



엔드포인트 통합보안 솔루션

Symantec Endpoint Protection 12

Symantec Korea

목차

1

Security Trend

2

Symantec Technology

3

Symantec Endpoint Protection 12



Security Trend

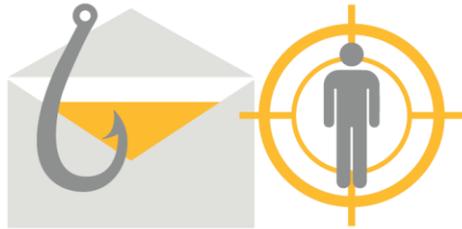
- 악성코드의 폭발적 증가

2012년에는 하루 백만개 이상의 악성코드 기반 신규 위협이 나타나고 있음



- 대표적 APT 초기 공격

스피어
피싱



표적으로 삼은
대상에게 이메일 발송

워터링홀
공격



웹 사이트를
감염시킨 후 잠복

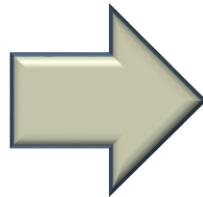
표적 공격은 주로 스피어 피싱 공격으로 시작

2012년 웹사이트 잠복 공격인 워터링홀 공격 기법이 새롭게 등장

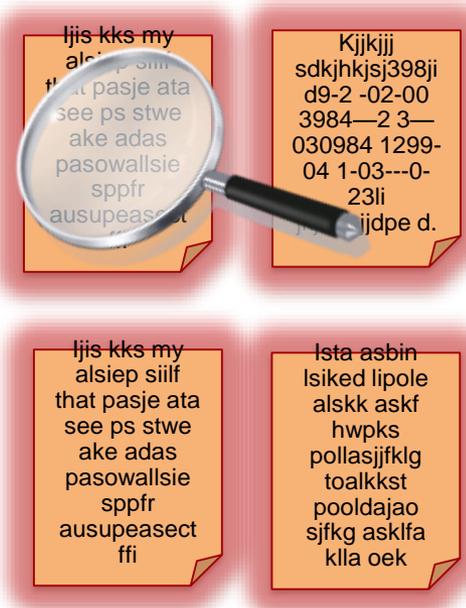
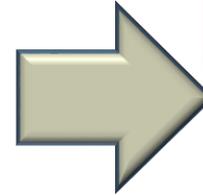
- 악성 코드 제작의 편리성



This is my first virus that I plan to use to steal key and passwords from unsuspecting victims.



툴을 이용하여
쉽게 여러 변종을
생성한다.

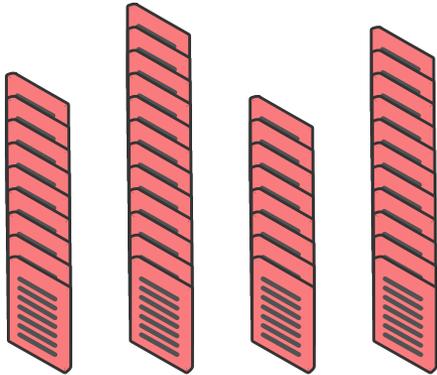


하나의 악성코드는
전혀 다른 악성코드로
수십, 수백개를 생성
가능하다. (Byte-Level)

바이러스 제작자가
원본 바이러스를
제작한다.

파일 기반의 전통적인 탐지 기법은 더이상 효과적인 대응책이 아니다.

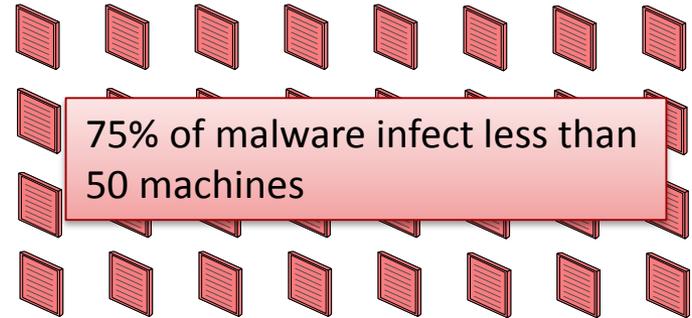
- 악성코드 제작자들의 전략 진화



From:

소수의 악성코드들을 대량 배포

- 소수의 악성코드를 무차별적인 배포
- 전세계에 걸쳐서 대규모의 확산과 피해를 일으킴



To:

많은 변종의 악성코드를 배포

- 많은 변종을 만들어 다양한 경로로 배포
- 정교하게 원하는 대상에게 악성코드를 배포
- 대규모 확산으로 연결되지 않음

안티바이러스 회사가 전세계에 존재하는 모든 악성코드를 수집할 수 있을까?
이런 현실에 어떻게 대응 할것 인가? 안티바이러스회사의 전략은?

- 현재 보호 기술의 한계

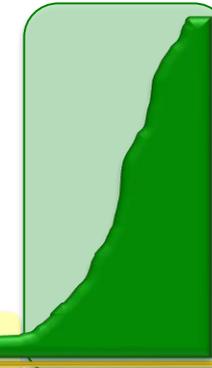
Today, both good and bad software obey a long-tail distribution.

악성 파일



불행하게도 수천수백만의 낮은
배포를 가진 파일에 대해 효율적인
기술이 없음.
(그러나 최근의 악성코드는 이러한
영역에 존재함)

좋은 파일



너머
범



blacklisting 방식이
잘 동작함

가운데 영역은 새로운
기술이 필요함



Whitelisting이 잘
동작함



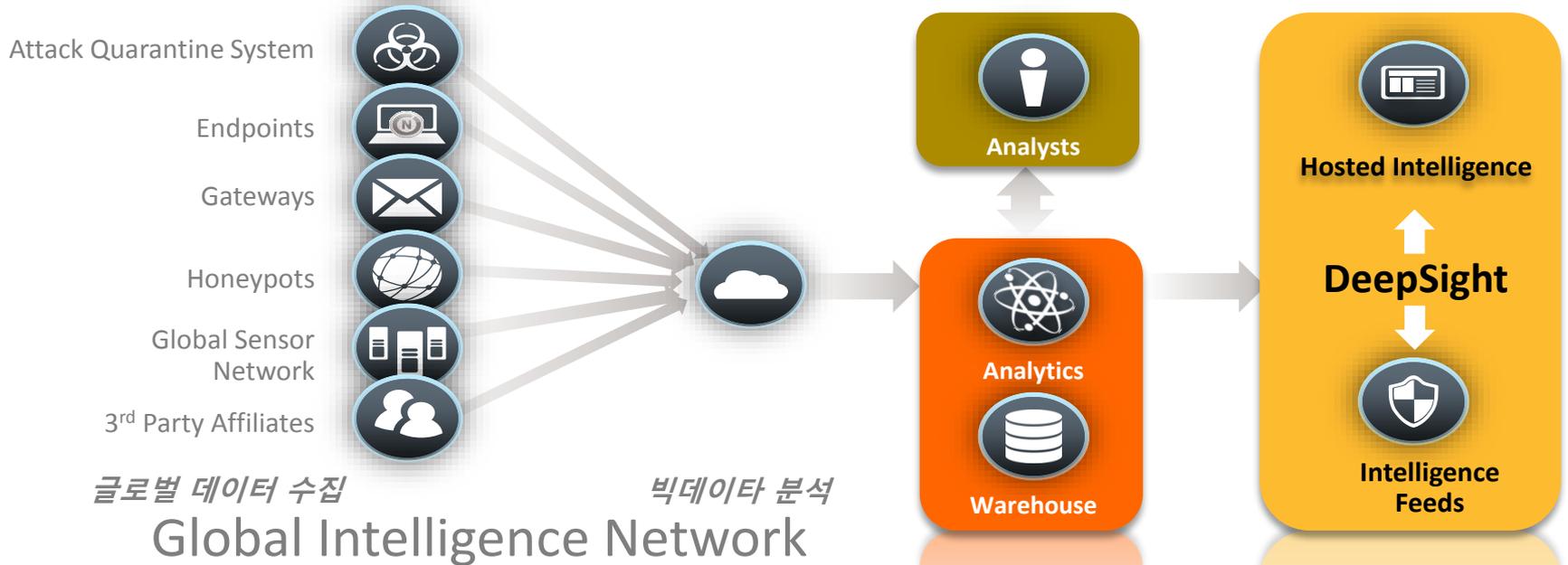
Symantec Technology

#1

In the Market

전세계에서 가장 포괄적인 인터넷 보안 위협 데이터 수집 체계

- 시만텍 글로벌 인텔리전스



전 세계에 지원

글로벌 지원 범위와 규모

24x7 이벤트 로깅

보안 위협 탐지

- 전세계 200여 개 국가의 6900만개 센서 가동

악성 코드 인텔리전스

- 1억 3천 3백만대의 서버, 클라이언트, 게이트웨이
- 글로벌 모니터링

취약점

- 5만 1천개 이상의 취약점
- 1만 6천개의 벤더
- 105,000여개 기술

스팸/피싱

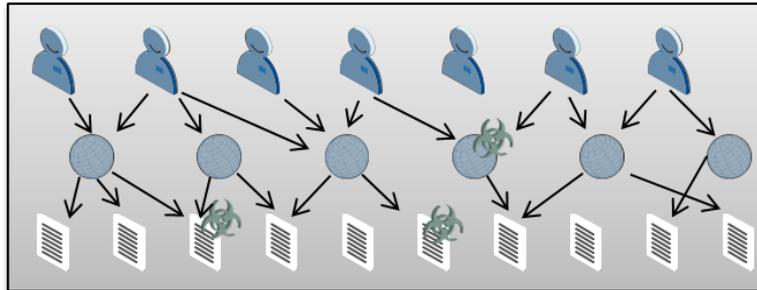
- 500만개의 유인 계정
- 매일 80억통 이상의 이메일 메시지와 14억건 이상의 웹 요청 처리

- 평판기술 (Reputation - Insight)

Global Scale - 전세계 1억 3천 3백만대의 클라이언트를 통해 수집된 파일 데이터 정보를 바탕으로, 파일 해쉬, 정상/악성 유무, 신뢰도, 분포도 등을 종합하여 Zero-Day Attack과 같은 신규 위협에 강력한 대응 기술을 제공하고 있습니다.

Norton Community Watch

옵트인 프로그램으로 익명으로
데이터 수집



Symantec 평판 엔진은

수집된 데이터를 안정성 평판
결정에 사용함

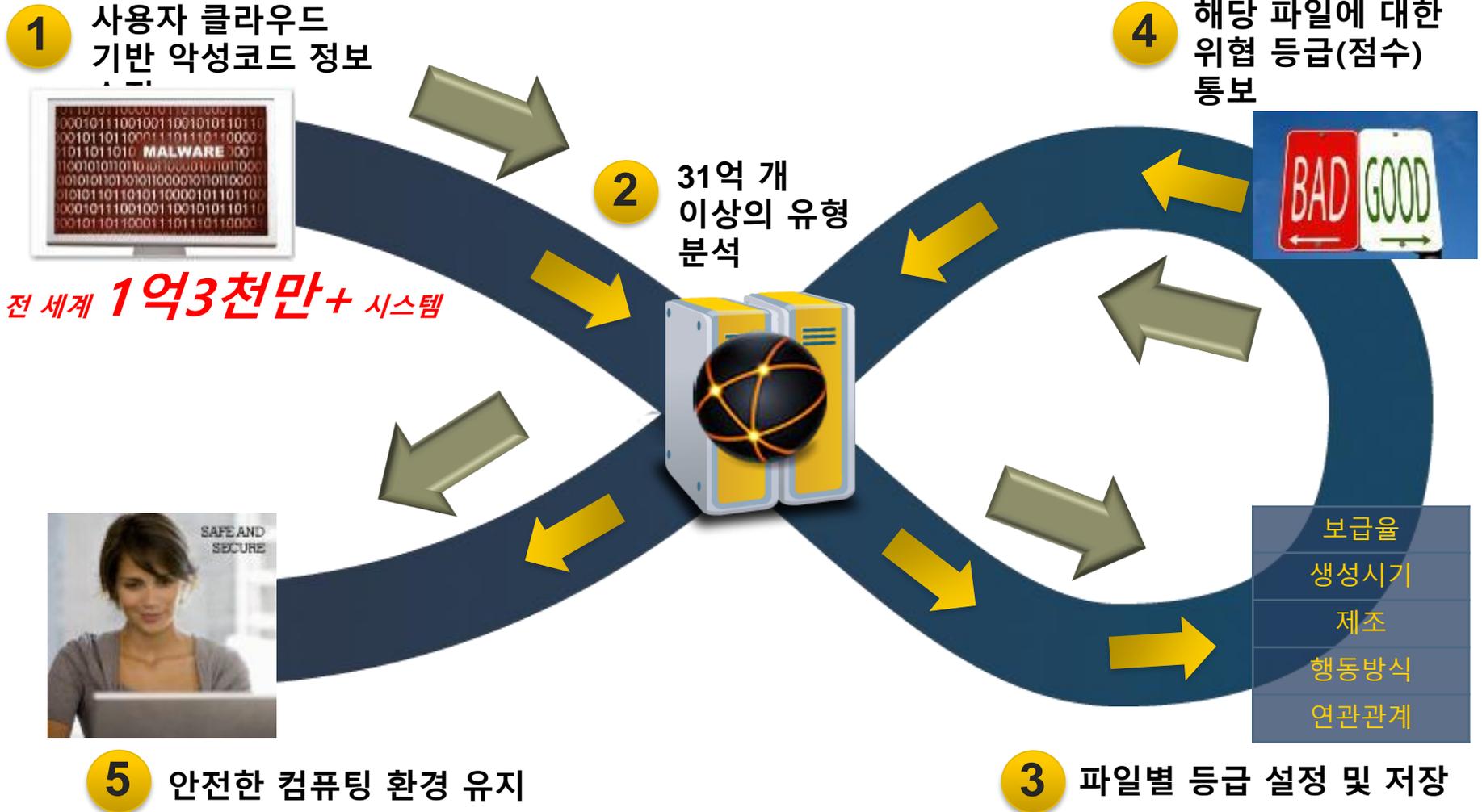


이 시스템은 전세계의 애플리케이션을 추적함

- 수십억개의 유일한 애플리케이션(버전/언어)
- 대상: 실행파일, 드라이버, DLL 및 플러그인
- 각 파일의 평판, 분포도, 발견일자
- 높은 정확도

시만텍 파일
안정성 평판

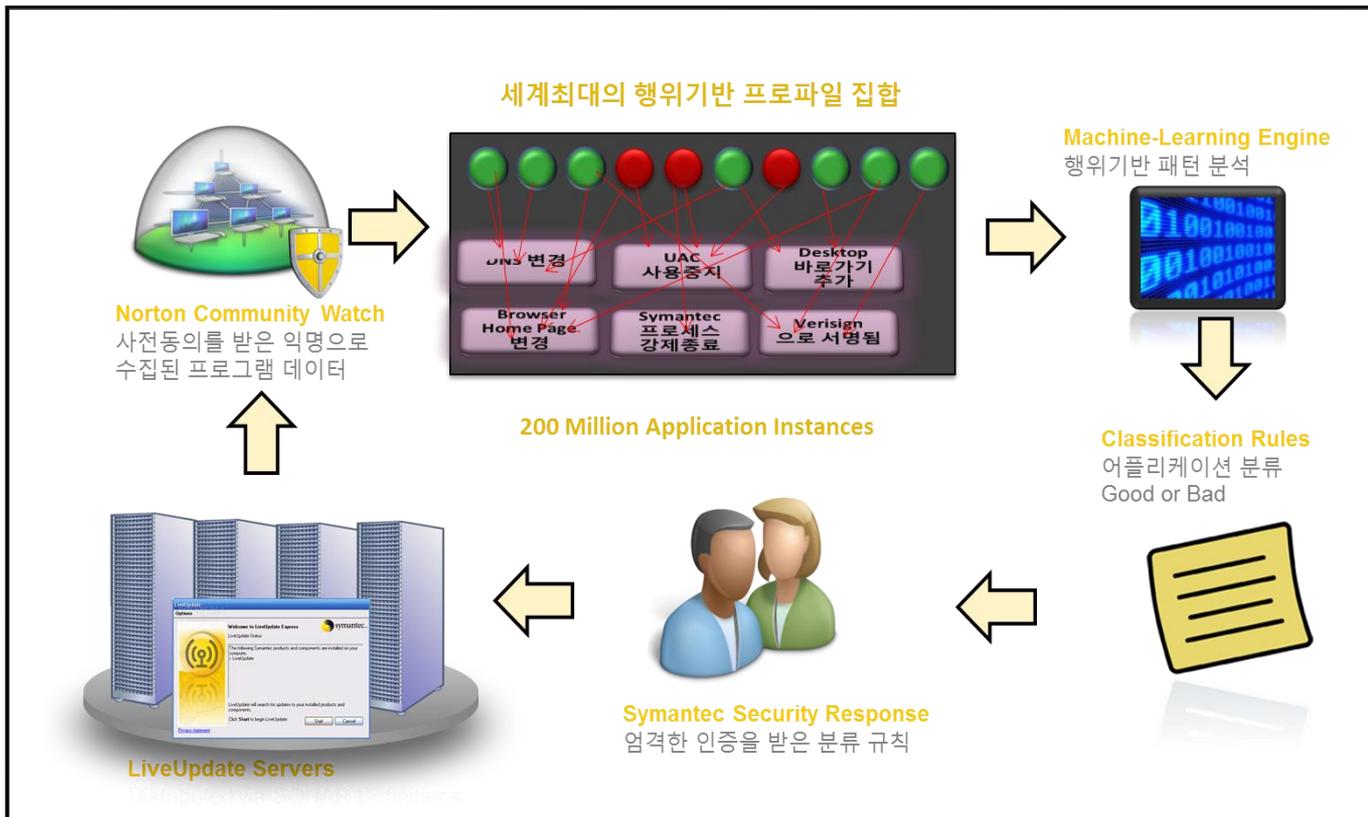
- . 평판기술 (Reputation - Insight)



- 행위기반 탐지(SONAR)

글로벌적으로 수집된 프로그램 데이터를 바탕으로 행위기반 프로파일 집합을 만들어, 바이러스 엔진에 포함되지 않은 새로운 위협에 대해 행동 기반의 차단을 수행합니다.

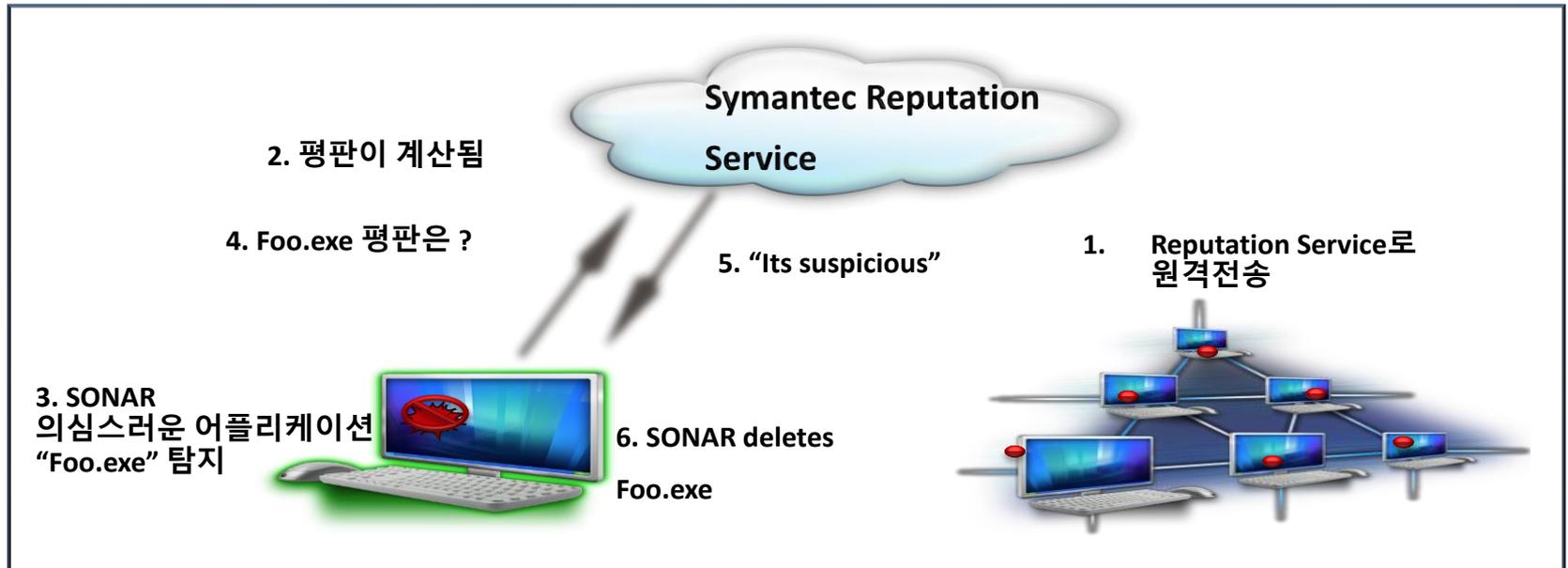
Symantec Cloud-based 평판 기술과 함께 동작하여 새로운 위협에 대한 대응이 가능합니다.



400 Behaviors

- 행위기반 탐지(SONAR)

악성 파일에 대해 SONAR 자체의 행위 탐지와 Cloud-based Reputation을 통한 이중 검증으로 오탐을 줄일 수 있습니다.



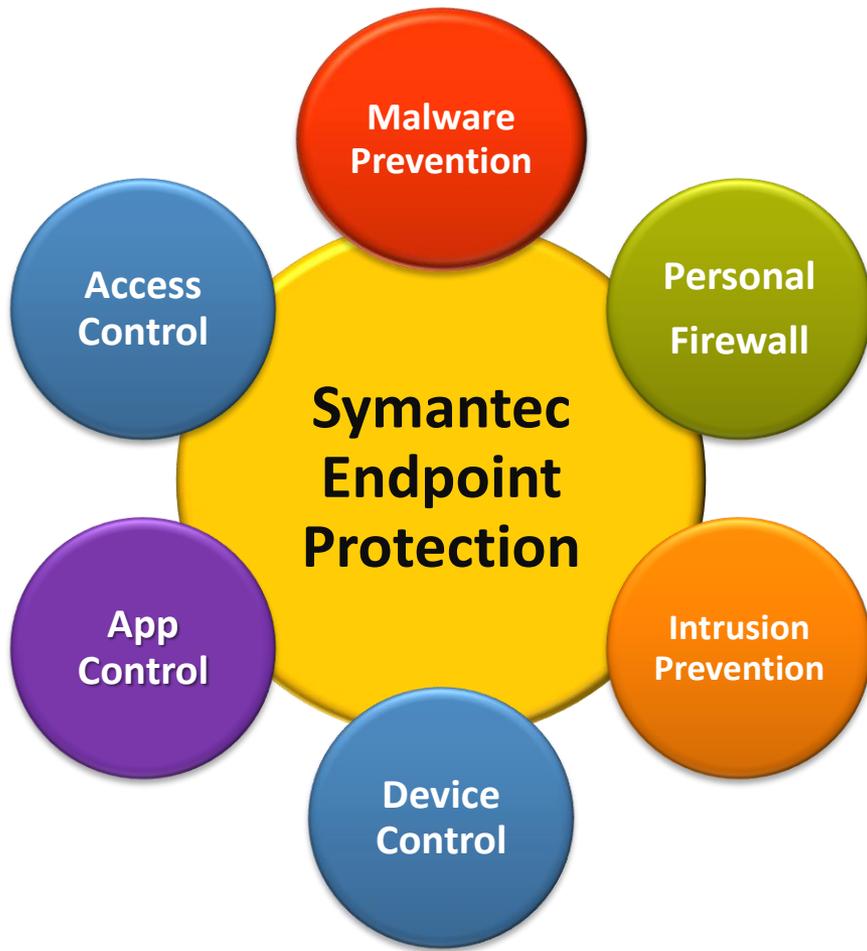
▪ Rules of Engagement

- ✓ Never Delete : OS에 해당하는 부분
- ✓ Never Delete : Microsoft 혹은 Symantec에 의해 디지털서명된 파일
- ✓ Never Delete : 신뢰할 수 있는 Class-3 수준의 인증기관에서 서명된 파일



Symantec Endpoint Protection 12 (SEP 12)

- . SEP12 기능 개요



악성코드
차단

세계 1위의 Anti-Virus 탐지

31억개 이상의 파일에 대한 평판기술과 400개의 행위탐지 기술을 바탕으로 최신 보안 위협에 대응합니다

네트워크
보호

강력한 네트워크 보호

어플리케이션 기반의 통제 설정과 위치에 따른 방화벽 정책 설정(시간, 도메인, 포트 등), 침입차단(IPS) 패턴을 통해 네트워크를 통한 악성코드 유입을 차단합니다.

매체 제어

매체에 대한 완벽한 통제

비인가 매체(USB, 블루투스, 이미지 장비 등)에 대한 차단/허용 및 인가된 매체에 대한 읽기/쓰기 권한 부여를 통한 매체 통제 기능을 제공합니다.

어플리케이션
제어

유연한 어플리케이션 통제

위험한 것으로 알려진 블랙리스트 애플리케이션의 실행을 차단하고, 회사 표준 이외의 어플리케이션 실행을 차단하여 사내 시스템을 보호합니다.

- 악성코드 차단 (1/2)

Symantec Protection Model *Defense in depth*



**Firewall &
Intrusion
Prevention**
NETWORK

멀웨어가 PC에
영향을 미치기 전에
차단



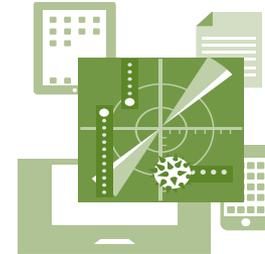
Antivirus
FILE

스캔 후 존재하는
멀웨어를 삭제



Insight
REPUTATION

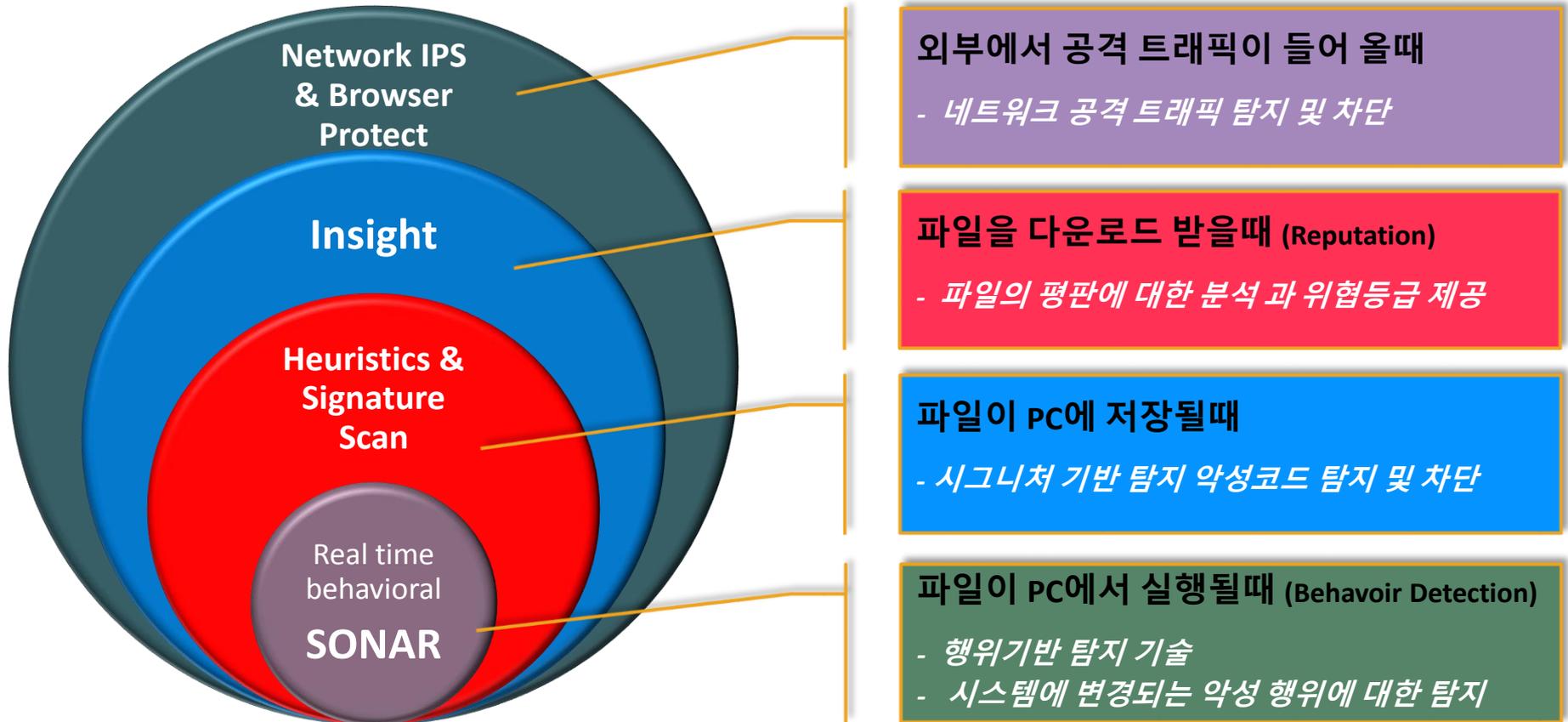
시만텍의 노하우를
이용한 파일이나
웹사이트의 안정성을
판단



SONAR
BEHAVIORS

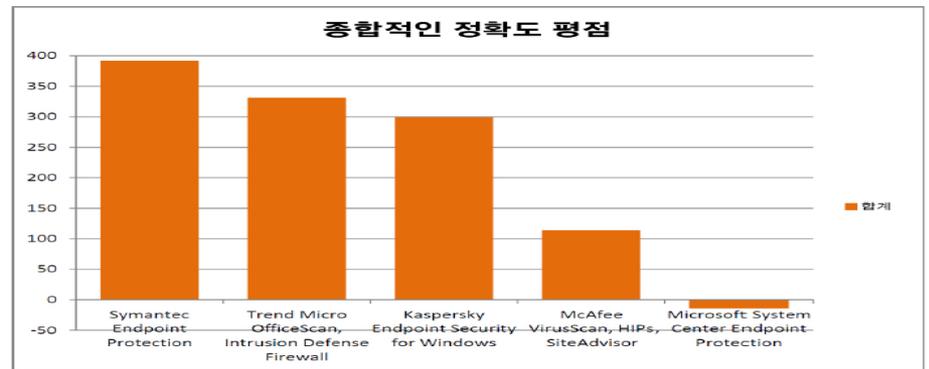
의심 행위를 보인
프로그램을 모니터
또는 차단

- 악성코드 차단 (2/2)

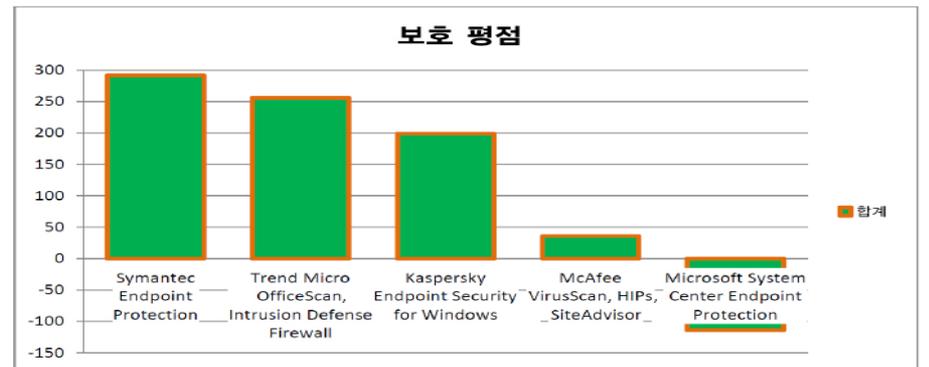


- 최고의 기술력

Gartner에서 Leader 그룹으로 분류되었고, 국제 백신테스트 표준기구인 'Dennis Technology Labs'이 실시한 독립 테스트에서 Symantec Endpoint Protection이 악성코드 차단 및 제거여부 평가에서 최고점수 AAA를 획득하였습니다.



종합적인 정확도 평점은 악성 코드와 합법적인 애플리케이션 모두에 대한 성공적인 작동과 실패한 작동 결과를 반영합니다.



보호 평점의 경우 보안 위협을 완벽하게 차단하는 제품에 가산점을 주고 보안 위협 차단에 실패하면 감점합니다.

- 네트워크 보호 ; 개인 방화벽 (Personal Firewall)

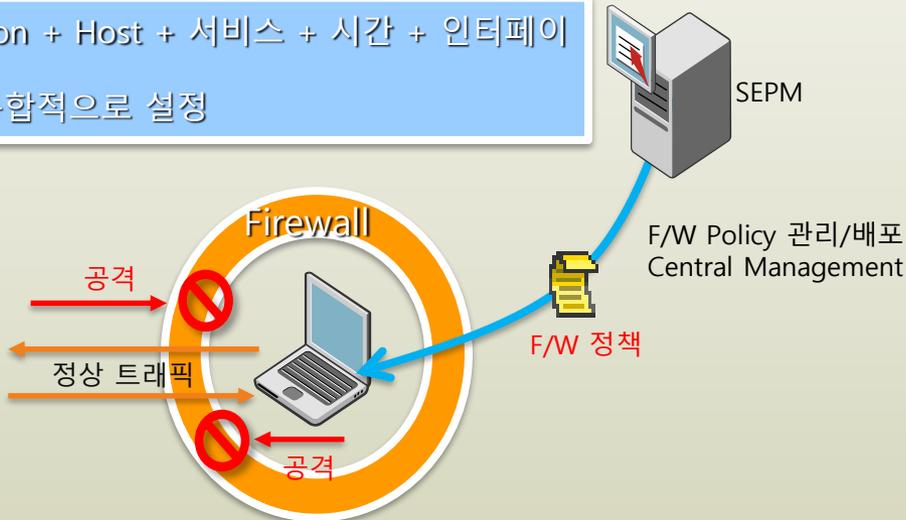
응용 프로그램 기반의 통제 설정이 가능하여 기존 네트워크 기반의 방화벽에서 수행할 수 없었던

메신저, P2P, 도메인 기반의 방화벽 정책 설정이 가능합니다.

또한, 공격을 시도한 클라이언트를 자동으로 일정시간 차단하여 추가 공격을 차단합니다.

향상된 Application Centric 기반 Firewall Rule 생성 지원

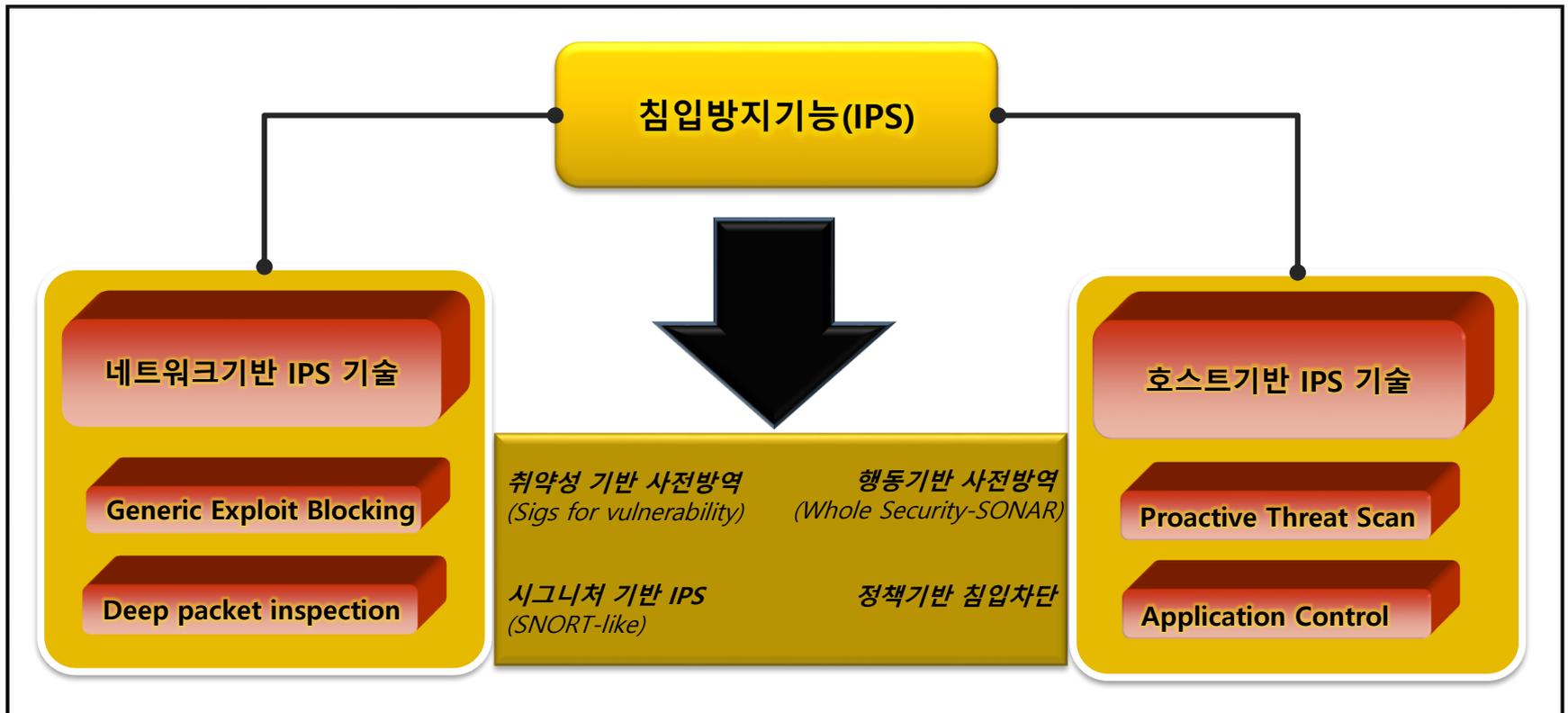
Application + Host + 서비스 + 시간 + 인터페이스
조건을 복합적으로 설정



No	En	Name	Action	Application	Host	Service	Log	Severity	Adapter	Time	Screen
1	<input type="checkbox"/>	Block IPv6	Block	Any	* Any	Ethe...	None	10-Minor	All Ada...	* Any	* Any
2	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (Ter...	Block	Any	* Any	UDP...	None	10-Minor	All Ada...	* Any	* Any
3	<input checked="" type="checkbox"/>	Block IPv6 over IPv4 (ISA...	Block	Any	* Any	P[41]	None	10-Minor	All Ada...	* Any	* Any
4	<input checked="" type="checkbox"/>	Block ICMPv6	Block	Any	* Any	P[50]	None	10-Minor	All Ada...	* Any	* Any
5	<input type="checkbox"/>	Block SIMP	Block	Any	* Any	SIM...	None	10-Minor	All Ada...	* Any	* Any
6	<input checked="" type="checkbox"/>	Allow fragmented packets	Allow	Any	* Any	P[fr...	None	10-Minor	All Ada...	* Any	* Any
7	<input checked="" type="checkbox"/>	Block wireless EAPOL	Block	Any	* Any	Ethe...	None	10-Minor	All Ada...	* Any	* Any
8	<input checked="" type="checkbox"/>	Allow USB over IEEE802...	Allow	Any	* Any	Ethe...	None	10-Minor	All Ada...	* Any	* Any
9	<input checked="" type="checkbox"/>	Allow Local File Sharing L...	Allow	Any	* Any	Remot...	TCP...	None	All Ada...	* Any	* Any
10	<input checked="" type="checkbox"/>	Block Local File Sharing	Block	Any	* Any	TCP...	Write...	10-Minor	All Ada...	* Any	* Any
11	<input checked="" type="checkbox"/>	Allow Bootp	Allow	Any	* Any	UDP...	None	10-Minor	All Ada...	* Any	* Any
12	<input checked="" type="checkbox"/>	Allow L2TP Discovery It...	Allow	Any	* Any	Remot...	UDP...	None	All Ada...	* Any	* Any
13	<input checked="" type="checkbox"/>	Block L2TP Discovery	Block	Any	* Any	UDP...	Write...	10-Minor	All Ada...	* Any	* Any
14	<input checked="" type="checkbox"/>	Allow Web Service requ...	Allow	Any	* Any	Remot...	TCP...	None	All Ada...	* Any	* Any
15	<input checked="" type="checkbox"/>	Block Web Service requ...	Block	Any	* Any	TCP...	Write...	10-Minor	All Ada...	* Any	* Any

- 네트워크 보호 ; 침입방지 (Personal IPS)

OS 및 어플리케이션의 취약점이 발견된 후, 점점 빨라지는 악성코드 출현(Zero-Day Attack)에 대응하기 위한 수단으로, 브라우저 보호 및 드라이브 바이 다운로드, 네트워크 기반 패킷 공격으로부터 시스템을 실시간 보호합니다.

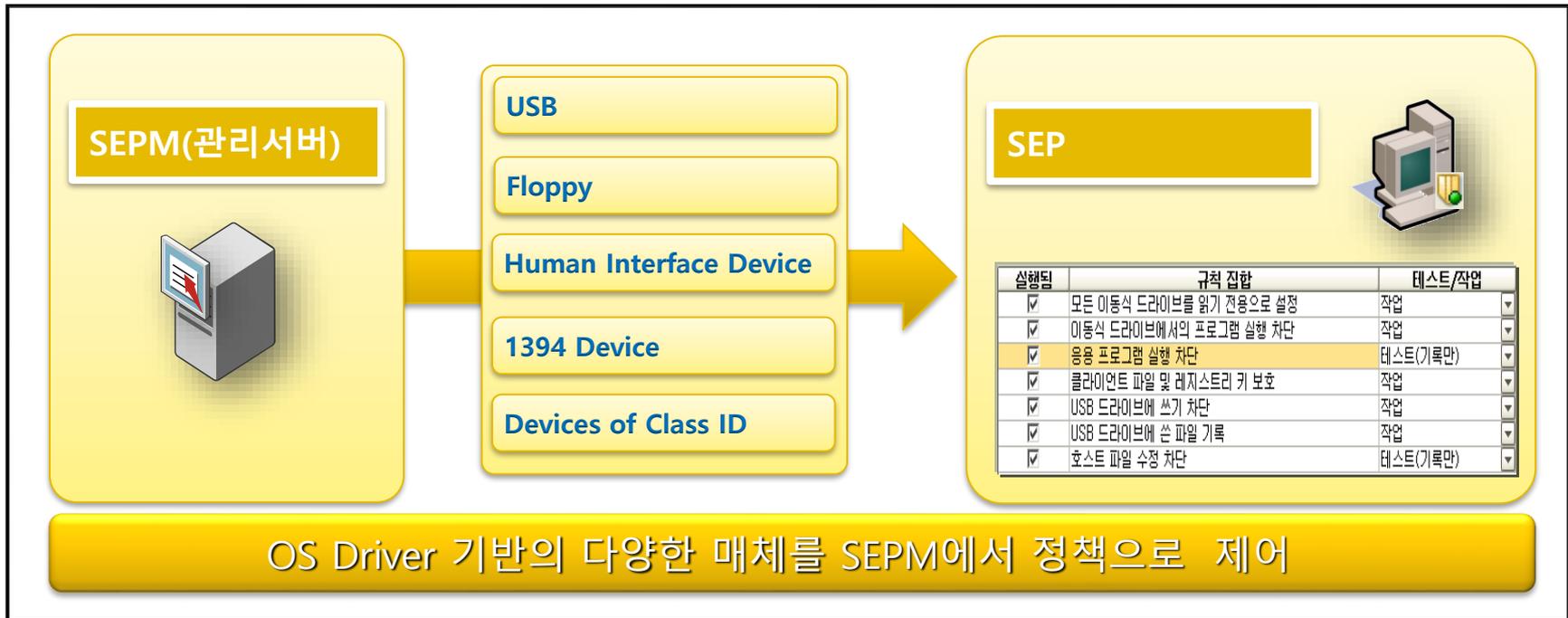


- 매체 제어(Device Control) (1/2)

Symantec Endpoint Protection의 매체제어는 허가되지 않은 장치를 차단하거나 허용하며, 장치별 사용 허용 권한 제어를 수행할 수 있습니다.

➤ 주요 기능

다양한 매체에 대한 읽기, 쓰기, 실행 통제 제공 및 이에 대한 로깅을 제공합니다.



- 매체 제어(Device Control) (2/2)

하드웨어 장치의 분류 기준이 되는 클래스 ID를 기반으로 한 통제와, 개별 장치를 인식하기 위한 Device ID를 기준으로 차단, 예외 or 로그 기록등을 수행합니다.

➤ 지원 매체

USB, Floppy, 1394, IDE, Tape, CD/DVD, 프린트 장비, PCMCIA, 이미징 장비(스캐너, 디지털 카메라 등) 적외선장비, 블루투스 등 무선장비, SCSI, 모뎀, 스마트카드 리더, 스토리지 볼륨 등의 시스템 장비 지원

The screenshot shows the Windows Device Control interface. A red box highlights the '응용 프로그램 및 장치 제어' (Application and Device Control) icon in the taskbar. Another red box highlights the '장치 제어' (Device Control) window, which is divided into '차단된 장치' (Blocked devices) and '차단에서 제외된 장치' (Devices excluded from blocking). A third red box highlights the '장치 선택' (Device Selection) dialog box, which lists various hardware categories and their corresponding Class IDs and Device IDs. A fourth red box highlights the '하드웨어 장치' (Hardware Device) dialog box, which is used to add a new device to the list, showing fields for '장치 이름' (Device Name), '클래스 ID' (Class ID), and '장치 ID' (Device ID).

장치 이름	ID
USB	클래스: {36fc9e60-c465-11cf-8056-444553540000}
USB 장치	클래스: {36fc9e60-c465-11cf-8056-444553540000}
Bluetooth Devices	클래스: {e0cbf06c-cd8b-4647-bb8a-263b4309574}

장치 이름	ID
Human Interface Devices (Mice, Joysticks, Ga...	클래스: {745a17a0-74d3-11d0-b6fe-00a0c9...
USB	클래스: {36fc9e60-c465-11cf-8056-4445535...
Floppy	클래스: {4d36e969-e325-11ce-bfc1-08002b...
1394 FireWire Host Controller	클래스: {6bdd1fc1-810f-11d0-bec7-08002b...
IDE	클래스: {4d36e96a-e325-11ce-bfc1-08002b...
Tape Drives	클래스: {6d807884-7d21-11cf-801c-08002b...
CD/DVD Drives	클래스: {4d36e965-e325-11ce-bfc1-08002b...
Printing Devices	클래스: {4d36e979-e325-11ce-bfc1-08002b...
PCMCIA	클래스: {4d36e977-e325-11ce-bfc1-08002b...
Imaging Devices (Scanners, Digital Cameras, e...	클래스: {6bdd1fc6-810f-11d0-bec7-08002b...
Infrared Devices	클래스: {6bdd1fc5-810f-11d0-bec7-08002b...
Bluetooth Devices	클래스: {e0cbf06c-cd8b-4647-bb8a-263b43...
SCSI	클래스: {4d36e97b-e325-11ce-bfc1-08002b...
Modems	클래스: {4d36e96d-e325-11ce-bfc1-08002b...
Smart Card Readers	클래스: {50dd5230-ba8a-11d1-bf5d-0000980...
Ports	클래스: {4d36e978-e325-11ce-bfc1-08002b...
Network Adapters	클래스: {4d36e972-e325-11ce-bfc1-08002b...
Biometric	클래스: {53d29e7-377c-4d14-864b-eb3a86...
Disk Drives	클래스: {4d36e967-e325-11ce-bfc1-08002b...
Storage Volumes	클래스: {71a27cdd-812a-11d0-bec7-08002...
Bluetooth Device	클래스: {95c7a0a0-3094-11d7-a202-00508b...
USB 장치	클래스: {36fc9e60-c465-11cf-8056-4445535...
CDROM	클래스: {4d36e965-e325-11ce-bfc1-08002b...
1394 Firewire 호스트 컨트롤러	클래스: {6bdd1fc1-810f-11d0-bec7-08002b...
플러피	클래스: {4d36e969-e325-11ce-bfc1-08002b...

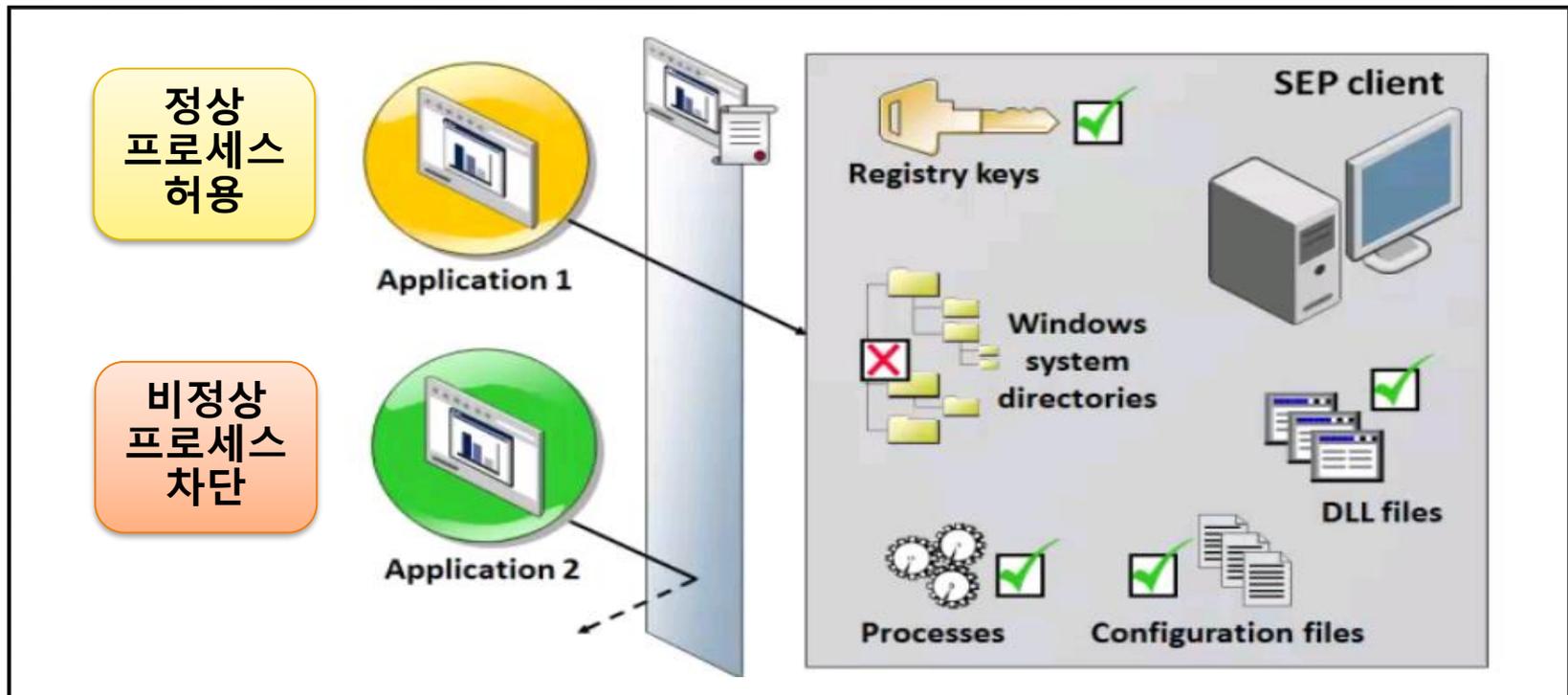
장치 이름: wibro
클래스 ID: {4d36e980-e325-11ce-bfc1-08002be10318}
장치 ID:

- 어플리케이션 제어 (Application Control) (1/2)

필수 프로세스, 파일 및 폴더, 중요 레지스트리를 악의적 위협으로부터 보호하고, 상용프로그램 등 응용프로그램의 실행을 제한합니다.

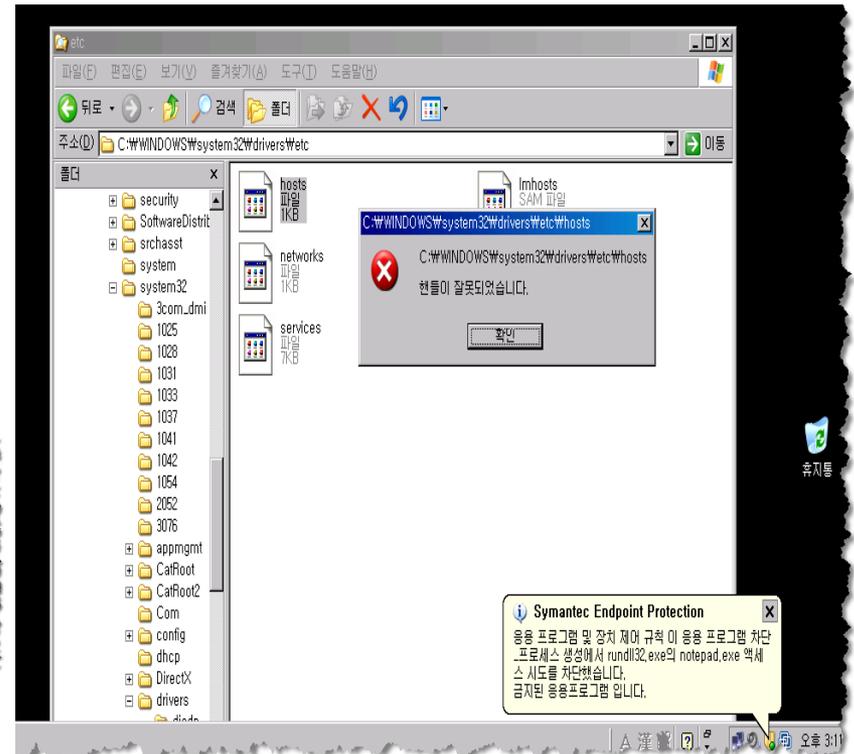
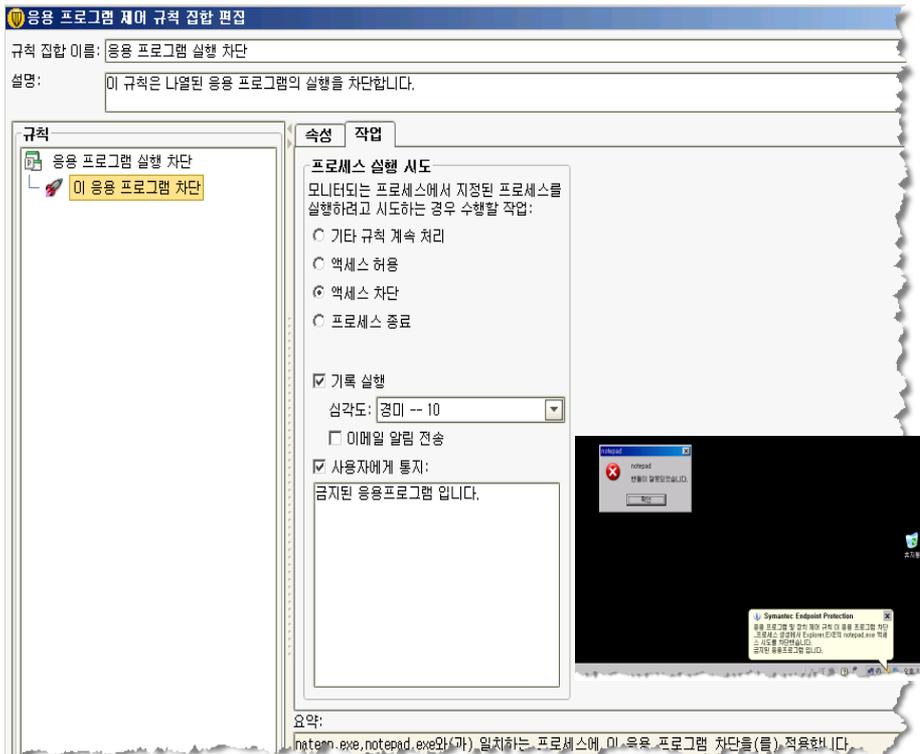
➤ 보호 영역

레지스트리, 파일 및 폴더, 프로세스, DLL Files



- 어플리케이션 제어 (Application Control) (2/2)

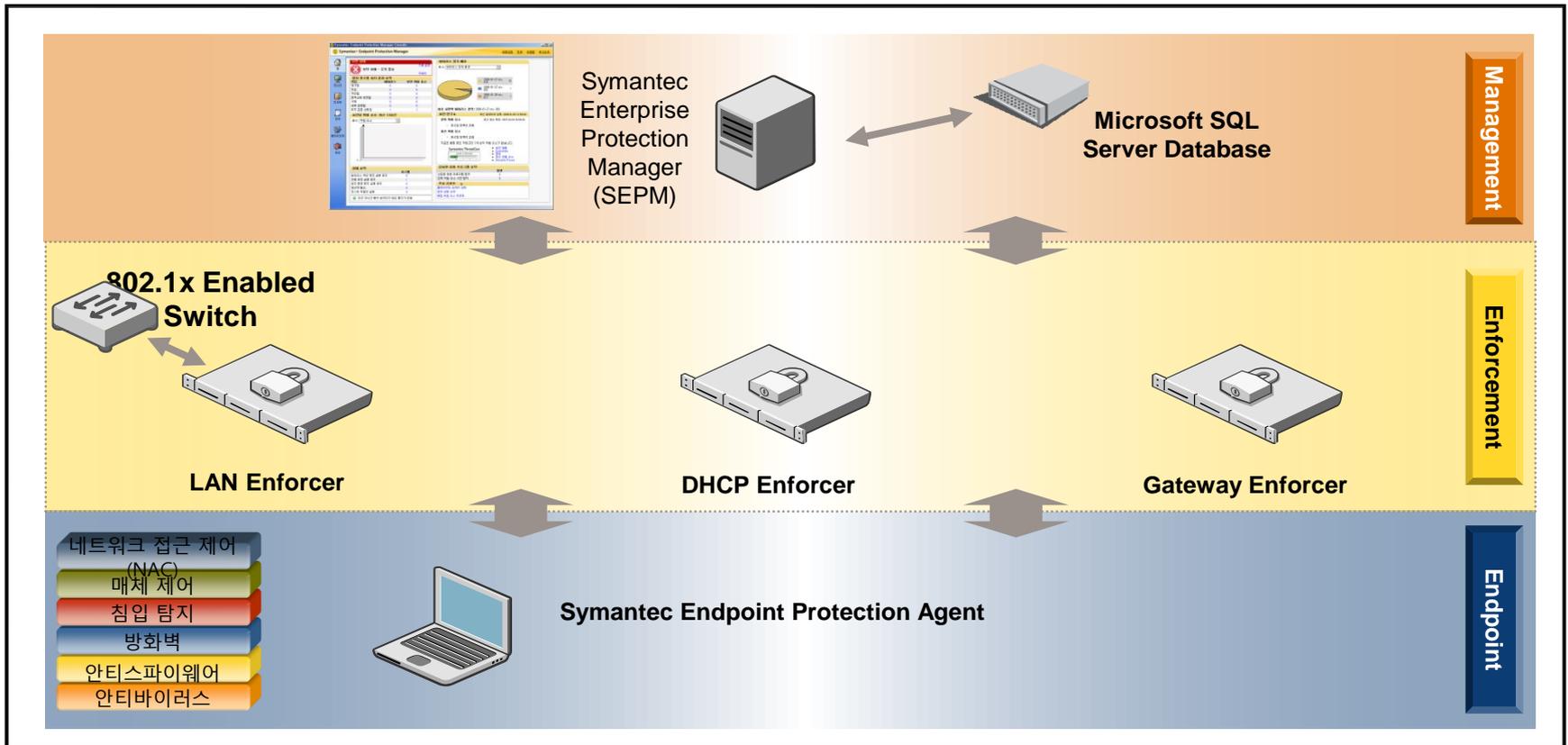
중요 파일에 대한 보호 기능을 통해 **허가되지 않은 프로세스를 통한 파일 접근 시도를 차단**합니다.
실행이 금지된 응용프로그램 등록을 통해 **프로그램 실행방지, 프로세스 강제종료, 로그기록, 사용자 알림** 기능을 수행합니다.



- NAC (Network Access Control)

타사 대비 별도의 Agent 설치없이 SEP를 통해 NAC 구성이 가능하므로,

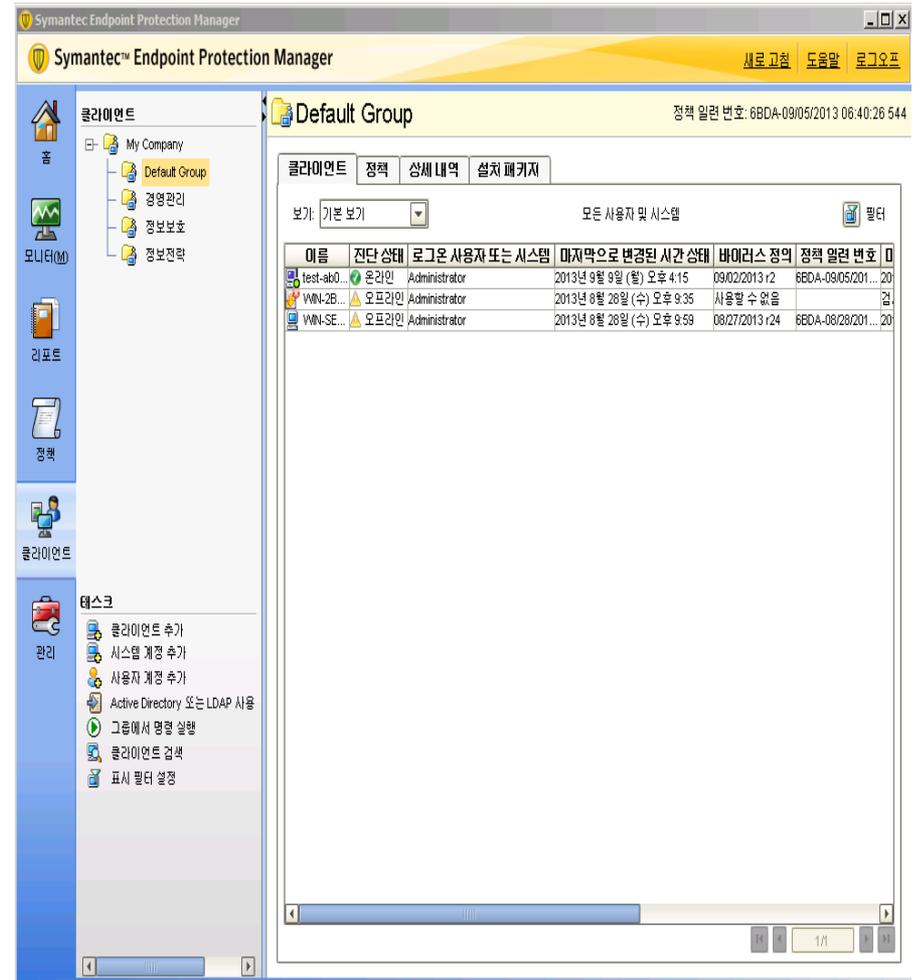
PC, 네트워크 시스템 자원에 대한 부하를 최소화하여 효율적이고 안전한 네트워크 접근제어 구성이 가능합니다.



- Management

· 중앙 집중 관리 기능 제공

- ✓ 클라이언트 상의 감염, 패턴 미업데이트, 자동 보호 기능 중지등의 이벤트 및 통계를 Dash Board 등을 통하여 파악
- ✓ 정의한 이벤트 경고 발생 시 (감염, 서비스 중지, 패턴 미업데이트) 중앙 콘솔을 통한 경고 발생
- ✓ 클라이언트 시스템 재시작, 강제 패턴 업데이트, 관리자에 의한 검색등의 명령 실행 시 중앙 콘솔을 통한 명령 실행 완료 여부 확인 가능
- ✓ 대규모 기업 환경에 따른 관리자 등록을 위하여, 정책 설정 권한 또는 보기 권한 등의 관리자 권한 부여 가능
- ✓ 다양한 리포팅 양식 제공
- ✓ 모니터 탭을 통한 실시간 모니터링 제공



Thank you!



솔루션사업부/컨설팅팀 김기준, 이세현
Email : soyou@bellins.net
서울특별시 서대문구 충정로 13 삼창빌딩 3층
Tel. 02-6925-1130 Fax. 02-2664-1575

Copyright © 2013 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.