McAfee™
Together is power.

Endpoint Data Loss Prevention

제품소개서

McAfee Gold Partner, VisualData

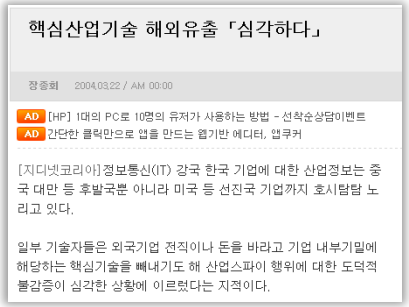
목차

제안 배경

제안배경

데이터 유출 사고로 인한 피해 증가

개인정보 침해 내용	소송 내용
담당자 실수로 단체메일에 고객 3만 명의 이름, 주민등록번호 등이 포함된 명단을 첨부	유출 피해자 1,024명, 손해 배상 소송 제기
L 전자회사 신입사원 응시자 400명의 입사원서 일부 노출	총 90명, 1인당 2천 만원, 배상 소송 제기
고객정보 DB 해킹 피해로 1,081만 명 개인정보 유출	총 24건 소송, 피해자 14만 명
600만 명 개인정보를 고객 동의 없이 TM업체에 제공, 전·현직 직원 22명 불구속 입건	소송 건수 20건, 피해자 1만 여명 소송참가
자회사 직원이 금전적 이득을 목적으로 1,100만 명 고객정보 DB 외부로 유출	소송건수 총 23건, 피해자 4만 985명



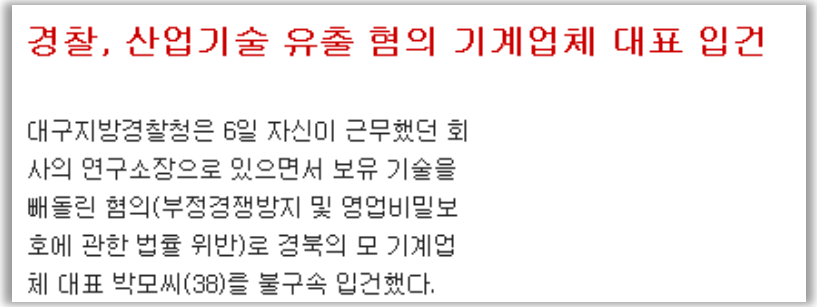
핵심산업기술 해외유출「심각하다」

장종회 2004.03.22 / AM 00:00

AD [HP] 1대의 PC로 10명의 유저가 사용하는 방법 - 선착순상담이벤트
AD 간단한 클릭만으로 앱을 만드는 웹기반 에디터, 앱쿠커

[지디넷코리아]정보통신(IT) 강국 한국 기업에 대한 산업정보는 중국 대만 등 후발국뿐 아니라 미국 등 선진국 기업까지 호시탐탐 노리고 있다.

일부 기술자들은 외국기업 전직이나 돈을 바라고 기업 내부기밀에 해당하는 핵심기술을 빼내기도 해 산업스파이 행위에 대한 도덕적 불감증이 심각한 상황에 이르렀다는 지적이다.



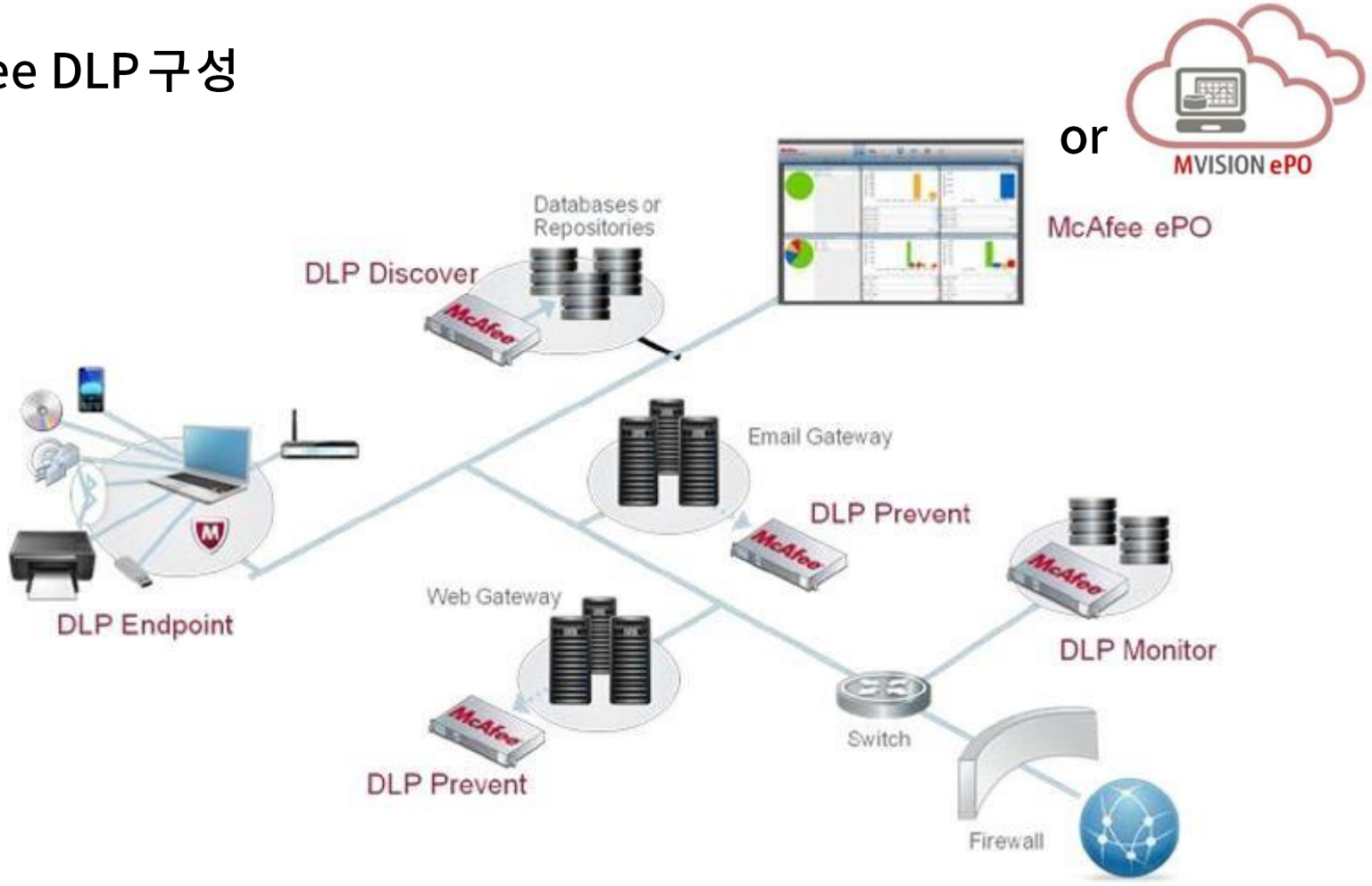
경찰, 산업기술 유출 혐의 기계업체 대표 입건

대구지방경찰청은 6일 자신이 근무했던 회사의 연구소장으로 있으면서 보유 기술을 빼돌린 혐의(부정경쟁방지 및 영업비밀보호에 관한 법률 위반)로 경북의 모 기계업체 대표 박모씨(38)를 불구속 입건했다.

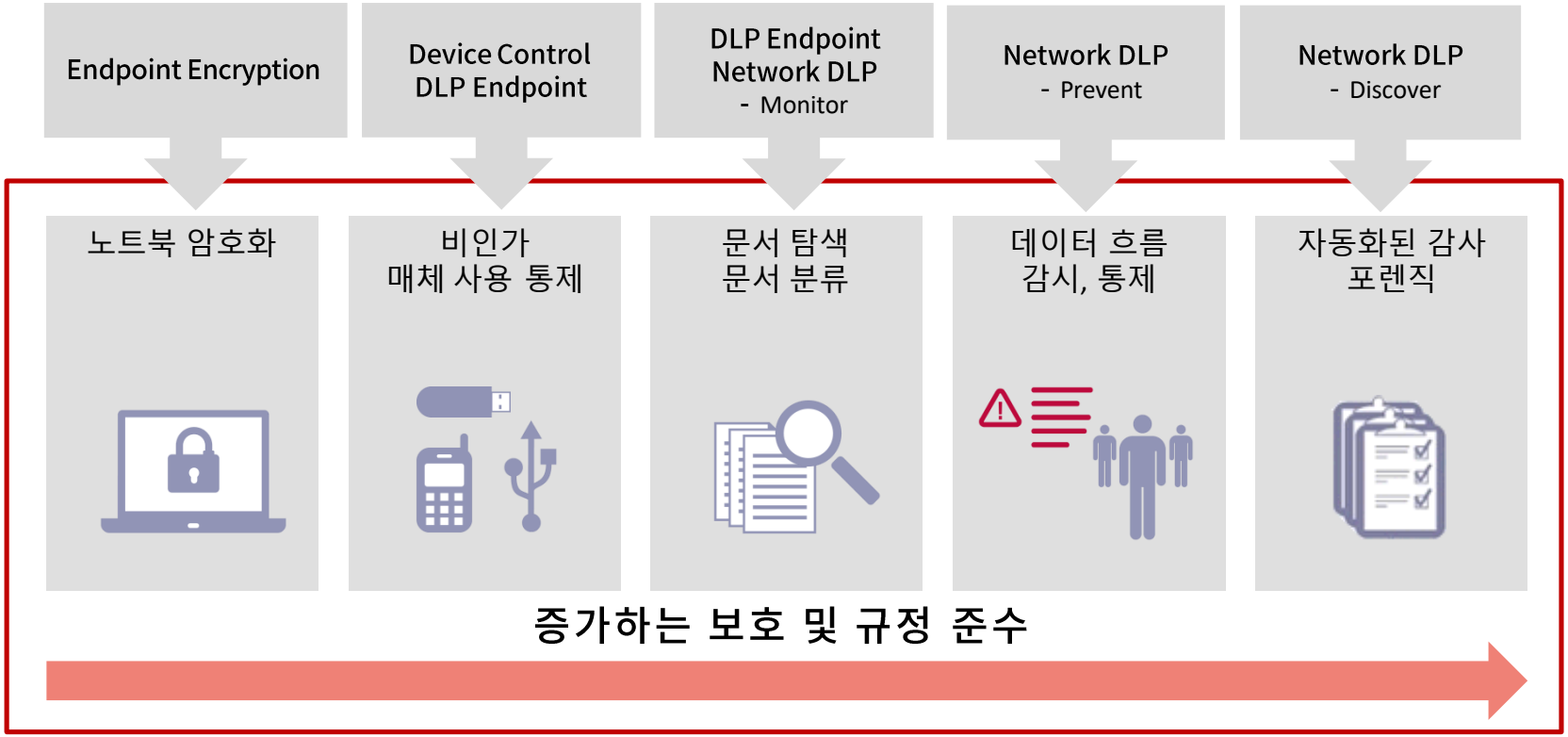
[출처 : 경찰청 사이버테러대응센터]

Endpoint DLP 개요

McAfee DLP구성



McAfee DLP 프로세스



엔드포인트 정보유출방지의 중요성

Data-in-Motion

~~1011011001~~10101001

Email/IM

Web Post

Data-at-Rest

011001101010011011

Cloud Apps

Desktop/Laptop

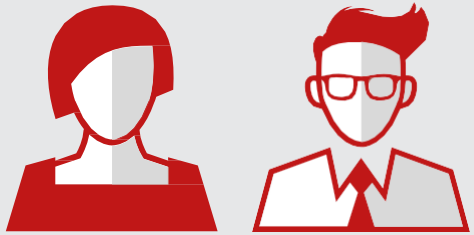
Data-in-Use

1011011001101001

Removable media / Mobile devices

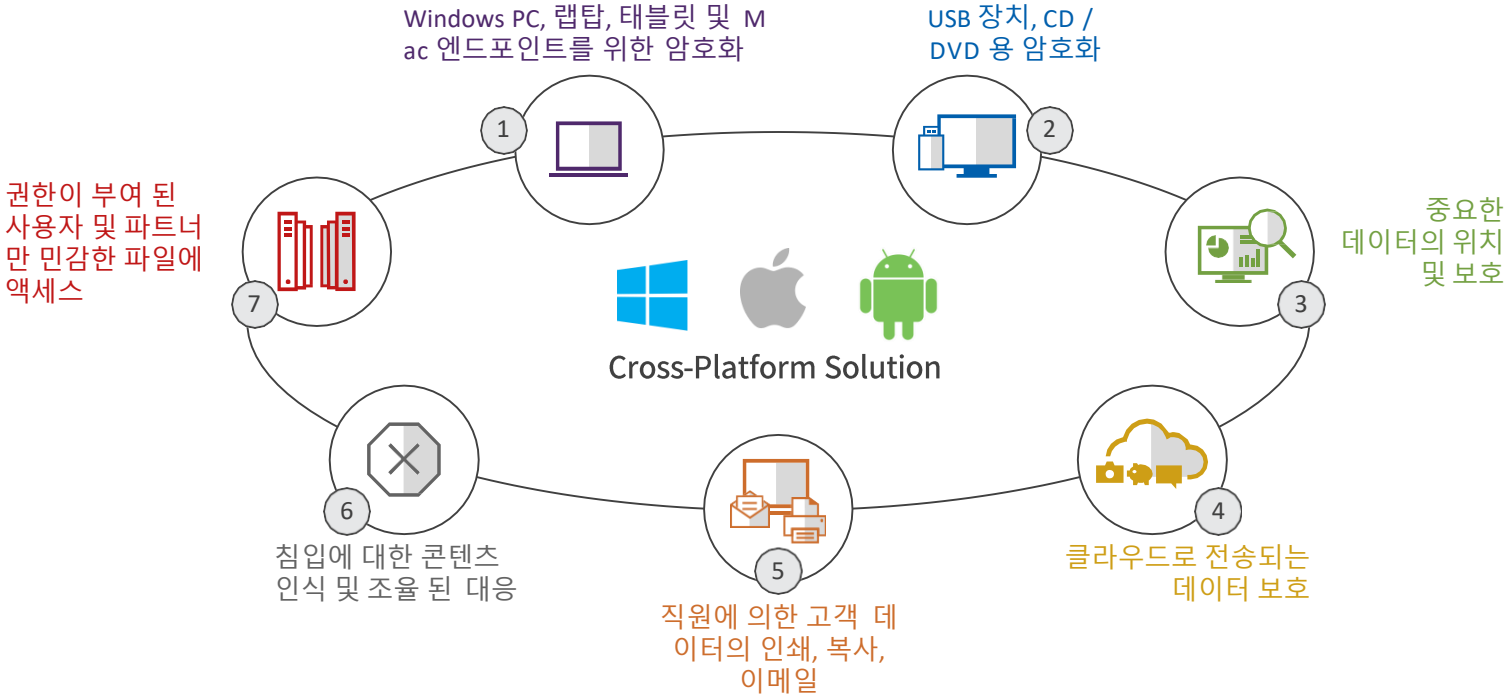
File & Clipboard

데이터 침해의 43 %는 내부 행위자에 의해 시작되었습니다 (의도적으로 또는 우연히)*



*McAfee Data Exfiltration Study: Actors, Tactics, and Detection, September 2015

엔드포인트 DLP 사용 사례



Endpoint DLP 기능

Endpoint DLP 포괄적 감시 차단 기능

✓ 단순한 매체 제어 외에 아래 10가지 경로에 대한 감시/차단 기능 제공

✓ 아래 룰은 관리자가 지정한 대로 특정한 어플리케이션, 태그된 데이터, 확장자 등에 국한하여 적용 가능

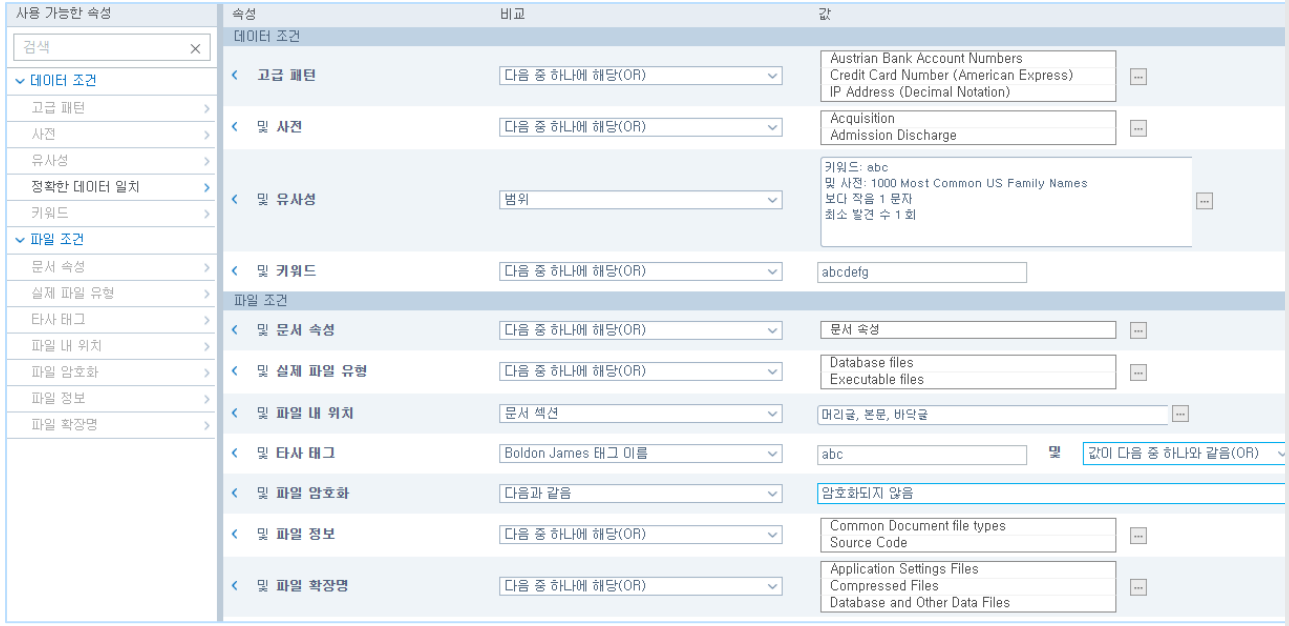
✓ 개별 룰에 따라 파라미터 정의 및 제공 액션의 차이 발생

Reaction rule	내 용	제공 액션
응용프로그램 파일 액세스 보호	지정한 응용프로그램(예:메신저, 브라우저)의 데이터 접근 감시	감시,경고, 차단, 증거저장
클립보드 보호 규칙	클립보드(복사/붙여넣기)사용을 통한 데이타 유출 방지	감시,경고, 차단, 증거저장
전자 메일 보호 규칙	MS Outlook을 통한 메일 감시(첨부, 본문)	감시, 경고,차단,증거저장
네트워크 공유 보호 규칙	다른 PC, 서버의 파일 시스템으로 나가는 데이터 감시	감시, 경고, 암호화, 증거저장
네트워크 보호 규칙	TCP/UDP지정된 서비스/포트 및 주소에 대한 유출 감시	감시, 경고,차단
인쇄 보호 규칙	로컬, 네트워크 프린터로 출력되는 데이터 감시	감시, 경고, 차단, 증거저장
이동식 저장소 보호 규칙	USB등 저장 장치로 복사되는 데이터 감시	감시, 경고, 차단, 암호화, 증거저장
화면 캡쳐 보호 규칙	중요 데이터의 화면 캡쳐를 방지	감시, 경고, 차단, 증거저장
웹 게시 보호 규칙	웹 브라우저에서 HTTP 업로드 되는 파일에 대한 감시	감시, 경고, 차단, 증거저장
클라우드 보호 규칙	클라우드 서비스를 통한 데이터 유출 감시	감시, 경고, 차단, RMS, 증거저장

Endpoint DLP 주요 기능

유출차단 분류 생성(Classification)

✓ 유출을 차단할 정보의 분류기준 생성

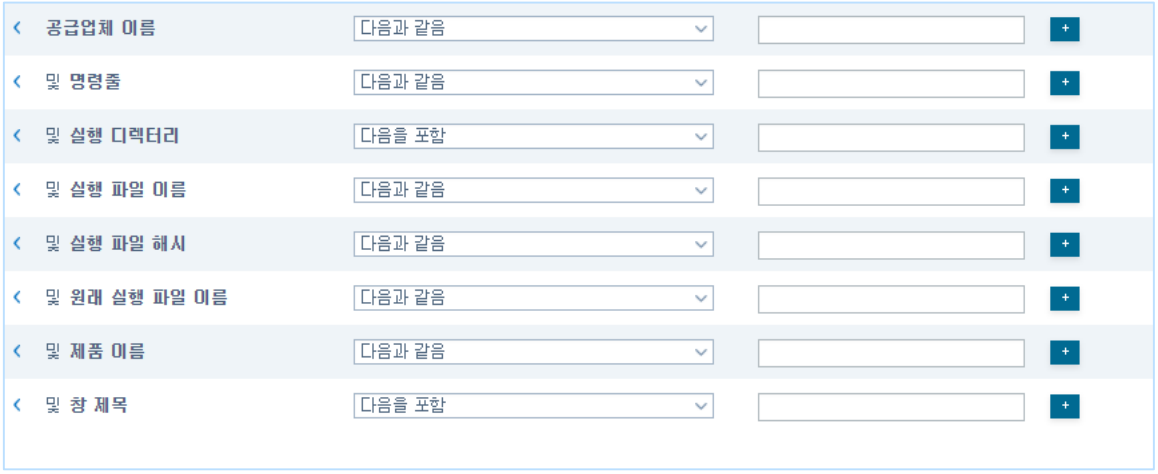


다양한 파라미터를 통해 유출차단 대상 데이터에 대한 정교한 분류기준 생성 가능

- 고급 패턴 (정규식)
- 사전
- 유사성
- 정확한 데이터 일치
- 키워드
- 문서 속성
- 실제 파일 유형
- 타사 태그
- 파일 내 위치
- 파일 암호화
- 파일 정보
- 파일 확장명

Endpoint DLP 주요 기능

보안문서 수동분류 (By Application): 관리자를 통한 중요데이터 수동분류 제공



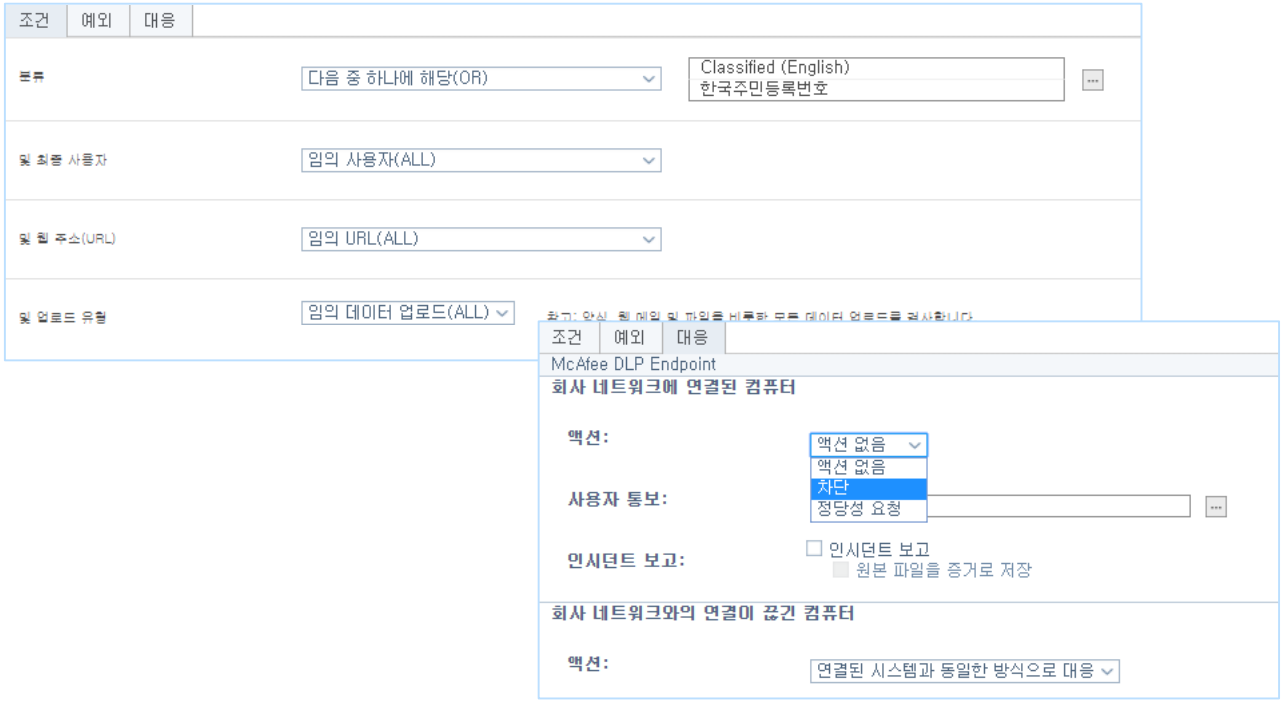
어플리케이션 정의 옵션의 다양화로 보다 정교한 데이터 분류, 강력한 정책 적용이 가능함

추가된 어플리케이션 정의 파라미터

- 공급업체 이름
- 명령줄
- 실행 디렉터리
- 실행 파일 이름
- 실행 파일 해시
- 원래 실행 파일 이름
- 제품 이름
- 창 제목

Endpoint DLP 주요 기능

컨텐츠 기반 웹 보호 (Web Protection) – 웹 브라우저를 통해 유출되는 중요데이터 제어



조건

1)분류: Classified 및 주민등록번호

2) 사용자: All

3) URL: Any URL

4) 업로드 유형: All

대응

1) 액션 없음, 차단, 정당성 요청

2) 알림 팝업

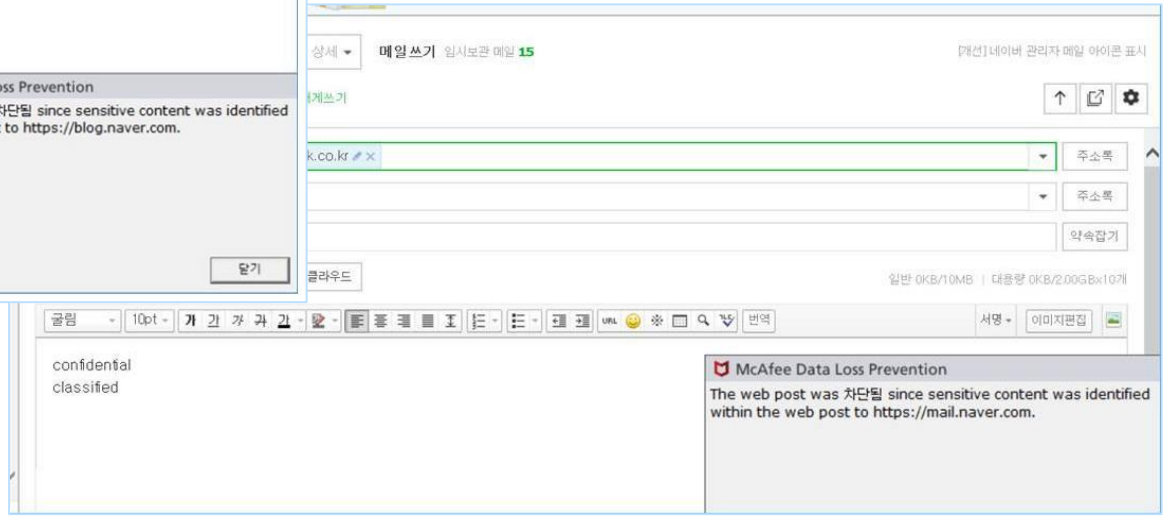
3) 인시던트 생성 및 증거저장

Endpoint DLP 주요 기능

컨텐츠 기반 웹 보호 (Web Protection) – 웹 브라우저를 통해 유출되는 중요데이터 제어

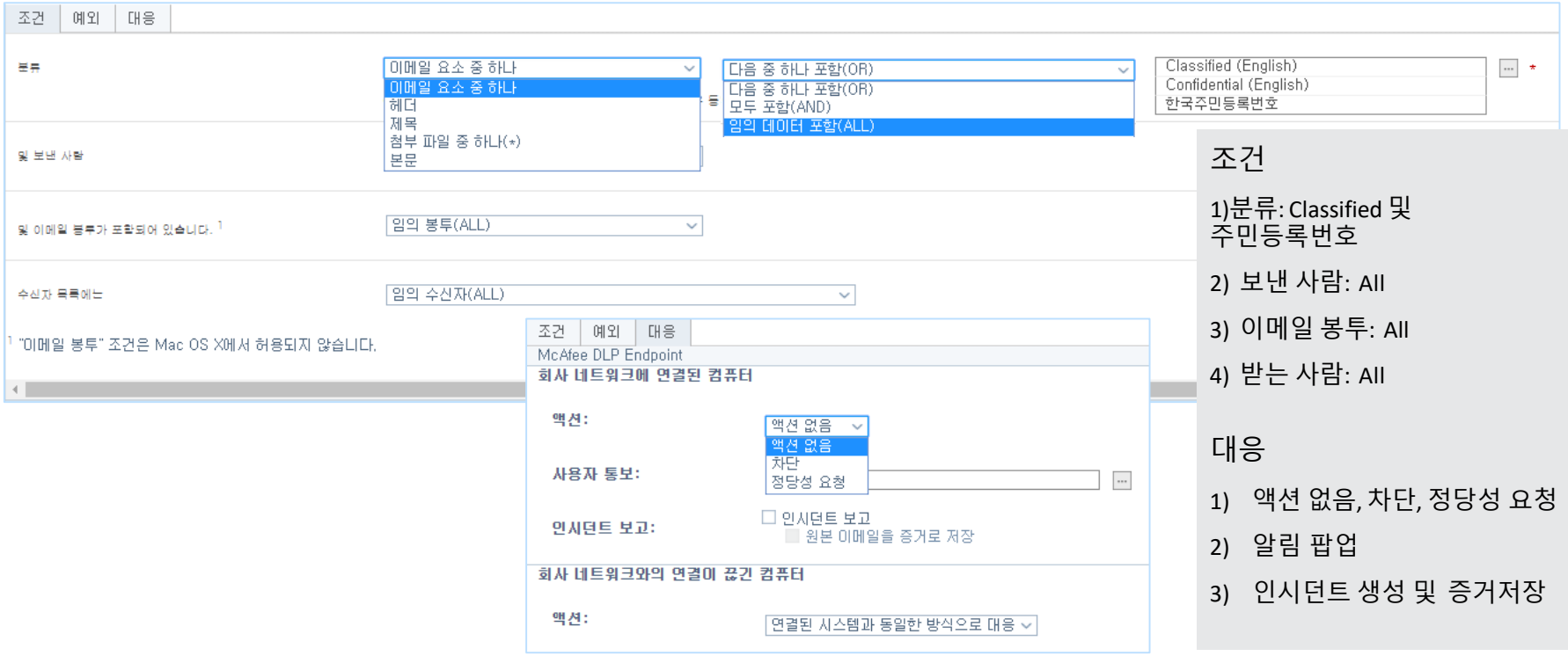
Naver Blog 포스팅 (Internet Explorer 11)

Naver 이메일 본문 작성 (Internet Explorer 11)



Endpoint DLP 주요 기능

컨텐츠 기반 이메일 보호 (Email Protection) – Outlook, Lotus 메일 클라이언트를 통한 이메일 제어



조건

1)분류: Classified 및 주민등록번호

2) 보낸 사람: All

3) 이메일 봉투: All

4) 받는 사람: All

대응

1) 액션 없음, 차단, 정당성 요청

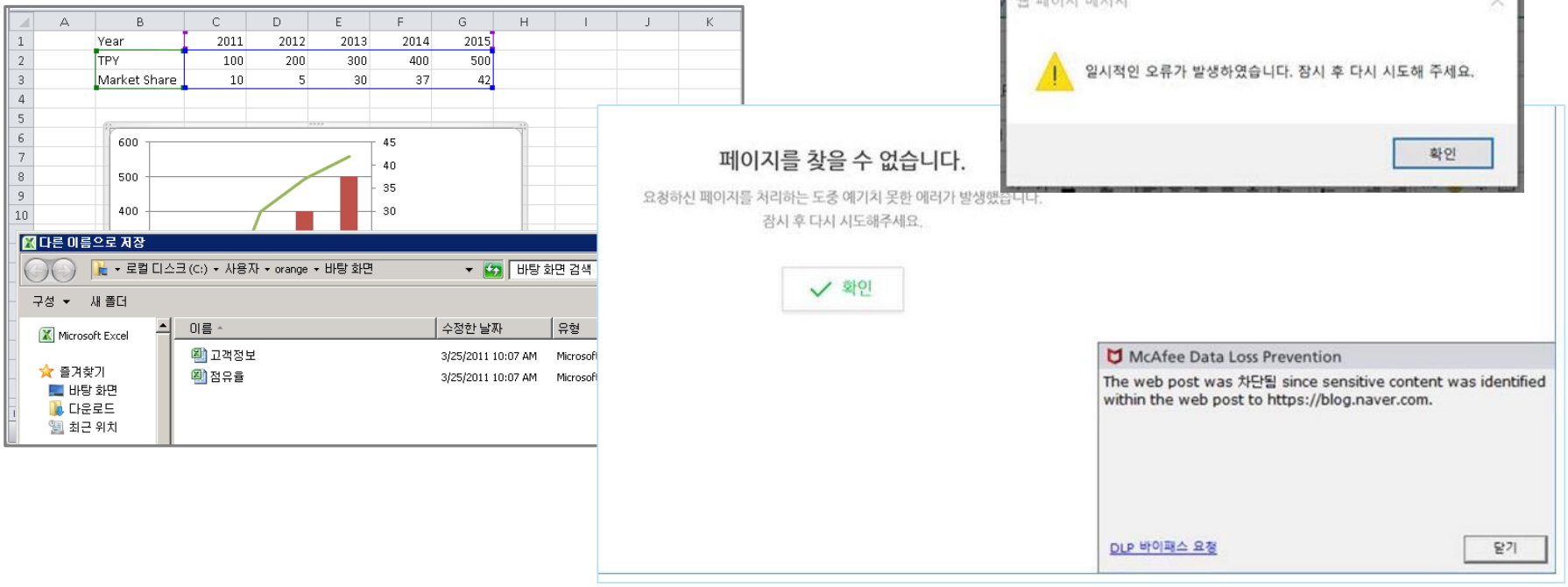
2) 알림 팝업

3) 인시던트 생성 및 증거저장

Endpoint DLP 주요 기능

응용프로그램 파일 액세스 보호

✓ 정책에 설정된 어플리케이션에서 만들어진 모든 파일을 차단.



Endpoint DLP 주요 기능

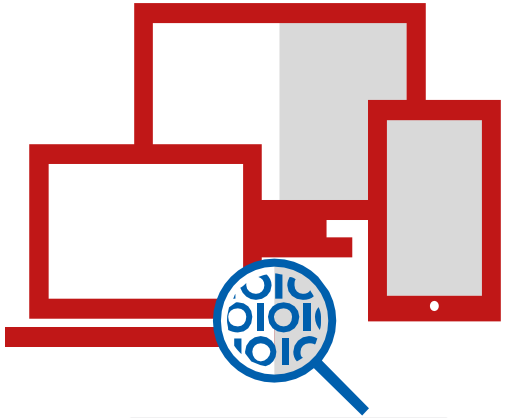
보안문서 자동분류 (Host Discovery)

개인PC의 디스크에 저장된 데이터를 아래 조건으로 탐색함

- 특정 파일 형식(그래픽 형식, 오피스 문서 등)
- 특정 파일 확장자
- 특정 키워드/정규식
- 파일 생성/수정 날짜
- 예약 탐색 지원

탐색된 데이터에 대한 대응

- 암호화, 권한 조정, 디스크의 격리 영역으로 격리, 관리자에게 보고(모니터링)

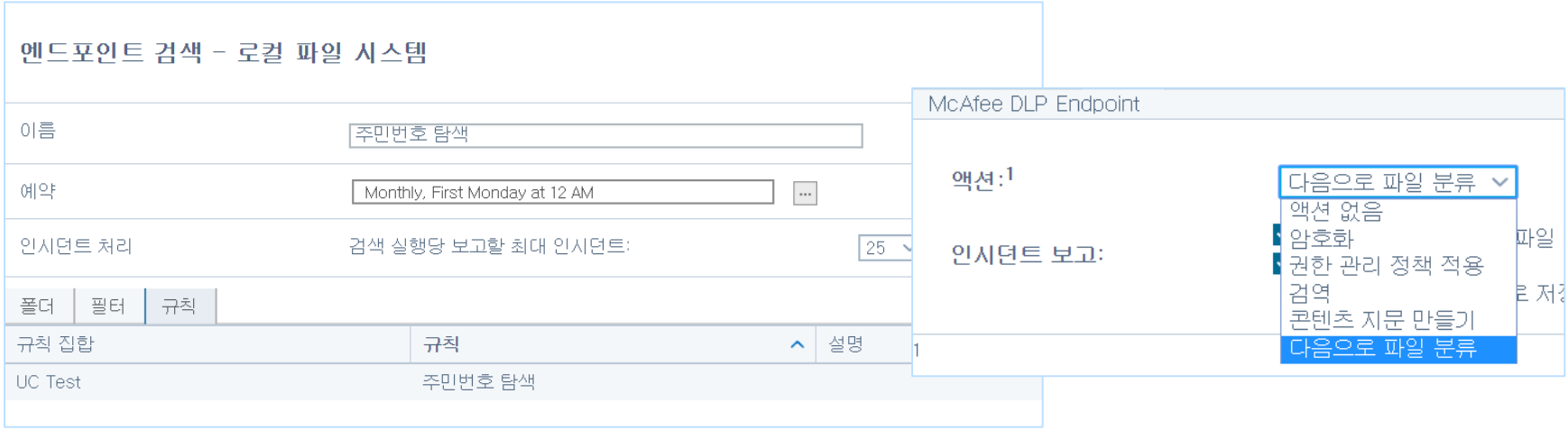


암호화 격리

Endpoint DLP 주요 기능

탐색을 통한 중요 데이터 자동분류 (Host Discovery)

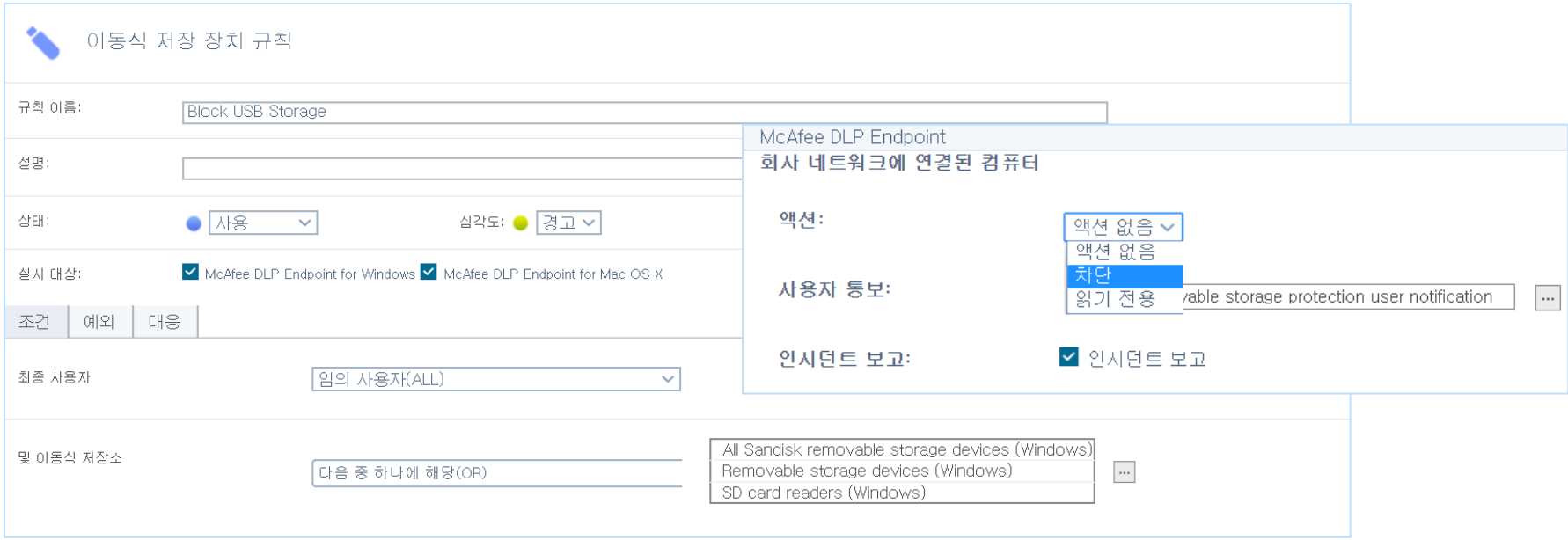
- ✓ 로컬 PC에 저장된 데이터에 대한 탐색 기능
- ✓ 탐색 후 보고, 암호화, 격리, 권한 조정 등 적절한 조치를 자동 수행
- ✓ Endpoint에서 에이전트가 수행하는 작업으로 서버 영향도 없음



Endpoint DLP 주요 기능

매체 제어 (Device Control)

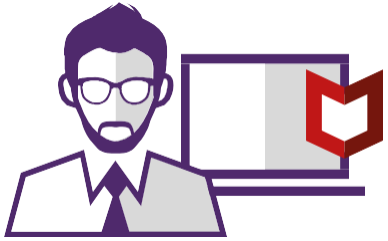
✓ 정책에 설정된 Device 의 연결을 모니터,읽기전용,차단



Endpoint DLP 특징

가시성 및 제어력 향상

✓ 데이터 분류, 암호화, 모니터링 및 차단 기능을 McAfee Cloud Data Protection과 통합하여 정보를 보호.
✓ 엔드포인트, 네트워크 및 클라우드 간에 정책 및 가시성 정보를 공유
✓ 모든 환경에서 포괄적인 데이터 보호 기능을 제공



데이터 손실 방지
엔드 포인트 및 장치 제어

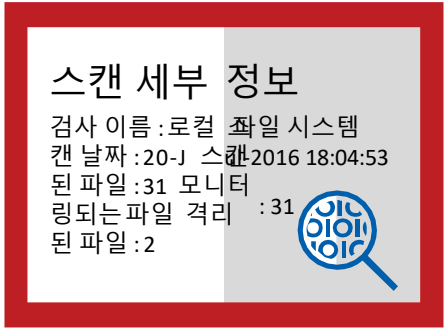
직원 코치 및 실시간 피드백

직원 교육: 운영부담 및 위험행동 감소효과

수동 분류

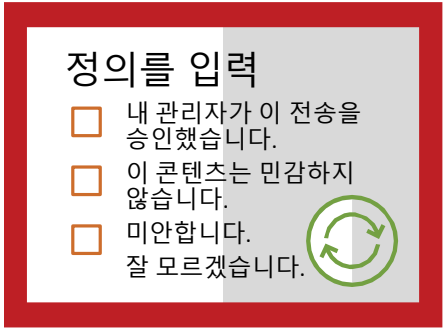
수동 분류는 사용자가 수동으로 문서를 분류하고 직원 데이터 보호 인식을 높이며 관리 부담 감소

자체 교정



사전, 정규식 및 유효성 검사 알고리즘, 등록 된 문서 및 타사 사용자 분류 솔루션 지원을 포함한 유연한 분류

실시간 피드백

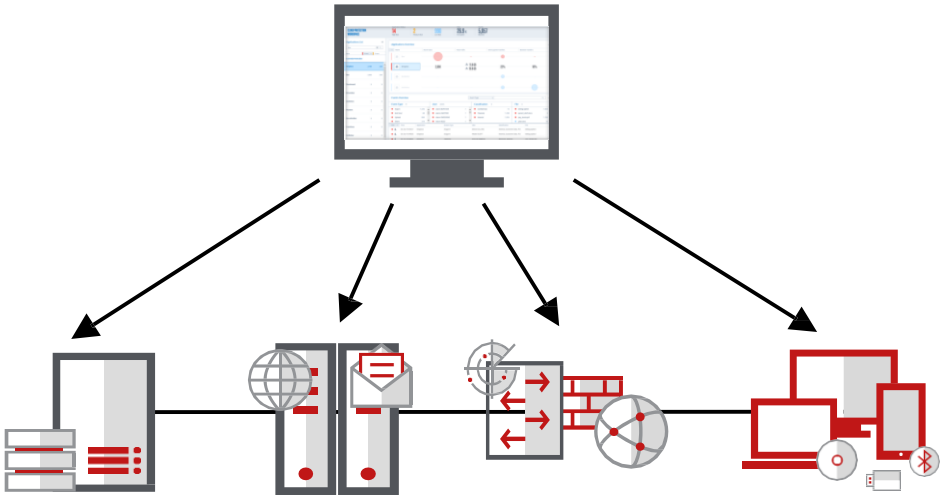


팝업을 통한 실시간 피드백은 기업의 보안 인식 및 문화 형성에 도움.

위험한 행동의 75 %이상 감소

ePO를 통한 중앙집중 관리

McAfee ePO or MVISION ePO



Data Repositories
DLP Discover

Email & Web Gateways
DLP Prevent

Egress points
DLP Monitor

Endpoints
DLP Endpoint
Endpoint Encryption

- 일반 분류 엔진, 사전, 정규식 엔진 및 구문을 통해 네트워크 및 엔드 포인트 DLP에서 통합 된 정책 관리
- 통합 된 사고 및 사례 관리
- 엔드 포인트 및 네트워크 DLP 전반에 걸쳐 일반 텍스트 추출 엔진을 사용하여 파일에 대한 정책 분석의 일관성 보장
- MVISION ePO를 통해 SecaaS 방식의 DLP Endpoint 관리 제공

Support 정보

직원 매체 제어 기능은 Window 외 Mac OS 적용 가능

Windows	Mac
• Microsoft Windows 7 SP1 or later, Enterprise and Business editions, 32-bit and 64-bit • Windows 8 and 8.1 or later Enterprise and Professional, 32-bit and 64-bit • Windows 10 32-bit and 64-bit • Windows Server 2008 R2 and 2008 SP2 or later, 32-bit and 64-bit • Windows Server 2012 and 2012 R2 or later, 64-bit • Windows Server 2016 and 2019	• macOS Catalina 10.15 • macOS Mojave 10.14 • macOS High Sierra 10.13 • macOS Sierra 10.12 • OS X El Capitan 10.11 • OS X Yosemite 10.10

Supported Browsers	McAfee ePO Software and Agents
• Internet Explorer version 11 • Mozilla Firefox 48 or higher • Google Chrome 65 or 79	• McAfee ePO software 5.9.1 and 5.10 • McAfee Agent for Windows 5.5 and 5.6 • McAfee Agent for Mac 5.5 and 5.6

고객 평가

교육용 팝업을 통한 실시간 피드백

McAfee DLP Endpoint 의 가장 큰 이점은 알림이 팝업 될 때 보안 인식을 높이는 것입니다.

미국 소재의 화학 회사

[McAfee DLP가 제공하는] 바이트 크기의 교육 기회 …

DDLP는 비즈니스 및 보안 문화에 막대한 영향을 줍니다 …

글로벌 인쇄 / 디지털 미디어 회사

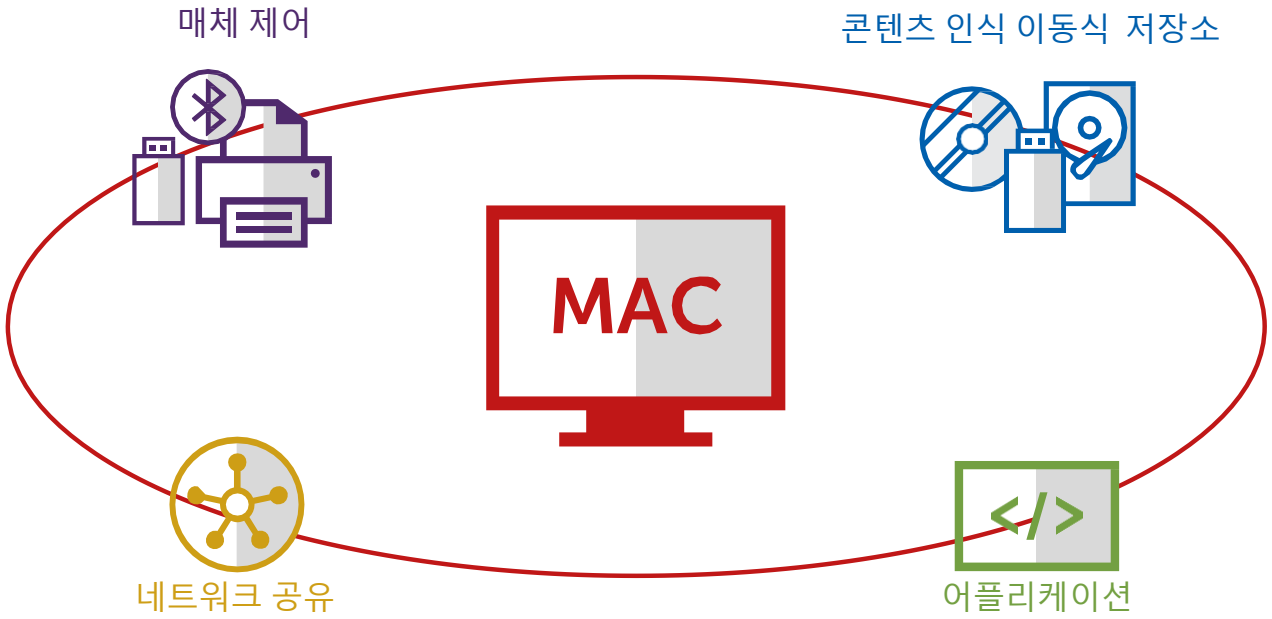
클라우드와 주고받는 데이터 보호

클라우드 보호 규칙
웹 보호 규칙

애플리케이션 태깅
위치 태깅

향상된 Mac OS X 보호

완벽한 McAfee ePO ™관리



국내 레퍼런스 사이트


한국가스공사


ADT캡스

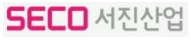

HYUNDAI
MnSOFT


AIA
THE REAL LIFE COMPANY


BNP PARIBAS
CARDIF


TAURUS
SYSTEMS GmbH


FESTO


SECO 서진산업


KCC


YAZAKI


한국남부발전㈜


KNOC
한국석유공사
KOREA NATIONAL OIL CORPORATION


KOEN
한국남동발전


한국지역난방공사
KOREA DISTRICT HEATING CORP.


한국동서발전


한국가스공사
KOREA GAS CORPORATION


S-OIL


ADT캡스


HYUNDAI
STEEL


Hyundai
Oilbank


SAMSUNG
삼성SDS


DSME
대우조선해양


SK
케미칼


SK
에너지


GS 칼텍스


LG전자


citibank


posco
ICT


한화에너지
Hanwha Energy


LOTTE CHEMICAL


McAfee™
Together is power.