DIGITAL GUARDIAN®

디지털가디언을 적용한 Endpoint Data Protection 방안

ToCSG 김주동

Total table of Contents

(주)투씨에스지는 오늘의 인연을 소중히 이어 가겠습니다.

01

(주)투씨에스지에 대한 소개

㈜ 투씨에스지는? (철학)

+Beyond×the/Security–

+ 좋은 솔루션을 만들어 고객의 가치를 더 하겠습니다.

× 고객의 가치실현을 위해 업무 효율을 곱하겠습니다.

/ 고객과 가치실현에 대한 즐거움을 함께 나누겠습니다.

– 고객의 문제를 함께 고민하여 위험을 줄이겠습니다.

㈜투씨에스지는? (일반)

투씨에스지는 오늘의 인연을 소중히 이어 가겠습니다.

대표이사	임 천 수
주소	서울특별시 영등포구 국제금융로 70 (여의도동, 미원빌딩 17층)
대표 연락처	02-320-5000, sales@tocsg.co.kr, http://www.tocsg.co.kr
설립연도	2008년 1월 24일
매출액	165억원 (2015년 기준)
가족 수	60명 (2015년 06월 기준)

㈜투씨에스지 주요 사업분야

㈜투씨에스지는 정보보안/데이타베이스/시스템통합관리 분야를 주요 사업분야로 하고 있으며 각 분야의 전문 인력으로 구성되어 있습니다.

DSC (Database Solution & Consulting)

Database 관련 사업

- CubeOne (Database암호화)
- Oracle / Tibero 구축
- Database 성능진단
- Database 운영
- MaxGauge (Database성능관리)

ITS (IT & Security Tech.)

시스템통합 및 기반 정보보안 사업

- IBM Tivoli (시스템관리)
- IBM TWS (배치작업관리)
- Mainframe 운영
- IBM Qradar (차세대 SIEM)
- Ca ControlMinder (서버보안)
- APPM (공유/특수계정 관리)
- 방화벽정책관리
- Endpoint 보안 솔루션 디지털가디언

DIGITALGUARDIAN®

Architecture

APT 대응 & 취약성 진단 사업

- FireEye (APT 대응솔루션)
- Nexpose (시스템 취약성 진단)
- Metasploit (모의해킹)
- IBM AppScan (웹 취약성 진단)
- CodeRay (소스코드 취약성진단)
- 취약성 진단 컨설팅

R & D

자사 Beyond the Security 솔루션 개발 및 보급

- BS-Insight (업무기반 취약성 진단/이행포탈)
- BS-USB PortLock (USB Port 사용 관제)
- BS-APT Simulation System (피싱 / 스미싱 모의훈련)
- BS-Policy Control (보안솔루션 통합승인시스템)

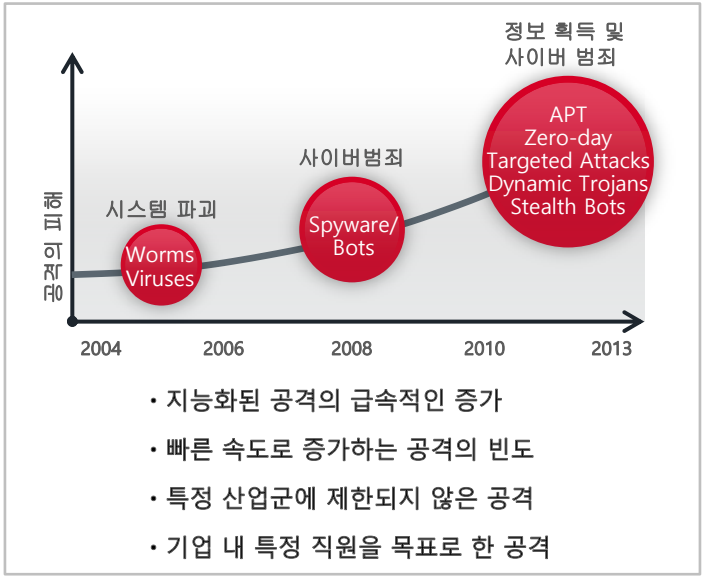
02

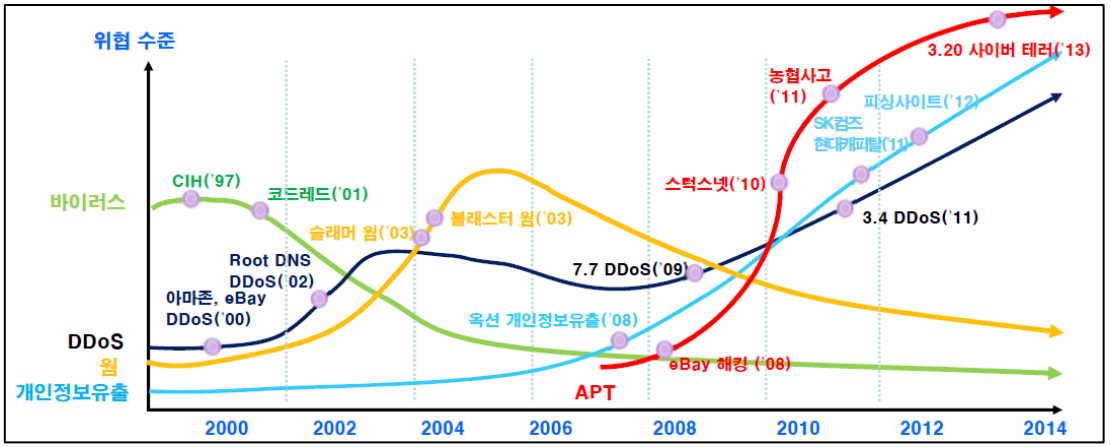
Endpoint를 중심으로 본 정보보호 동향

최근 정보보안 동향

정보보안 동향과 위협추세

1. 고도로 지능화된 외부 위협의 증대
   - APT, Spear Phishing, Zero-day Attack, Ransomware, hacktivism 등
2. 지속적인 내부 취약점 및 위협의 증가
   - ICT 기술발달과 더불어 내재된 보안 취약점의 지속적 증가
   - 보호대상 자산의 증가, 지속적인 취약성의 증가와 존재, 내부 불만세력이나 무지 또는 부주의에 의한 정보 유출 등
3. 준수해야 할 규제의 증가
   - 법 규제, 산업규제 강화, 기업의 경쟁
4. IT 신기술의 대두와 예측 불가한 침해 기술의 발전
   - IoT, M2M, SCADA 보안, Cloud, Virtualization, IPv6, Big data, SNS, Mobile 등



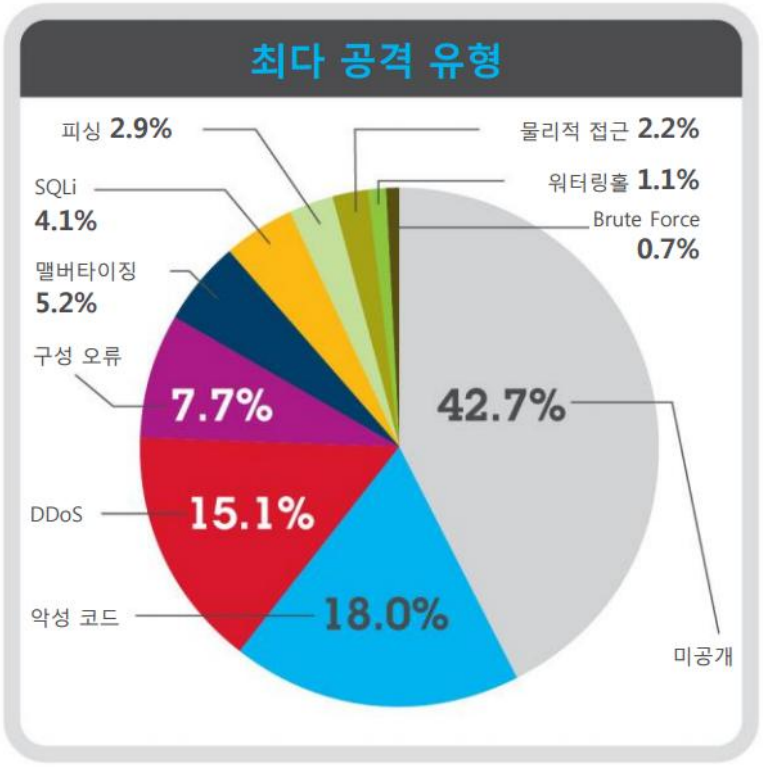


[그림: 침해 사고 동향]

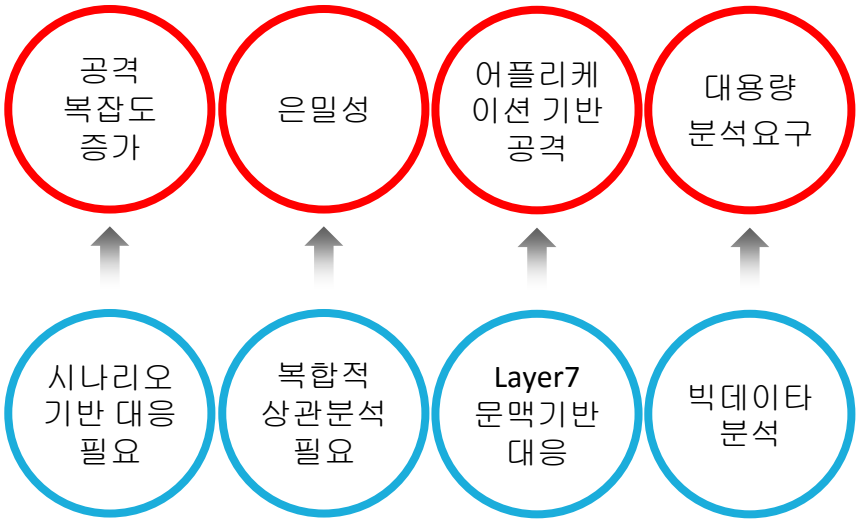
[그림: 침해의 특징과 가시성 확보]

최근 공격유형의 공통적 특징과 대응

2015년 주요 공격 유형

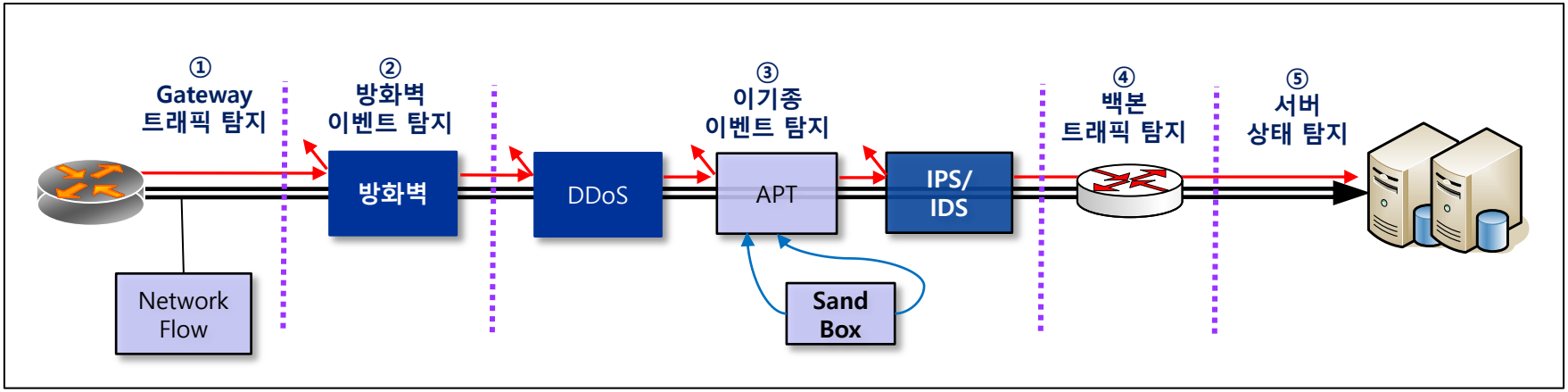


SOURCES: Xforce 2016 1Q Report



- 고도로 지능화된 공격의 급속적인 증가
- 공격 복잡성의 증가로 일반적인 임계치 기반 대응에 대한 우회 공격
- 장기간의 지속적인 공격을 은밀하게 수행
- 임계치 내 데이터 전송을 통한 탐지 우회

전통적 보안솔루션들의 한계



1. 고도로 지능화된 공격에 대한 방어 한계 존재

2. 단위 영역 (경계선)에 대한 보안에 집중, 징후에 치중

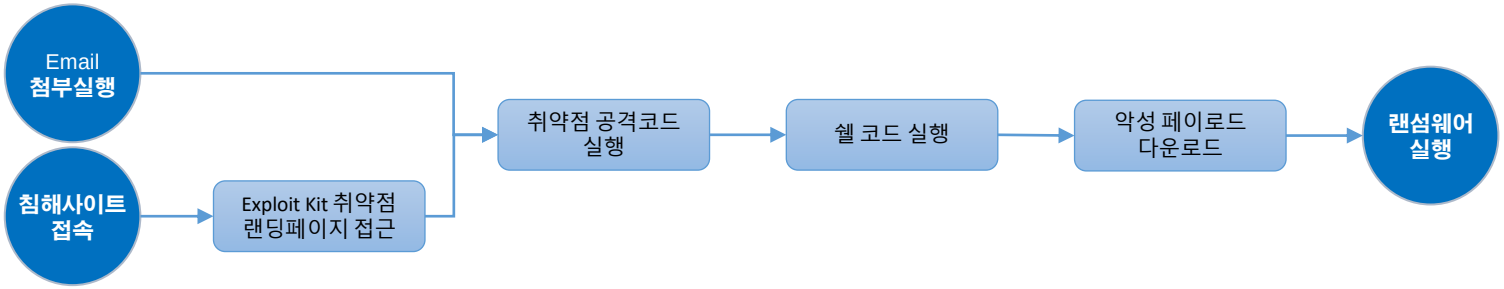
3. IT 활동 전반에 걸쳐 숨겨진 문제에 대한 가시성 제공 불가

랜섬웨어(Ransomware)

1. Ransom + Software : 중요 시스템이나 데이터를 인질로 잡고 금전을 요구

2. Email, 웹 기반 Drive-By-Download) 방식의 감염경로를 주로 사용

3. Endpoint 상에 존재하는 취약점을 사용하여 악성코드 실행



4. 지속적으로 진화하고 있고 2013~2014년도 크립토 랜섬웨어는 약 250% 증가

5. 랜섬웨어의 유형은 락커(36%)와 크립토(64%)이며 크립토의 비율이 증가 추세임

6. 크립토월 3.0이 6개월 동안 약 3억2500만달러 수익, 크립토월 4.0으로 진화

7. 웨어러블 기기, IoT 기기로 확장, RaaS(Ransom-as-a-Service) 등장

Endpoint 보안 현황

새로운 사용환경 (Cloud, Mobile, BYOD 등) 의 대두로 정보의 보호 요건이 증대되고 있고
개인용 PC, 타블렛, 스마트폰 등과 같은 Endpoint Device들이 조직 내에서 사용되고 있음

88% of enterprise

개인 PC의 업무용 활용 허용

79% of organizations

사용자의 조직 네트워크
접근에 대한 고민

57% of organizations

조직 네트워크 접근에 대한
디바이스 가시성 미확보

1 in 5

조직 네트워크의 5대 중
1대가 모바일 디바이스

2 in 3 Android

3대 중 2대의 안드로이드
스마트폰이 스크린락 사용

2 in 3 iPhones

3대 중 2대의 아이폰이
Touch ID를 사용

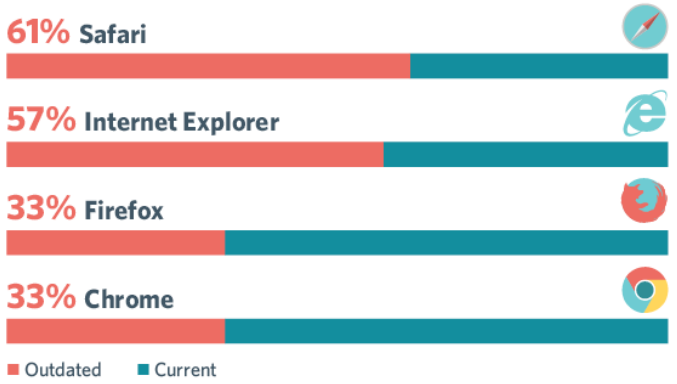
SOURCES: Duo Labs, CVE Details, Adobe, AndroidCentral, Cnet

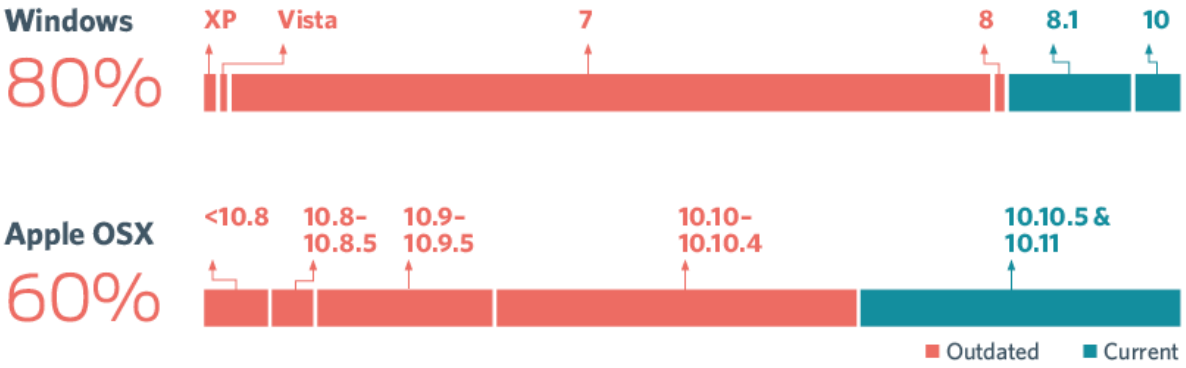
Endpoint 보안 현황

Endpoint에 사용되는 브라우저와 운영체제 중 상당수가 오래된 것을 사용하거나 패치되지 않아 상당히 많은 취약점을 보유하고 있음

46%

오래된 버전의 브라우저,
Flash, Java를 사용





SOURCES: Duo Labs, CVE Details, Adobe, AndroidCentral, Cnet

최근 주요 공격 타겟, 한번만 더 생각해 보겠습니다.

- APT 공격의 주 타겟은 ?
- Phishing 타겟 ?
- Injected Bad File 타겟 ?
- 랜섬웨어 타겟 ?
- 상용/무료 SW 취약점 타겟 ?
- Watering Hole 공격 타겟 ?

다음 중, 고르시오

(1) Database

(2) Network Devices

(3) Server

(4) Web Application

(5) Endpoints

(6) Security Devices

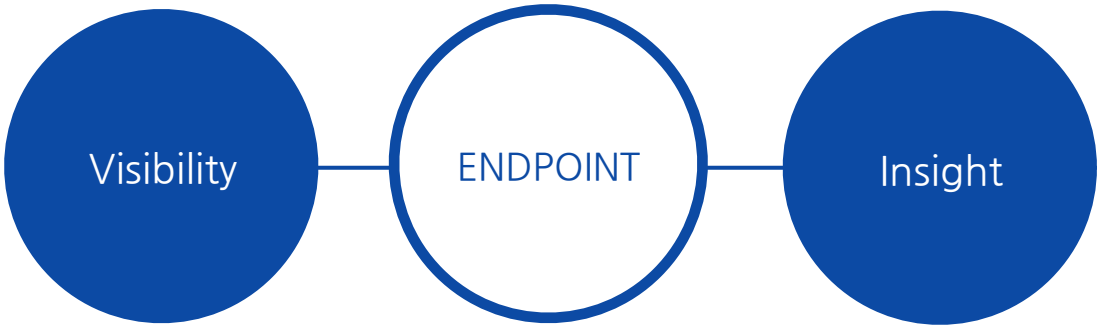
Why Endpoint?

실제 업무가 일어나는 곳이자 매우 다양한 형태로 존재

업무와 개인 사용의 혼재(BYOD)로 인한 정보보호와 통제의 한계 존재

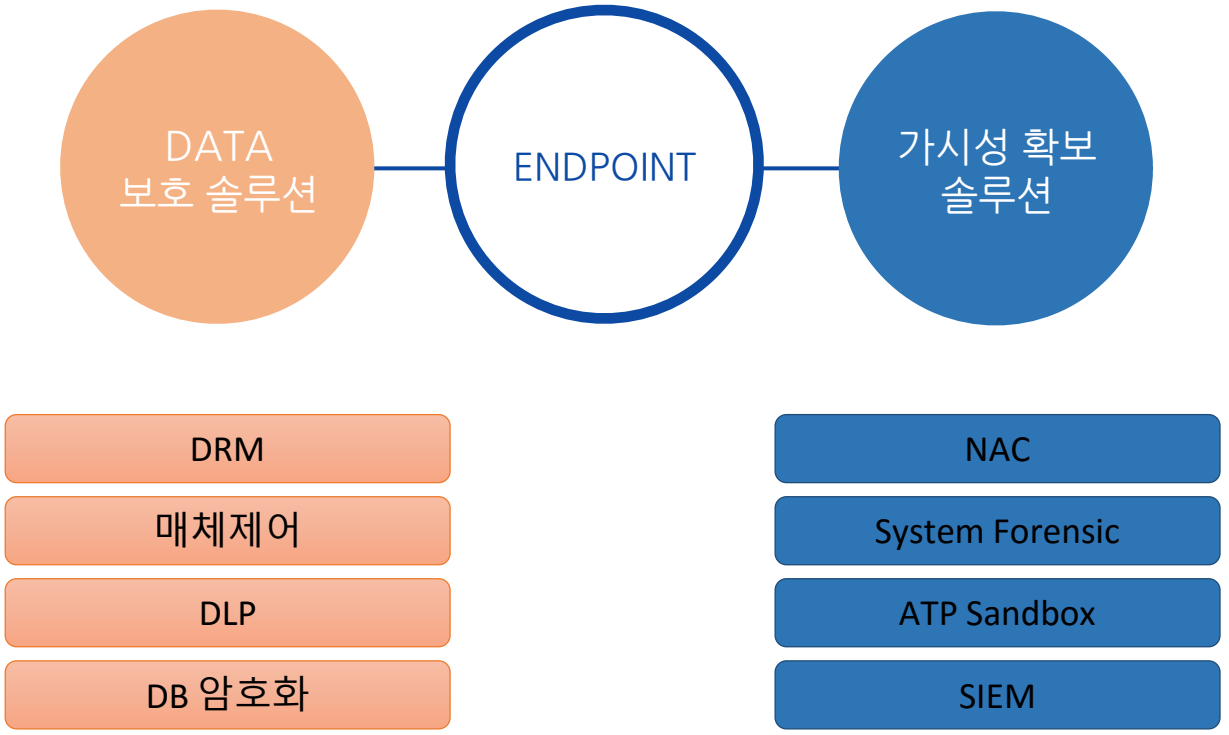
정보유출과 위해 행위의 시작 지점 (APT 공격의 69%가 Endpoint를 공격경로로 사용 –버라이즌-)

중요하지만 제일 관리하기 어렵다.



여러분들의 **Endpoint**는 안전합니까?

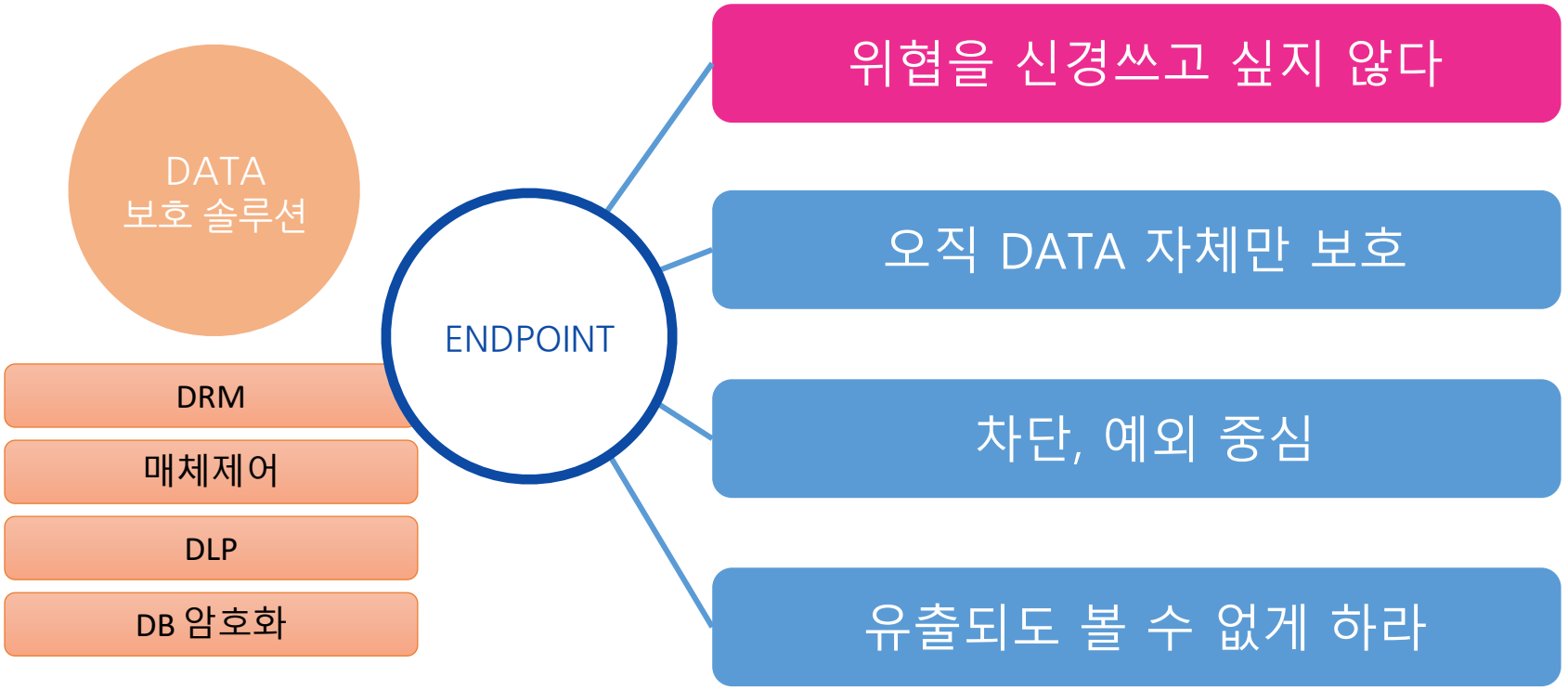
보호의 궁극적 대상은? Information & Data



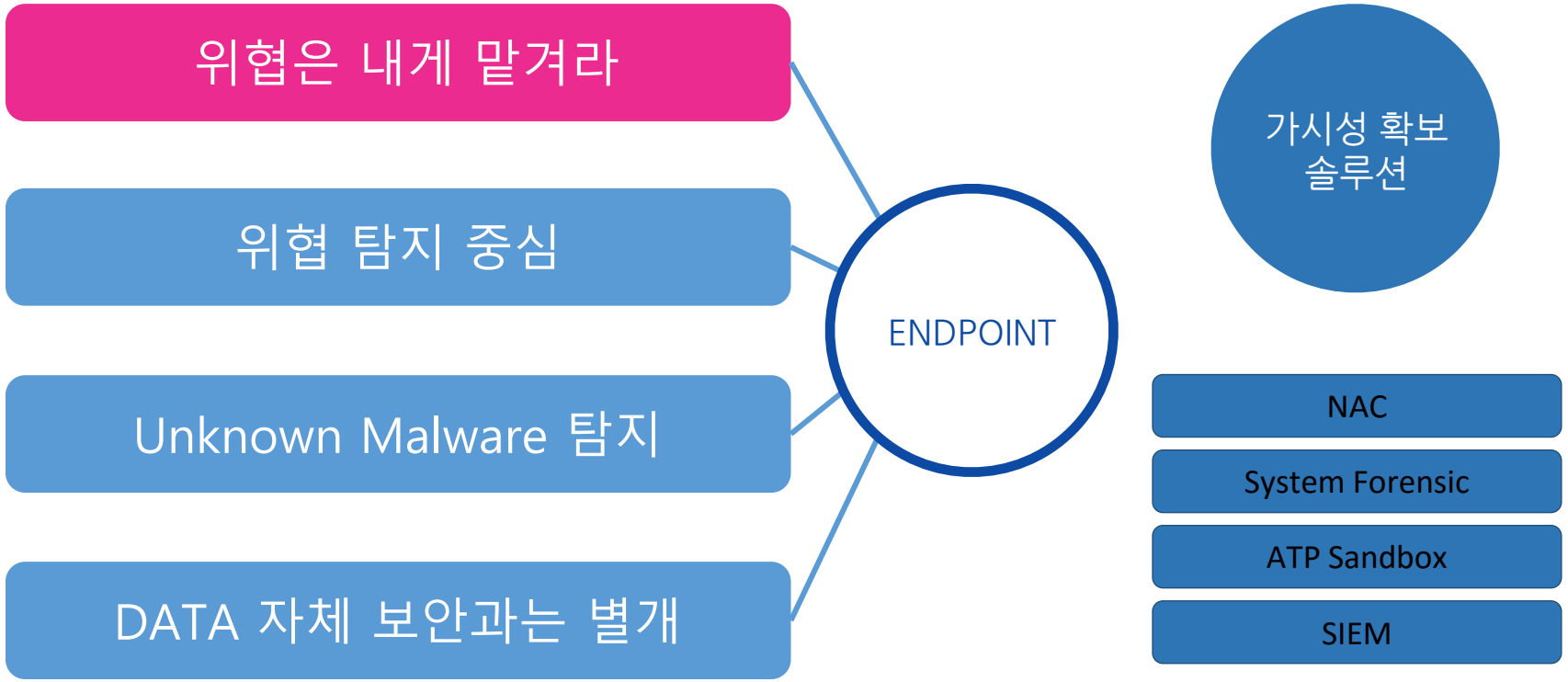
여러분들의 **Endpoint**는 안전합니까?

Data security

threat detection



Visibility security with threat detection without data-awareness



Only Data Security - 고려사항

기존 DATA 암호화 고려 사항

- **예외 정책 적용 시**
  - 평문 데이터 Life-cycle 추적성 ?
  - 데이터 중심의 육하 원칙 관리 ?
  - 데이터에 접근하는 위협 관리 ?
- **데이터 적용 범위**
  - Windows, Mac OS X, Linux
  - 정형 / 비정형 데이터 전폭 수용

기존 DATA 유출 차단 고려 사항

- **Content 제어 범위**
  - 오직 해쉬, 키워드, 파일타입 한계
  - Context 기반의 제어 가능?
- **차단의 범위**
  - 스태가노그래피 데이터 탐지/차단
  - 악성코드에 의한 유출 탐지/차단
  - 악성행위에 의한 유출 탐지/차단

Only Threat Visibility – 고려사항

기존
Threat Visibility
고려 사항

위협 탐지 방법론

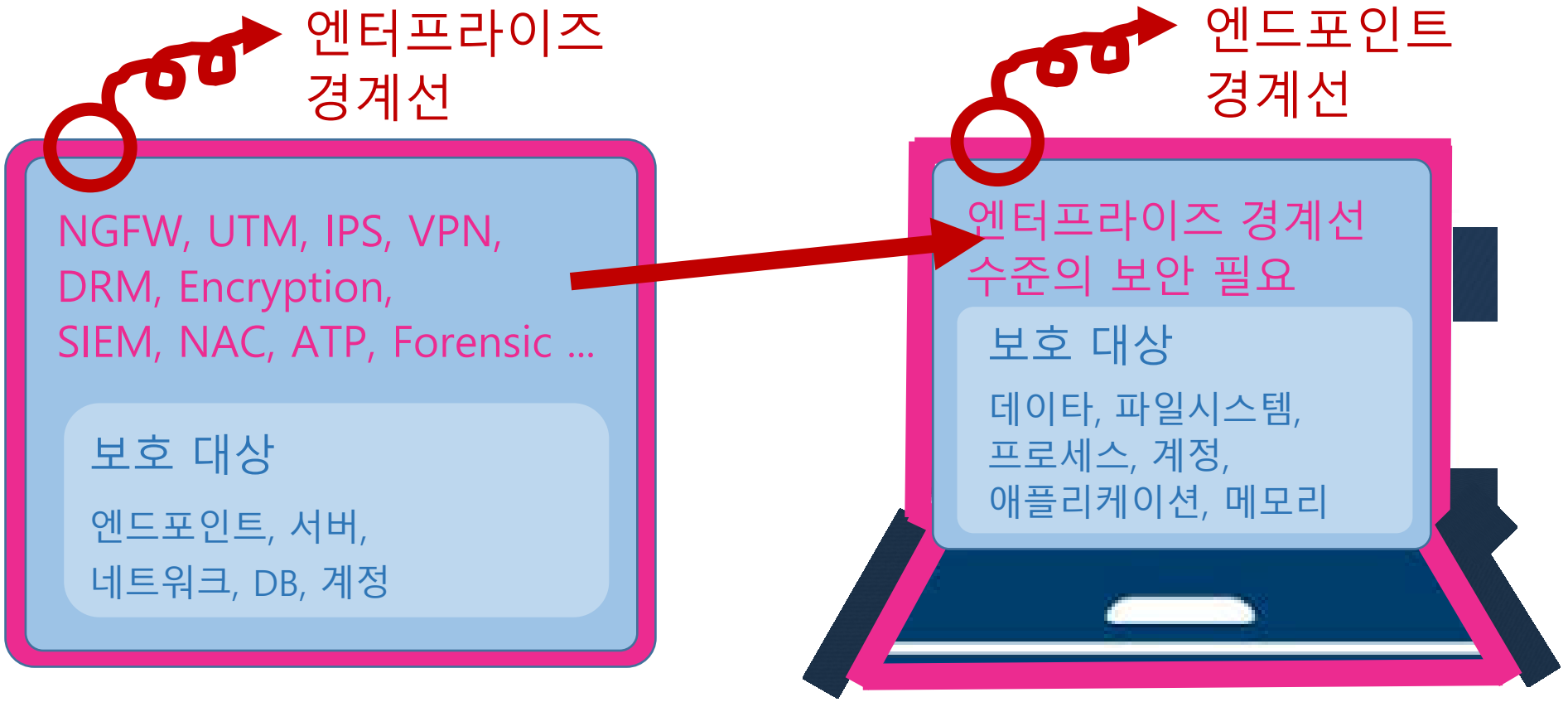
- Signature
- Behavioral
- Sandboxing
- Event / Traffic Correlation

Unknown Threat
탐지 / 제어 부문

- Malware 중점
- 정말 위험한 상황인가?
- 우회 방법은 존재하지 않는가?
- Windows, Mac, Linux 지원성
- 멀웨어가 터치한 데이터와 터치하지 못한 데이터 구분 ?
- 멀웨어 탐지 시, 차단 및 추가 확산 방지 대책?

발상의 전환

엔드포인트 "크기만 작은 또 하나의 엔터프라이즈"



지속적으로 보안투자를 하고 있지만 여전히
데이터유출과 같은 보안사고를 걱정하고 있는 이유?

Endpoint에 대한 침투 및 변경 과정부터
중요 데이터에 어떤 행위가 이루어 지고 있으며,
제대로 방어되고 있는지에 대한
실시간 모니터링과 행위증거(포렌식) 감사를 통한
가시성이 제공된다면?

ETDR 기본 정의

ETDR (Endpoint Threat Detection & Response)

- Endpoint – not network & not server
- Threat – not only malware, but also incidents
- Goal – Tools for detection and incident response

EDR 확장 정의

EDR (Endpoint Detection & Response)

- Continuous detection and response to advanced threats
- Security monitoring, threat detection and incident response
- Record many detailed endpoint and network events
- Store all information in a centralized DB
  for deep detection analysis, investigation reporting and alerting
- Analytic tools are used to continuously search
- Early identification of ongoing threats
- Rapidly respond to detected attacks
- Should include Inside threats and Outside threats

가트너 EDR 정리

Gartner

EDR
Endpoint Detection Response

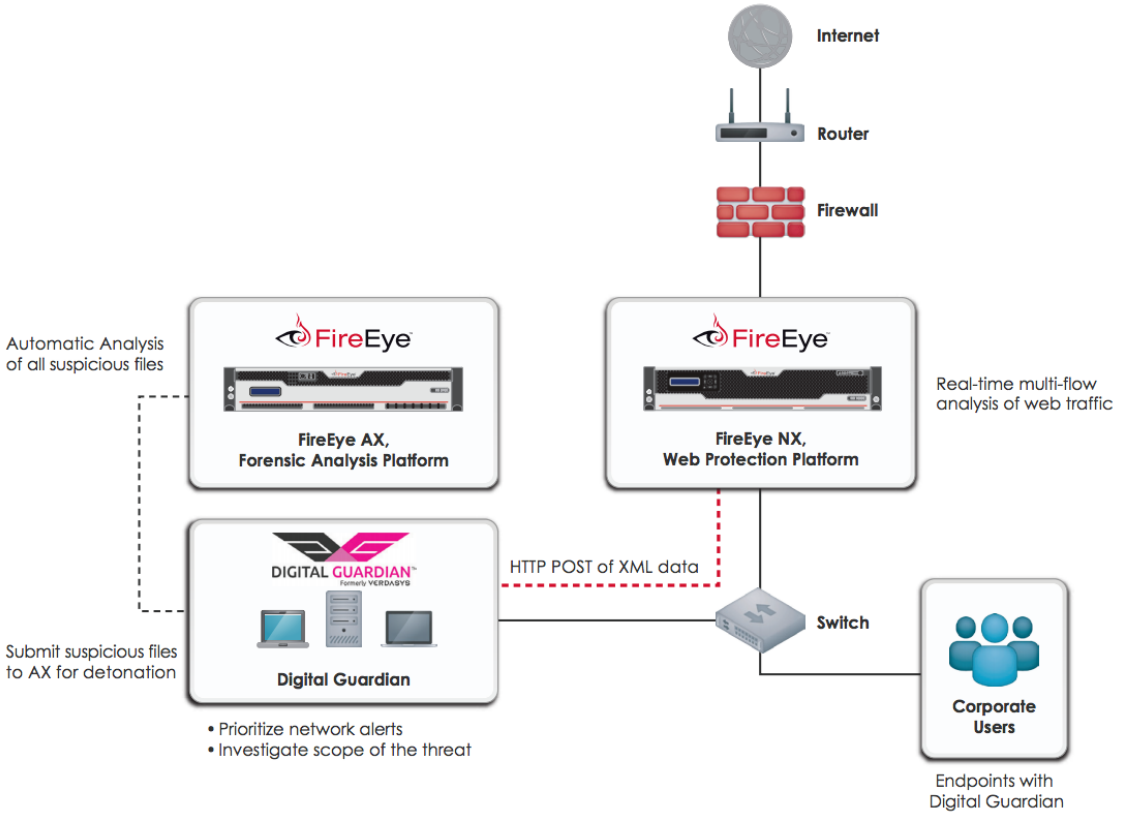
Investigation (Collection)	Detection	Remediation
▪ 엔드포인트 데이터 수집/저장 (registry, process, read, write, upload, call 등) ▪ 지속적인 모니터링 ▪ Event Triggered 스케쥴기반 시스템 스캐닝	▪ 내장된 Anomaly 탐지 및 자동 차단 기술 ▪ Rogue Scripts & 메모리 인젝션 기술 ▪ Intelligence Feeds & IOC 연동 기술 ▪ Future Attacks 방어 기술	▪ 네트워크 격리 & Process Kill ▪ Alerts ▪ Mitigation response ▪ 3rd Party 연계 대응

EDR Echo Systems 샘플

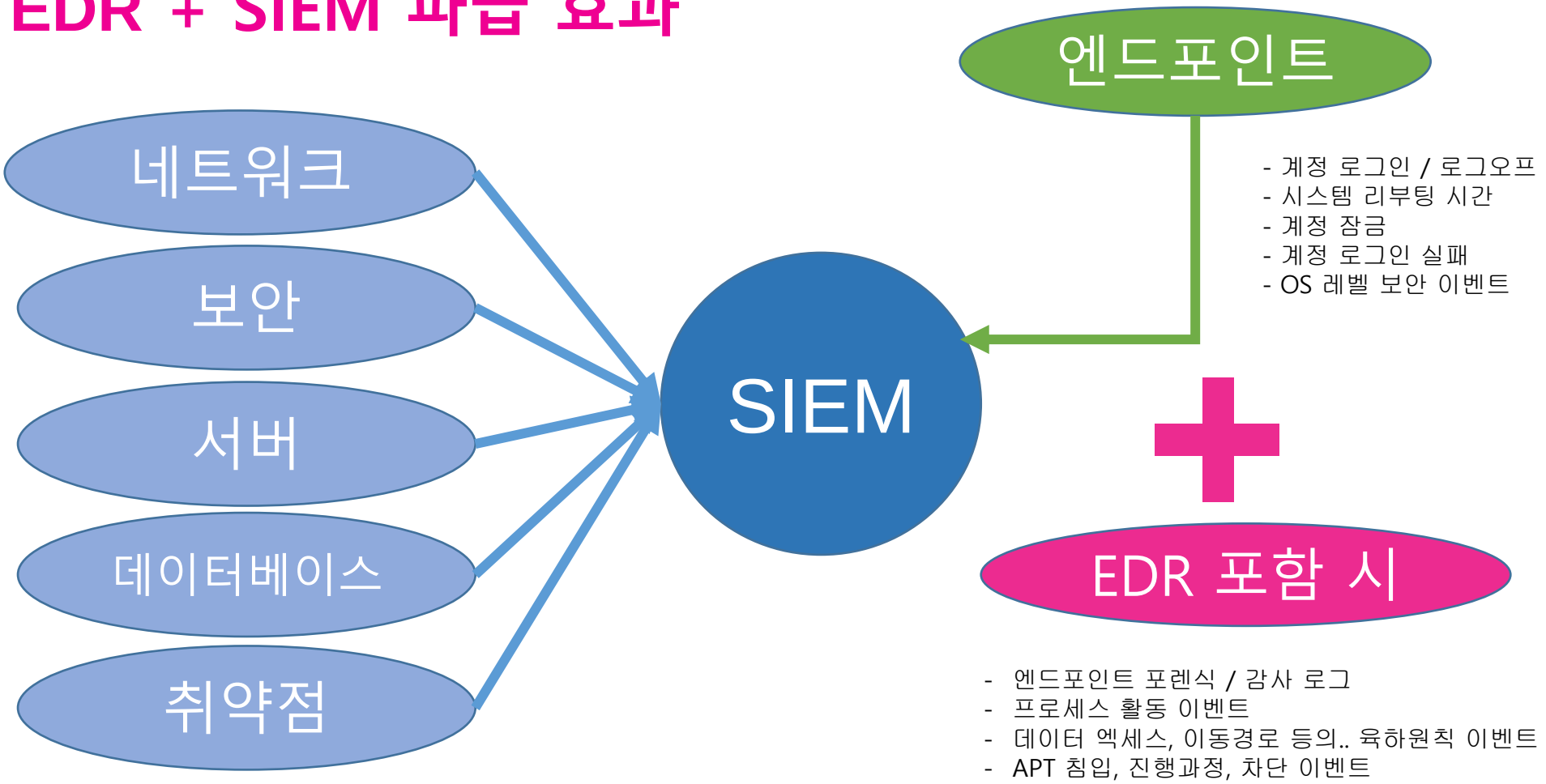
FireEye

FireEye and Digital Guardian

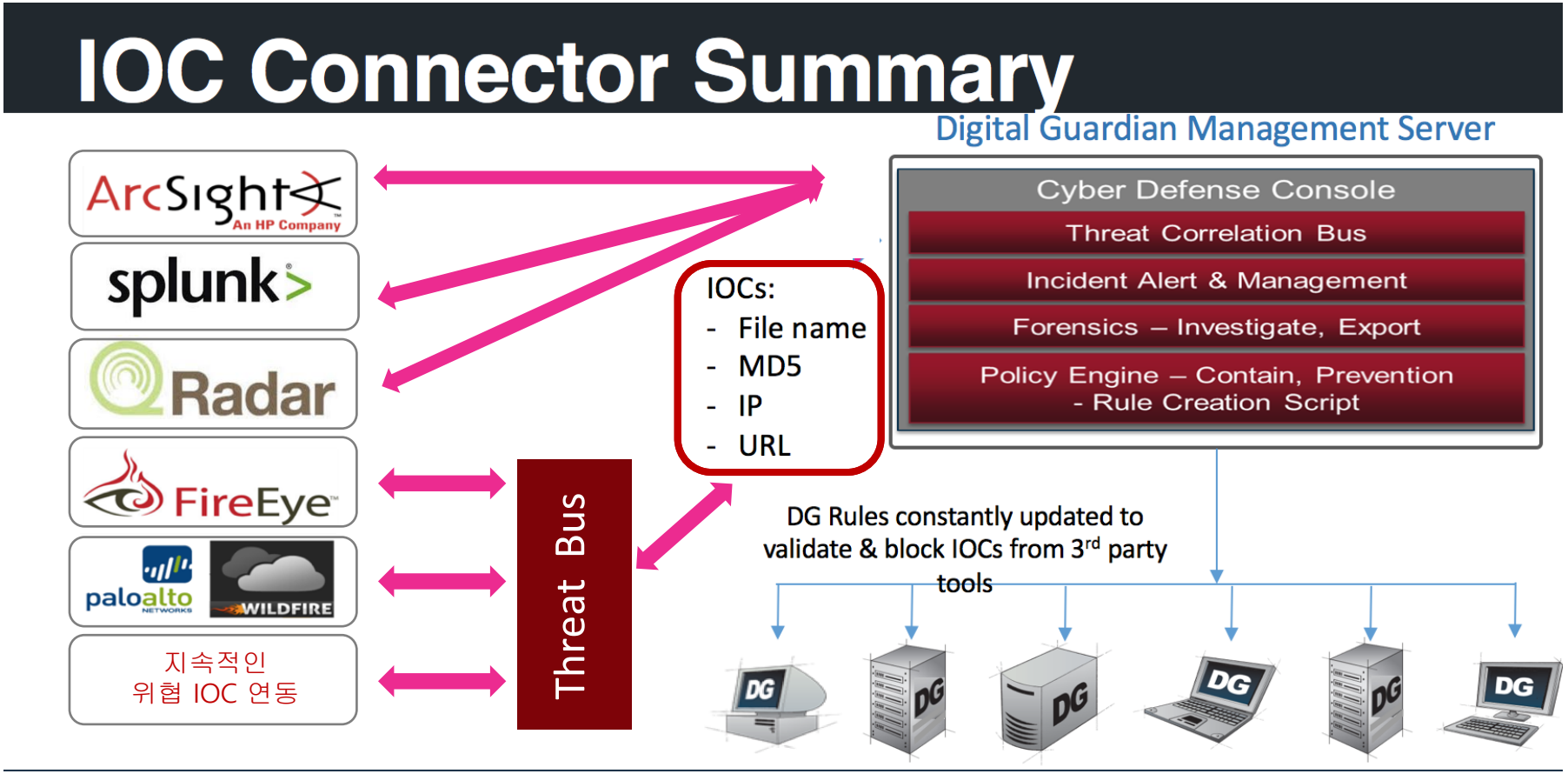
Next-Generation Defense to Protect Your Most Sensitive Information



EDR + SIEM 파급 효과



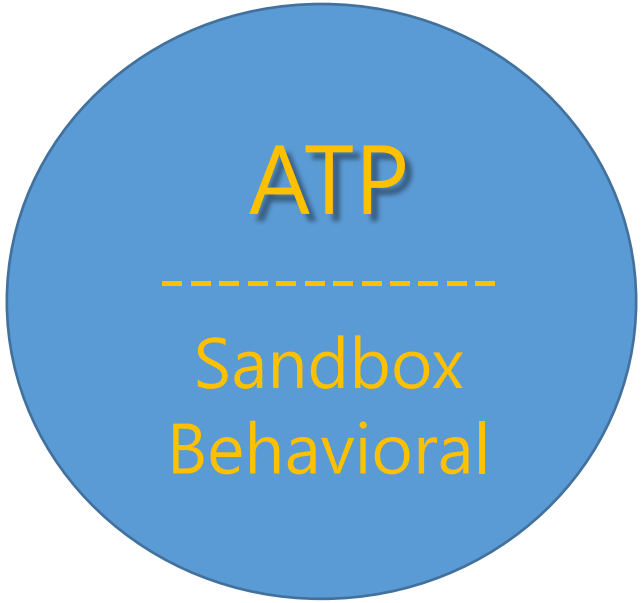
Security Eco-Systems 연동 아키텍쳐



Endpoint에 대한 보안 Visibility와 Insight 요소

엔드포인트

Malware Prevention

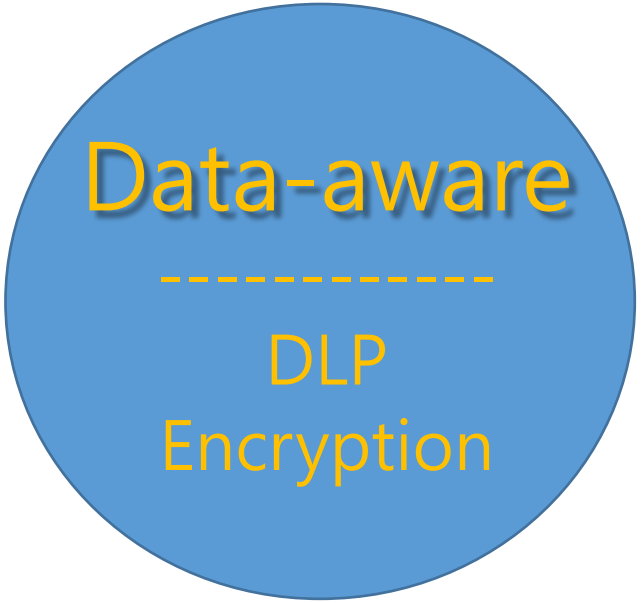


엔드포인트

Full Visibility

엔드포인트

Data Protecton



03

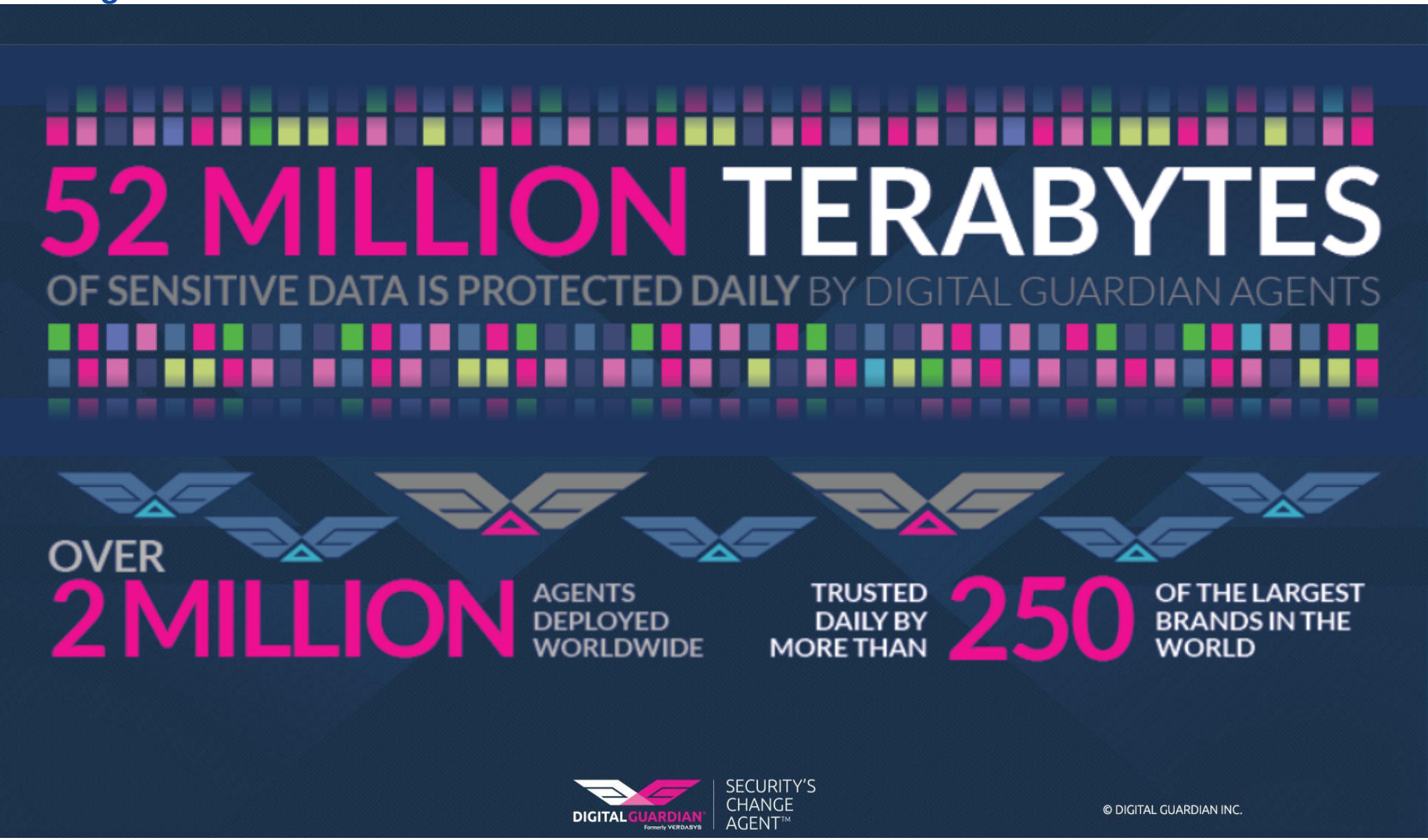
차세대 엔드포인트 보안솔루션
- 디지털가디언 -

Digital Guardian?

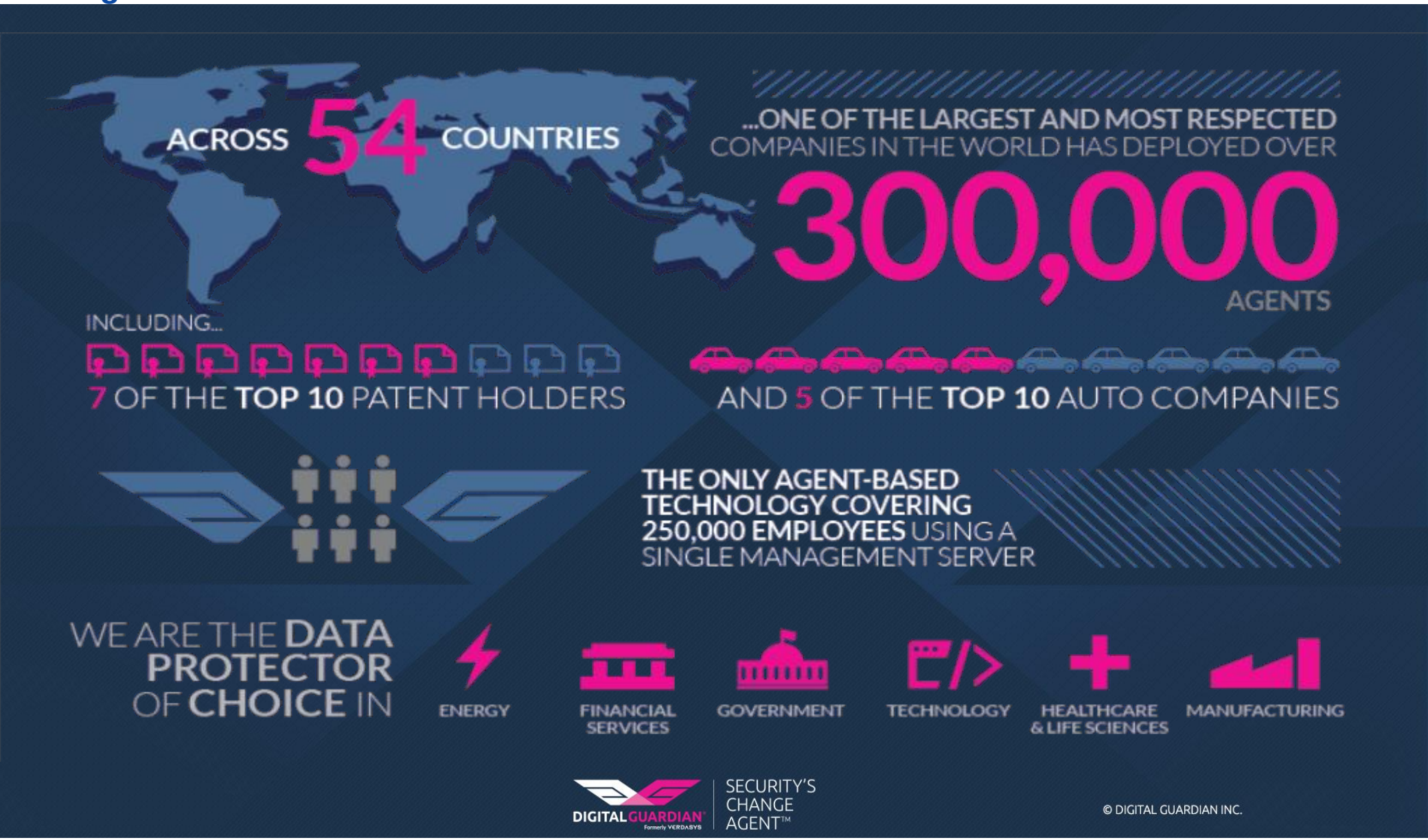
- Founded 2003
  - Leader – Gartner Magic Quadrant for Enterprise DLP
  - Over 20 patents
- Global presence
  - Headquartered Waltham, MA
    - London, Amsterdam, Paris, Munich, Tokyo, Korea office
  - Deployed in 54 countries
- Leader in Data-centric Security
  - 2.5 million agents deployed
  - 300,000 Endpoint - Single customer
  - Delivered on-premise or managed service
- Persistent Data Protection
  - Windows, OSX, Linux, offline/online
  - Protects data independent of the threat or the system
  - Encryption, Application Control, Device Control, Forensics

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Digital Guardian?



Digital Guardian?



Digital Guardian?

미 연방준비은행 Federal Reserve Bank

Company

- Finance / Banking
- United States
- 25,000 여개 엔드포인트 디바이스
- 13개 지사
- Champion – Chicago CISO
- Value – $1.5M

Technology

- 25,000 Core & ACI
- 2010년 시카고에서 1,500 개 에이전트로 프로젝트 시작
- 2013년에 13개 지사, 25,000 개의 에이전트로 확대
- 주 용도는 PII/PCI 컴플라이언스

Use Case

- PII/PCI 데이터의 이동경로를 감지/확인하고, 승인 절차를 강화하고자 도입.

Success Story

- 한번 생성된 태그에 대해 문서 변환/컨텐츠 복제시에도 계속 추적되는 기능 구현
- 디지털가디언의 가시화 능력이 연방준비은행 도입 이유. The visibility we bring is why they purchased us.
- 권한별 승인 절차를 위해 별도의 인터페이스를 통합

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

DuPont 듀퐁

"" IP 내 위협을 감지하는 많은 솔루션들이 있지만, 다양한 위협을 감지하고 그에 대해 적절하게 반응하는 솔루션은 디지털 가디언 하나 뿐이다." Larry Brock, CISO

디지털 가디언을 이용하여 글로벌 협업 환경을 클라우드로 성공적으로 이행

Use Case Coverage

- 지적 재산권 보호 & 협업 환경 보호
- 장소에 상관없이 내부 사용자에 대한 완벽한 협업환경 구현
- 외부 접근 관리

Future Coverage

- 프라이빗 클라우드 환경에서의 Protection 으로 확대 예정

Critical Differentiators

- 기존 솔루션과는 차별되는 데이터 감지/발견/분류 기능
- 문서 통합 기능

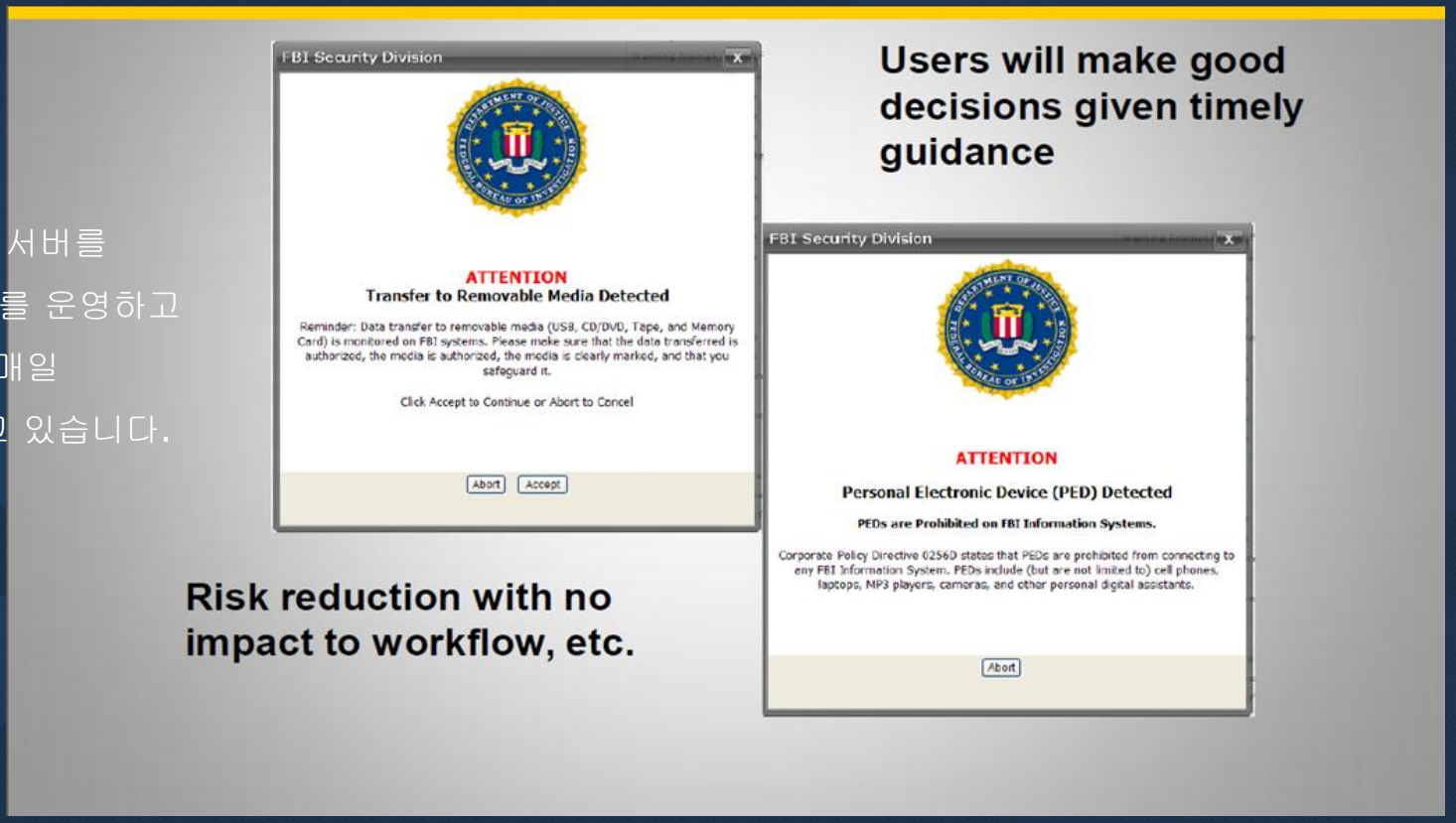
문서통합을 가능하게 함으로써 기존 솔루션 개발비/별도 구입비용을 $3M 가까이 절감

IP 침입을 차단함으로써 중요한 문서 유출로 발생할 수 있는 $200M 가까운 비용을 절감

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

미국 법무부 FBI

미 법무부 소속 FBI 는 1대의 서버를 통해 125,000 개의 에이전트를 운영하고 있으며 디지털가디언을 통해 매일 15,000 여 이벤트를 수집하고 있습니다.



Source: Patrick Reidy

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Operating System Support

- windows XP
- vista (32 Bit/ 64 Bit)
- windows 7,8 (32 Bit/ 64 Bit)

- Mac OS X

- Linux OS(커널 2.6~3.2)
(redhat/ CentOS/ fedora/ Ubuntu 등)

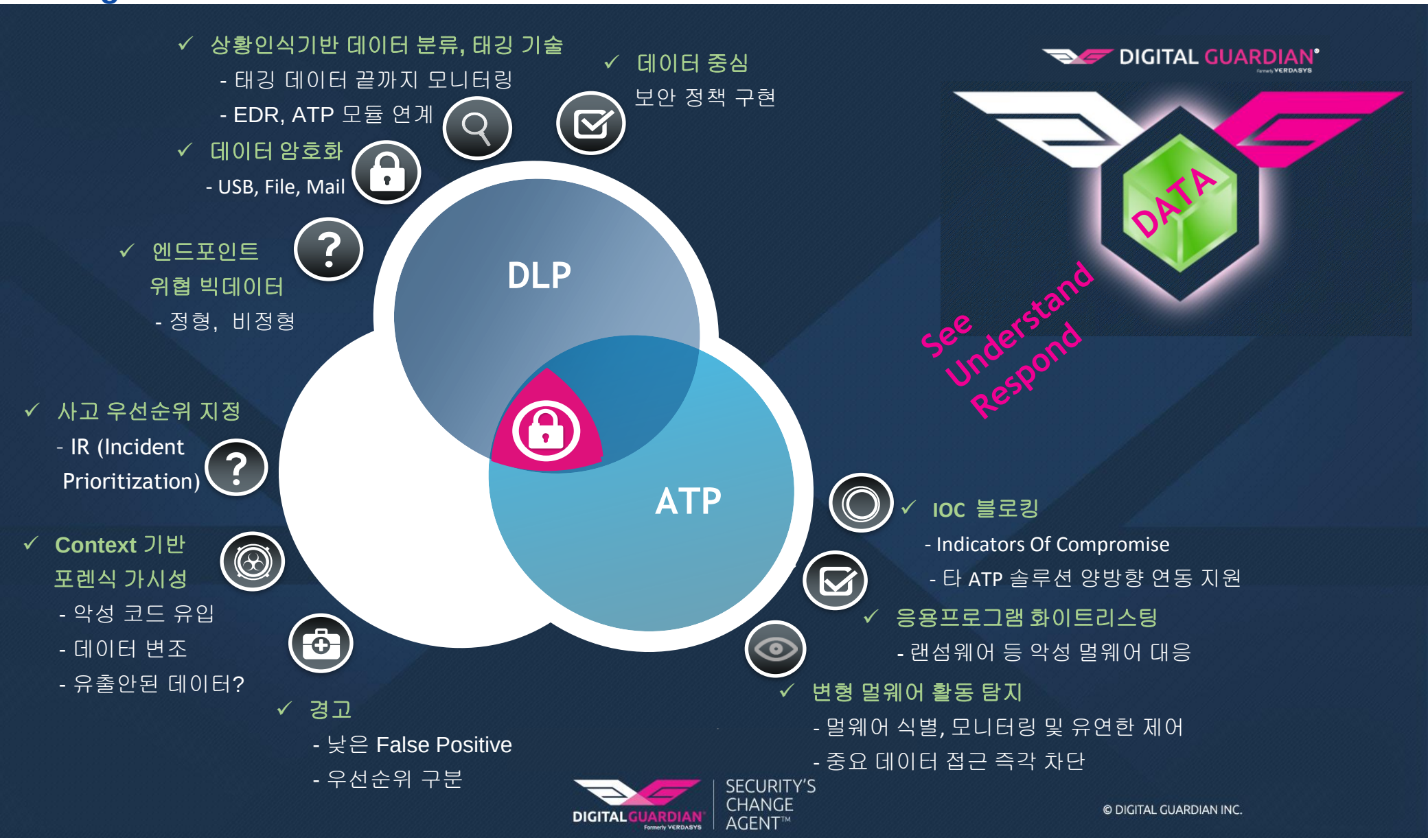
모든 OS
지원

- windows Server 2003/2008/2012(R2)
- Linux Server

- 가상화 서버 (Virtualization Server)

서버,가상화
OS 지원

Digital Guardian 주요 기능 요소



Digital Guardian 기능 요소 (Endpoint Data Visibility & Control)

- **기능 목적**
  - 누가 중요 데이터를 사용하고, 어떤 실행 파일에 의해서 접근되고 있는지 실시간 모니터링 및 감사
  - Online / Offline 모두 강력한 모니터링 및 제어 정책 적용
  - Windows, Mac, Linux 운영체제 모두 지원 (Virtual Machine 환경 지원)

- **지속적인 포렌식 목적의 가시성 확보 ➔ 핵심 차별화 포인트**
  - 지속적인 포렌식 이벤트 수집 / 저장 / 감사
  - 시스템 이벤트, 애플리케이션 이벤트, 데이터 이벤트, 네트워크 이벤트, 사용자 레벨 이벤트 모두 포함
  - 중요 데이터분류 및 사용자, 프로세스, 데이터가 행하는 모든 사용 현황 실시간 로깅
  - 육하원칙에 따른 파일 변경 추적 시스템 구현 제공 (데이터 태깅 기술 적용 및 변경 추적)

- **정책 적용 대상**
  - Machine 기반
  - User 기반

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Digital Guardian 기능 요소 (Endpoint Data Loss Prevention)

- **컨텐트(Content) 기반의 데이터 분류 및 제어**
  - 키워드(Keywords), 정규표현식(Regular Expression), 사전(Dictionary) 검색
  - 관리자 정의된 "기업 특화 키워듸" 추가

- **컨텍스트(Context) 기반 데이터 분류 및 제어 ➔ 핵심 차별화 포인트**
  - 200+ 추가 파라미터 조합 및 데이터 분류 방법론
  - 파일, 프로세스, 메일, DLL, 네트워크, 레지스트리, 훅(Hook), 디바이스, 프린트 관련된 액션이벤트 조합

- **유연한 사용자 제어 옵션**
  - Alert (관리자 콘솔 경고 로그)
  - User awareness (엔드유저 팝업 및 명확한 로그 제시 후, 인지시키도록 다이나믹 팝업 메세지 제공)
    : Block (차단 / 첨부파일 제거)
    : Justification (유저 스스로 사유 작성)
    : Warning (데이터 전송행위를 허용하되, 유저에게 알림)
  - 팝업 메세지 커스터마이징 기능 내장 (XML / HTML5 기반 + 변수기반의 구체적인 내용 표시)

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

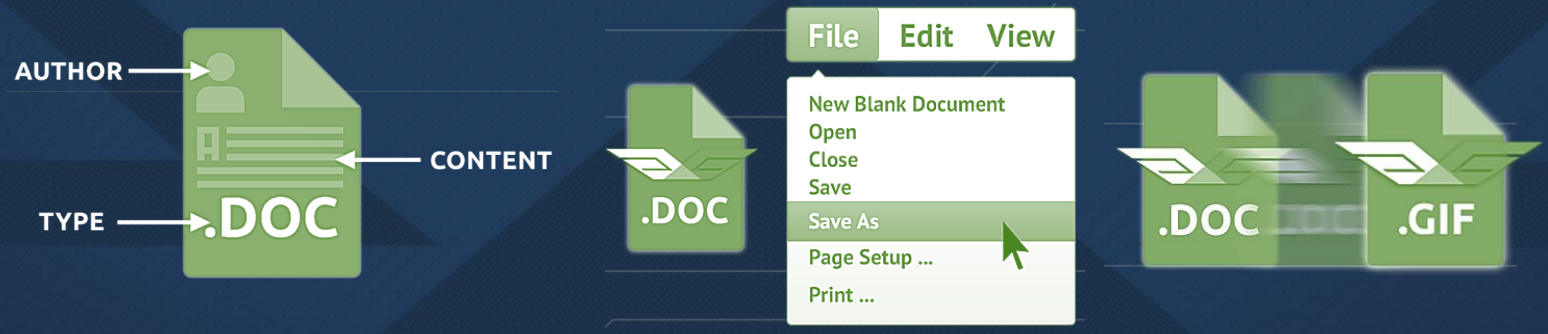
Digital Guardian 기능 요소 (Endpoint Data Loss Prevention)

- Kernel Level Data Visibility
  - Deepest visibility to all events at point of risk/egress (Endpoint, Network, and Servers)
  - Broadest coverage of systems (Windows, MAC OS X and Linux)
  - Broadest coverage of environments (Network, Cloud, Virtual, Online and Offline)

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

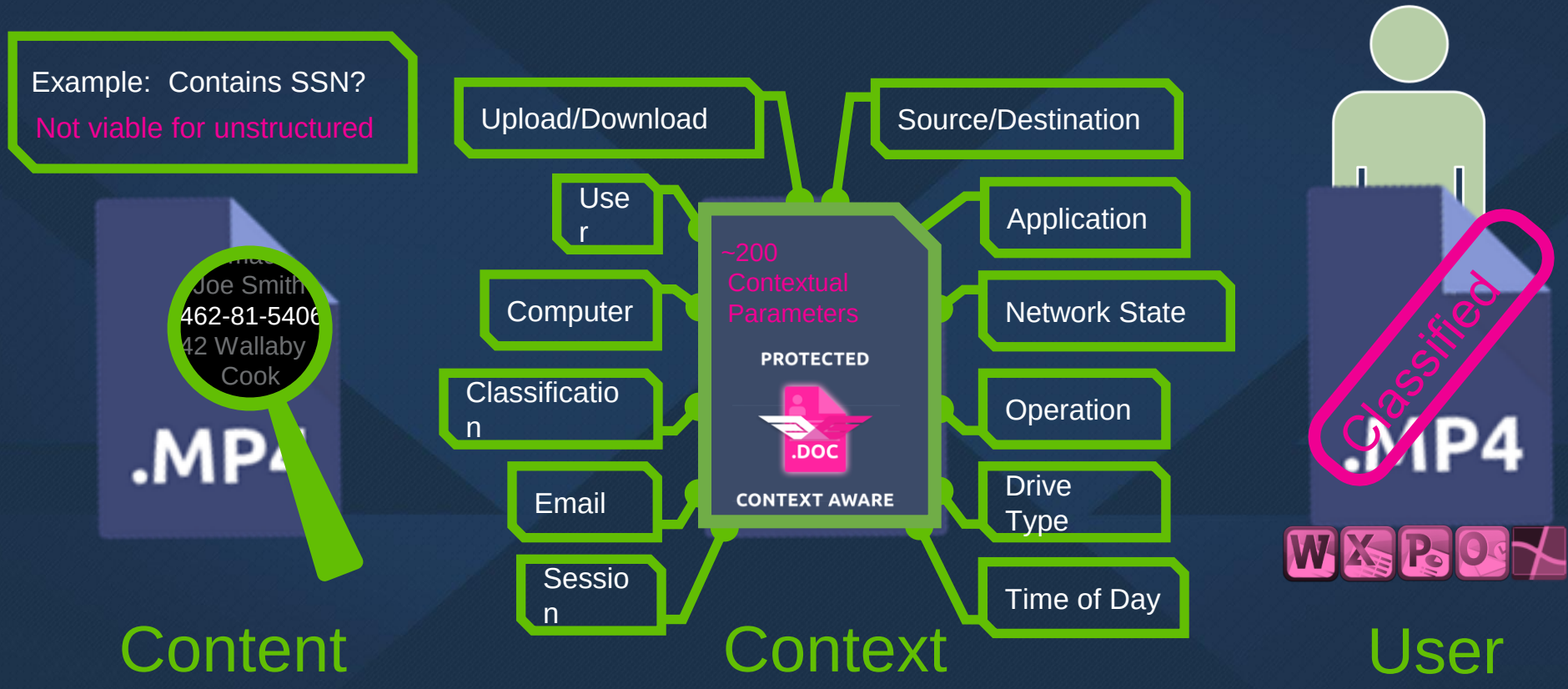
Digital Guardian 기능 요소 (Endpoint Data Loss Prevention)

- Automatic Content & Context Driven Data Classification
  - Classify based on context, content, and user-definition
  - Classify ALL data types (structured, unstructured, MSOffice, CAD, source code, media, video, and more)
  - Apply persistent and inheritable classification tags



DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Auto & User Classification



DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

The Context Advantage

Threat Vector	User Awareness	Access	System Ops	Data Awareness	Event Awareness		Policy
Messaging	Executive	Desktops	App Starts	# Strings	Rename	Network Drive	Monitor
Website	Engineer	- Win	Drivers	Key Words	Dropbox	USB Device	Block
Physical	Admin	- Linux	DLL	CAD Files	Attach	Web	Warn
Network	Finance	- Mac	PID	Source Code	Archive	Local Drive	Justify
	Contractor	Servers	File Type	Video/Images	Move	E-mail	Encrypt
	Supplier	Network	File Hash	Customer	Copy/Paste	Print	Allow
	Sales	Offline	Registry	Classification	Executable	Create	Classify
	System	Virtual	Net Ops	Application	Screen Cap	CD/DVD	Control

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Digital Guardian 기능 요소 (Endpoint Advanced Threat Protection)

▪ 실시간 행위기반 악성 코드/행위 탐지 및 차단

- 변조된 공격 벡터(Attack vector)에 상관없이, 실시간 악성코드 및 행위를 "**엔드포인트레벨 탐지 및 차단**"
- 시스템, 사용자, 데이터에 대한 공격 탐지 및 차단
- 사용자에게 공격 탐지 알림창 팝업, 공격 차단, 보안관리자에게 알림 (포렌식 감사 로깅 자료 제공)

▪ 포렌식 분석 시간 단축 및 사고 관리 역량 강화

- Correlated event를 발생시킨 룰(rule) 알림 및 관련된 이벤트 검색 기능
- 진행중인 공격 차단기능 강화
  - : 의심, 악성코드에 감염된 모든 파일 추적하는 "바이너리 분석" 기능 제공 / 감염 시스템 분류
  - : 아직 감염되지 않은 주변 엔드포인트 시스템에, "이미 발견된 멀웨어 즉시 차단" 정책 전파

▪ 외부 ATP 시스템 연동 및 공동 대응 체계 지원

- IOC (Indicator of Compromise) 연동 및 엔드포인트 기반 차단 제공
  - : FireEye Sanbox ATP, PaloAlto WildFire ATP, Bluecoat 연동
  - : VirusTotal 연동 (파일 해쉬값 정보 공유 후, 악성코드 감염된 파일의 차단 또는 경고)

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Digital Guardian 오퍼링 소개

DG for Data Visibility 가시화 & Control 통제

- 데이터/시스템 액세스 가시화
- 데이터 이동/프로세스 액티비티 가시화
- Data operations & classification of PII, PHI and PCI
- 데이터 오퍼레이션 & PII, PHI, PCI의 분류
- Device Control for removable media
- 이동식 기기(USB 등) 컨트롤
- Alert Triage – 경고 / 케이스 분류
- Systems: Windows, VDI (OSX/Linux Partial Support)
- Required license for DLP &/or ATP upgrades

Data Loss Prevention (DLP)

- 데이터 자동 분류 – 정형 vs. 비정형
- 사용자 기반 분류 (add-on licenses required)
- 프롬프트메시지, 특정 상황에 대한 실시간 사용자 해명요청
- 컨트롤
  - 파일/이메일 암호화 (add-on licenses required)
  - 어플리케이션/사용자행동 블락(Block)
- Systems: Windows, OSX, Linux, VDI

Advanced Threat Protection (ATP)

- 위협 감지
- 프로세스 블락, 파일액세스 방지, 엔드포인트/사용자 격리, 허가되지 않은 사용자의 침입 방지
- Alert and Triage – 경고 / 케이스 분류
- 엔드포인트 이벤트에 대한 IOC 간 상관관계 감지
- Systems: Windows, Linux/OSX (Q2 2015)

All offered as On Premise Perpetual Software License or as a Managed Service

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Flexible Deployment Models – 다양한 도입 환경

"By selecting the managed service deployment option, we were able to be up and running in a matter of weeks. The added visibility into how our confidential data is being used is invaluable."

CISO, Regional Bank

Option 1

On Premise 온프레미스

- 사내 구축/운영/관리 환경
- 정책, 모니터링, 리포트 생성 등 모든 프로세스를 IT 관리자가 직접 설정/관리
- 필요한 경우에만 유지보수/서비스 전문가 고용

Option 2

Managed Service 매니지드 서비스

- 자체 구축된 프라이빗 클라우드 내에서 운영
- 디지털가디언 서비스 담당자에 의해 운영
- 정책/관리/리포팅 등에 대한 접근 관리, 직접 생성하지 않음
- 정기 회의를 통한 상황 업데이트

Option 3

Hybrid 하이브리드

Managed Service On Premise

- 사내 구축 환경
- 디지털가디언 서비스 담당자에 의해 리모트로 운영
- 데이터는 사내 보유

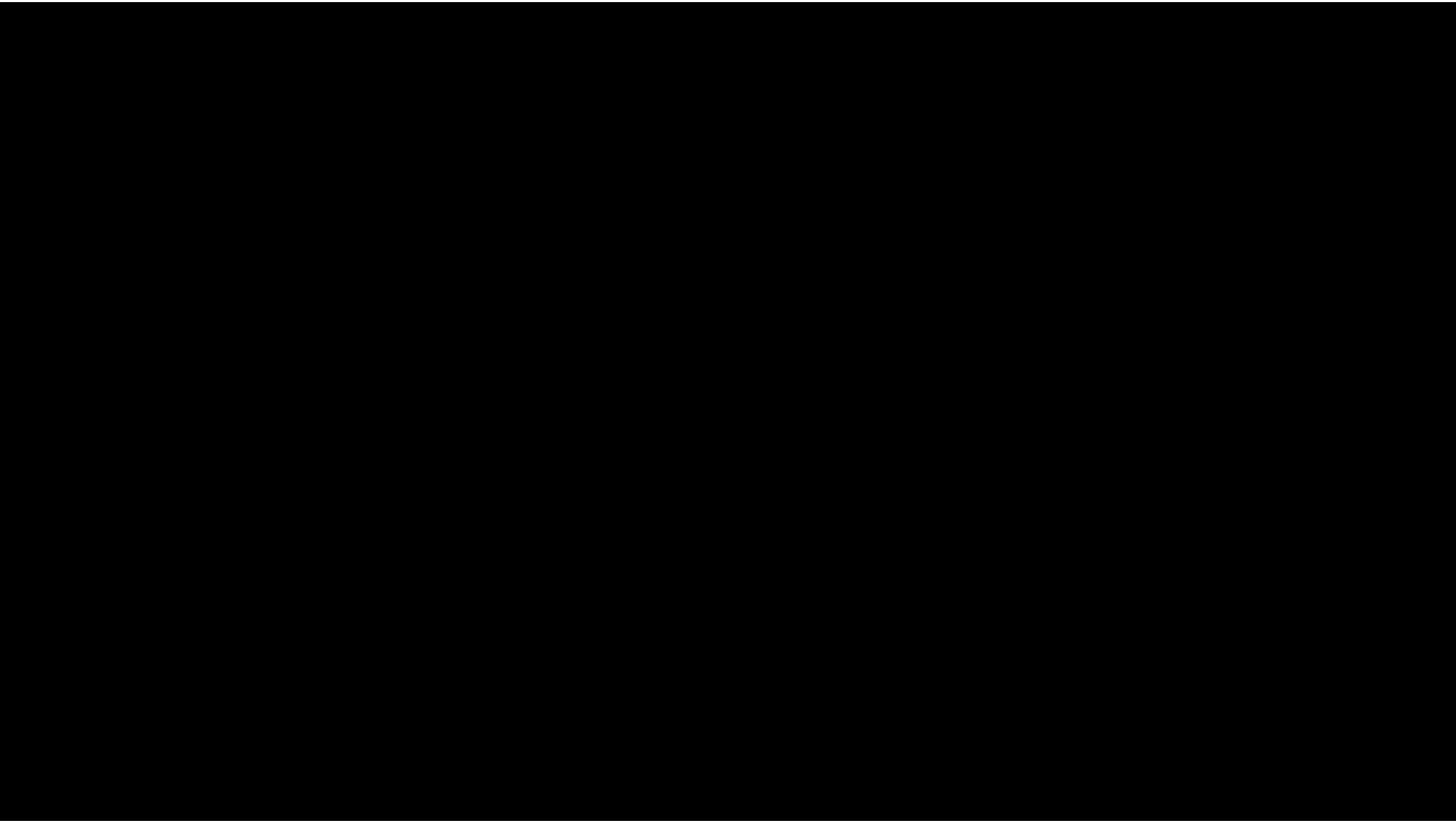
DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

04

디지털가디언
Data Protection Demo

Demo #.1

Demo #.2



05

디지털가디언 맺음말

EDR + ATP + DATA awareness = Digital Guardian

EDR

- 분석
  - 포렌식 분석
  - 사고 과정 분석
  - 데이터 중심이 아님
- 대응
  - 향후 대응을 위한 IOC 메트릭 생성
  - 사고 이후의, 전체 사고 과정에 대한 프로세스 분석
- System Visibility

+

ATP

- 멀웨어와 끊임없는 전쟁
  - IOC → 시그니쳐 대체
  - 멀웨어 중심의 행위 탐지
  - 데이터 중심이 아님
- 탐지 및 위협 대응
  - 단, 위협 식별후 제어는?
  - Full Zero-day 방어 실현?
  - 위협 탐지 실패 시, 데이터는 위험한 상태로 남게 됨
- Threat Visibility

+

DATA awareness

- 정형 데이터
  - PII/PCI/PHI
  - Content 기반 (키워드기반)
- 비정형 데이터
  - IP/Trade Secrets
  - Context 기반 (상황인식 기반)
- 영구 식별 기술
  - 메타 태그
  - 암호화 식별
  - 상속 식별
- Data visibility

=

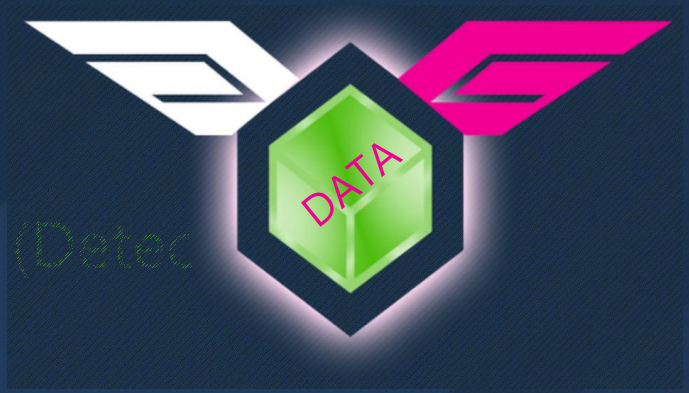
DIGITAL GUARDIAN

- 시스템, 데이터, 위협 식별 및 보호
  - 인지 불능 컨텐트 보호
  - 지속적인 포렌식 캡쳐
  - 실시간 이벤트 상관 분석
  - 데이터 중심, Context 인지기반 보호
- 상황 인식기반 보호
  - "Unknown & Unknown" 위협 대응
  - 현실적인 정책 적용 및 예외 처리
  - 파일, 응용프로그램, 네트워크 활동(activities) 혼합 컨트롤
  - 위협 유발 프로세스의 권한 정지
- Visibility for System, Threat and Data

분석 / 위협 중심 -- "데이터 위험 존재"

데이터 중심으로 이동 -- "위협 탐지 및 데이터 보호"

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™



→ See

모든 위협을 모니터링하고 있는가?

→ Understand

뭔가 발생한 상황과, 발생하지 않은 상황을 증명할 수 있는가? (Prove)

→ Respond

허용되어서는 안될 위험을 방어할 수 있는가? (Prevent)

DIGITAL GUARDIAN Formerly VERDASYS | SECURITY'S CHANGE AGENT™

Gartner Enterprise DLP Magic Quadrant

As of January 2016

- 리더 그룹 중,
  유일한 Private Company
- 기술 중심 "리더" 포지셔닝
- EDR 내장 유일한 DLP

Gartner

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Data Loss Prevention

Contact Us!

언제나 여러분과 함께 하겠습니다.

Our website:
http://www.tocsg.co.kr

Facebook:
http://www.facebook.com/tocsg2008

E-mail:
sales@tocsg.co.kr

Telephone:
02-320-5000

BLOG:
http://tocsg.tistory.com

김주동 전무이사
jdkim@tocsg.co.kr

02-320-5030
010-2016-2101

Thank You