[제15회] 2020년 전망,
금융 IT INNOVATION 컨퍼런스

Hongso Chae
Quest Software Korea | Solutions Consultant

Windows 10, 금융권의 보안혁신은 선택이 아닌 필수

Quest

Windows 10 환경을 바라보는 우리의 시각은?

Windows 10 업그레이드 필요한가?

- **바이러스 백신 프로그램이 설치되어 있어도 위험한가요?**
  - 신규 보안 취약점이 출현하면, 백신 프로그램만으로는 운영체제의 근본적인 취약점이 해결 되지 않아 안전하게 컴퓨터를 이용할 수가 없습니다.
  - 실제로 2017년 발생한 워너크라이 사태의 경우 보안업데이트를 하지 않은 윈도우 시스템(PC, 서버 등)의 보안 취약점을 악용하여 공격에 악용되었습니다.

- **현재 윈도우7을 사용하고 있는데 어떻게 해야 하나요?**
  - 해킹 등 사이버침해사고로 인한 피해를 예방하시고자 할 경우 **2020년 1월 14일** 이전까지 다른 **운영체제***로 **교체**하시거나 **상위버전**(윈도우10)으로 **업그레이드**하시는 것을 권장 드립니다.

    * **교체 가능 운영체제** : 하모니카OS, 구름OS, Red Hat, CentOS, fedora, TIZEN, ubuntu, LinuxMint 등

Windows 10은 7에서 숫자만 변경?

업그레이드 꼭 해야 하나?

출처 : KISA 인터넷 보호나라 : https://www.boho.or.kr/cyber/window7Finish.do

Windows 10 업그레이드 이점은?

검색엔진에서 윈도우 10 업그레이드 검색

Windows 10 업그레이드만 하면 모든 문제가 해결?

마이크소프트의 업데이트 지원만 받으면 보안 해결?

Quest

그렇다면 Windows 10은 무엇이 달라졌나?

Windows 10 vs Windows 7: Microsoft's newer OS is almost 'twice as secure'

The volume of malware seen on Windows 10 devices is far lower than on Windows 7 machines, according to one security firm.

https://www.zdnet.com/article/windows-10-vs-windows-7-microsofts-newer-os-is-almost-twice-as-secure/

"선택 아닌 필수" 윈도우 10 도입은 모던 PC와 함께

많은 중소기업에서 인력과 예산을 이유로 운영체제 및 PC 관리의 우선순위가 낮은 상황이다. 하지만 모든 일이 PC에서 시작된다 해도 과언이 아닐 정도로 PC는 업무 환경의 기초다. 구형 운영체제와 낡은 PC는 보안 문제를 야기하고 잦은 고장 등 업무 생산성을 위협한다.

2020년 1월 14일 윈도우 7의 지원 종료를 앞둔 상황에서 여전히 윈도우 7과 오래된 PC에 의존하고 있는 중소기업들에게 남은 선택지는 윈도우 10으로의 마이그레이션뿐이다. 윈도우 10은 지속적인 보안 업데이트를 제공하고, 윈도우 헬로, 윈도우 디펜더, 비트라커 등 서드파티 소프트웨어 없이도 PC를 안전하게 지켜준다. 디자인, 성능, 사용자 환경 측면에서 모빌리티와 클라우드가 기본인 오늘날의 업무 환경에 꼭 맞는 모던 PC와 윈도우 10을 함께 사용한다면, 보안과 생산성, 두 마리 토끼를 한 번에 잡을 수 있을 것이다.

http://www.itworld.co.kr/techlibrary/133887

MS가 보안 분야에 연간 10억달러씩 투자하는 이유

MS는 보안 회사다?

공유 19 댓글 0

언어 선택 Google 번역에서 제공

"마이크로소프트가 보안에 매년 투자하는 금액은 10억달러 수준이다. 글로벌 보안 회사의 연간 매출이 60억달러 정도인 점에 비춰봤을 때 보안에 대한 투자 비용이 상당하다."

글쓴이

이기범

spirittiger@bloter.ne

사랑과 정의의 이름으로 기술을 바라봄와 게임, 인공지능, 가상현실 등을 다룸

http://www.bloter.net/archives/326395

Quest

Windows 10 Security

Required
- BitLocker, MBAM, LAPS
- SecureBoot, UEFI, TPM
- OS Hardening, A/V, Firewall

Optional
- Credential Guard
- Windows Defender ATP
- Microsoft Edge Application Guard

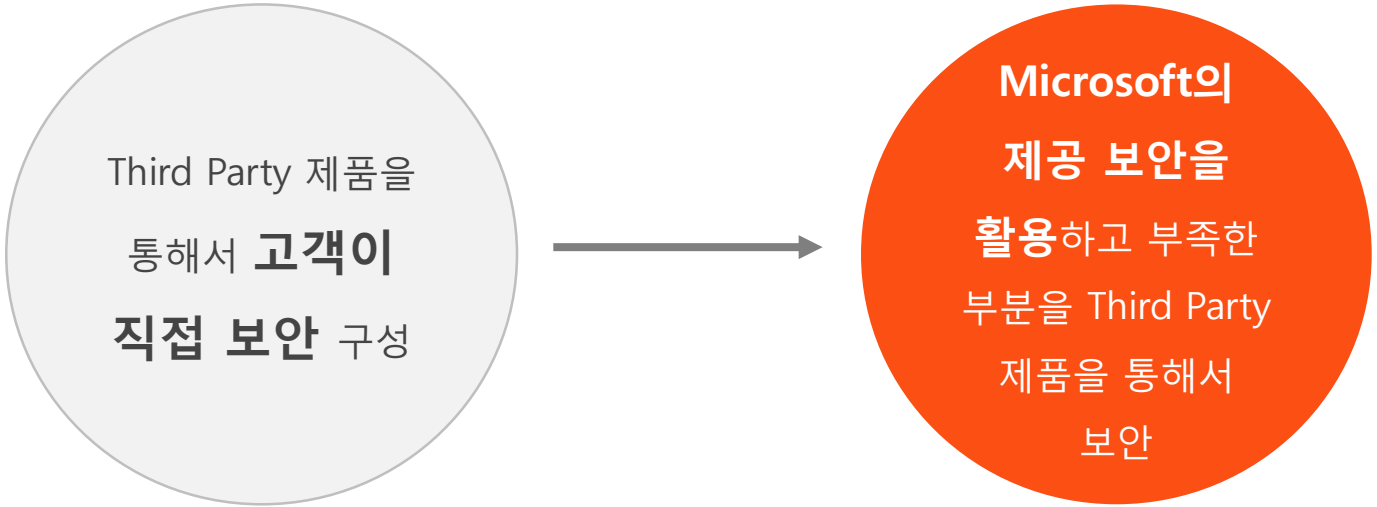
Future
- Device Guard
- Windows Information Protection
- Windows Hello for Business

Windows 10은 새로운 보안 전략의 시작으로 이를 이해하고 활용하는 전략 필요

	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.

Windows 10 환경 보안

Windows환경 보안의 변화



윈도우 환경에 대한 정의된 **단순한 형태**의 보안 **이해 필요**

윈도우 환경에 **높은 기술수준**의 보안 이해를 통한 **활용 필요**

그렇다면 중앙에서 통합적으로 관리는 어떻게?

권한 관리

Active Directory

통합 인증

Windows OS

네트워크 장비

3rd Party Solution

In House Application

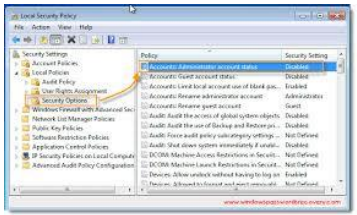
통합 관리(GPO)

디펜더

Windows Defender

방화벽

로컬 보안 정책



기타 보안 기능들

Quest

Active Directory의 발전

Windows 2000

Active Directory개념 정립

Windows 2008

AD에 보안 개념들이
추가되기 시작

Windows 2016 / Windows 10

OS 보안 아키텍처의 대대적인 변화
보안영역으로 완벽히 자리잡음

START

FINISH

Windows 2003

AD v2, v3

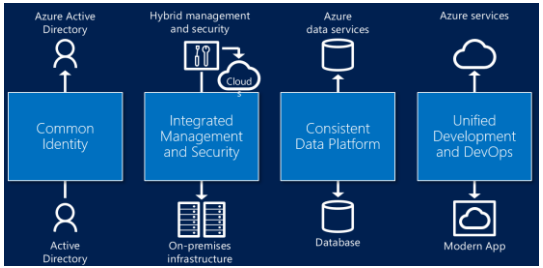
많은 개선과 AD의 실질적인 시작점

많은 조직에서 AD를 적용하기 시작

Windows 2012

Credential을 보호하는데 중점

보안영역으로의 이동



글로벌 하게 Window 2003부터 통합인증을 , Window 2008부터 보안 관점으로 활용 시작

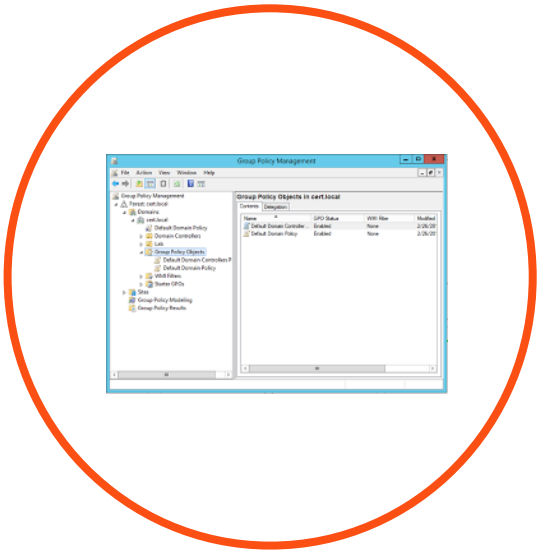
Quest

Windows 10 보안 관리의 핵심 요소는?

Active Directory

안전하게 **보호**되어야 하는 서비스

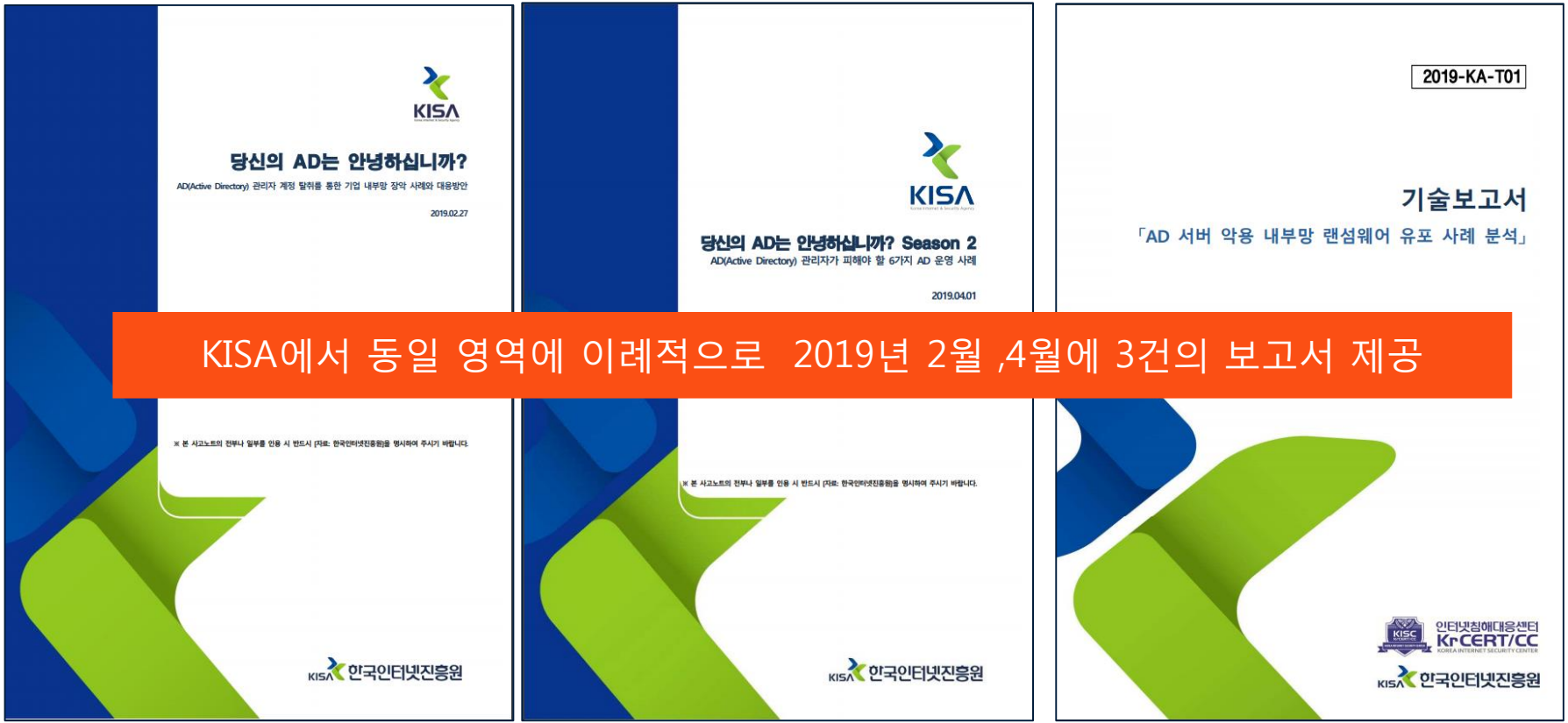
GPO(Group Policy Object)



효율적으로 **활용**되어야 하는 서비스

국내 환경 및 대응은?

윈도우 환경에서의 국내 주요 보안 위협들

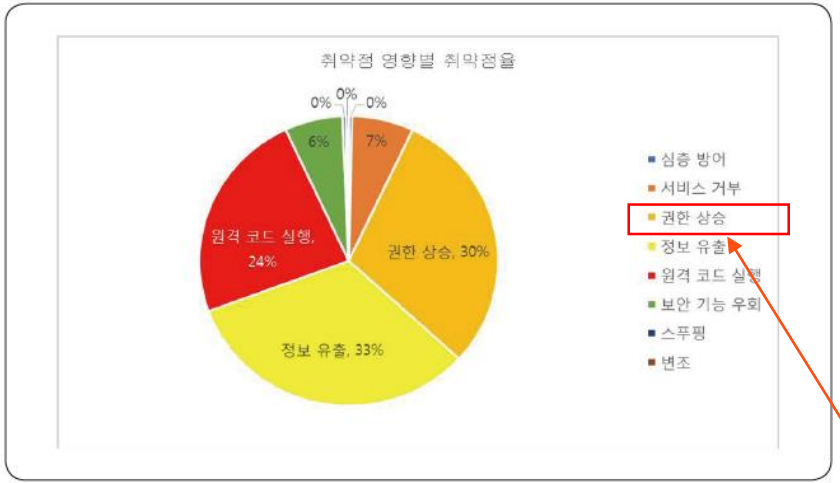


KISA에서 동일 영역에 이례적으로 2019년 2월 ,4월에 3건의 보고서 제공

Quest

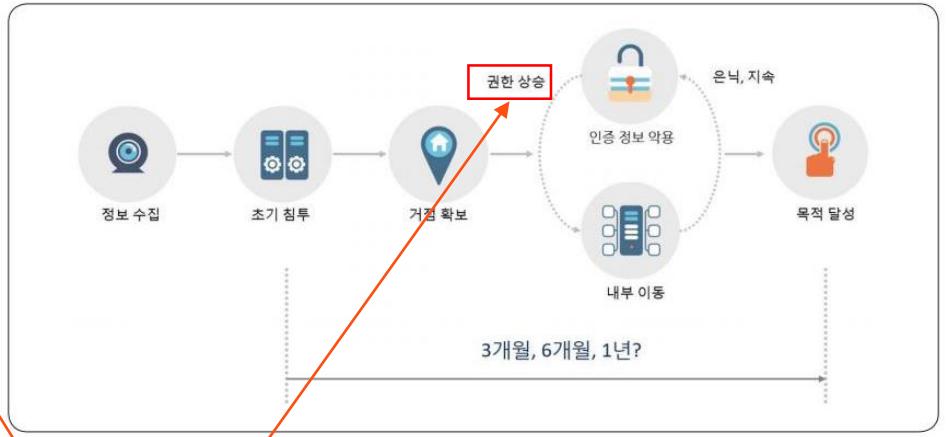
윈도우 환경에서의 국내 주요 보안 위협들

출처 : KISA 보호나라 : 2019년 2분기 주요 사이버 위협 보고서



[그림 2-48] 2016/04 ~ 2019/06, 취약점 영향별 Windows 보안 취약점 비율

출처 : KISA 보호나라



[그림 2-25] 타겟형 공격의 단계

Active Directory환경에서는 Active Directory가 주요 타겟이 되는 이유

Quest

윈도우 10환경에 대한 국내 현황은?

과학기술정보통신부 KISA 한국인터넷진흥원 2017. 12

주요정보통신기반시설

기술적 취약점

분석 · 평가

상세가이드

새로운 보안 이슈들은 어떻게 대응? 이슈 별로 별도 제품?

컴플라이언스나 권고만 만족하면 된다?

보안은 좋은 보안 제품만 사용하면 된다?

분야	세부 버전
1. 유닉스	• AIX 7.1
	• Windows Server 2000, NT 5.0 • Windows Server 2003 Standard SP2 x64 • Windows Server 2008 Standard R2 SP1 x64 • Windows Server 2012 Stand
3. 보안 장비	• 범용 벤더 (F
	• Passport
5. 제어시스템	• Piolink PLOS • 범용 벤더 (HMI, PLC, Data Historian 등)
6. PC	• Windows XP Professional SP3 x86 • Windows 7 Professional SP2 x64 • Windows 8.1 Professional x64 • Windows 10 Professional x64
7. 데이터베이스	• Oracle Database 11 • MS SQL Server 2014 • MySQL 5 • Tibero 6 • ALTIBASE 6
8. 웹 (Web)	• 소스 코드 (웹 서버, 웹 방화벽 등)

표. 분야별 점검대상 테스트 세부 버전

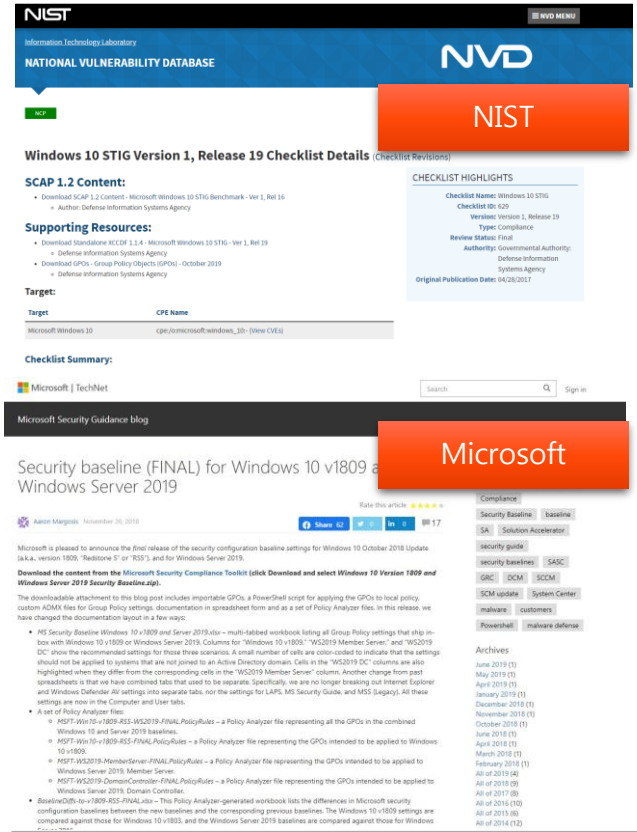
분류		항목 중요도	항목코드
	바꾸기	상	W-01
	Guest 계정 상태	상	W-02
	불필요한 계정 제거	상	W-03
	계정 잠금 임계값	상	W-04
	장 해제	상	W-05
	포함	상	W-06
	one 사용권한을 익명 사용자에 적용 해제	중	W-46
1. 계정 관리	계정 잠금 기간 설정	중	W-47
	패스워드 복잡성 설정	중	W-48
	패스워드 최소 암호 길이	중	W-49
	패스워드 최대 사용 기간	중	W-50
	패스워드 최소 사용 기간	중	W-51
	마지막 사용자 이름 표시 안함	중	W-52
	로컬 로그온 허용	중	W-53
	익명 SID/이름 변환 허용 해제	중	W-54
	최근 암호 기억	중	W-55
	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중	W-56
	원격터미널 접속 가능한 사용자 그룹 제한	중	W-57
2. 서비스 관리	공유 권한 및 사용자 그룹 설정	상	W-07
	하드디스크 기본 공유 제거	상	W-08
	불필요한 서비스 제거	상	W-09
	IIS 서비스 구동 점검	상	W-10
	IIS 디렉토리 리스팅 제거	상	W-11
	IIS CGI 실행 제한	상	W-12
	IIS 상위 디렉토리 접근 금지	상	W-13

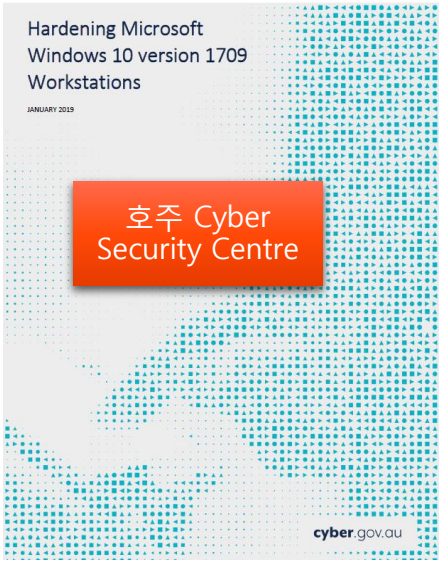
출처 : KISA 보호나라

Quest

그렇다면 해외는 어떻게 대응?

Global Trend

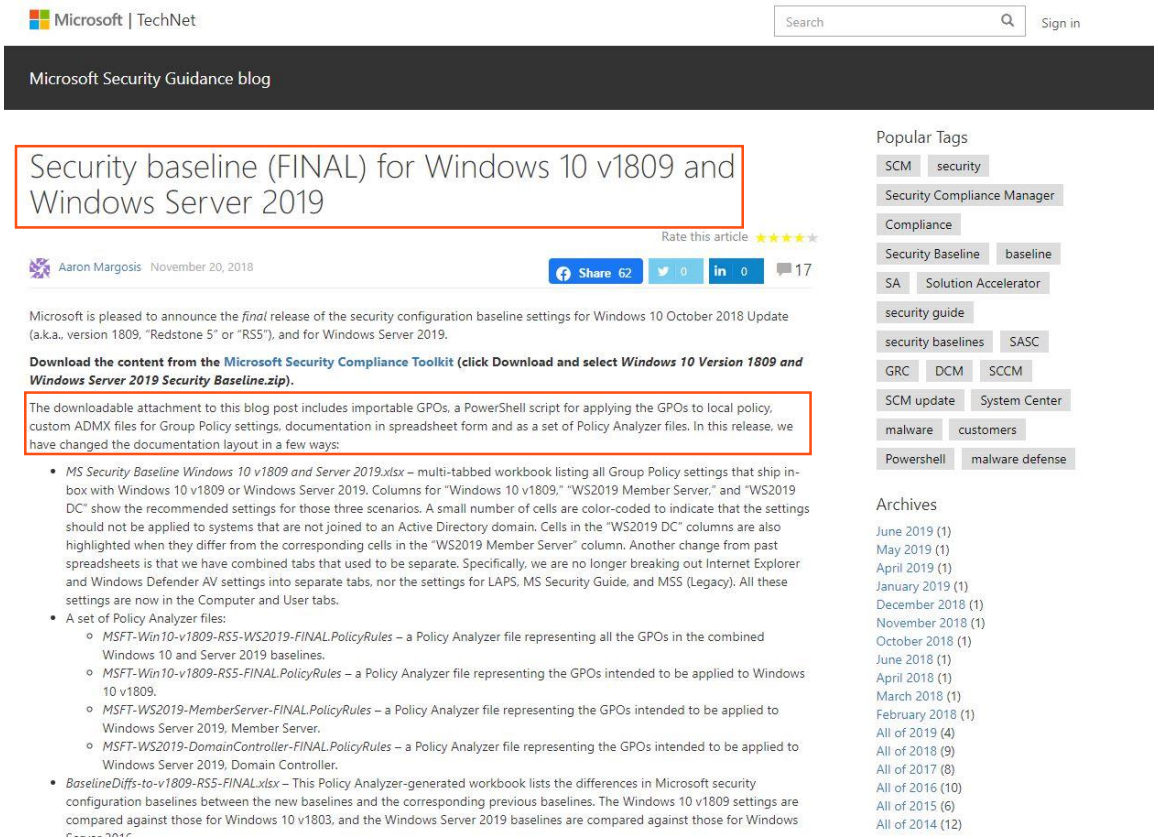




Active Directory기반의 GPO를 통한 보안이
Microsoft의 권고사항 이며 글로벌 표준

Quest

Microsoft



Microsoft | TechNet

Search

Sign in

Microsoft Security Guidance blog

Security baseline (FINAL) for Windows 10 v1809 and Windows Server 2019

Rate this article

Aaron Margosis November 20, 2018

Share 62 0 0 17

Microsoft is pleased to announce the *final* release of the security configuration baseline settings for Windows 10 October 2018 Update (a.k.a., version 1809, "Redstone 5" or "RS5"), and for Windows Server 2019.

Download the content from the Microsoft Security Compliance Toolkit (click Download and select *Windows 10 Version 1809 and Windows Server 2019 Security Baseline.zip*).

The downloadable attachment to this blog post includes importable GPOs, a PowerShell script for applying the GPOs to local policy, custom ADMX files for Group Policy settings, documentation in spreadsheet form and as a set of Policy Analyzer files. In this release, we have changed the documentation layout in a few ways:

- *MS Security Baseline Windows 10 v1809 and Server 2019.xlsx* – multi-tabbed workbook listing all Group Policy settings that ship in-box with Windows 10 v1809 or Windows Server 2019. Columns for "Windows 10 v1809," "WS2019 Member Server," and "WS2019 DC" show the recommended settings for those three scenarios. A small number of cells are color-coded to indicate that the settings should not be applied to systems that are not joined to an Active Directory domain. Cells in the "WS2019 DC" columns are also highlighted when they differ from the corresponding cells in the "WS2019 Member Server" column. Another change from past spreadsheets is that we have combined tabs that used to be separate. Specifically, we are no longer breaking out Internet Explorer and Windows Defender AV settings into separate tabs, nor the settings for LAPS, MS Security Guide, and MSS (Legacy). All these settings are now in the Computer and User tabs.
- A set of Policy Analyzer files:
  - *MSFT-Win10-v1809-RS5-WS2019-FINAL.PolicyRules* – a Policy Analyzer file representing all the GPOs in the combined Windows 10 and Server 2019 baselines.
  - *MSFT-Win10-v1809-RS5-FINAL.PolicyRules* – a Policy Analyzer file representing the GPOs intended to be applied to Windows 10 v1809.
  - *MSFT-WS2019-MemberServer-FINAL.PolicyRules* – a Policy Analyzer file representing the GPOs intended to be applied to Windows Server 2019, Member Server.
  - *MSFT-WS2019-DomainController-FINAL.PolicyRules* – a Policy Analyzer file representing the GPOs intended to be applied to Windows Server 2019, Domain Controller.
- *BaselineDiffs-to-v1809-RS5-FINAL.xlsx* – This Policy Analyzer-generated workbook lists the differences in Microsoft security configuration baselines between the new baselines and the corresponding previous baselines. The Windows 10 v1809 settings are compared against those for Windows 10 v1803, and the Windows Server 2019 baselines are compared against those for Windows

Popular Tags

SCM security Security Compliance Manager Compliance Security Baseline baseline SA Solution Accelerator security guide security baselines SASC GRC DCM SCCM SCM update System Center malware customers Powershell malware defense

Archives

June 2019 (1)
May 2019 (1)
April 2019 (1)
January 2019 (1)
December 2018 (1)
November 2018 (1)
October 2018 (1)
June 2018 (1)
April 2018 (1)
March 2018 (1)
February 2018 (1)
All of 2019 (4)
All of 2018 (9)
All of 2017 (8)
All of 2016 (10)
All of 2015 (6)
All of 2014 (12)

NIST

Microsoft Windows 7 (Version 1, Release 30)	Microsoft Windows 7	Defense Information Systems Agency	10/31/2019	– SCAP 1.2 Content - Sunset - Microsoft Windows 7 STIG Benchmark - Ver 1, Rel 36 – GPOs - Group Policy Objects (GPOs) - October 2019 – Machine-Readable Format - Sunset - Microsoft Windows 7 Audit Benchmark – Standalone XCCDF 1.1.4 - Sunset - Microsoft Windows 7 STIG - Ver 1, Rel 30
Microsoft Windows 2008 R2 STIG (Version 1, Release 33)	Microsoft Windows Server 2008 R2 Microsoft Windows Server 2008 r2 Itanium Microsoft Windows Server 2008 r2 x64 Microsoft Windows Server 2008 R2 Service Pack 1 Microsoft Windows Server 2008 r2 Service Pack 1 Itanium Microsoft Windows Server 2008 r2 x64 Service Pack 1	Defense Information Systems Agency	10/31/2019	– SCAP 1.2 Content - Microsoft Windows 2008 R2 DC STIG Benchmark - Ver 1, Rel 32 – SCAP 1.2 Content - Microsoft Windows 2008 R2 MS STIG Benchmark - Ver 1, Rel 33 – GPOs - Group Policy Objects (GPOs) - October 2019 – Standalone XCCDF 1.1.4 - Microsoft Windows 2008 R2 DC STIG - Ver 1, Rel 31 – Standalone XCCDF 1.1.4 - Microsoft Windows 2008 R2 MS STIG - Ver 1, Rel 30
Windows Firewall STIG and Advanced Security STIG (version 1, release 7)	windows firewall	Defense Information Systems Agency	10/31/2019	– SCAP 1.2 Content - Microsoft Windows Firewall STIG Benchmark - Ver 1, Rel 7 – GPOs - Group Policy Objects (GPOs) - October 2019 – Standalone XCCDF 1.1.4 - Microsoft Windows Firewall STIG and Advanced Security STIG - Ver 1, Rel 7
Windows 10 STIG (Version 1, Release 19)	Microsoft Windows 10	Defense Information Systems Agency	11/01/2019	– SCAP 1.2 Content - Microsoft Windows 10 STIG Benchmark - Ver 1, Rel 16 – GPOs - Group Policy Objects (GPOs) - October 2019 – Standalone XCCDF 1.1.4 - Microsoft Windows 10 STIG - Ver 1, Rel 19
Microsoft Windows Server 2016 STIG (Version 1, Release 11)	Microsoft Windows Server 2016	Defense Information Systems Agency	11/01/2019	– SCAP 1.2 Content - Microsoft Windows Server 2016 STIG Benchmark - Ver 1, Rel 11 – GPOs - Group Policy Objects (GPOs) - October 2019 – Standalone XCCDF 1.1.4 - Microsoft Windows Server 2016 STIG - Ver 1, Rel 9
Microsoft Windows Defender Antivirus STIG (Ver 1, Rel 6)	Microsoft Windows Defender	Defense Information Systems Agency	11/01/2019	– SCAP 1.2 Content - Windows Defender AV STIG Benchmark - Ver 1, Rel 4 – GPOs - Group Policy Objects (GPOs) - October 2019 – Standalone XCCDF 1.1.4 - Microsoft Windows Defender Antivirus STIG - Ver 1, Rel 6
Microsoft Windows Server 2019 (Ver 1, Rel 2)	Microsoft Windows Server 2019	Defense Information Systems Agency	10/31/2019	– SCAP 1.2 Content - Microsoft Windows Server 2019 STIG Benchmark - Ver 1, Rel 1 – GPOs - Group Policy Objects (GPOs) - October 2019 – Standalone XCCDF 1.1.4 - Microsoft Windows Server 2019 STIG - Ver 1, Rel 2

Gartner

Windows 10 Enhances Security

Published: 20 September 2018

ID: G00346139

Analyst(s): Peter Firstbrook

Summary

Improved security is one of the biggest benefits of adopting Windows 10. This research explores new Windows threat resistance security features that are important to security and risk management leaders.

Table Of Contents

Figure 1. Magic Quadrant for Endpoint Protection Platforms

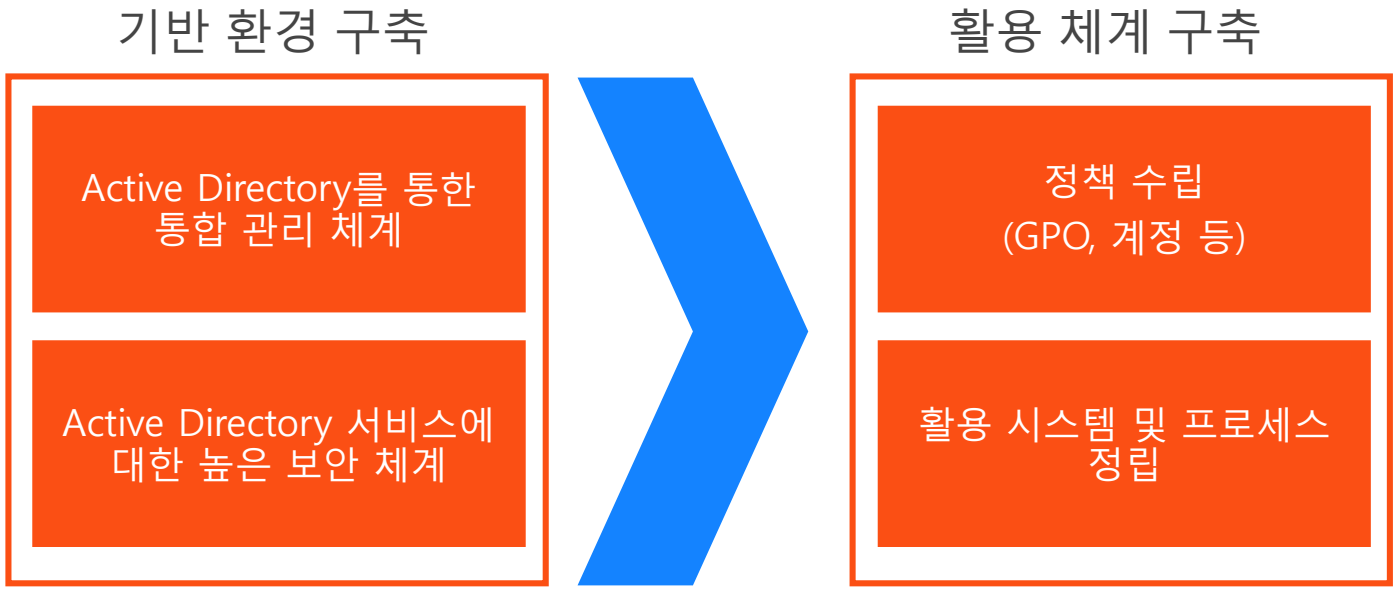
Source: Gartner (August 2019)

출처 : Gartner - https://www.gartner.com/en/documents/3890175/windows-10-enhances-security

Quest

Quest의 Windows 10 환경 보안 전략

Active Directory 서비스 보안 강화 및 보안체계 구축



활용 체계 확대

- Linux 연계
- 네트워크 장비 인증
- 3rd Party Solution 인증

서비스 보안

편리성 및 가시성

Quest

기반 환경 구축

기반 환경 구축

Active Directory를 통한 통합 관리 체계

Active Directory 서비스에 대한 높은 보안 체계

높은 보안 기반의 Active Directory서비스로 통합된 관리 체계

Quest

(Active Directory)서비스 보안 체계?

Active Directory는

통합 시스템 계정 + 보안 정책 + 권한 + 개인정보

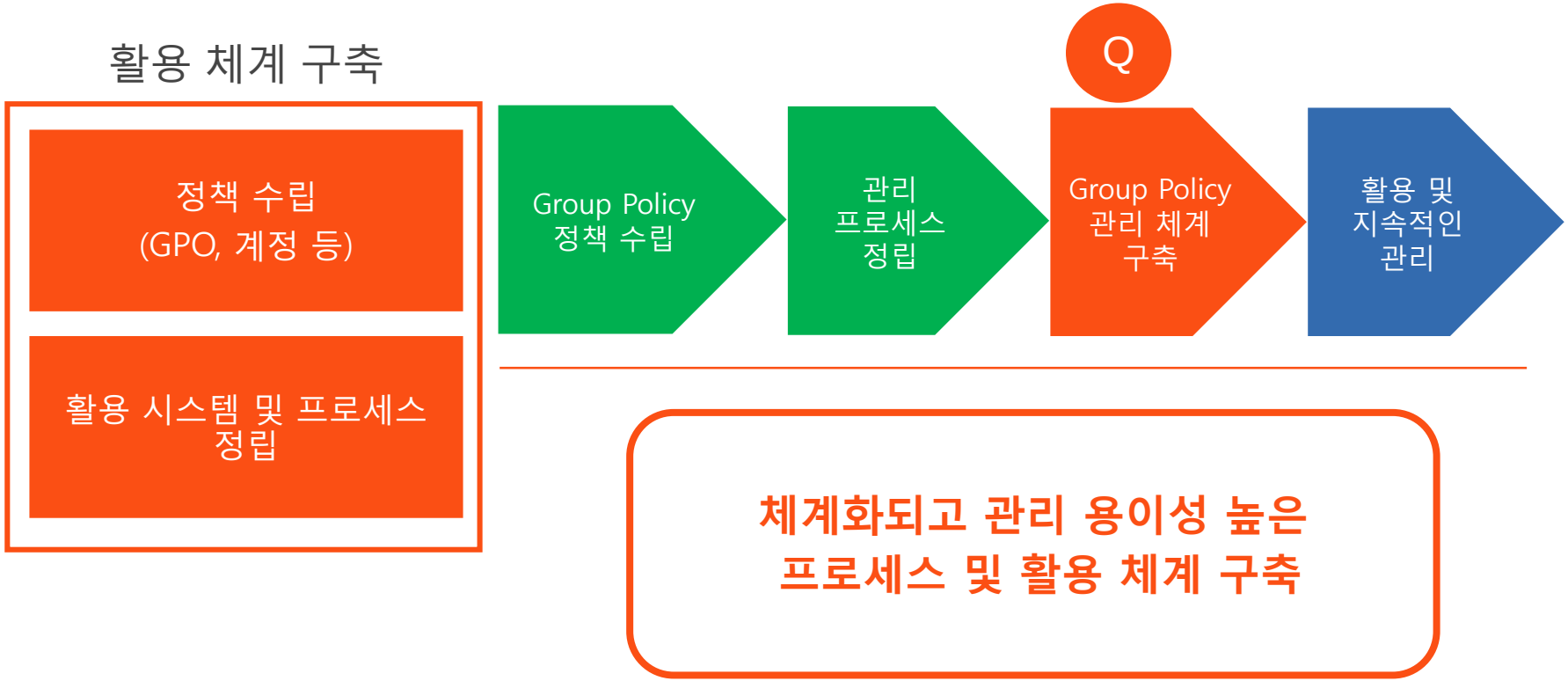
등의 높은 보안을 필요로 하는 데이터가 저장

주요한 보안
위협의 타겟

보안 사고로 인한
엄청난 피해

가장 높은 수준의 보안이 필요

활용 체계 구축

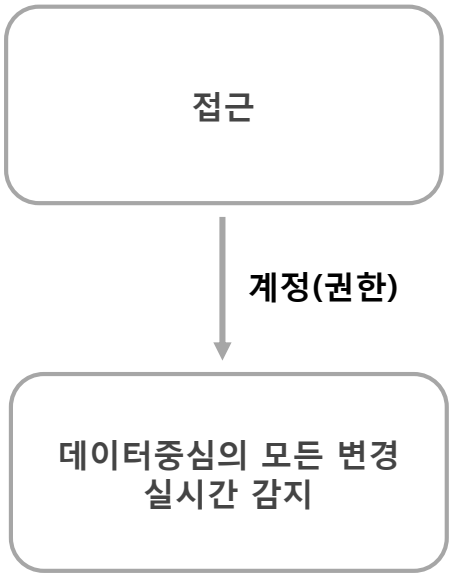


Quest

그렇다면 Quest의 전략과 솔루션은?

체계적인 Active Directory 보안 및 활용 체계

Active Directory 보안은 크게 접근/계정/데이터 변경 감시로 구성됨



보안 체계

Active Directory 보안은 크게 접근/계정/데이터 변경 감시

보안 시스템 구성

접근 통제 및 최소권한 관리

사전보안

실시간 감시 체계

데이터 변경에 대한 실시간 감시

즉시 대응 체계

데이터 변경에 대한 즉시 복구

실시간 감지 및 대응 체계

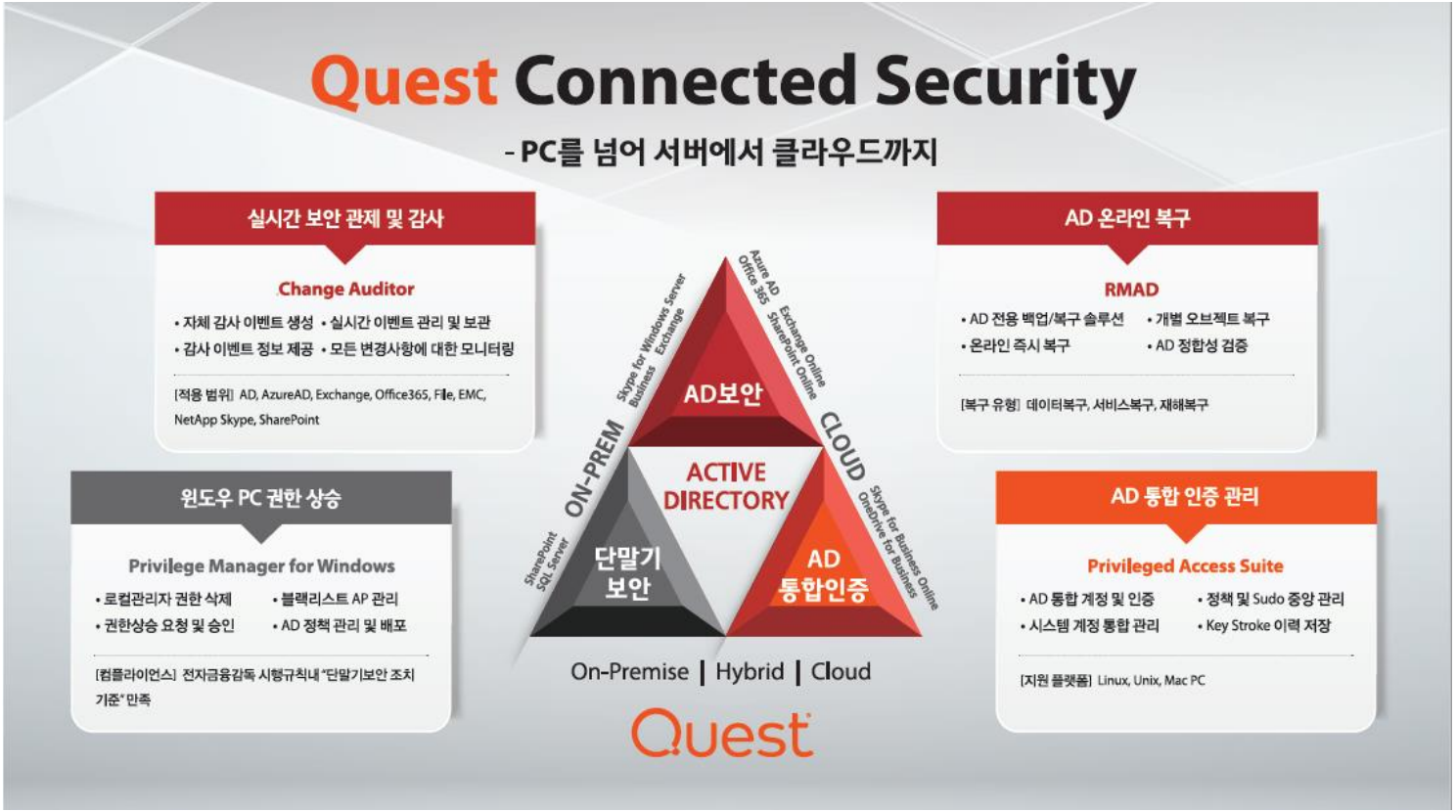
Active Directory를 통한 IT 보안 체계 구축

보안 정책에 대한 효율적 관리를 통한 높은 수준의 단말,서버, 서비스 보안

효율적 활용 및 관리

Quest

Active Directory 서비스에 대한 검증된 솔루션을 통한 높은 보안 제공



Active Directory 서비스 보안 강화 및 보안체계 구축

Active Directory 서비스 보안 강화

실시간 감지 및 중요 데이터 보호

즉시 대응 체계 구축

"보안 강화를 통한 활용 체계 기반 구축"

제안 : *Change Auditor for AD*

Recovery Manager for AD

단말 보안 체계 구축

최소 권한 관리를 통한
단말 보안 강화

컴플라이언스 준수 및 위협 최소화

제안 : *PMW(Privilege Manager for Windows)*

PAS(Privileged Access Suite)

로컬 보안 정책(GPO) 효율적 활용 체계 구축을 통한 IT자산의 효율적 보안 체계 구축

보안 정책의 개선 및 보완

"지속적인 높은 수준의 보안 정책 효율적 운영 체계 구축"

제안 : *Desktop Authority*

금융권을 위한 Windows 10환경 보안 전략

전문화된 솔루션 및 전략
(Quest)

높은 수준의 기술력을 통한
구축 및 컨설팅
(Quest Partner or 전문기업)

높은 보안 수준의
기반 환경 구축

- AD기반 관리 체계 구축
- 실시간 위협 감시 및 대응 체계 구축

효율적이고 가시성 있는
관리 체계 구축

- 회사 Group Policy 정책 수립
- 높은 가시성 기반의 관리 용이성을 제공하는 관리 체계 구축
- 단말 관리자 권한 삭제 대응

비용 효율적인
관리영역 확대

- Linux / Mac 환경에 대한 통합 인증
- 네트워크/보안장비의 통합 인증
- AD 통합인증기반의 시스템 계정관리

마이크로소프트의 Windows 10 환경
보안 정책 및 글로벌 트렌드 → 기업 자체적인 시스템(윈도우, Linux, 장비) 보안 및 인증 정책