금융사 단말 보안위협 대응 전략

- Active Directory 침해 탐지를 통한 랜섬웨어 대응 -

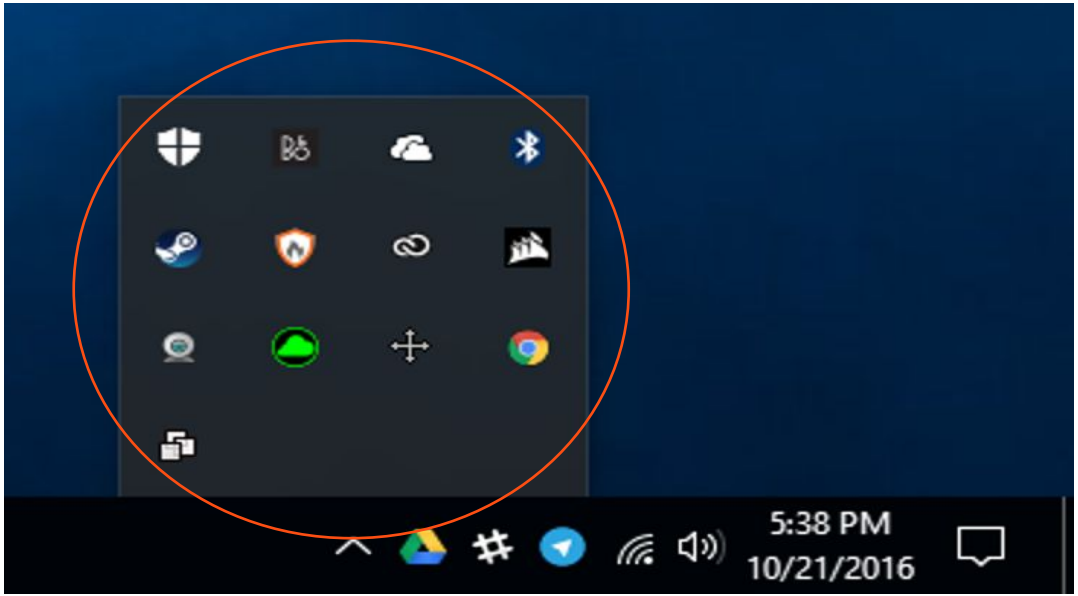
Solution Consultant

Hongso Chae(hongso.chae@quest.com)

Quest

Where Next Meets Now.

단말에 설치된 트레이 아이콘 = 단말 보안 ?



변화들…

새로운 단말환경

Windows 10

- 호환성
- 보안강화
- 보안 서비스

재택근무

망 분리 예외 허용

보안 위협의 증대

랜섬웨어

증가하고 있는 보안 사고들…

[재택근무에 따른 주요 보안 위협 (출처 : 美 NIST) **]**

구 분	주요 보안 위협
외부 단말기의 물리적 통제 미흡	- 재택근무에 사용되는 외부 단말기의 분실·도난이나 타인의 정보 훔쳐보기 시 단말기 內 데이터가 유·노출 - 외부 단말기를 통한 허가되지 않은 내부 네트워크 접근
안전하지 않은 네트워크 사용	- 공용 유무선 네트워크를 통해 내부망 접속 시 도청, 중간자 공격(MITM) 등으로 중요정보가 유출
악성코드 감염에 따른 네트워크 침해	- 악성코드에 감염된 외부 단말기로 내부 네트워크 연결 시 시스템 침해 가능
내부 자원의 원격접근 위협	- 내부에서만 접근 가능했던 내부 자원에 외부 단말기도 접근 가능해짐에 따라 비인가 접근 등 보안위협

<별표 7> 망분리 대체 정보보호통제

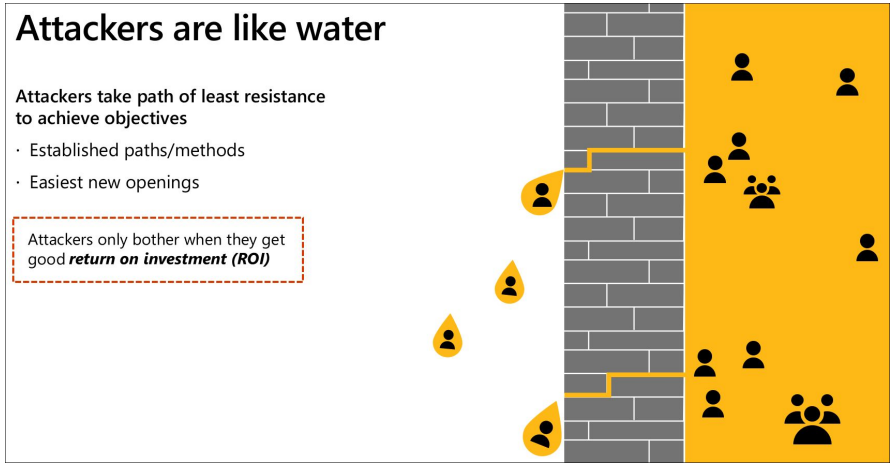
구분	통제 사항		
공통	○ 외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 감염여부 진단·치료 ○ 지능형 해킹(APT)차단 대책 수립·적용 ○ 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링		
메일 시스템	○ 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립·적용 ○ 메일을 통한 정보유출 탐지·차단·사후 모니터링 대책 수립·적용		
업무용 단말기	○ 사용자의 관리자 권한 제거 ○ 승인된 프로그램만 설치·실행토록 대책 수립·적용 ○ 전산자료 저장 시 암호화		
원격 접속	외부 단말기	공통	○ 백신 프로그램 설치, 실시간 업데이트 및 검사 수행 ○ 안전한 운영체제 사용 및 최신 보안패치 적용 ○ 로그인 비밀번호 및 화면 보호기 설정 ○ 화면 및 출력물 등으로 으로 인한 정보유출 방지대책 적용
		업무용 단말기를 점유하여 내부망에 접속하는 경우 (간접접속)	○ 외부 단말기와 업무용 단말기의 파일 송·수신 차단
		외부 단말기에서 내부망에 직접 접속하는 경우 (직접접속)	○ 인가되지 않은 S/W 설치 차단 ○ 보안 설정 임의 변경 차단 ○ USB 등 외부 저장장치 읽기/쓰기 차단 ○ 전산자료 (파일, 문서) 암호화 저장 ○ 단말기 분실 시 정보 유출 방지 대책적용 (하드디스크 암호화, CMOS비밀번호 적용 등)
	내부망 접근통제	○ 업무상 필수적인 IP, Port에 한하여 연결 허용 ○ 원격접속 기록 및 저장(예: 접속자 ID, 접속일자, 접속 시스템 등)	
	인증	○ 이중 인증 적용(예: ID/PW + OTP) ○ 일정 횟수(예 : 5회) 이상 인증 실패 시 접속 차단	
	통신 회선	○ 안전한 알고리즘으로 네트워크 구간 암호화 ○ 내부망 접속시 인터넷 연결 차단 (단, 직접 내부망으로 접속하는 원격 접속 단말기는 인터넷 연결 상시 차단) ○ 원격 접속 후 일정 유휴시간 경과 시 네트워크 연결 차단	
	기타	○ 원격접속자에 대한 보안서약서 징구 ○ 공공장소에서 원격 접속 금지	

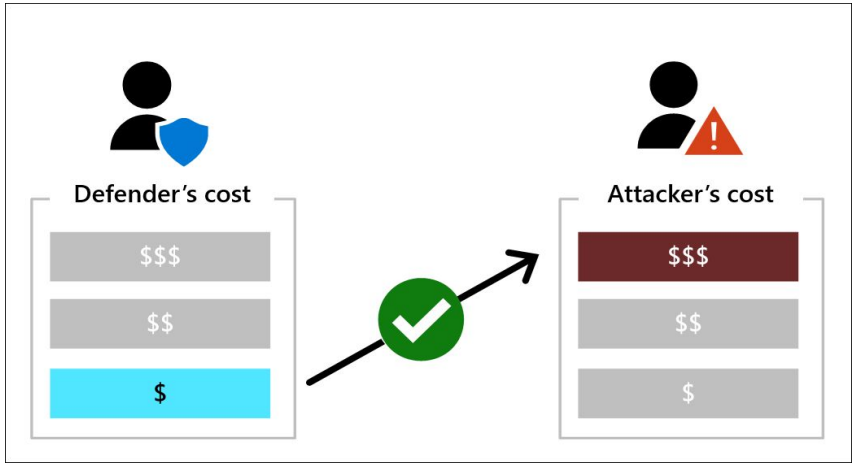
원자력연구원의 해킹 통로 전락한 VPN, 공공기관 취약점 점검 나섰다

출처 : 보안뉴스

단말 보안의 기본 정책

단말 보안 전략 기반





출처 :
마이크로소프트

단말 보안 적용 기본원칙

4가지를 기준으로 하여 진행

Window10 보안의 핵심

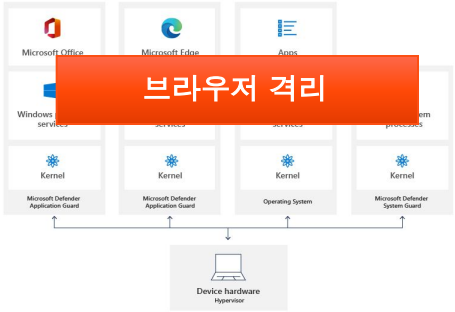
Quest

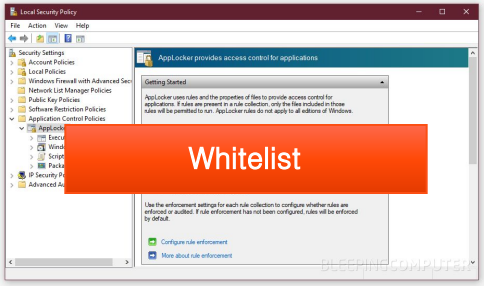
Where Next Meets Now.

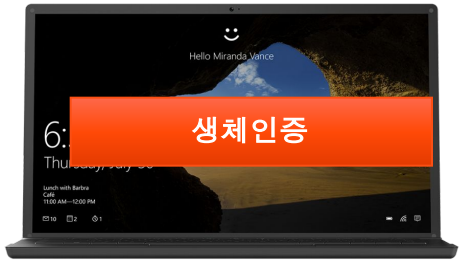
새로운 보안 서비스

	Windows 7	Windows 10
IDENTITY PROTECTION	Today's multi-factor solutions are often cumbersome and costly to deploy.	**Microsoft Passport** is an easy-to-use and easy-to-deploy, multi-factor, password alternative.
	Phishing attacks on your users' passwords are increasingly successful.	**Windows Hello** uses biometrics to provide a more secure way of accessing your device, Microsoft Passport, apps, data, and online resources.*
	Pass the Hash attacks enable attackers to steal identities, traverse across networks, and evade detection.	**Microsoft Azure Active Directory** provides a comprehensive identity and access management solution for the cloud.
DATA PROTECTION	BitLocker offers optionally configurable disk encryption.	**BitLocker** is much improved, is highly manageable, and can be automatically provisioned on most new devices.
	Data loss prevention (DLP) requires the use of additional software and frequently third-party capability.	**Enterprise Data Protection** addresses the needs for DLP, includes a deeply integrated data separation and containerisation solution, and provides encryption at the file level.
	DLP solutions often compromise the user experience in the interest of security, resulting in low adoption and varying experience between the desktop and mobile devices.	**Enterprise Data Protection** provides a seamless user experience across mobile devices and the desktop, and is integrated with Azure Active Directory and Rights Management Services.
THREAT RESISTANCE	All apps are trusted until they're determined to be a threat or are explicitly blocked.	**Device Guard** offers protection on the desktop that is similar to lockdown on a mobile platform (full app lockdown).
	With more than 300,000 new threats per day, blocking them through detection (block on known bad) is a losing battle.	With **Device Guard,** an application must prove itself to be trustworthy before it can be run.
	Windows provides a series of defense solutions, but too many malware threats impact users before detection-based antivirus solutions can catch up.	**Device Guard** will be the most disruptive malware-resistance capability Microsoft has ever shipped in the desktop.
DEVICE SECURITY	Platform security is based entirely on what software can do on its own, and once infected there is no assurance that system defenses can perform their function and remain tamper free.	**Hardware-based security** and the level of trust it offers helps to maintain and validate hardware and system integrity.
	Malware can hide within the hardware or in the operating system itself, and there is no way to validate integrity once it has been compromised.	**UEFI Secure Boot** helps prevent malware from embedding itself within hardware or starting before the OS. Trusted Boot helps maintain the integrity of the rest of the OS.

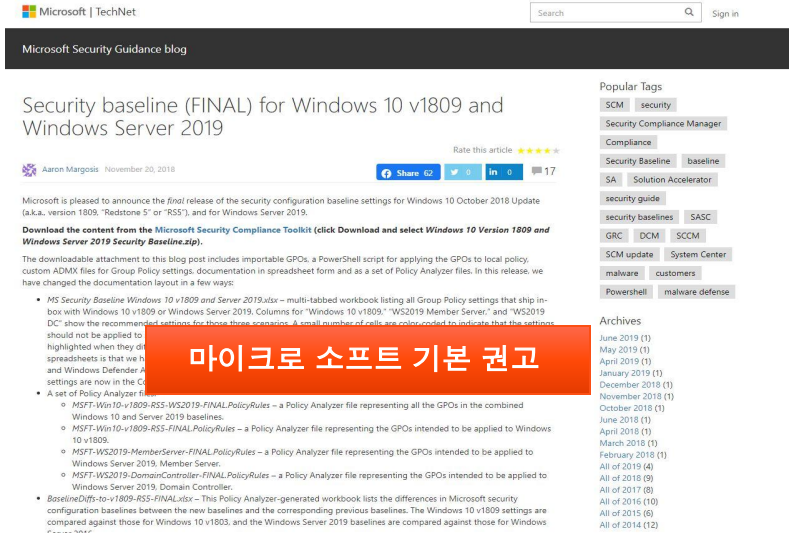
Hardware isolation of **Microsoft Edge** & **Microsoft Office** with **Microsoft Defender Application Guard**





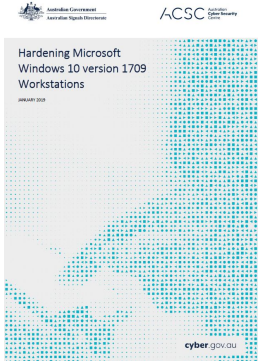


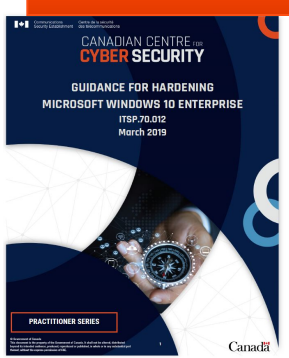
GPO(보안정책)를 통한 OS Hardening

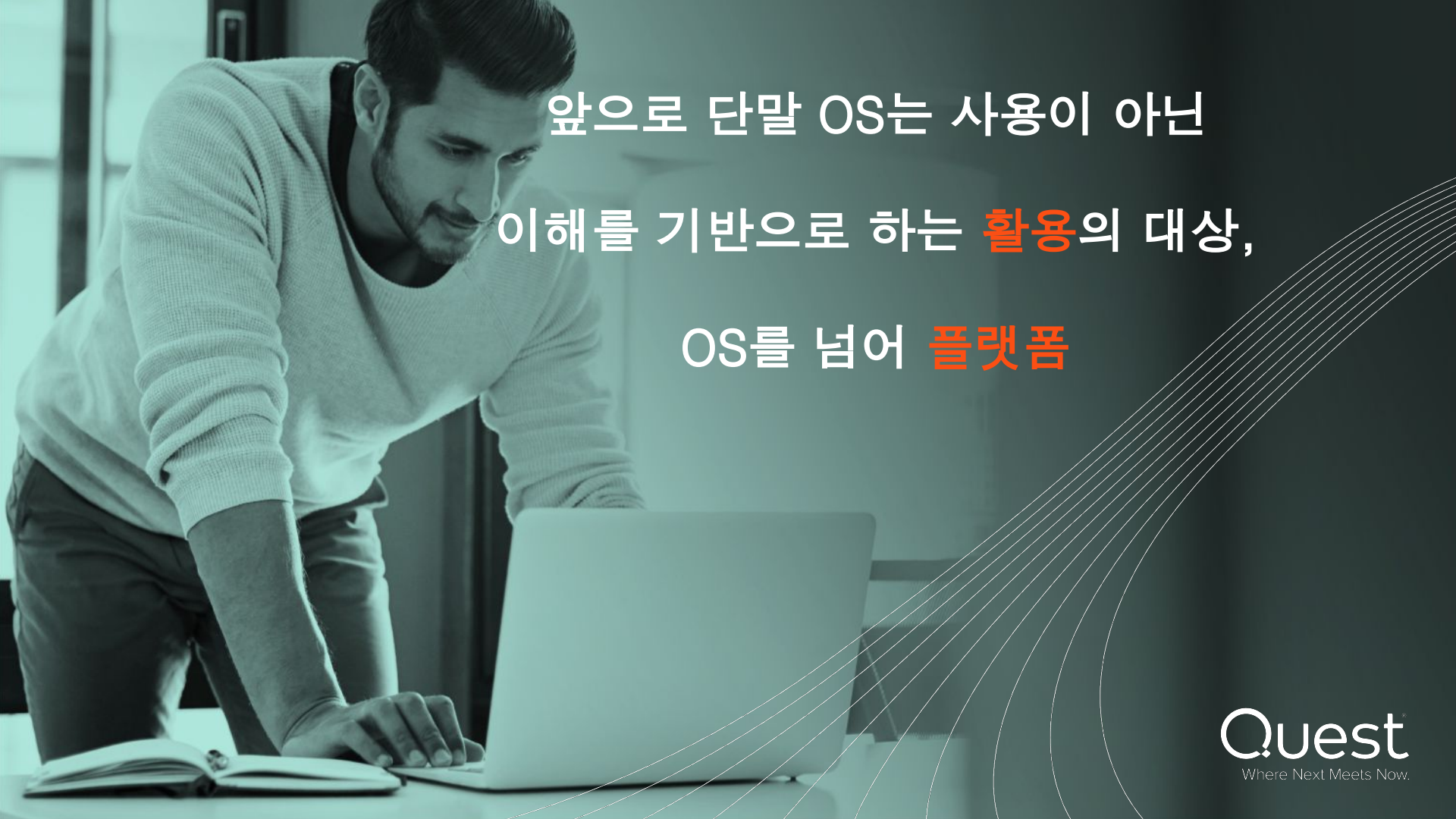


마이크로 소프트 기본 권고

마이크로 소프트 기본 권고
기반의 컴플라이언스

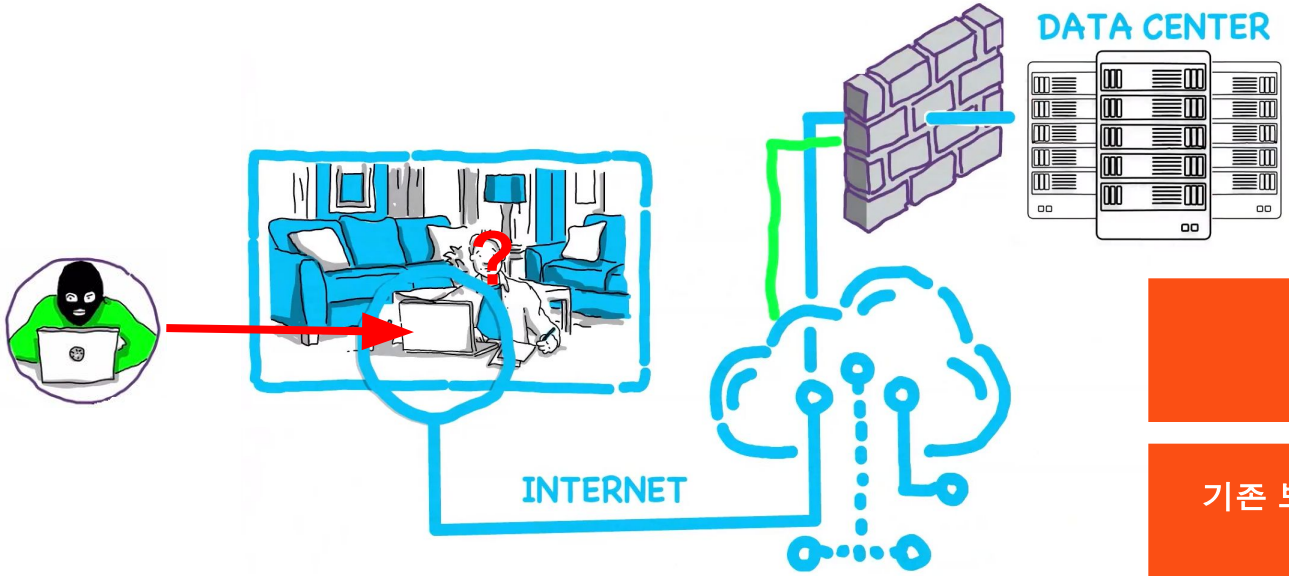





앞으로 단말 OS는 사용이 아닌
이해를 기반으로 하는 활용의 대상,
OS를 넘어 플랫폼
Quest
Where Next Meets Now.

재택근무 환경에 대한 대응

새로운 형태의 보안위협 경로:재택근무

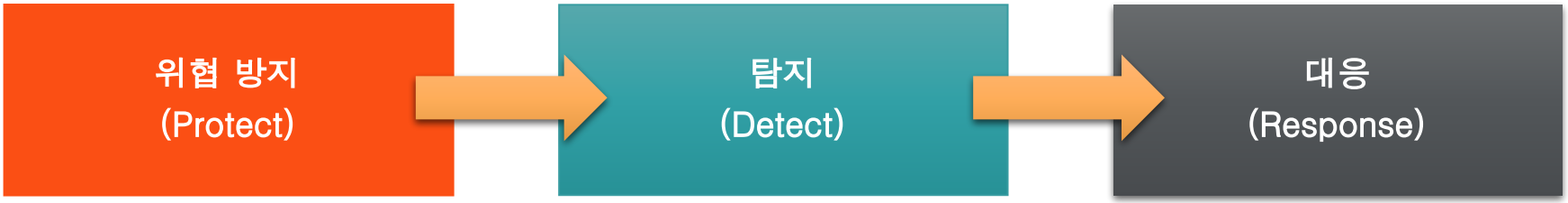


보안위협 가능성 높아짐
(완전한 해결이 어려움)

기존 보안체계로는 대응에 한계가 있음
(주로 인프라레벨 보안)

보호만으로는 한계 > 탐지의 고도화

단계별 주요 적용



위협이 들어오지 못하게 방지

- 알려진 위협 대응 (백신, 패치 등)
- GPO기반 OS Hardening
- AI기반 탐지 (XDR, NDR, EDR 등)
- Infra 보안 (F/W, IPS, IDS 등)
- Isolation , 망분리, 접근통제, 계정관리 등

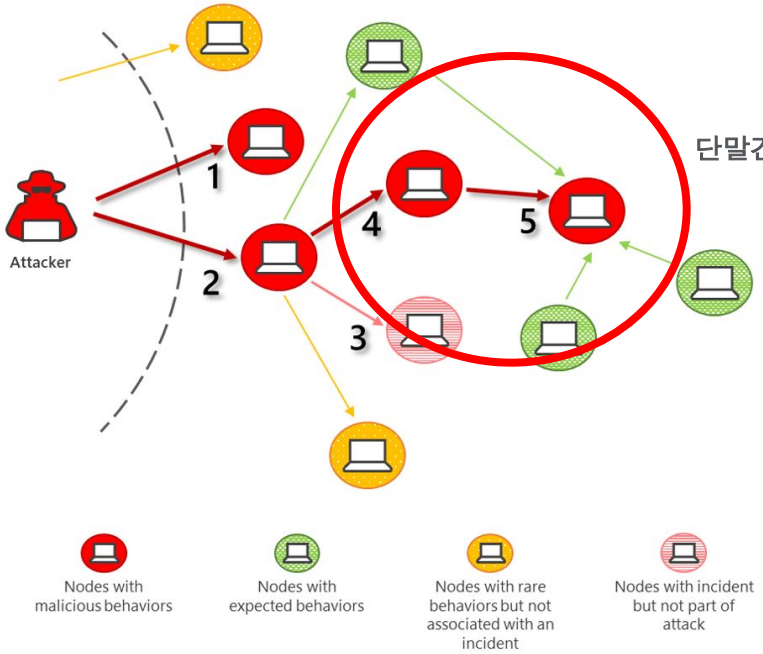
내부전파를 최소화(차단, 탐지)

- 실시간 탐지 (보안관제 등)
- 보안 감사
- 전파를 최소화 (접근통제 등)

위협 이전으로 복구 및 분석

- 백업/복구
- 위협에 대한 분석

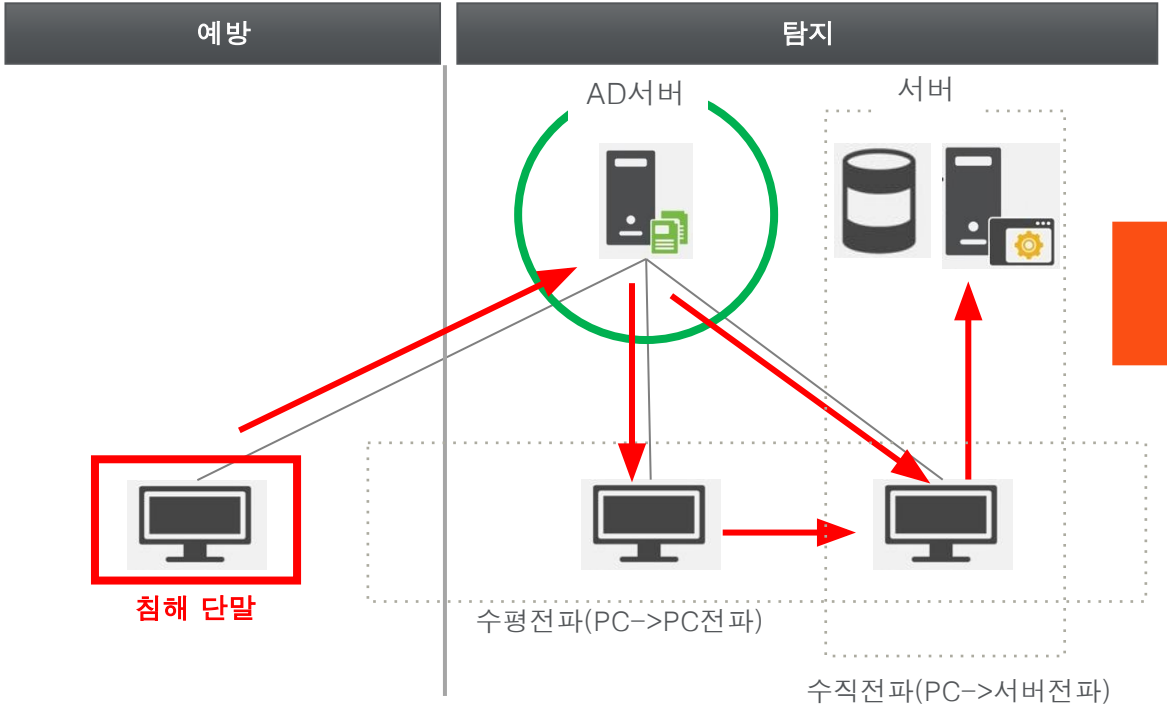
위협의 전파를 탐지하고 대응



단말간 보안위협의 전파를 실시간으로 탐지하고 대응

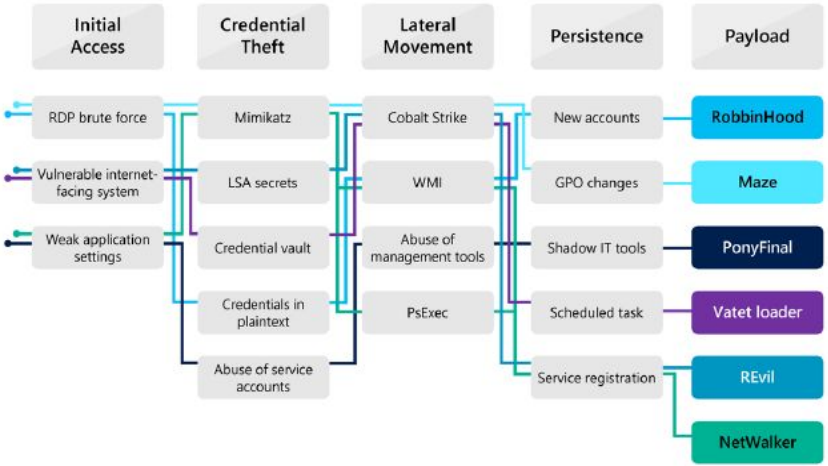
출처 : KISA

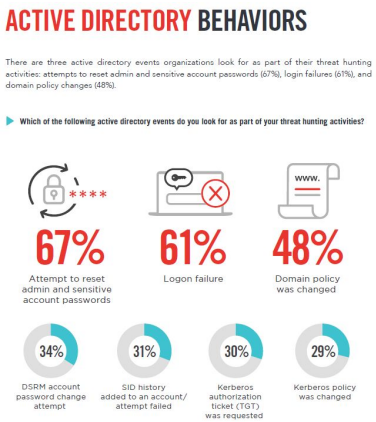
내부 단말간 위협전파는 어떻게 이루어 지는가?



이러한 위협 전파는 주로 AD를 통해서 이루어짐

KISA / Microsoft의 리포트





AD기반 환경의 주요한 공격대상인 GPO, 계정에 대한

모니터링 체계 구축 필요

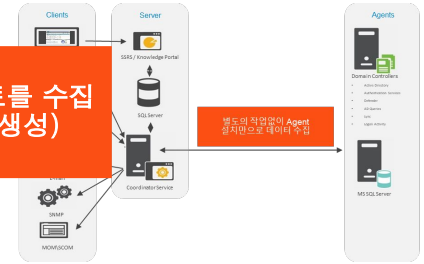
AD보안 위협의 실시간 탐지는 어떻게?

Quest

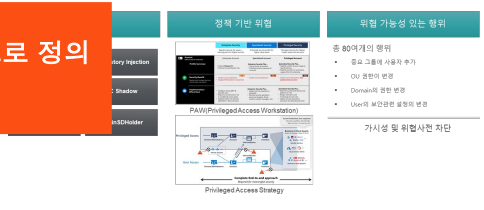
Where Next Meets Now.

체계화된 위협분류와 이를 탐지하기 위한 데이터

모든 행위 이벤트를 수집
(자체 데이터 생성)



위협을 체계적으로 정의
및 탐지



글로벌/국내에서
유일하게 검증되고
다수의 구축 경험

탐지

인사정보 자동동기화(입사,퇴사,
이동)

Tier0 Secure Zone

Provisioning/De-Provisionin
g

On-premises Active
Directory

Azure AD Connect
Server

Azure AD

Office 365

Your Apps

Saas Applications

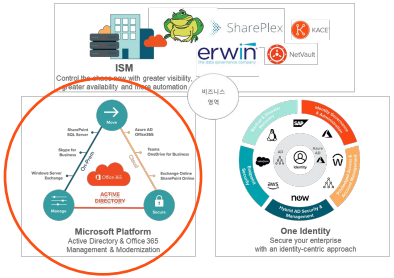
Join

Windows 10

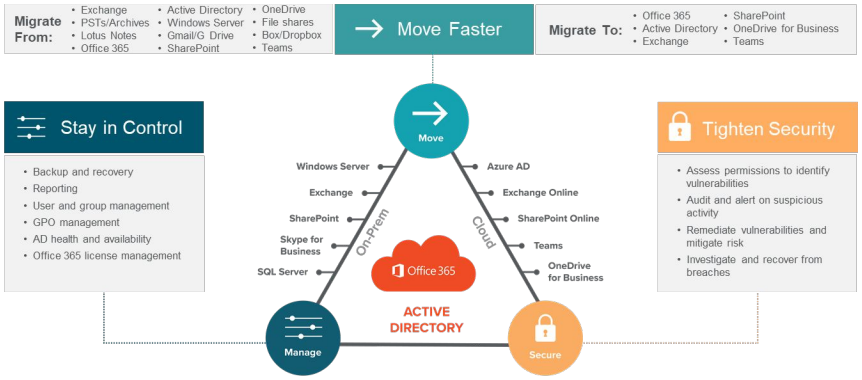
통합콘솔로 접근통로
단일화
(직접 접근 제한)

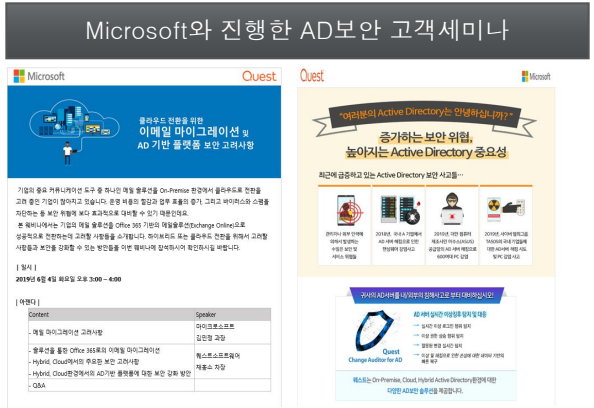
PAW(SAW
)

Quest는 국내 / 글로벌 AD보안 리더



Quest 3개 BU중 하나가
Microsoft Platform 영역





퀘스트 AD 보안 솔루션 웨비나 보기
- Microsoft와 함께하는 Quest AD 보안이야기

웨비나 보기

#2
Azure Consumed Revenue

#5
Us Cosell Wins

100% YoY Growth

Quest

Where Next Meets Now.


Thank You
Quest
Where Next Meets Now.