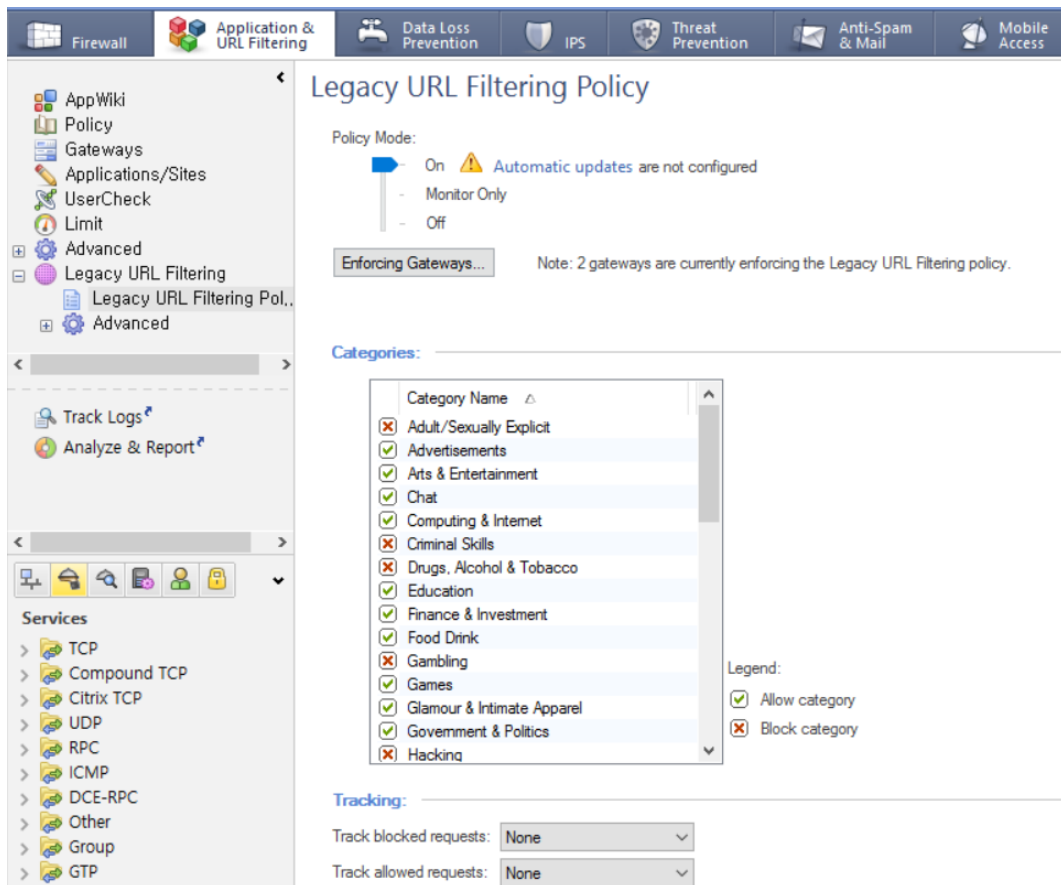


플리케이션  
소셜네트워크

고리  
e & Video,

appwiki.checkpoint.com

# URL Filtering 블레이드



- 커스터마이징 가능한 차단 통보 또는 리다이렉트 페이지 제공
  - 사용자가 회사의 URL Filtering 정책을 위반할 경우 즉각 사용자에게 경고 알림
- 2 천만개 이상의 URL 커버
  - 2 천만개 이상의 URL을 보유
  - 인터넷에서 발생하는 최신 변화를 반영
- 40 개 이상의 이미 설정된 카테고리
  - URL filtering 정책이 빠르고 쉽게 적용될 수 있도록 주제별 (음란사이트, 불법 소프트웨어 등) 카테고리 제공
- 지속적인 업데이트
  - URL Filtering 정책이 인터넷상에서 일어나는 실시간 변화를 정확하게 반영할 수 있도록 지속적인 업데이트 제공
- 화이트 리스트 및 블랙 리스트 기능 제공
  - White list(접근허용 사이트)와 black list(접근차단 사이트)를 이용하여 기업 요구에 따른 맞춤형 정책 제공

# App Control & URLF

## - 클라우드 기반 업데이트



클라우드 기반 분류 DB  
지속적인 업데이트

99.2%의 쿼리가 캐쉬에  
서 즉각 조회

삭제된 사이트는 실시간  
으로 캐쉬에서 제거

## 웹 보안의 모든 측면을 통합 제어



Websites —  
URL Filtering

통합된 카테고리 —  
URLs and applications

| Source                                                                                       | Sites / Applications                                                                                                                                                                            | Action                                                                                     |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
|  Any        |  Violence<br> Games           |  Block  |
|  Marketing |  Media Streaming<br> Skype |  Allow |

 User/Group Granularity

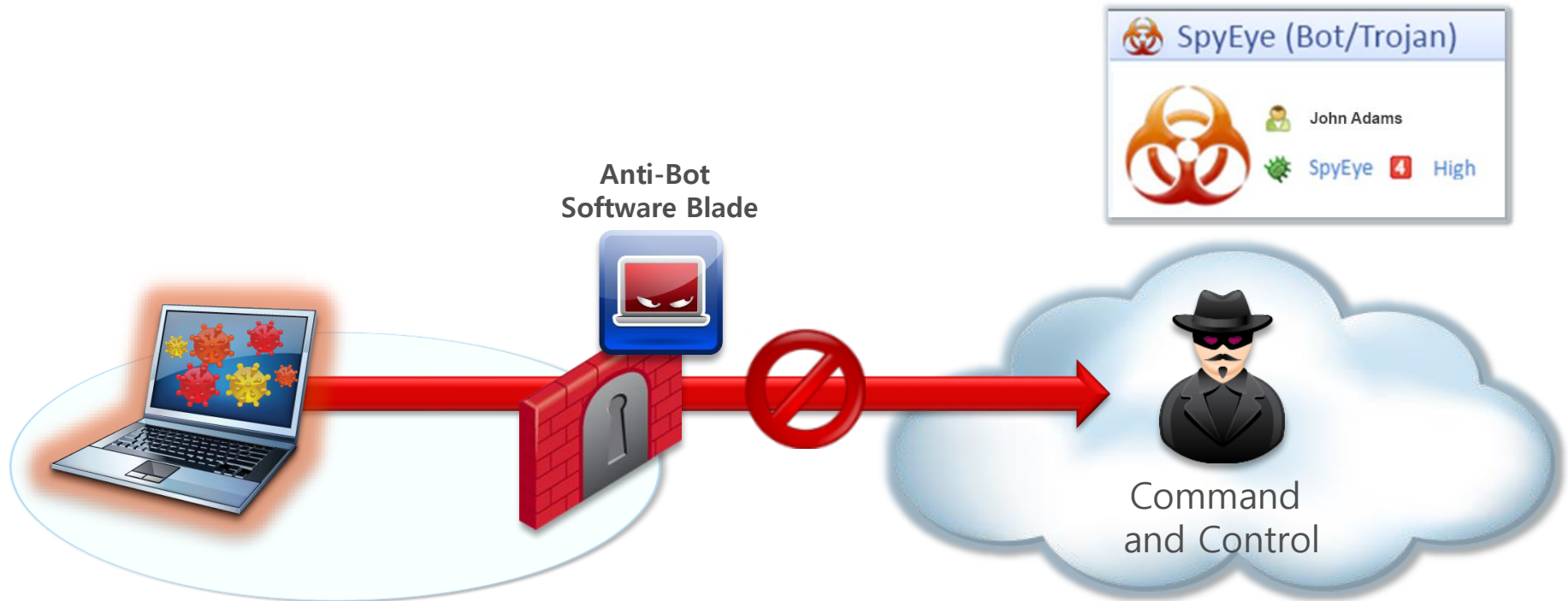
Applications —  
Application Control

# Anti-Bot 블레이드

감염된  
컴퓨터를 탐지

봇(Bot)의  
피해를 방지

Forensics  
정보제공



# 다계층 Bot-탐지 ThreatSpect™ 엔진

1

공격자의  
은신처



IP/URL/DNS을  
이용한 공격자의  
명령 제어 탐지

2억5천만개 이상의  
IP주소!

2

공격자의  
통신기법



공격자의 독특한  
통신 패턴 탐지

2천개 이상의  
Botnet families!

3

공격자의  
공격행위



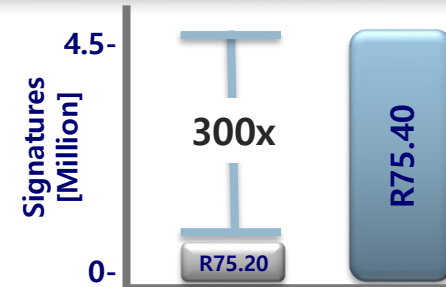
공격 신호와 유형  
탐지  
(spam, click fraud...)

하루 2백만 건  
발생!

## Extended Protection using ThreatCloud™

**Stop Incoming  
Malware  
Attacks**

**Protect with 300x  
more signatures!**



**Prevent Access  
to Malicious  
Sites**

**Over 300,000 sites!**



**Constantly  
updated**

**Security intelligence  
with ThreatCloud™**



# ThreatCloud™

- 사이버공격을 방어하기 위한 최초의 협업 네트워크 체계



SensorNET



봇넷 주소

멀웨어 사이트

시그니처



체크포인트  
ThreatCloud™



매 분 단위의  
지능적 보안  
업데이트

발생하는 위협을  
식별하는 글로벌  
네트워크 센서

게이트웨이로부터  
공격정보 수집

업계 최대의 멀웨어  
정보 제공





## 안티바이러스 + 안티봇



### 통합된 정책 설정

| Name         | Protected Scope                                               | Action                  | Track                   |
|--------------|---------------------------------------------------------------|-------------------------|-------------------------|
| Internal Net | internal_network                                              | Prevent_All             | Log                     |
| WiFi Net     | WiFi_Net                                                      | WiFi_Antivirus          | Log                     |
| Finance Net  | Finance_Server<br>Finance_Users_Role<br>Corporate-finance-net | Finance_AntiBot_Prev... | Alert<br>Packet Capture |

### 통합된 멀웨어 분석



## See the BIG malware picture

### MALWARE REPORT

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

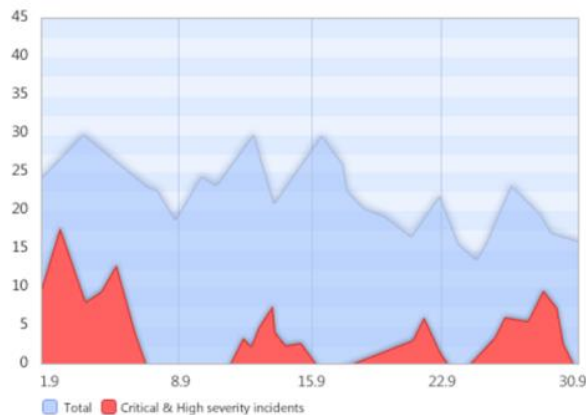


Anti-Bot Blade: ✔ Active Anti-Virus Blade: ✔ Active

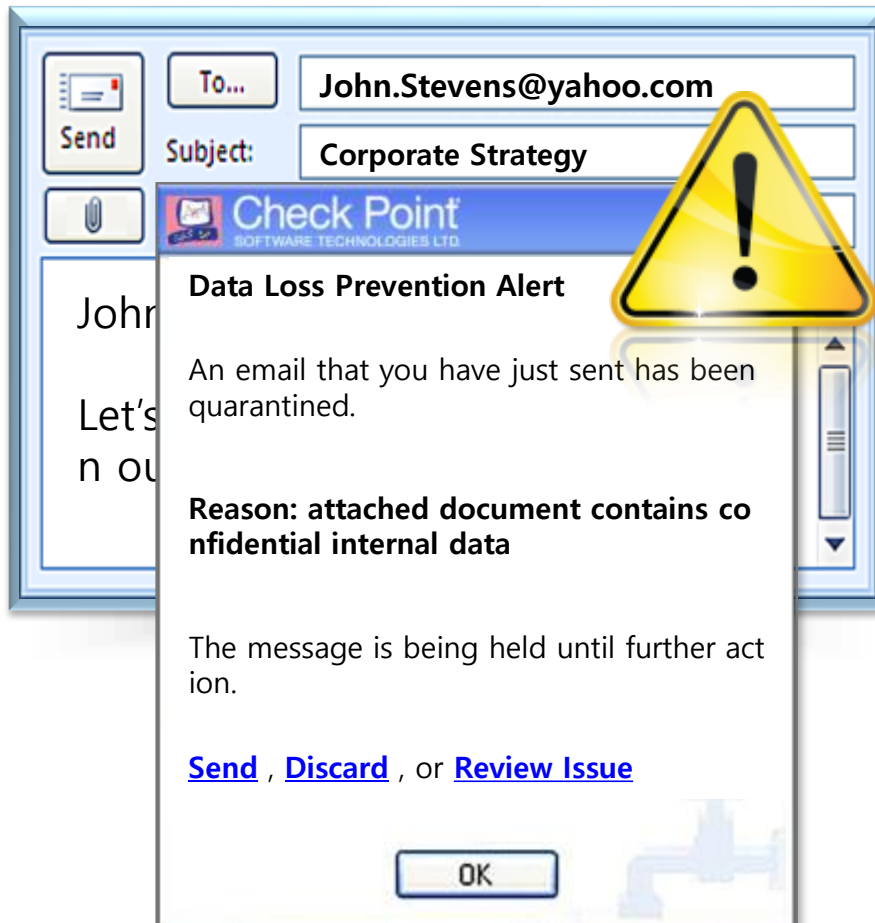
Generated by Check Point SmartEvent®, on September 2nd 2011 10:35AM 1



### Incidents in the Last Month



## 효과적인 DLP 구현을 위해 기술과 프로세스를 결합



### 차단

Move from detection  
to prevention

### 교육

Users on corporate  
data policies

### 강제

Data loss  
business processes

## MultiSpect 탐지 엔진

다양한 소스 data 에서  
상관관계 분석을 통한 탐지

| Item No. | Name          | Social Security Number | Job Title    | Salary    |
|----------|---------------|------------------------|--------------|-----------|
| 1        | John Smith    | 987-65-4320            | CEO          | \$200,000 |
| 2        | Kevin Brian   | 987-65-4221            | VP R&D       | \$150,000 |
| 3        | Margret White | 769-65-7522            | VP Marketing | \$140,000 |
| 4        | Bob Johns     | 342-62-3323            | CFO          | \$140,000 |
| 5        | Mike Riddle   | 777-43-4324            | COO          | \$180,000 |

600개 이상의 파일 포맷 지원

사전 정의된 250개 이상의  
데이터 유형 검사



# 중앙 통합 관리 기능

## 중앙 통합관리 화면 – SmartConsole

Demo Mode - Check Point SmartDashboard R75.20 - IPS

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

Enforcing Gateways  
Profiles  
Protections  
By Type  
Signatures  
Protocol Anomalies

Overview

IPS provides protection from network, application and web attacks. [Getting Started](#)

IPS in My Organization

15 Security Gateways are enforcing IPS

Messages and Action Items

New update package (v.624115429) is available. [Update](#)

Firewall NAT IPS Application Control Anti-Spam & Mail SSL VPN Data Loss Prevention Anti-Virus & URL Filtering IPSec VPN QoS Desktop

Overview  
Application Control Policy  
Enforcing Gateways  
AppWiki  
Advanced

### Application Control Policy

Type to Search

|                                       | Name                                                                   | Source        | Destination | Application                               | Action                | Track |
|---------------------------------------|------------------------------------------------------------------------|---------------|-------------|-------------------------------------------|-----------------------|-------|
| <b>Malicious applications (2)</b>     |                                                                        |               |             |                                           |                       |       |
| 1                                     | Block High risk applications                                           | Any           | Internet    | High risk applications                    | Block                 | Log   |
| 2                                     | Block malwares                                                         | Any           | Internet    | Used By Malware<br>Anonymizer             | Block                 | Log   |
| <b>Exceptions (1)</b>                 |                                                                        |               |             |                                           |                       |       |
| 3                                     | Allow TeamViewer application for specific user - ticket #88721         | John Smith    | Any         | TeamViewer                                | Allow                 | Log   |
| <b>Corporate access by groups (6)</b> |                                                                        |               |             |                                           |                       |       |
| 4                                     | Allow remote admin for IT Dept only                                    | IT_Department | Any         | Radmin                                    | Allow                 | Log   |
| 5                                     | Allow Messengers for Support group and warn about this once in a month | Support       | Internet    | Yahoo Messenger<br>Windows Live Messenger | Inform (once a month) | Log   |

**Summary**  
Blocking 2165 applications in 10 categories.

For Help, press F1

Read/Write NUM

# 중앙 통합 관리 기능

## 통합 로그 화면

- 각각의 보안 기능 별로 검사된 트래픽 로그 확인 - SmartView Tracker
- 다양한 type 의 경고 설정 기능 - Log, Account, Alert, User defined 등
- 3가지 모드의 로그 Viewer
  - Network & Endpoint : 일반적인 Traffic 의 Historical Log
  - Active : 현재 연결되어 있는 Active connection 에 대한 로그
  - Management : 접속한 관리자의 세부 행위에 대한 감사 로그

모든 보안 블레이드  
별로 기록된 로그 선택  
확인

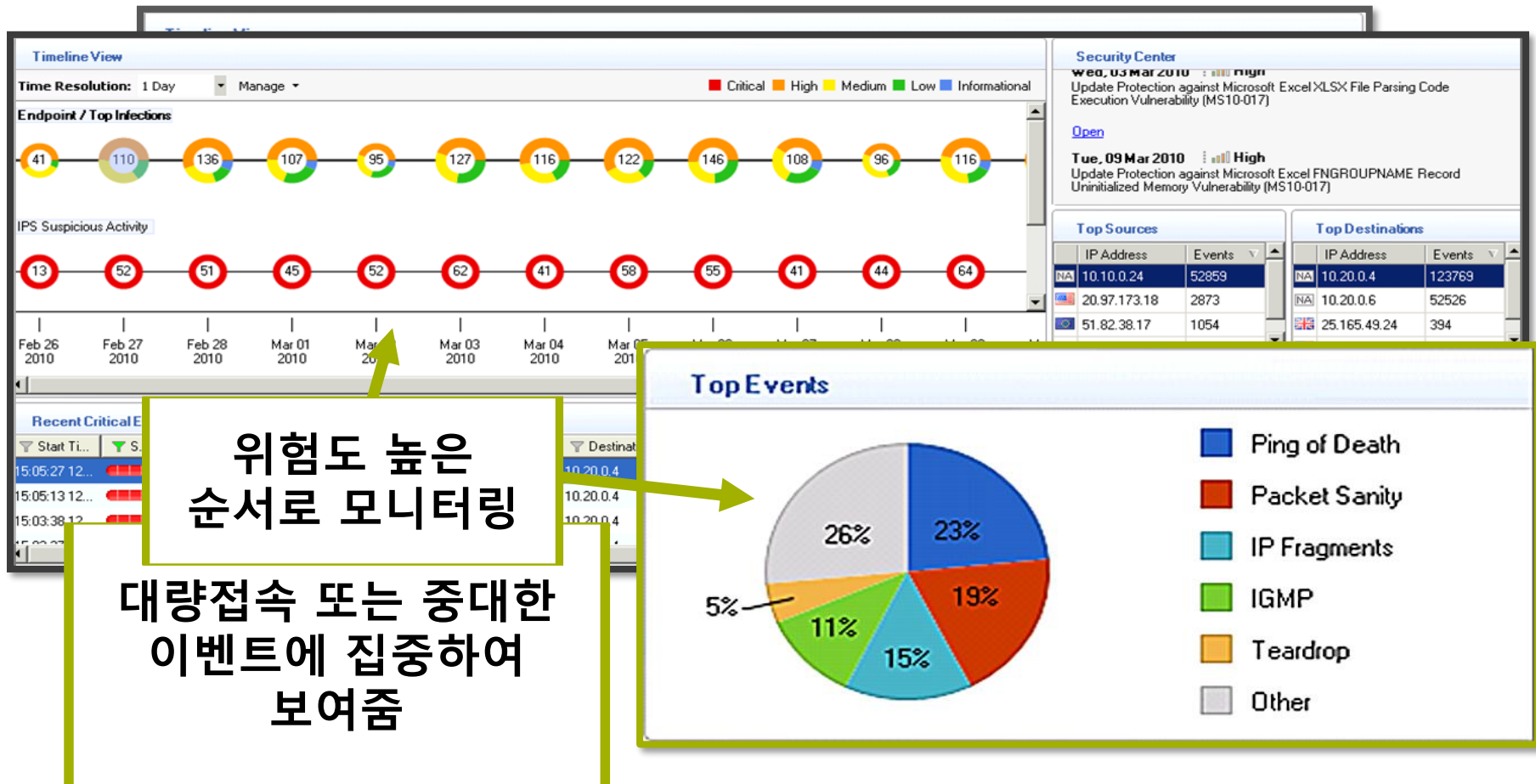
보안로그, 실시간  
세션로그, 관리자 감사  
로그 통합 조회

원하는 정보를  
신속하게 검색  
할 수 있으며  
세부내용 확인

The screenshot displays the Check Point SmartView Tracker interface. On the left, a tree view shows various security blades under 'Predefined' and 'Application and URL Filtering'. The main pane shows a list of log entries with columns for No., Date, Time, and Priority. A 'Record Details' window is open, showing the details of a selected log entry. The 'Log Info' tab is active, displaying fields like Product, Date, Time, Number, Type, and Origin. The 'Traffic' tab shows Source, Destination, Service, Protocol, Interface, and Source Port. The 'Policy' tab shows Policy Name, Policy Date, and Policy Management. The 'More' tab shows Action, Rule, Current Rule Number, Rule Name, and User. The 'Information' tab shows XlateDst and message\_info. The bottom pane shows a list of log entries with columns for No., Date, Time, Priority, and Action.

| No. | Date      | Time     | Priority | Action |
|-----|-----------|----------|----------|--------|
| 14  | 30Oct2008 | 19:45:21 | Sec      | Reject |
| 15  | 30Oct2008 | 20:15:54 | Sec      | Reject |
| 16  | 30Oct2008 | 20:28:59 | Sec      | Reject |
| 17  | 30Oct2008 | 21:20:14 | Sec      | Reject |
| 18  | 30Oct2008 | 22:29:20 | Sec      | Reject |
| 19  | 30Oct2008 | 22:35:14 | Sec      | Reject |
| 20  | 1Nov2008  | 1:10:55  | Sec      | Reject |
| 21  | 1Nov2008  | 1:10:59  | Sec      | Reject |
| 22  | 1Nov2008  | 1:11:02  | Sec      | Reject |
| 23  | 1Nov2008  | 1:11:29  | Sec      | Reject |
| 24  | 1Nov2008  | 15:00:41 | Sec      | Reject |
| 25  | 1Nov2008  | 15:06:33 | Sec      | Reject |
| 26  | 1Nov2008  | 15:41:29 | Sec      | Reject |
| 27  | 1Nov2008  | 16:43:13 | Sec      | Reject |
| 28  | 1Nov2008  | 17:43:28 | Sec      | Reject |
| 29  | 1Nov2008  | 18:35:11 | Sec      | Reject |
| 30  | 1Nov2008  | 18:35:14 | Sec      | Reject |
| 31  | 1Nov2008  | 18:39:42 | Sec      | Reject |
| 32  | 2Nov2008  | 8:10:20  | Sec      | Reject |
| 33  | 2Nov2008  | 8:11:22  | Sec      | Reject |
| 34  | 2Nov2008  | 8:11:30  | Sec      | Reject |
| 35  | 2Nov2008  | 8:12:29  | Sec      | Reject |
| 36  | 2Nov2008  | 8:14:36  | Sec      | Reject |
| 37  | 2Nov2008  | 8:14:38  | Sec      | Reject |
| 38  | 3Nov2008  | 11:14:26 | Sec      | Reject |
| 39  | 15Mar2009 | 1:00:1   | Sec      | Reject |
| 40  | 15Mar2009 | 2:14:36  | Sec      | Reject |

## 상세한 이벤트 분석결과 조회 - SmartEvent



## 통합 모니터링 화면

- 방화벽 시스템의 상태 확인
  - SmartView Monitor는 모든 방화벽의 보안정책 상태, CPU, Memory, HDD, Connection 상태 등을 하나의 화면에서 보여줍니다.

The screenshot displays the Check Point SmartView Monitor interface. The left sidebar shows a navigation tree with categories like Custom, Gateways Status, Traffic, System Counters, and Tunnels. The main panel is titled 'All Gateways' and contains a table listing various gateways with their IP addresses, status, CPU usage, memory, and disk frequency. Below the table, a detailed view for 'Remote-1-gw' is shown, including its IP address, version, OS, and a list of security services like Firewall, Security Management Server, Endpoint Security, IPSec VPN, and Anti-Spam.

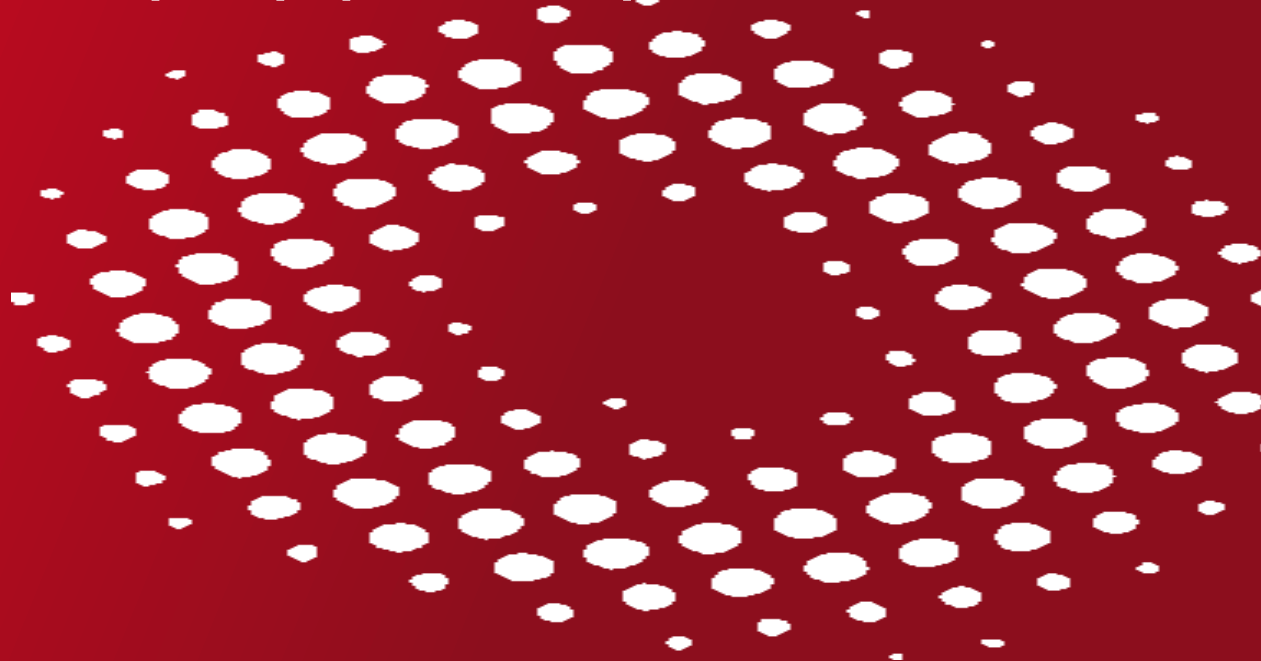
| Gateway Name              | IP Address     | Status  | Average CPU | Active Virtual Me... | Disk Fre... | Version   |
|---------------------------|----------------|---------|-------------|----------------------|-------------|-----------|
| Remote-1-web-server       | 192.168.2.2    | OK      | 11%         | 369 MB               | 67          | NGX (R70) |
| Corporate-internal-ter... | 172.16.1.10    | OK      | 73%         | 174 MB               | 3           | R75, 40   |
| Remote-1-gw               | 198.51.100.1   | OK      | 2%          | 233 MB               | 92          | NGX (R70) |
| Management-b              | 172.16.1.201   | OK      | 1%          | 471 MB               | 45          | R75, 40   |
| Remote-2-windows-d...     | 10.0.2.10      | OK      | 36%         | 56 MB                | 23          | R75, 40   |
| Remote-4-gw               | 10.125.100.1   | OK      | 50%         | 77 MB                | 76          | R75, 40   |
| Remote-branch_gw          | 198.85.100.120 | OK      | 0%          | 138 MB               | 24          | R75, 40   |
| Remote-3-gw               | 100.75.25.1    | Problem | 4%          | 983 MB               | 82          | R77       |

**Remote-1-gw**  
IP Address: 198.51.100.1  
Version: NGX (R70)  
OS: Windows2000 Service Pack: 4.0  
[System Information](#), [Network Activity](#), [Licenses](#)

- Firewall** (Status: OK) Security Policy: Standard, Installed On: 01.08.04, [More...](#)
- Security Management Server** (Status: OK) Connected clients: 0, [Certificate Authority](#), [More...](#)
- Endpoint Security** (Status: OK) [More...](#)
- IPSec VPN** (Status: OK) [More...](#)
- Anti-Spam** (Status: OK) [More...](#)

# Contents

1. 체크포인트 회사 소개
2. 체크포인트 제품 소개
3. 체크포인트 어플라이언스 소개



# 체크포인트 보안 어플라이언스

61000 System and  
21000 Appliances



12000 Appliances  
(3 Models)



4000 Appliances  
(4 Models)



2200 Appliance



*Ultra High-End*

*Datacenter Grade*

*Small Office /  
Desktop*

*Enterprise Grade*





Check Point 2200 Appliance

## The Small Office – Desktop Model

- 3 Gbps firewall throughput
- Less than \$4,000



Check Point 4000 Appliances  
(4 Models)

## Enterprise Grade

- 3 to 11 Gbps firewall throughput
- 2 to 6 Gbps IPS throughput



Check Point 12000 Appliances  
(3 Models)

## Data Center Grade

- 15 to 30 Gbps firewall throughput
- Hot-swap power supply and HDD



Check Point 21000 Appliances  
(3 Models)

## Ultra Data Center Protection

- 50 to 100 Gbps firewall throughput\*
- High availability and serviceability
- Optional acceleration with low latency

\* With optional acceleration card (available 2012)



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

---

**BellI&S**  
Bell Information&Solutions 

**BellI&S**  
Bell Information&Solutions 

 Tel) 02-6925-1130~1 / Fax) 02-2664-1575



[본사]서울시 서대문구 충정로 8  
(종근당빌딩 8층)

E-Mail : shlee@bellins

