망분리 대체 정보보호통제 PC 사용자의 관리자 권한 제거 대응를 위한

PowerBroker for Windows(PBW)

최소 권한 and Application Control for Windows Servers and Desktops

2018.09

세종정보보안 BizHuB

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

Contents

PowerBroker

Privileged Access Management Platform

세종정보보안 BizHub

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

I Why PowerBroker ?

PowerBroker 필요성

PowerBroker

Privileged Access Management Platform

세종정보보안 BizHub

금감원 망분리 대체 정보보호통제 대응

전자금융감독규정 시행세칙 제2조의2 (망분리 적용 예외)

전자금융감독규정 망분리 관련 조항

관련 규정	전자금융감독규정 상세 내용
전자금융감독규정 제15조(해킹 등 방지대책)	3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지 **(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)**
전자금융감독규정시행세칙 제2조의2 (망분리 적용 예외)	① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 내부 업무용시스템을(규정 제12조의 중요단말기는 제외한다) 업무상 필수적으로 특정 외부기관과 연결해야 하는 경우를 말한다 (다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).
	③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 <별표 7>에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

제12조(단말기 보호대책) 3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것

<별표 7> 망분리 대체 정보보호통제

대책	세부사항
내부망 보안 강화	▪ 업무망에 반입되는 전산자료 대상으로 악성코드 감염여부 진단·치료 대책 수립
외부망 보안 강화	▪ **지능형 해킹(APT)차단 대책 수립** ▪ 외부망을 통해 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링 대책 수립
단말기 보안 강화	▪ **PC 사용자의 관리자 권한 제거** ▪ **승인된 프로그램만 설치·실행토록 대책 수립** ▪ 단말기 전산 자료 암호화 저장

금감원 망분리 대체 정보보호통제 대응

PC 사용자 관리자 권한 제거

구분	PowerBroker 기능
Application	▪ 설치나 실행 시 프로세스 단위 Admin 권한의 임시 부여
시스템 작업	▪ 시스템 작업 시 자유로운 Admin 권한 부여 : IP변경, Time 설정, 프린터 설정 등
CUI 작업	▪ 시스템관리자나 유저의 명령어 작업에 대한 Admin 권한 부여의 용이성

PC(단말)에 임의 프로그램 설치 방지를 위한 권한 통제 필요

PowerBroker

유저의 변경 없이 일반 유저에서 필요한 PROCESS 및 TASK 단위로 관리자 권한을 부여

금감원 망분리 대체 정보보호통제 대응

승인된 프로그램만 설치·실행토록 대책 수립

• 승인된 프로그램은 Installation Program & Portable Program & Device Driver 등 모든 프로그램을 포함

통제 요구 사항

- 단말에 어떤 소프트웨어도 임의로 설치 불가
- 승인된 프로그램만 설치 및 실행 가능

승인되지 않은 프로그램의 설치 방지로 라이선스 및 자산 관리 필요

PowerBroker : 최소 권한 + WhiteListing

- WHITELISTING과 최소 권한을 구현하는 솔루션
- 최소 권한 + WHITELISTING = RANSOMWARE 방지
- WINDOWS O/S는 하나의 AGENT에서 지원하며, MAC O/S도 지원

공공기관 정보보안 세부 지침 준수

국가정보보안 기본지침에 대한 공공기관 "정보보안 세부 지침" 준수

- 「국가정보보안 기본지침」에 따라 공공기관의 정보보안업무에 필요한 세부 사항의 준수
- 대부분의 공공기관은 「국가정보보안 기본지침」를 기초로 각 기관의 특성에 맞도록 정보보안 세부 지침을 수립
- PC(단말)에 업무와 무관한 비인가 프로그램의 설치 및 사용을 할 수 없도록 통제 적용 필요
- 비인가 프로그램의 설치를 통제할 수 있도록 PC의 Admin 권한에 대한 통제
- 사용자의 접근권한과 범위를 업무별 · 자료별 중요도에 따라 차등 부여

공공부분 정보보안 세부 지침 내용(예시)

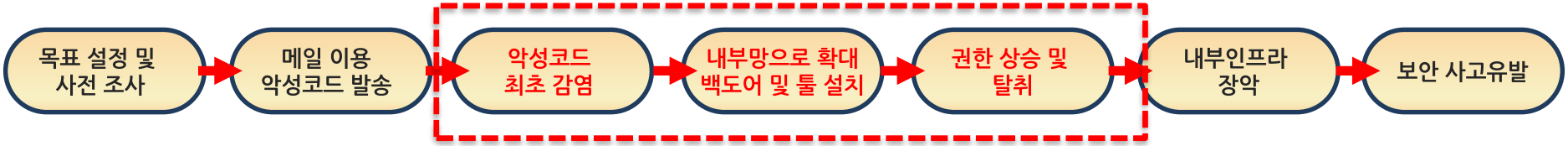
관련 규정	단말 및 서버 운영 통제 관련 정보보안 세부 지침 내역
제33조 (PC 등 단말기 보안관리)	4. **업무와 무관하거나 보안에 취약한 응용프로그램 설치 금지** 및 공유 폴더의 삭제 5. 그 밖에 국가정보원장이 안전성을 확인하여 배포 승인한 프로그램의 운용 및 보안권고문
제34조 (인터넷PC 보안관리)	정보보안담당관은 비인가자가 인터넷과 연결된 PC(이하 인터넷PC)를 무단으로 조작하여 전산자료를 절취, 위 · 변조 및 훼손시키지 못하도록 다음 각 호의 보안대책을 사용자에게 지원하며, 사용자는 이를 준수 1. 메신저 · P2P · 웹하드 등 업무에 무관하거나 Active-X 등 보안에 취약한 프로그램과 **비인가 프로그램 · 장치의 설치 금지** 2. 특별한 사유가 없는 한 문서프로그램은 읽기 전용으로 운용
제35조 (서버 보안관리)	② 서버 관리자는 서버내 저장자료에 대해 **업무별 · 자료별 중요도에 따라 사용자의 접근권한을 차등 부여** ③ 서버 관리자는 사용자별 자료의 접근범위를 서버에 등록하여 인가여부를 식별토록 하고 인가된 범위 이외의 자료접근을 통제
제44조 (악성코드 방지대책)	2. 사용자는 **출처, 유통경로 및 제작자가 명확하지 않은 응용프로그램 사용을 금지**하고 인터넷 등 상용망으로 자료 입수시 신뢰할 수 있는 인터넷사이트를 활용하여야 하며 최신백신으로 진단후 사용.

랜섬웨어에 대한 대비 필요

APT 솔루션을 운영하고 있어도 새로운 APT 공격 방어에는 취약

01 Zero-Day 공격	제로 데이 공격(또는 제로 데이 위협, Zero-Day Attack)은 컴퓨터 소프트웨어의 취약점을 공격하는 기술적 위협으로, 해당 취약점에 대한 패치가 나오지 않은 시점에서 이루어지는 공격
02 Unknown 공격	기존 APT 방어 솔루션들은 '알려진 위협'(Known threat)을 차단하고 있어서 '알려지지 않은 위협'(Unknown threat)은 방어가 불가능
03 내부 우회 공격	기존 APT 방어 솔루션은 Perimeter(외부 방벽) 모델로 해커가 우회하여 내부로 진입할 수만 있다면(**메일 수신 이후 등**) 그 이후부터는 정상 유저와 해커의 구분이 어려워 탐지와 조치가 매우 어려움

기존의 APT 대응 솔루션으로는 다양한 형태의 APT 공격에 대한 방어가 취약



Ransomware를 비롯한 모든 Malware 방지를 위한 기본 준수 사항은
최소 권한의 실행으로 Admin(관리자) 및 특권유저실행을 금지하는것과 Application Control 기능 입니다

PowerBroker 솔루션 개요

PowerBroker 주요 기능 요약

서버보안강화(최소 권한)	▫ 유저권한분리/공유ID제거 ▫ 최소 권한 부여(Admin/dba/sap등 관리자 권한 제거) ▫ 슈퍼유저의 남용방지
Session 관리	▫ 작업자가 특정 Session 동안 Key-in/Mouse Click한 모든 내역의 Display (Key Stroke Logging) ▫ 키워드 Search 기능
자산 Scanning	▫ H/W, S/W User 등의 사내 모든 자산(Unix/LINUX/WINDOW/NETWORK등)에 대하여 H/W, S/W User 등의 자산 Scanning & Reporting
Event Logging	▫ 언제 작업을 수행 했는가? , 어떤 유저가 프로그램을 요구 했나 ? ▫ 어떤 시스템에서 작업했는가?, 어떤 프로그램을 시도 했는가 ? ▫ 어떤 시스템에서 Execution 실행하게 했나?, 누가 Admin 유저로 수행 하였나 ?
File Integrity Monitoring	▫ 중요 파일의 변동 방지 ▫ 파일이나 폴더에 대한 Location, Ownership, Permissions, Size, Date/Time, File hash등을 보관 ▫ 중요 System Binary, Product Binary 나 구성파일들의 위 변조 방지 ▫ 중요 파일들에 대한 변경 내역 트래킹(변경/추가/삭제/Policy 위반) ▫ 변조된 파일이나 명령어 실행금지 및 스크립트내의 Auditing 가능
Application Control	▫ Whitelisting 방식의 Application Control ▫ Ransomware 방지 ▫ 서버나 단말의 설치 소프트웨어 통제

PowerBroker 솔루션 구성

서버 및 네트워크 장비에 대한 통합 접근 및 권한 통제 솔루션

PBUL	PowerBroker For Unix/Linux	Unix/Linux에 대한 특권권한 통제 솔루션
PBWS	PowerBroker For Windows Server	Windows Server에 대한 특권권한 통제 솔루션
PBWD	**PowerBroker For Windows Desktop**	**Windows PC에 대한 특권권한 통제 솔루션**
PBNW	PowerBroker For Network	N/W 장비에 대한 특권권한 통제 솔루션
PBPS	PowerBroker Password Safe	모든 계정에 대한 패스워드 관리 솔루션
PBIS	PowerBroker Identity Services	Unix/Linux 계정에 대한 AD 연동 솔루션

THE POWERBROKER PRIVILEGED ACCESS MANAGEMENT PLATFORM

Server Privilege Management
Control, audit and simplify access to business-critical systems
UNIX | LINUX | WINDOWS

Enterprise Password Security
Provide accountability and control over privileged credentials and sessions
APPS | DATABASES
DEVICES | SSH KEYS | CLOUD | VIRTUAL

Endpoint Least Privilege
Remove excessive user privileges and control applications on endpoints
WINDOWS | MAC

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

II PowerBroker for Windows

최소 권한 and Application Control
for Windows Servers and Desktops

PowerBroker

Privileged Access Management Platform

세종정보보안 BizHub

솔루션 서비스 개요

BeyondTrust PBW(PowerBroker for Windows)는 사용자의 생산성을 유지하면서 물리적 또는 가상의 Windows Server나 사용자 단말의 최소 권한(관리자 권한 통제)를 강화하기 위해 사용자 개입없이 프로그램별 권한 상승과 파일/폴더의 무결성 유지 등 다양한 기능을 제공합니다.

- Prefix에 의한 프로그램 실행이 아닌 사용자 정책에 따른 실행 프로세스의 보안 토근을 변경하는 On-the-fly 형식
  - Patent 받은 Elevation Technology
  - OS 및 다른 보안 솔루션과 충돌 없음
  - 프로그램 또는 사용자에 의한 Elevation이 아님
  - GUI 및 CLI 에 Transparent

- 최적의 멀웨어 및 랜섬웨어 실행 방지 솔루션 (Whitelisting)
  - 신뢰되지 않은 프로그램 Blocking
  - 신뢰되지 않은 디렉토리 Blocking
  - Malware DB 연동에 의한 실행 차단

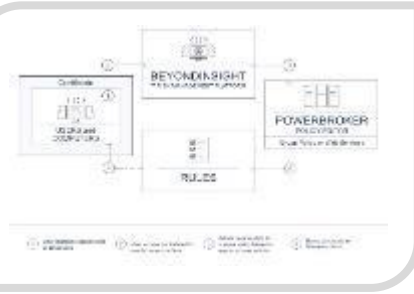
특허 받은 권한 상승(Elevation) Technology

랜섬웨어 및 멀웨어 실행 방지

BeyondTrust
PowerBroker for Windows

손쉬운 정책 구성 및 관리

이벤트 분석을 통한 다양한 보고서 제공



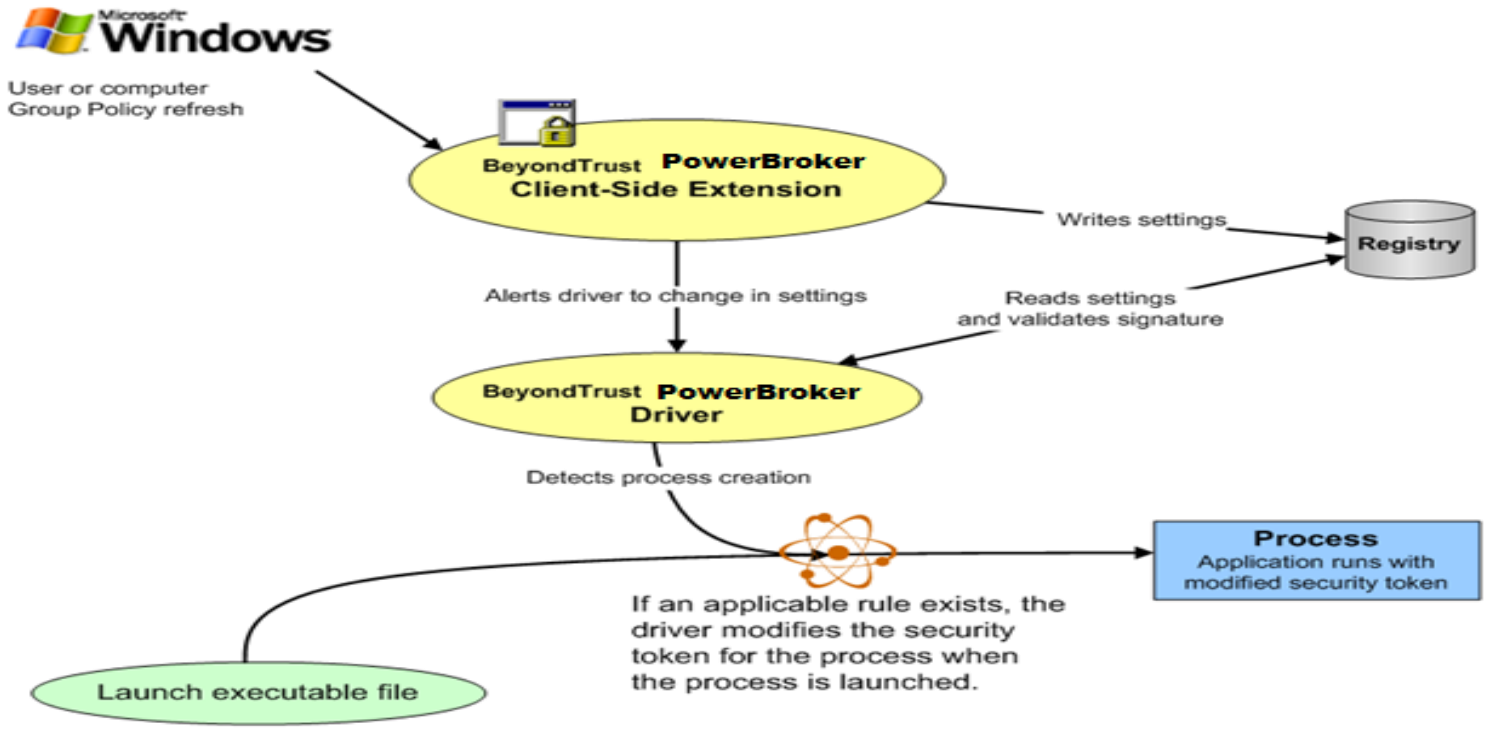
- ActiveX 구체적 통제
- 사용자의 실행 프로그램 행위 파악
- 사용자 실행 규칙 작성의 편의성 제공
- AD / non-AD(Workgroup) 환경 적용
- Item Level Targeting : OU 단위가 아닌 다양한 조건별(사용자, 그룹, 시간, 날짜, 특정 환경변수, LDAP Query, 사용자 단말, 언어 등) 권한 제어

- 감사에 대비한 정책 관리
- 감사에 대비한 사용자 실행 행위 관리
- 다양한 보고서 및 통계 정보 제공
- 사용자의 행위 이벤트 관리를 통한 리포팅 제공

솔루션 서비스 개요

특허 받은 "권한 상승 통제" 기법

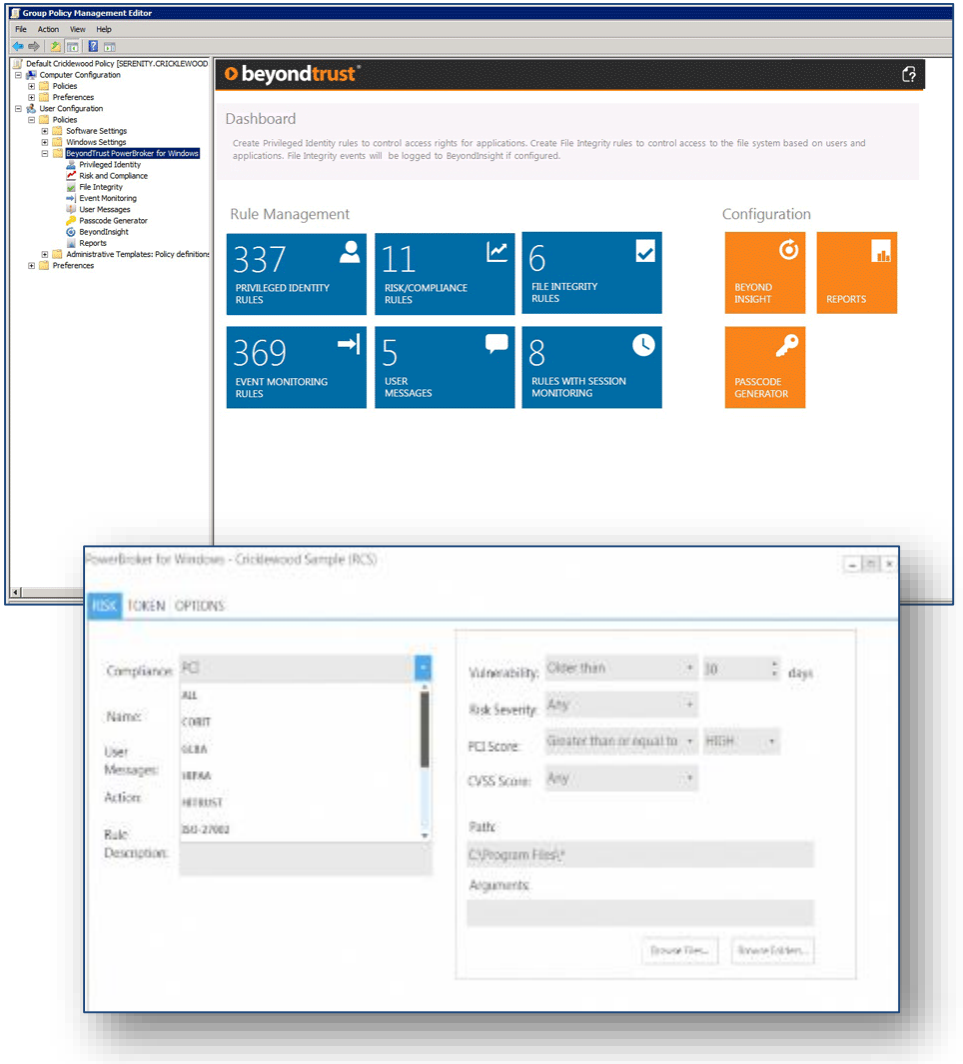
- "권한 상승"시 유저가 속하는 그룹을 변경함으로써 "권한 상승"을 하여서는 안됨
- 어느 한 순간이라도 유저가 Admin 속성을 지니는 그룹에 속해서는 안되며, 유저가 아닌 Process만 "권한 상승"이 되어야 함
- Windows XP 부터 Windows 2016까지 하나의 Agent에서 지원



PowerBroker(PBWD) 기능 상세

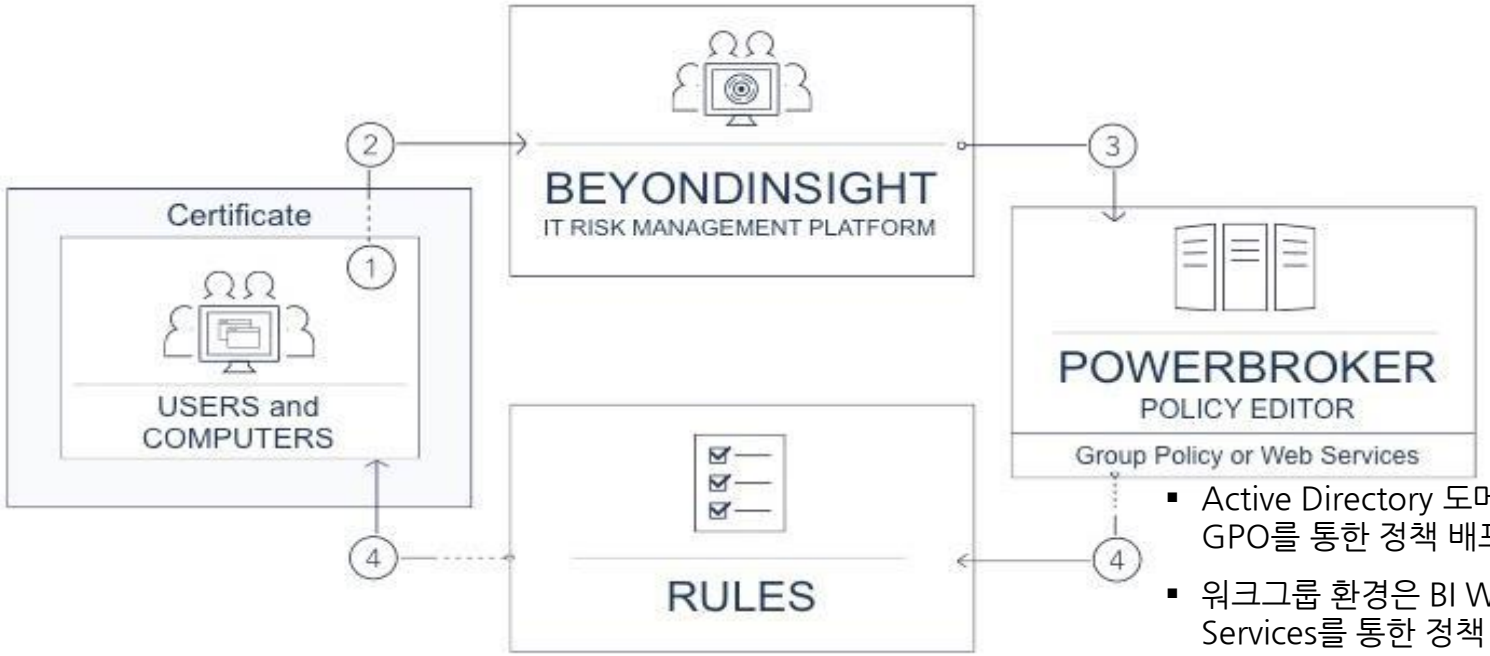
PowerBroker(PBWD) 제품 개요

- 사용자의 생산성을 유지하면서 물리적(Physical) 또는 가상(Virtual)의 Windows Server나 사용자 단말의 최소 권한(관리자 권한 통제)를 강화하는 Endpoint Solution
- 사용자 개입 없이 프로그램별 권한 상승
- 상황인식 위험 인지를 위한 직관적인 UI 제공
  - ✓ Retina 취약점 Database를 통한 이벤트 자동 연관성
  - ✓ 발생한 이벤트에 대한 특정 자산이나 사용자에 대한 정책을 생성



PowerBroker(PBWD) 기능 상세

동작 방식



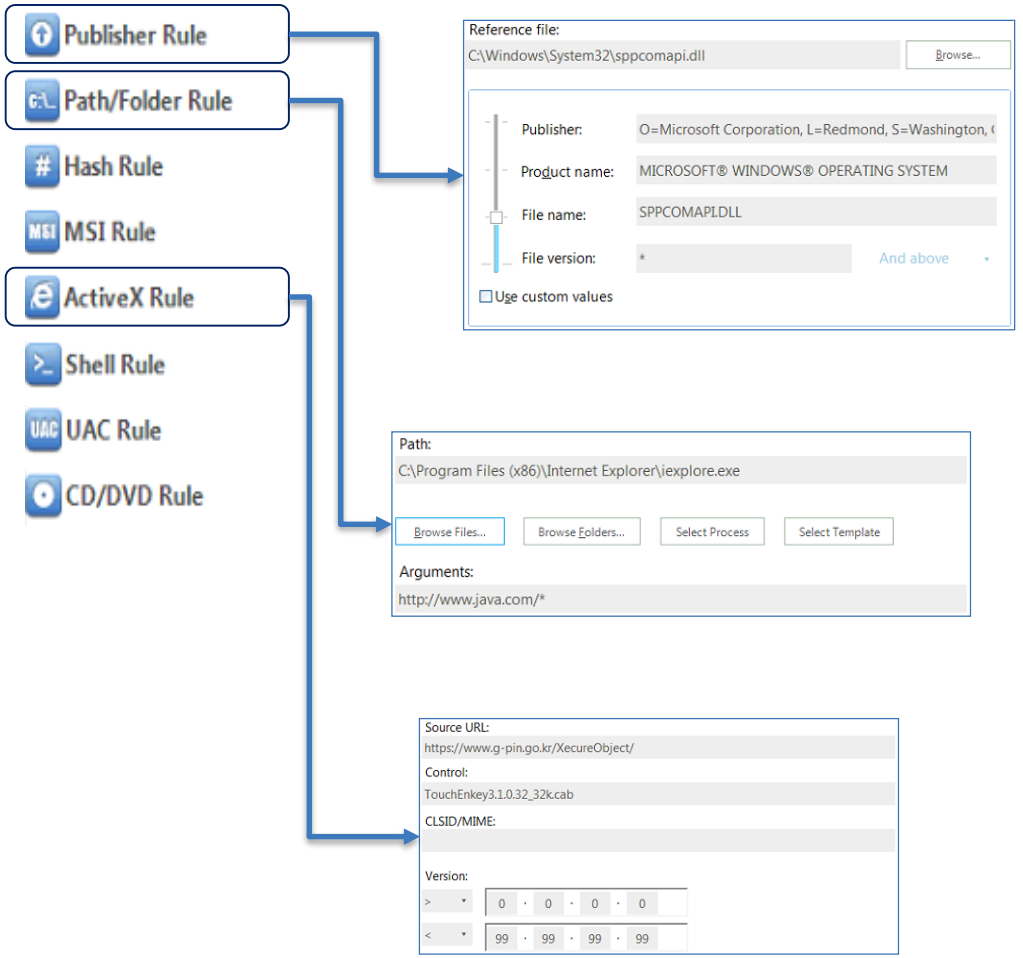
- Active Directory 도메인환경은 GPO를 통한 정책 배포
- 워크그룹 환경은 BI Web Services를 통한 정책 배포

1. User launches applications or processes
2. User actions centralized for events, sessions, files
3. Admin reviews data & creates policy based on approved user actions
4. Rules sent back to Windows client

PowerBroker(PBWD) 기능 상세

Rule 및 Rule 설정

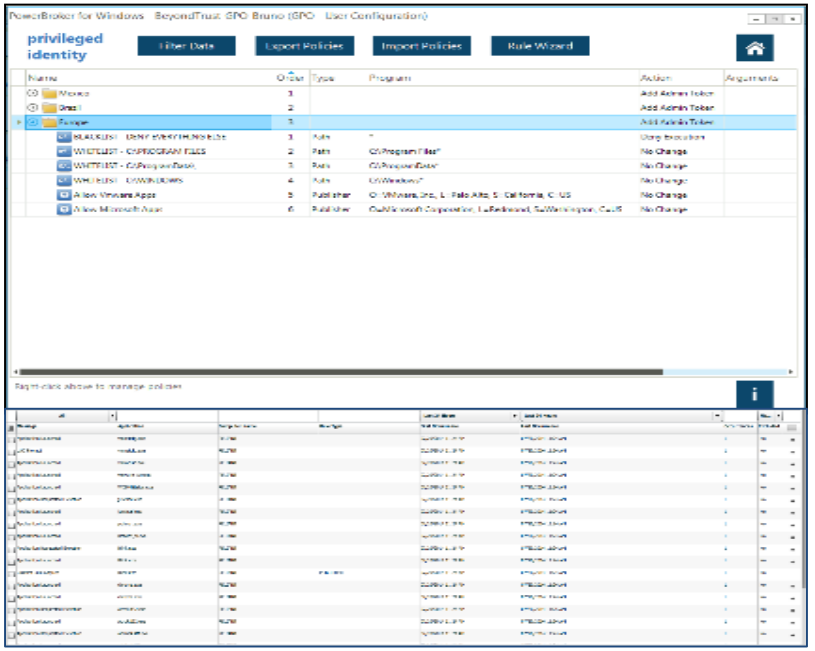
- Publisher : 디지털 서명된 파일을 기반 룰 적용
- Path/Folder : 폴더/파일명 기반 룰 적용
- Hash : 파일의 Hash 값 기반 룰 적용
- MSI : .MSI 파일 기반 룰 적용
- ActiveX : ActiveX control 기반 룰 적용
- Shell : On Demand성 룰 적용
- UAC : UAC에 의해 구동되는 application 대상 룰 적용
- CD/DVD : CD 또는 DVD상의 application 대상 룰 적용
- File Integrity Rule : File 관련 룰 적용



PowerBroker(PBWD) 기능 상세

Application Control

- 어플리케이션의 Whitelisting 과 Blacklisting 기법을 통한 프로그램 실행 제어
- 승인되지 않은 어플리케이션의 설치 및 실행 금지
- 승인된 어플리케이션이 특정 위치에서 실행 허가
- Digital Signatures, Path, Hash, Vulnerability 그리고 여러 가지 룰에 의한 Application Control



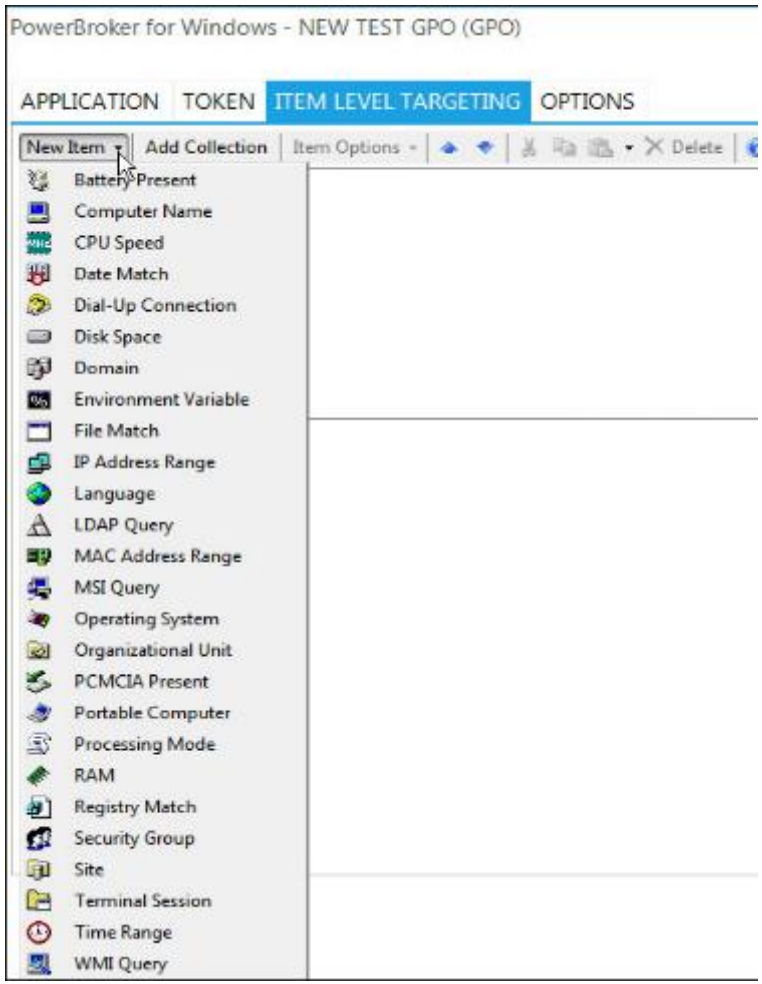
Name	Ord...	Type	Program	Arguments	Action	Ses...	Enab...
All Deny Applications except trusted applications	1				Add Admin T...	☐	☐
All Deny Applications except trusted applications	1	Path	*		Deny Execution	☐	☑

Event Id	Message	Application	Time Created	Computer Name	Process Type	User Name	Justific...	Rule Type	Event T...	Exclud...
3217	Denied Rule Applied	bcoccibrull.exe	09/04/2018 3:01 PM	BHW07VM	Standard User	BHW07VM\lctestus...		PATH	28698	No
3214	Denied Rule Applied	cycys.exe	09/04/2018 3:01 PM	BHW07VM	Standard User	BHW07VM\lctestus...		PATH	28698	No
3210	Denied Rule Applied	Explorer++.exe	09/04/2018 3:00 PM	BHW07VM	Standard User	BHW07VM\lctestus...		PATH	28698	No
3209	Denied Rule Applied	Bat_To_Exe_Convert...	09/04/2018 3:00 PM	BHW07VM	Standard User	BHW07VM\lctestus...		PATH	28698	No

PowerBroker(PBWD) 기능 상세

Item Level Targeting

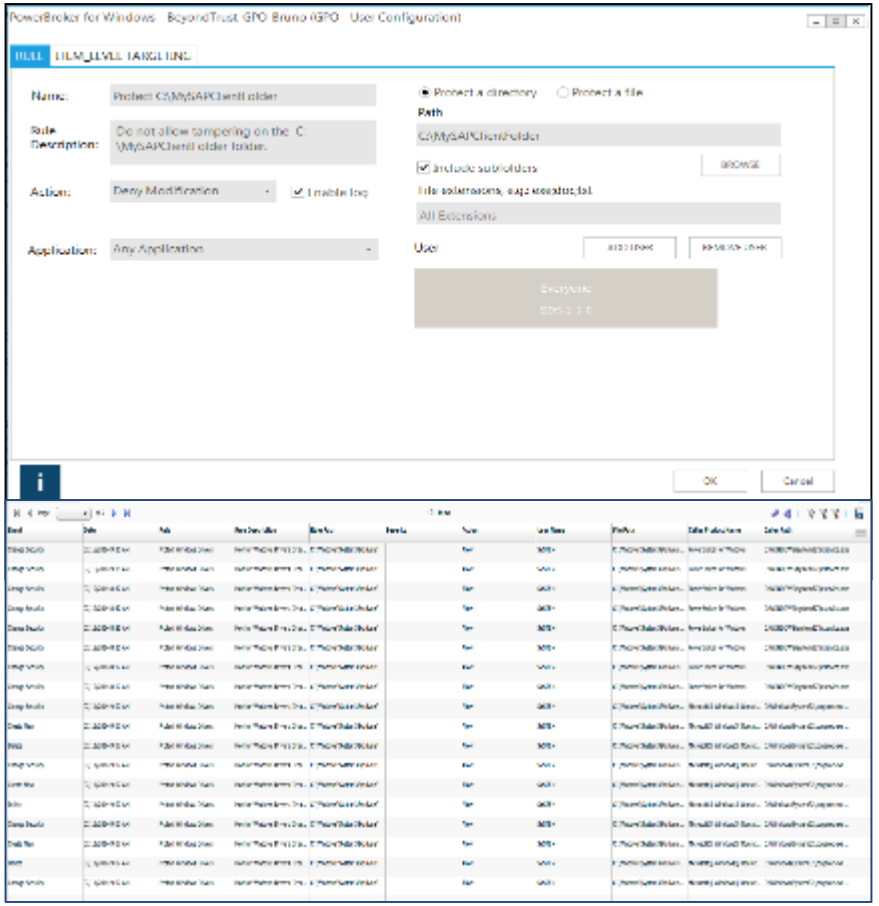
- Policy 를 OU 단위로 주지 않고 다양한 유형으로 적용 가능
- Item Level Targeting 기능을 통해 다양한 조건별(특정 사용자, 그룹, 시간별, 날짜별, 특정 환경변수 정보, LDAP Query 정보, 사용자 단말 사용 언어별 등) 권한 제어 가능



PowerBroker(PBWD) 기능 상세

File Integrity Monitoring

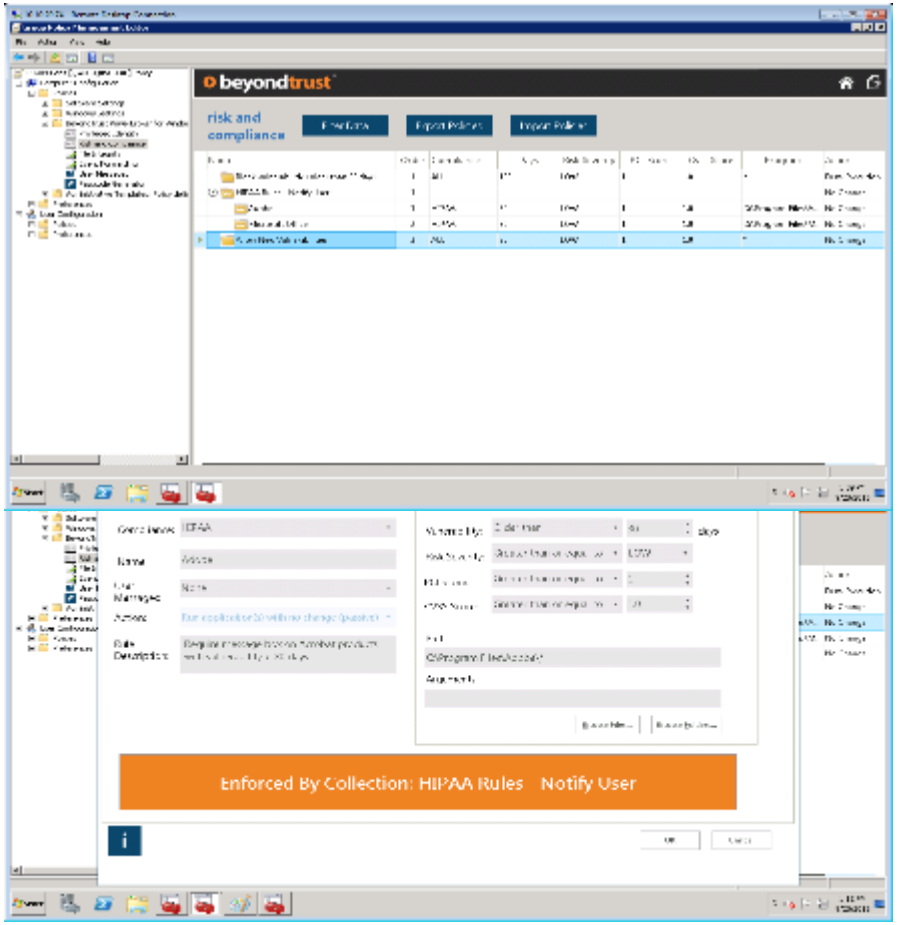
- 어떤 Application이 어떤 자산의 어떤 파일을 접근 하였는가?
- OS의 기본 File Permission 상의 Additional Security Layer
- Elevation이 수행된 Directories 관찰
- 변경 관리 하에 있는 디렉토리의 접근 허가/거부



PowerBroker(PBWD) 기능 상세

Risk Compliance

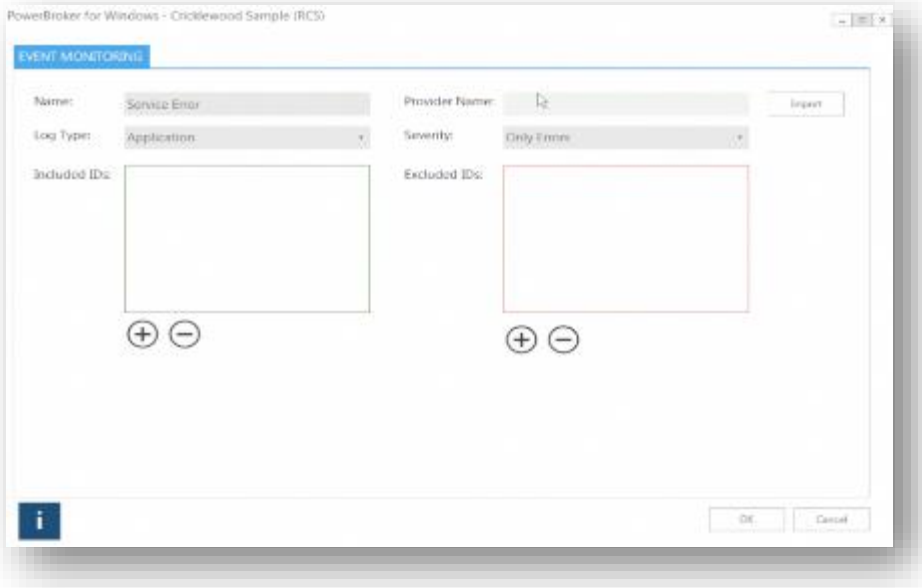
- Regulatory compliance 와 취약점(Vulnerabilities)을 근거로 한 정책 적용 가능
- Passive monitoring, allow or deny privileged escalation for application, or session monitoring 기능
- Risk compliance를 위한 특별 Reporting
- 실시간 application-based 취약점 분석
- 취약점을 근간으로 한 Audits 가능

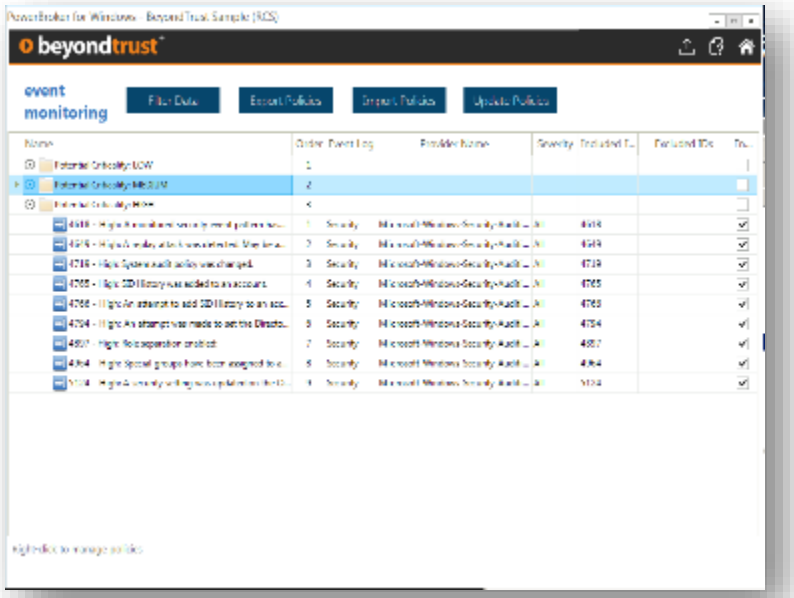


PowerBroker(PBWD) 기능 상세

Windows Event Log Monitoring

- Windows Event Log의 중앙 집중화
- Windows Event Log의 Pattern Matching (System, Application & Severity)
- Real time Notification
- Microsoft Recommend Monitoring Rule 제공



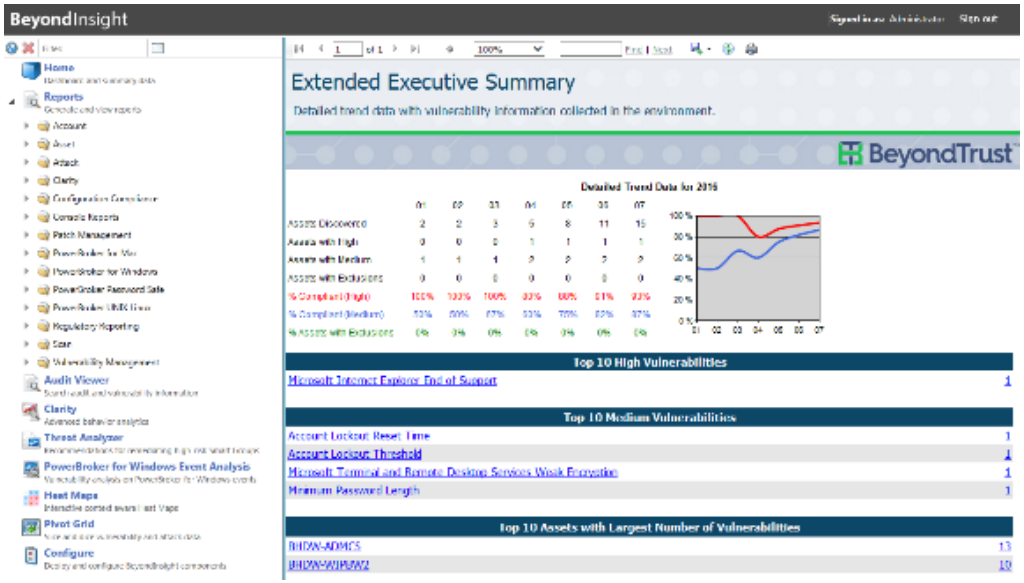


PowerBroker(PBWD) 기능 상세

다양한 보고서 제공

BeyondInsight는 사용자 단말을 사용하는 사용자의 수행된 Action에 대하여 Audit 가능하며 이를 PDF,XLS,CSV 및 DOC 등의 다양한 보고서 출력이 가능합니다.

- ✓ 사용자, 날짜, 행위 등 Audit
- ✓ Monitors Actions
  - Actions
    - ☐ Add, Delete, Edit
    - ☐ Schedule
    - ☐ Add Vuln. Exclusion
    - ☐ …
  - Section
    - ☐ Address Groups
    - ☐ Reports
    - ☐ Scan
    - ☐ …

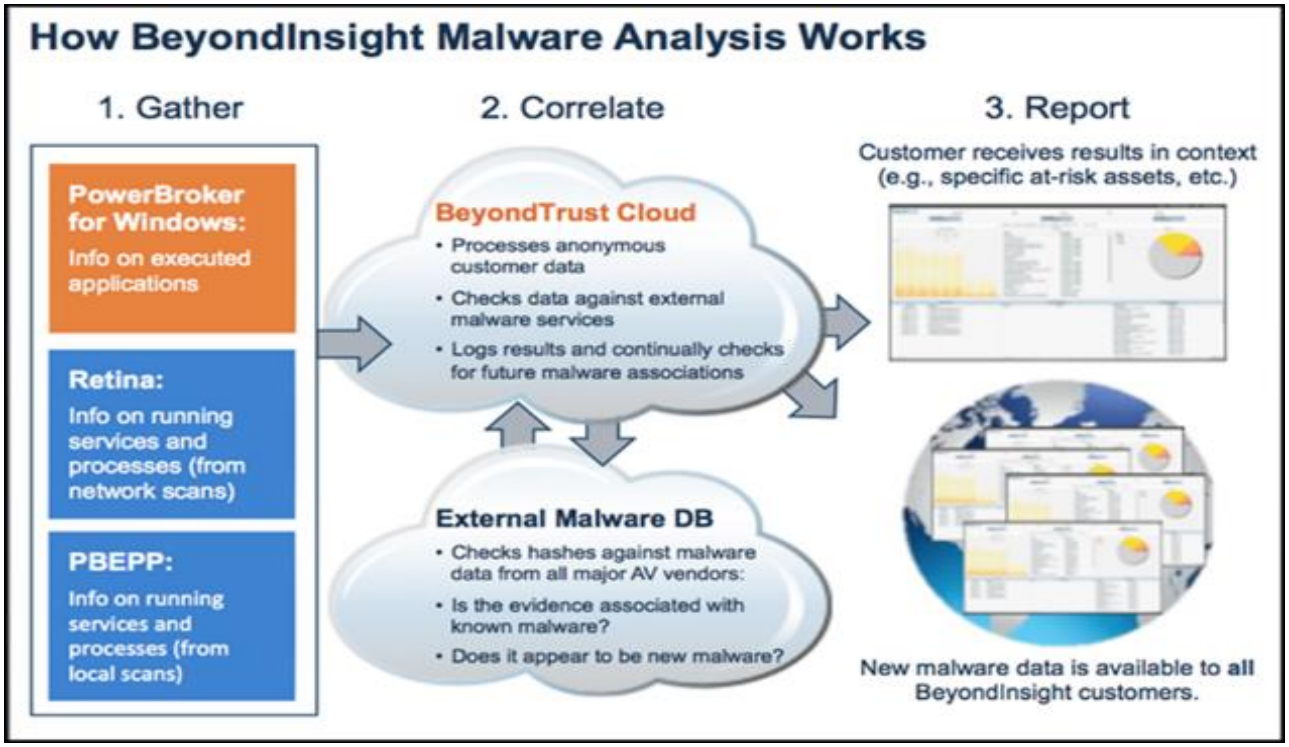


- Application Active X Details
- Applications by Computer
- Applications by Hash Report
- Applications by Path Report
- Dashboard Report
- File Integrity by Asset
- File Integrity by Rule
- Justification Report
- Data Export

- PowerBroker Events by Hour
- PowerBroker Events by Month
- PowerBroker for Windows Rollup Grid
- Privileged Rule Impact Dashboard
- Requested Elevation Impact Dashboard
- UAC Impact Dashboard
- PowerBroker Event Analysis

PowerBroker(PBWD) 기능 상세

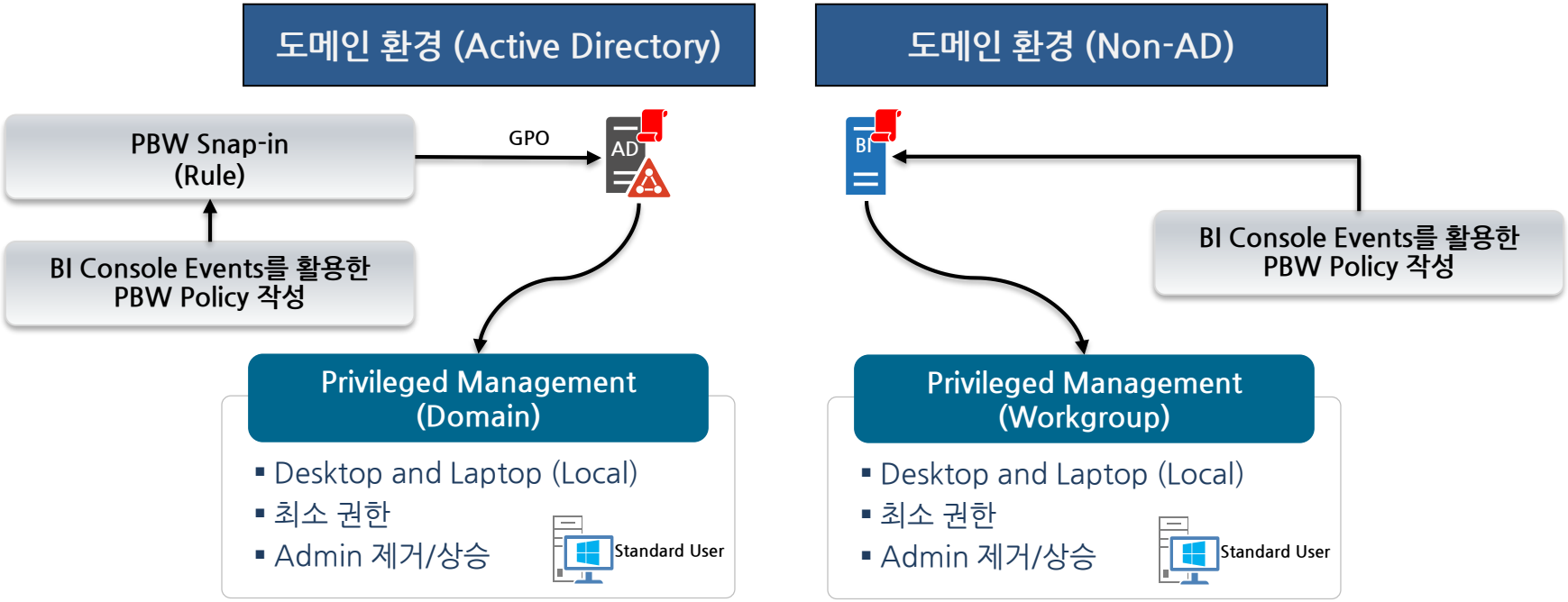
실행 Application Malware 분석



※ 금융 망분리 환경에서는 적용이 불가할 수 있음

1. BeyondTrust Cloud로 전송되는 모든 데이터는 익명성을 보장하고 수집 전송되는 데이터는 실행 서비스나 프로그램의 Hash 정보와 사용자 정보가 유효한지 라이선스 키를 통해 검증하고 전송 데이터에는 시스템, 고객 정보 등 중요 정보는 전송되지 않습니다.
2. 만약 알려지지 않은 Hash 정보의 경우 BeyondTrust Cloud 서비스로 해당 Hash 정보 분석을 위해 제공합니다.
3. 제공된 Hash 데이터가 Malware와 관련된 사항인 경우 해당 정보를 모든 고객들에게 제공됩니다.

PowerBroker(PBWD) 구성 환경



Scanning Asset (BI Console)

- 소프트웨어 사용내역 기록 (어떤 사용자가 어떤 PC에서 어떤 소프트웨어 사용하였나)
- 외부해커나 내부직원 및 협력직원에 의한 Malware 설치 방지
- 내부 직원의 소프트웨어 제거 방지
- 내부 직원의 구성변경 방지
- 내부 직원과 협력 직원에 의한 비인가 소프트웨어 설치방지
- Session Logging (작업내역기록)
- ActiveX 제어

PowerBroker(PBWD) 지원 O/S

PBW 지원 O/S

Windows & Mac Version	지원 O/S
Windows	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 SP1 or later Windows Server 2012 Windows Server 2016 Windows 7 Windows 8 Windows 10 Pro, Enterprise and Enterprise LTSB **※ Windows XP 부터 Windows 2016까지 하나의 Agent에서 지원**
MAC	Apple OS X El Capitan 10.11 Apple OS Sierra Mac OS High Sierra 10.13.x **※ Windows O/S만 지원하는 국내 유사 솔루션과 다르게 Mac O/S 도 지원**

PowerBroker for Windows Client (32 Bit) 7.6.msi	2018-08-22 오후 4	Windows Installer...
PowerBroker for Windows Client (64 Bit) 7.6.msi	2018-08-22 오후 4	Windows Installer...
PowerBroker Policy Editor (64 Bit) 7.6.msi	2018-08-22 오후 4	Windows Installer...

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

III PowerBroker 평가 및 레퍼런스

세계 최대 은행 8/10이 사용하는 PowerBroker

PowerBroker

Privileged Access Management Platform

세종정보보안 BizHub

PowerBroker에 대한 평가

- 모든 제품군을 구비한 대표적 벤더(“… ‘Representative vendor’ for all five key feature Solution categories”)
- PAM 분야의 통합 제품 제공(“…Integrated, one-stop approach to PAM…”)
- 많은 고객 보유(“…Pure-player in the…market; significant position in the market”)
- Frost & Sullivan의 “PowerBroker Password Safe“ 에 대한 찬사
- PBW - 어드민 유저를 쉽게 제거 솔루션("Leverage a Solution like BeyondTrust’s PowerBroker for Windows to transparently remove Administrator privileges“)
- PAM 분야 메이저벤더 : Major Player’ in Privileged Access Management”
- 권장할수 있는 벤더(“BeyondTrust is a vendor you can rely on… impressive set of flexible and tightly integrated auditing tools”)
- 윈도우 뿐만 아닌 유닉스/리눅스/맥 OS에도 적용 가능한 제품

PowerBroker Reference - 국외

세계 최대 은행 8/10이 사용하며, 미국 내 최대 은행 7/10이 사용

Energy

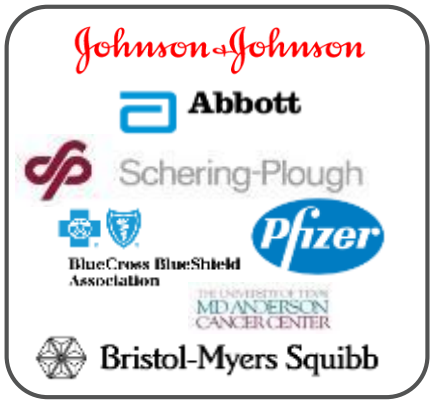
Financial Services

Government

Manufacturing & Technology

Media / Telecom

Health Care & Pharmaceuticals



- 세계 최대 은행 8/10이 사용하며, 미국 내 최대 은행 7/10이 사용 중
- 세계 최대 항공우주산업 및 방위산업 회사 중 7/10이 사용 중
- 미국 내 최대 제약사 7/10이 사용 중
- 다우존스 등록된 회사의 절반 이상이 사용 중

PowerBroker Reference - 국내

KB국민은행, 삼성생명 등 대형 금융기관에서 사용

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

IV PowerBroker 경쟁 기술 비교

최소 권한 and Application Control
for Windows Servers and Desktops

PowerBroker
Privileged Access Management Platform

세종정보보안 BizHub

PowerBroker vs AD (Active Directory)

주요 기능	PBWD	Active Directory
일반 사용자 권한에서 어드민 권한 상승 - 인증된 소프트웨어에 대한 설치, 업데이트, 변경 - 프로그램, 웹사이트 - 사용자, 그룹 등 다양한 그룹핑 기능 제공	지원	Windows 제공하는 UAC(권리자 패스워드 입력),ACT(프로그램 호환성 툴킷),ACL(보안 권한 변경) 형태로 적용할 수 있으나 실 적용하기 어려움
	On-the-fly 방식의 특허 받은 Elevation 기법	- AD의 Group에 의한 Elevation - runas 기법의 Elevation - 많은 문제점 발생 - OU 단위의 적용(OU내의 특정 유저들의 조합을 위하여 끈임 없는 OU생성 필요)
Whitelisting	지원	Applocker로 지원 • 윈도우 기본 기능인 Applocker 이용 • No Central Management Interface • 로그가 로컬에 저장됨 (중앙집중화는 파워셀을 사용해야함) • Admin 유저에서 Application Identity Service Disable 가능 • LOCAL 컴퓨터의 어드민이 Local GPO내의 Applocker Policy 변경가능 • Shell Script 같은 Interpret Code처리 불가 • APPLOCKER 통과하는 많은 방법이 이미 시중에 존재
세션 모니터링 - 정책별 모니터링 작업 수행	지원	-
ActiveX Control - 승인된 웹사이트에 대한 설치 실행 권한 제공	지원	-
자산 정보 수집 - Hardware, Ports, Users, Software, Processes, Services 등	지원	일부 지원
Malware 정보 분석	지원	-
Vulnerability 정보 분석	지원	-
사용자 단말의 프로그램 사용 현황 정보	지원	-
특정 파일 또는 디렉토리에 대한 변경 관리	지원	-
사용자 단말의 다양한 로그 정보에 대한 분석 리포트 제공	지원	-

PowerBroker vs AD (Active Directory)

주요 기능	PBWD	Active Directory
Elevation 관련 보고서	풍부	미약
Windows Version에 따른 변화	거의없음	Win7 -> Win10 시 권한상승 프로그램 재 개편 가능성

PowerBroker vs 아이큐패드

기능	PBW (PowerBroker for Windows)	I 사	비 고
Agent	**단일 Agent (win7/Win10/Win2012/Win2016)**	OS에 따른 에이전트의 변화 및 윈도우 서버 버전 없음	OS Upgrade시 난이도 발생 가능성
적용 환경	**도메인 환경, 워크그룹 환경**	도메인 환경,워크그룹환경	I사는 워크그룹환경에 레퍼런스 소규모 1군데뿐이 없음
멀티 OS 지원	**Win7,Win10,Win2012,Win2106,Mac OSX, Linux, UNIX**	Win7, Win10	PBW는 Win7에서 Win10으로 Upgrade시 Migration Tool 제공
제공 정책	Hash / Publisher / Path MSI / ActiveX / Shell File Integrity (중요 폴더 접근 제한)	Hash/Publisher/Path 방식	타사는 정책 룰이 많지 않아서 룰 작업 시 권한상승이 안되는 경우 발생 (특히 Web의 Drag & Drop)
Admin 권한상승	**SECURITY Token 변경 (개발 된지 20년 이상과 글로벌 5,000개 레퍼런스)**	SECURITY Token 변경 (개발이 1년 정도된 것으로 레퍼런스 거의 없음, 신뢰성 문제 발생 가능성)	I사는 2016년 이전의 V1은 유저 변경방식. 2016년부터 Security Token 방식을 만들었다 하며 이전의 V1과는 완전 다른 제품. V2는 국산인지 외산인지 불분명. 국내외 레퍼런스 거의 없을듯.
	GUI/CLI/시스템 작업이 동일 방식	명령어 Elevation 기능이 없음	타 솔루션은 시스템 작업 시 어드민 유저 필요
Admin 권한 제거	**완전한 일반유저 상태**	일부 특권그룹에 속해야함	I 사는 Network Configuration Operators 그룹이라는 특권 그룹 필요
정책 적용 단위	**AD OU 또는 자체 그룹 단위 으로 적용하고 OU간의 동일 속성끼리 상세 적용 대상을 지정 가능**	AD OU 또는 자체 OU 만들어서 OU단위 지속적인 OU를 만들어야함	정책 적용이 유연함
Whitelisting	가능	Whitelisting 기능 없음	타 솔루션은 Portable 프로그램설치 및 랜섬웨어 대응을 못함. 또한 금감원 요구사항을 만족치 못함.
멀웨어 및 랜섬웨어 실행 방지	**All Deny 규칙을 통해 신뢰되지 않은 프로그램에 대한 실행 차단**	미 지원	
자산정보수집	**가능**	미 지원	
파일 변경 검출	**지원**	미지원	
레퍼런스	**전세계 5,000여 개 Reference 국내 생명보험사 레퍼런스 7개**	국내 일부 (시큐리티 토큰 변경 방식은 레퍼런스 거의 없음) 국내 생명보홈사 레퍼런스 흥국생명1군데 500대가 전부	V2는 V1과 다른 제품. V2는 국내에서 프로젝트 종료 기준으로 레퍼런스 없는것으로 판단됨. 또한 국적 불분명

PowerBroker vs 아이큐패드

기능	PBW (PowerBroker for Windows)	ADLockdown(IQPAD)	비 고
관리서버 유저 Interface	모든 Agent OS 버전 동일	OS 버전마다 다름, 자체 소프트웨어 버전마다 다름	
리포팅	풍부 (여러 조합에 따라 많은 리포팅 생성)	Text Based 일부 리포팅	
이벤트 전송	룰 필요시 관련 이벤트 자동 추출	룰 필요시 관련 이벤트를 관리자가 파악해야 함	

PowerBroker vs 소프트넷

	PBW	소프트넷(ADEP+) Ver3	소프트넷(ADEP+) Ver10
제품생산	• 25년 이상	• 2017년 12월 단종	• 2018년 생산으로 안전성 및 레퍼런스 문제
권한상승방식	• 어플리케이션 Token 변경 방식	• Run As 방식	• ?????
개요	• 동일 유저의 Credential을 이용하여 어플리케이션이 필요한 Security Token을 변경하여 Elevation	• Secondary Logon Service를 이용하여 다른 유저의 Credential과 그룹 멤버십을 이용하여 실행	
장단점	• 사용자계정과 실행 계정의 일치 (User Context Switching 일어나지 않음) • 프로파일 불일치 없음	• 사용자 계정과 실행 계정의. • Windows update 할 수 없음. SCCM에 의존. • 네트워크 IP 변경 등을 위하여 Network Configuration Operators라는 그룹에 유저를 넣어서 권한 상승을 시킴. • Credential 이 해킹 될수 있음 (Pass the hash 로부터 안전하지 않아서 마이크로소프트사가 사용을 제한하는 방법)	
Application Control	• 기능 있음 • 포터블프로그램이나 랜섬웨어 대응	• 기능 없음 • 포터블 프로그램이나 랜섬웨어 대응 부재	• 기능 없음 • 포터블 프로그램이나 랜섬웨어 대응 부재
Program Restart	• 필요 없음	• 필요함	• 필요 없음
Agent	단일 Agent (win7/Win10/Win2012/Win2016)	OS에 따른 에이전트의 변화	OS에 따른 에이전트의 변화
적용 환경	도메인 환경, 워크그룹 환경	도메인 환경	도메인 환경, 워크그룹 환경 (워크그룹 레퍼런스 없음)
멀티 OS 지원	Win7,Win10,Win2012,Win2106,Mac OSX, Linux, UNIX	Win7	Win7, Win10 (Migration Path가 있는지 확인 필요)
제공 정책	Hash / Publisher / Path MSI / ActiveX / Shell File Integrity (중요 폴더 접근 제한)	Hash/Publisher/Path 방식	Hash/Publisher/Path 방식

PowerBroker vs 소프트넷

기능	PBW	소프트넷(ADEP+) Ver3	소프트넷(ADEP+) Ver10
Admin 권한상승	SECURITY Token 변경 (개발 된지 20년 이상과 글로벌 5,000개 레퍼런스)	권한상승용 별도 계정 이용 방식(사용자 계정/세션 불일치/룰 적용후 리부팅 필요)	-별도계정 이용방식과 토큰방식의 혼용으로 보임 (???) -프로그램 소스 수정 필요성 많음.
	GUI/CLI/시스템 작업이 동일 방식	명령어 Elevation 기능이 없음	명령어 Elevation 기능이 없음
정책 적용 단위	AD OU 또는 자체 그룹 단위 으로 적용하고 OU간의 동일 속성끼리 상세 적용 대상을 지정 가능	AD OU 또는 자체 OU 만들어서 OU단위 지속적인 OU를 만들어야함	AD OU 또는 자체 OU 만들어서 OU단위 지속적인 OU를 만들어야함
Whitelisting Blacklisting	둘다 가능	둘다 기능 없음	Blacklisting
권한 요청 시 관련 이벤트	자동 Gathering & 전송	기능없음	기능없음
권한 신청 절차	자동	반자동	반자동
멀웨어 및 랜섬웨어 실행 방지	All Deny 규칙을 통해 신뢰되지 않은 프로그램에 대한 실행 차단	미 지원 Application Control 기능이 없어서 안됨)	미 지원 Application Control 기능이 없어서 안됨)
자산정보수집	가능	미 지원	미 지원
파일 변경 검출	지원	미 지원	미 지원
레퍼런스	전세계 5,000여 개 Reference 국내 생보사 레퍼런스 : 7개 (교보생명/라이나생명/라이나금융서비스/메트라이프생명/처브생명/AIA생명/BNP-Pariba Cardif)	국내 일부 (극히 소수) 국내 생보사 래퍼런스 소프트넷 : 1개 (동부생명)	현대차투자증권이 유일한 레퍼런스 (700대 소규모, 프로젝트 진행 중)
관리서버 유저 Interface	모든 Agent OS 버전 동일	OS 버전마다 다름, 자체 소프트웨어 버전마다 다름	OS 버전마다 다름, 자체 소프트웨어 버전마다 다름
리포팅	풍부 (여러 조합에 따라 많은 리포팅 생성)	Text Based 일부 리포팅	Text Based 일부 리포팅

감사합니다
Thank you

세종정보보안㈜
강 윤 채 / 부대표
T : 010-2047-5543
E : yckang@sejonginfo.co.kr

BizHuB BeyondTrust