
CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

MS플랫폼 하에서의 Connected Security

- PC에서 서버를 넘어 클라우드까지

Hongso Chae | Quest Software Korea

Quest소개

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Quest는 빠르게 변화하는 엔터프라이즈 IT 환경을 위한 소프트웨어 솔루션을 제공합니다.

Quest는 데이터 폭발, 클라우드 확장, 하이브리드 데이터 센터, 보안 위협 및 규정 요구사항으로 인한 문제를 단순화할 수 있도록 지원하며 Fortune 500 대 기업의 95%와 Global 1000 대 기업의 90%를 포함하여 100 개국 130,000여 기업에 글로벌 서비스를 제공하고 있습니다.

고객중심의 비즈니스로 전세계
100개국, 13만 고객사 보유

퀘스트소프트웨어를 판매하는
7,000개의 파트너

베스트 프랙티스를 자체 공유하는
400만 명의 커뮤니티 구성원

포춘 500대 기업 중 95%가
퀘스트 제품 사용자

Microsoft 2018 Winner's Circle Member
Global Managed IP Co-Sell Partner

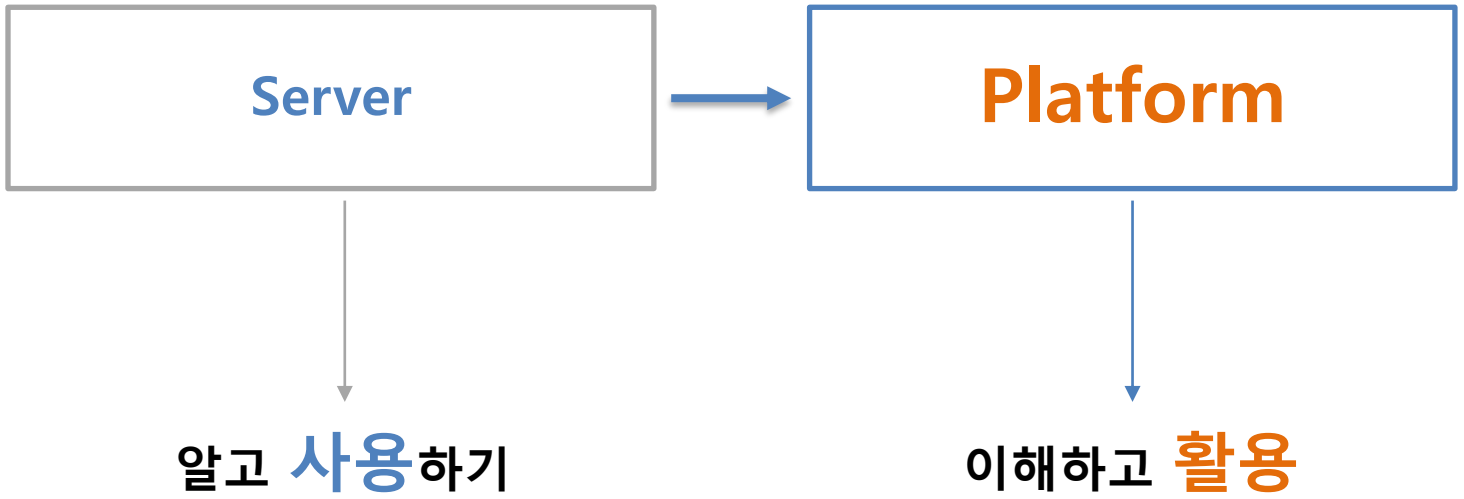
2018 STEVIE GOLD WINNER – AMERICAN BUSINESS AWARDS
2018 STEVIE SILVER WINNER – AMERICAN BUSINESS AWARDS
2018 STEVIE BRONZE WINNER – AMERICAN BUSINESS AWARDS
Microsoft Partner of the Year 2016 Finalist – Messaging Award
Info Security Products Guide 2016 GLOBAL EXCELLENCE AWARDS
PEOPLES CHOICE STEVIE AWARDS FOR FAVORITE NEW PRODUCTS 2018 WINNER
Microsoft Content Services Partner Program Charter Member
Microsoft Preferred Content Services
SIIA CODiE AWARDS
V3 TECHNOLOGY AWARDS 2017

퀘스트소프트웨어의 솔루션

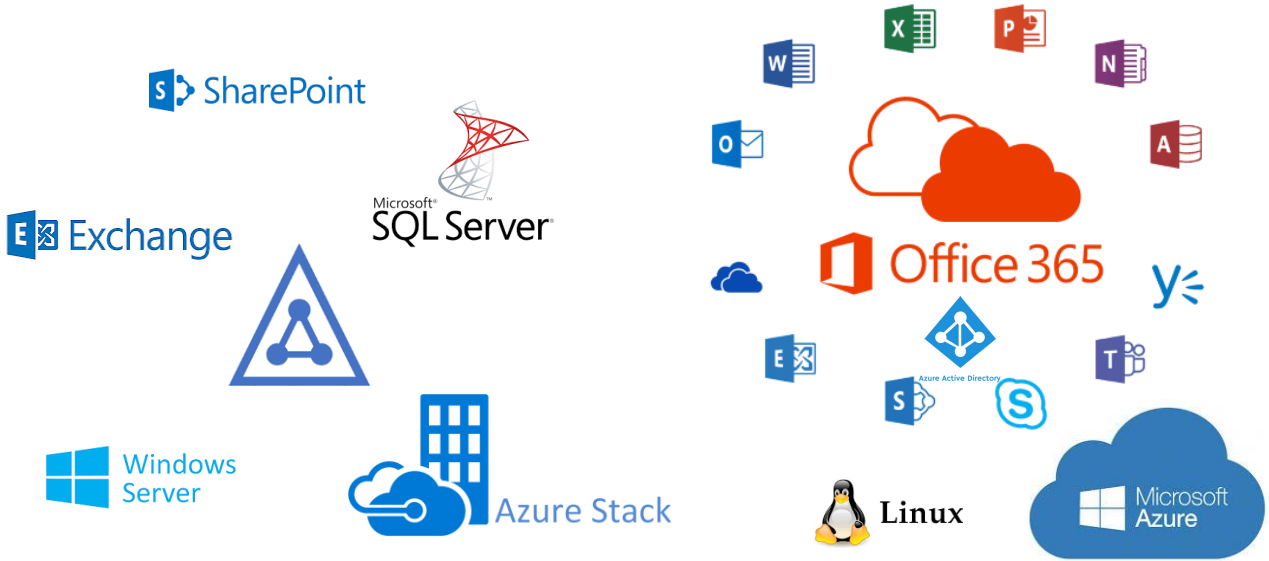
- 데이터베이스 관리
- 데이터보호
- 통합 엔드 포인트 관리
- ID 및 액세스 관리
- Microsoft 플랫폼 관리

#cloudsec

Microsoft Platform?



Microsoft Platform Overview



Quest Connected Security

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Quest Connected Security for Microsoft Platform

접근 전략

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

보안이 고려된 관리

DevOpsSec

데이터 및 행위 중심

보안 관제

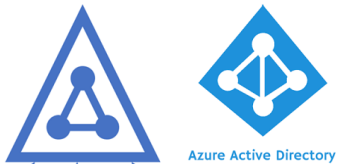
가시성 기반

보안 감사

보안의 주요 대상

인증/정책/권한 정보

운영 체제



Active Directory의 위협(보안)은
운영체제의 위협(보안)

제한 / 신속한 탐지 및 복구

관리 / 통제

데이터 중심

행위 중심

MS Platform 보안의 시작은
인증 / 정책 / 권한 관리

(Azure) Active Directory

Active Directory

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

출처 : https://jumpcloud.com/blog/google-identity-management-active-directory/

Active Directory: The Time to Modernize Is Now

Published: 25 September 2018

ID: G00354886

Analyst(s): Paul Rabinovich

Summary

Organizations must prepare Windows Active Directory for the new era of hybrid, cloud and multicloud IT. This document provides technical professionals with guidance on preparing AD for a world in which an ever-increasing proportion of enterprise IAM functionality will be delivered from the cloud.

출처 : https://www.gartner.com/en/documents/3890763/active-directory-the-time-to-modernize-is-now

주요 보안 대상 – Active Directory

- 계정관리 및 인증
- 정책관리 및 배포
- 권한관리

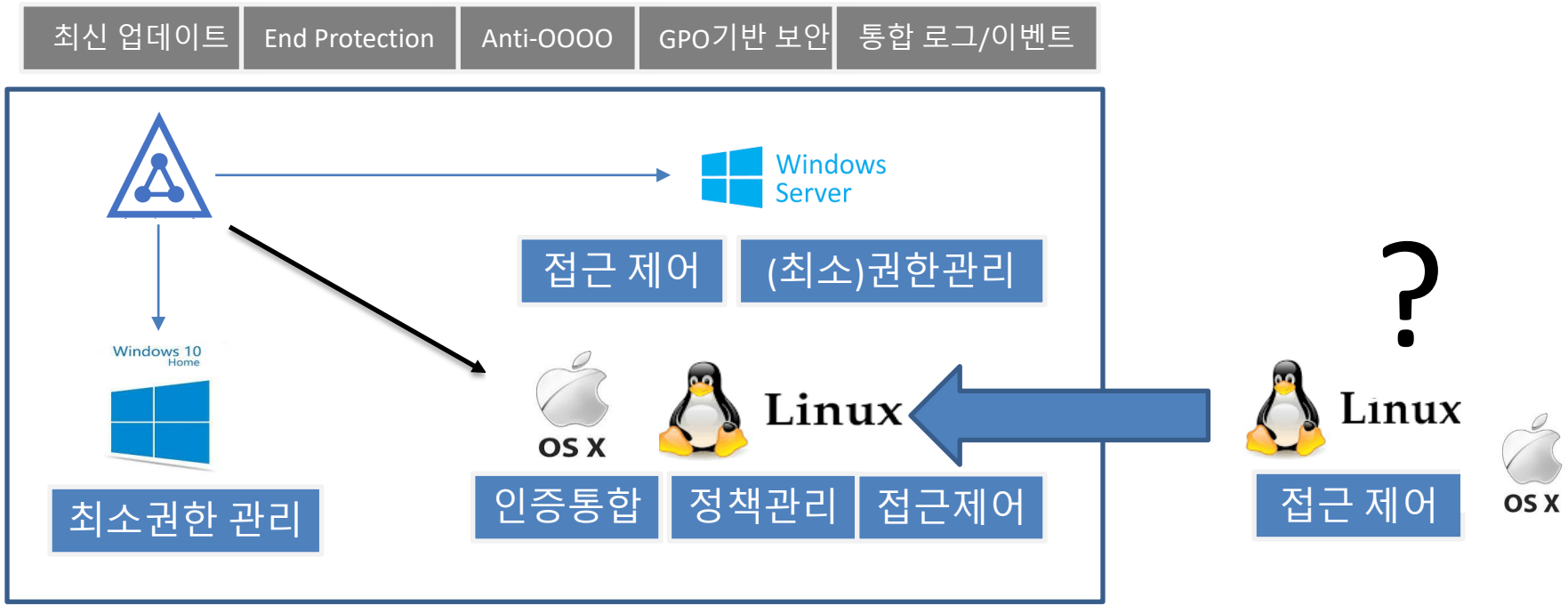
AD특화 접근 제어	최소 및 세분화된 권한 관리	변경 감지 및 관리
▪ 제한된 인원에 권한 할당 ▪ 지정된 지역(PC, IP)에서만 접근 ▪ 지정된 접근 방식(RDP, 전용 어플 등) ▪ 접속방식 및 접속정보의 제어	▪ 담당자별 권한의 세분화된 할당 ▪ 반드시 필요한 권한만을 제공	▪ 계정 정보의 변경 ▪ 정책의 변경 ▪ 특권계정(높은 권한을 가지는 계정)의 변경 ▪ 시스템의 보안 및 주요설정 변경

운영 체제 보안의 핵심은

AD기반 통합 인증 및 정책 과 최소 권한 관리

주요 보안 대상 – 운영체제

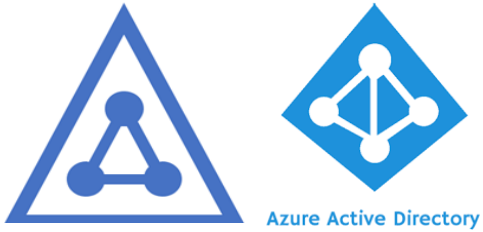
CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.



그렇다면 **Quest**는
Microsoft Platform에 대한
어떤 보안전략을 가지고 있나?

Quest의 보안 전략 for Microsoft platform

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.



Quest 보안 전략 #1. Active Directory서비스를 Secure Zone으로 관리

- 완벽한 접근통제를 통한 **극히 제한되고 승인된 경로나 방식으로만 접근**
- 시스템기반 패스워드 관리를 통한 **패스워드 유출 원천 차단**
- 모든 변경에 대한 실시간 감시를 통한 **데이터 기반 보안 위협행위 실시간 탐지**
- 완벽한 복구 체계 구성을 통한 **신속 복구를 통한 피해 최소화**

Quest의 보안 전략 for Microsoft platform

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Windows Server

Quest 보안 전략 #2. AD기반 Windows서버 접근 관리 및 보안 가시성 확보

- 완벽한 접근통제를 통한 **승인된 경로나 방식으로만 접근**
- 시스템기반 패스워드 관리를 통한 **패스워드 유출 원천 차단**
- 할당된 권한정보(폴더, 디렉토리, 파일, 로컬계정)에 대한 **가시성 확보**
- Active Directory기반의 **통합 인증 및 중앙 보안정책관리**
- 로그인 데이터 분석을 통한 **이상 접속 차단**
- 이벤트 통합을 통한 **실시간 감지 및 분석 체계**

Quest의 보안 전략 for Microsoft platform

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Quest 보안 전략 #3. AD기반 사용자 PC의 최소권한 관리

- 일반 계정 사용으로 **보안위협 최소화**
- Active Directory기반의 **통합 인증 및 중앙 보안정책관리**

Quest 보안 전략 #4. MAC/Linux도 AD 관리영역으로 편입

- Active Directory기반의 **통합 인증 및 중앙 보안정책관리**

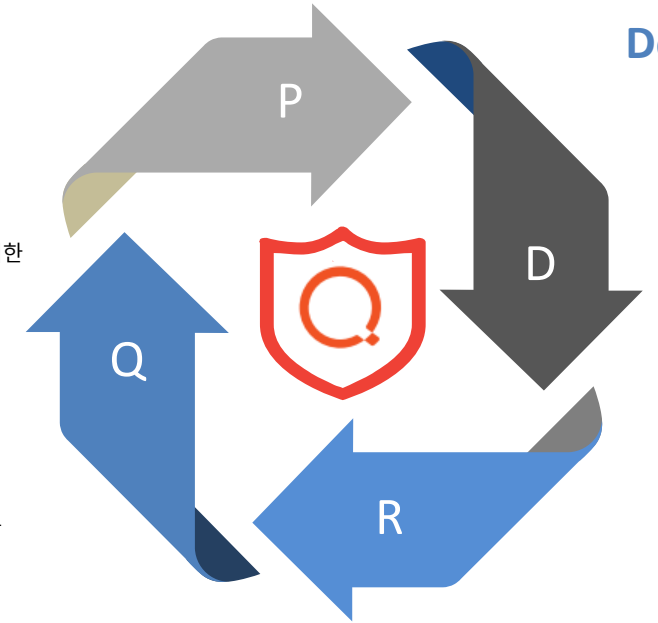
Quest Connected Security

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Quest Connected Security
for Microsoft Platform

Protect : 사전 예방

- 접근 통제 및 패스워드 관리
- 주요 데이터 보호
- 관리자 권한 제거 및 보안 GPO
- AD연계를 통한 통합인증/정책관리
- 가시성을 확보하고 보안 위협 요건들에 대한 지속적인 검증



Detect : 신속한 이상 감지

- 위협 및 이상행위 실시간 알람
- 이상 접속 실시간 알람
- 실시간 윈도우 이벤트 통합 및 PowerShell 실시간 이상 감지

Qualify : MS IP Co-Sell

- MS Platform환경에 검증된 솔루션
- 새로운 환경에 안정적인 솔루션 제공 가능

Recovery : 신속 복구 & 분석

- AD 특화 데이터/시스템/서비스 백업/복구
- 이벤트 및 로그 통합을 통한 원인분석

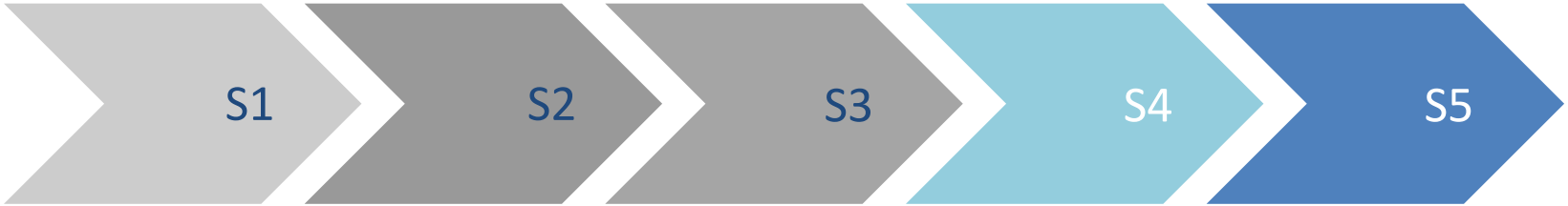
#cloudsec

단계별 적용 방안

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

S2: AD를 Secure Zone으로 구성
AD에 대한 위협에 대한 사전
대응 및 탐지 체계 구성

S4: 실시간 탐지, 대응 및 감사 체계 구축
실시간 이상 및 위협 탐지와 이에 대한 대응 체계 구축/
지속적인 위협 제거를 위한 감사 체계 구축



S1: AD기반 플랫폼 구성
모든 윈도우 환경을 AD로 Join하여
AD기반 통합인증 체계구축

S3: GPO 정책 적용 및 PC관리자권한 제거
GPO를 통한 Join된 Windows
환경에 대한 보안 정책 관리 및
단말에 대한 보안 강화

S5: Mac / Linux를AD로 통합
기존 Windows환경의 보안
영역으로 Mac과 Linux도 편입

단계별 Quest 보안전략 #1

Protect

Quest 보안전략 #1. Protect

CLOUDSEC2019 PICTURE THIS! SEE. SECURE. GO FURTHER.

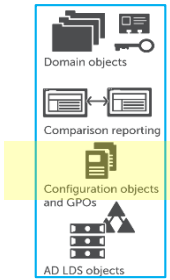
- **AD를 Secure하게**

#.1 접근 제어

- 접근가능 계정(담당자) 지정
- 접근 가능 방식(PC, IP, 프로토콜) 지정
- 접속자 검증(2FA)

#2. 최소 권한 관리

- 개별 계정 할당
- 계정마다 권한을 세분화 하여 할당
- White List형태로 필요한 권한만 할당



#3. 접근정보(패스워드)의 안전한 관리

- 자동화된 패스워드 관리
- 승인을 통한 자동 접속

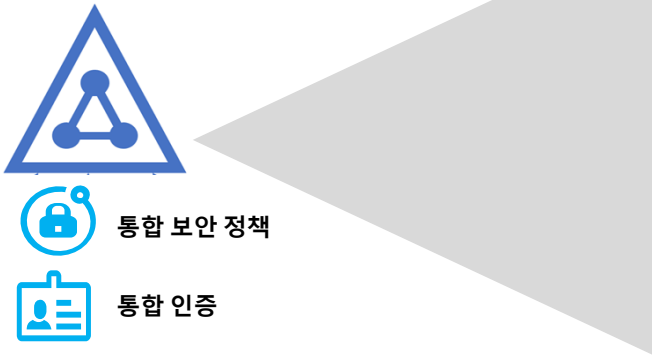
#4. 중요 데이터에 대한 Protection(변경금지)

- 중요한 데이터에 변경 금지

Quest 보안전략 #1. Protect

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- **AD를 통해 Secure하게**



Windows 10 Home

#1. GPO기반 보안 및 최소권한(관리자 권한 삭제)

- GPO기반의 통합 정책관리를 통한 보안
- 일반 계정(관리자 권한 제거)을 통한 위협 최소화
- 제한된 권한 할당을 통한 위협가능성 최소화

Linux

OS X

#2. Linux, Unix, Mac을 AD 관리 및 보안 영역으로 연결

- 통합 인증
- 통합 정책 관리
- Sudo관리(Linux)

Quest 보안전략 #1. Protect

지속적 보안 위협 제거를 위해서는 아래 2가지 요소가 필요

자동화

- 필요한 데이터를 자동으로 수집
- 특정 조건의 데이터를 자동 리포트화
- 리포트의 자동 발송

가시성

- 사용자가 원하는 데이터를 손쉽게 조회
- 보안 위협 단위로 리포트 정의

Quest 보안전략 #1. Protect

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- **AD 및 Windows에 대한 Visibility**

#.1 AD에 대한 가시성

- 보안 위협이 될 수 있는 사항들에 대한 리포트
- BI 형태의 사용자 데이터 조회
- 정기적인 리포트 전달

#3. 주요한 보안관련 변경에 대한 지속적인 리포팅

- 주요 정책(GPO)변경
- 높은 권한 획득 사용자
- OU단위의 권한 변경 등

#2. 윈도우 서버에 대한 권한 가시성

- 윈도우 로컬 계정에 대한 통합 관리
- 모든 폴더 및 시스템 내에 할당된 권한 정보 통합 조회

단계별 Quest 보안전략 #2

Detect

Quest 보안전략 #2. Detect

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

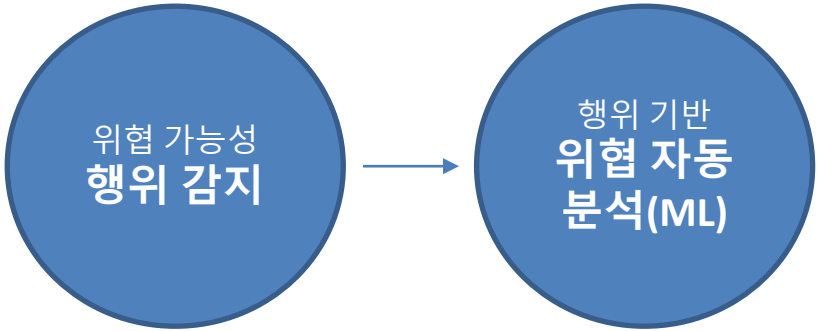
- 위협의 형태

허용되지 않는 행위

충분한
데이터

다양한
사용자 정의 Rule

예측하지 못하는 위협



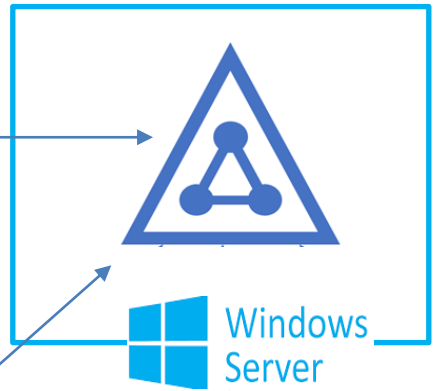
Quest 보안전략 #2. Detect

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

- **주요 감지 형태**

#1. 모든 변경 내역에 대한 실시간 감시 및 위협도 분석

- AD에서 발생하는 모든 변경에 대한 감시
- 변경 요건에 따른 위험도 분석
- 허용되지 않거나 위험한 행위에 대한 감시



#03. 모든 이벤트에 대한 통합을 통한 실시간 감시

- 윈도우 이벤트에 대한 실시간 수집 및 감시
- PowerShell과 같은 작업에 대한 위험 명령어 실행 감시

#2. 주요한 변경사항에 대한 실시간 감시

- 위험도 높은 파일이 생성
- 이상 로그인 시도
- 주요 Registry 생성 / 변경

단계별 Quest 보안전략 #3

Recovery

Quest 보안전략 #3. Recovery

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

데이터

온라인 기반의 즉시 및 개별 복구

서비스

통합화면을 통해서 한번의 클릭으로
손쉽고 빠르게 복구

시스템

통합된 복구를 손쉽고 빠르게 수행

“Active Directory와 같은 특화된 서비스는 특화된 복구 체계가 필요”

Quest 보안전략 #3. Recovery

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Active Directory의 복구의 핵심은 **속도**(서비스 무중단), **데이터의 무손실**(정합성)

서비스 중단 없는
신속한 복구

- 개별 객체단위 복구
- 온라인에서 서비스 중단없이 복구
- 클릭만으로 즉시 복구

최신 데이터로 의
정확한 복구

- 항상 최신의 데이터를 자동 백업
- 자동 백업된 데이터를 통한 데이터 손실없이 복구
- 데이터 정확성을 통한 보안 이슈 해결

Quest 보안전략 #3. Recovery

CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

"데이터 손실 및 불일치로 인한 보안의 위협을 원천적으로 제거 "

데이터 복구

온라인 에서 원하는 데이터만 즉시 복구

서비스 복구

서비스에 대한 손쉽게 빠른 복구 + **데이터 복구**

시스템 복구(재해복구)

시스템에 대한 손쉽게 빠른 복구 + **서비스 복구 + 데이터 복구**

Quest Solutions

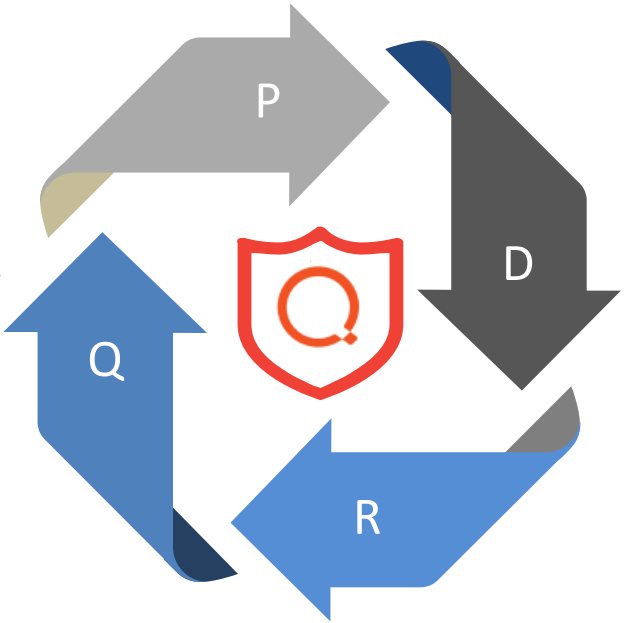
CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.

Quest Connected Security

for Microsoft Platform

Protect : 사전 예방

- 승인 기반 패스워드 및 접근통제 통합관리 : Safeguard
- 윈도우 권한상승 : PMW
- MAC/Linux/Unix AD통합 및 최소권한관리 : PAS
- GPO전문 관리 : GPOAdmin
- 마이크로소프트 플랫폼 BI : Enterprise Reporter
- 윈도우 권한정보 통합검색 : Security Explorer



Detect : 데이터 기반 신속한 이상 감지

- 실시간 이상탐지 및 감사 : Change Auditor
- 실시간 윈도우 이벤트 통합 관제 : InTrust, syslog-ng
- 실시간 모니터링 : Foglight
- 머신러닝 기반 이상탐지 : Threat Detection

Qualify : MS IP Co-Sell

- MS Platform환경에 검증된 솔루션
- 새로운 환경에 안정적인 솔루션 제공 가능

Recovery : 서비스 신속 복구

- 서비스 특화 복구 : Recovery Manager for AD/Exchange


CLOUDSEC2019
PICTURE THIS!
SEE. SECURE. GO FURTHER.
THANK YOU
Hongso Chae | Quest Software Korea
www.cloudsec.com | #cloudsec