

디지털 트랜스포메이션을 통한
비즈니스 혁신과 4차 산업혁명 대응을 위한

GIT 솔루션즈 데이

디지털 업무 환경의 변화

2018, 10 / 김병철 이사 (VMware)

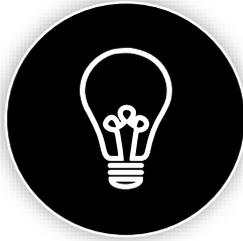
디지털 비즈니스 환경은 업무형태를 바꾸고 있습니다.



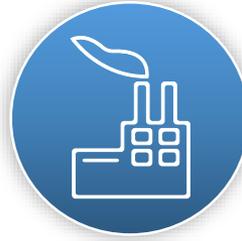
Healthcare



Education



**Power and
Utilities**



Manufacturing



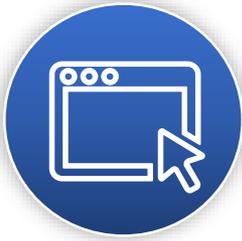
Banking



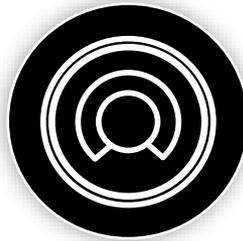
Devices



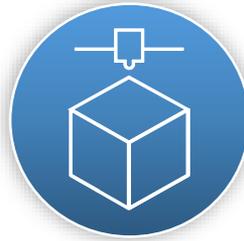
mHealth



**Massive Open
Online Courses**



**Smart
Grid**



**Custom
Manufacturing**



**Mobile
Finance**



IoT

직원의 역량이 강화되면 생산성이 향상됩니다.

직원 역량 강화

기업이 직원을 위해 애플리케이션을 손쉽게
사용하도록 지원할 때 가능



수동 프로세스에 소요되는 시간을
거의 **20% 단축**



팀 협업 및 의사 결정 속도가
16% 향상

그러나 직원과 CIO의 의견이 항상 일치하지는 않습니다.



CIO

최종 사용자

매우 동의...

72%

40%

회사에서 선도적으로 직원에게 첨단 기술을 제공한다.

47%

24%

회사에서 직원에게 원하는 애플리케이션을 제공한다.

38%

16%

회사에서 직원들이 애플리케이션에 손쉽게 액세스하도록 지원한다.

28%

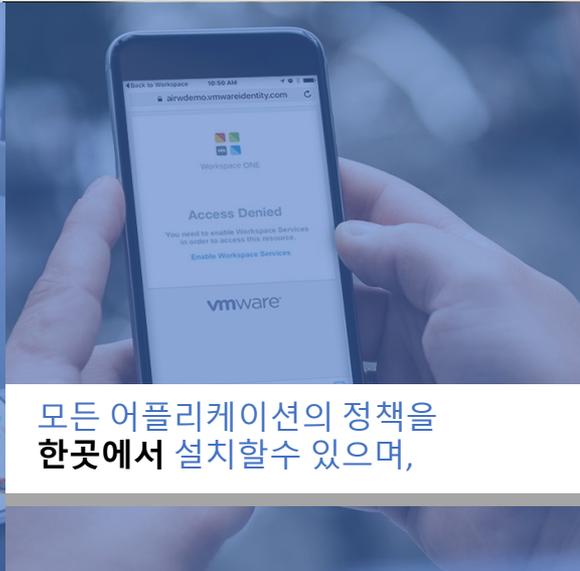
10%

직원이 회사 외부에서도 비즈니스 애플리케이션을 자유롭게 이용할 수 있다.

Digital Workspace가 가능하게 하는 일



새로운 직원에게 **한시간 이내**에 새로운 기기를 제공 할수 있고,



모든 어플리케이션의 정책을 **한곳에서** 설치할수 있으며,



72 초 안에 업무 플로우를 처리 할수 있게 할 수 있고,



몇 분안에 어디서든 회사 노트북을 Provision 하는것이 가능 합니다.



Fast Deployment



Contextual Control



Mobile Access



Remote Management

원격 업무환경의 요건은 증가하고 거부할수 없습니다.



직원의 생산성 향상은 경계 보안 정책을 해체하고

유연한 업무 방식



어디에서나
애플리케이션
사용

다양한
기기 지원



가시성 부족으로 위협은 증가 합니다.

유연한 업무 방식



어디에서나
애플리케이션
사용

다양한
기기 지원



기능별 보안은 더이상 유효하지 않을수 있습니다.

인프라 보안

Network Firewall
 Check Point, Palo Alto Networks, Cisco, Fortinet, Juniper, Blue Coat, SonicWall, Mikrotik, Snort, Snort3, Snort4, Snort5, Snort6, Snort7, Snort8, Snort9, Snort10, Snort11, Snort12, Snort13, Snort14, Snort15, Snort16, Snort17, Snort18, Snort19, Snort20, Snort21, Snort22, Snort23, Snort24, Snort25, Snort26, Snort27, Snort28, Snort29, Snort30, Snort31, Snort32, Snort33, Snort34, Snort35, Snort36, Snort37, Snort38, Snort39, Snort40, Snort41, Snort42, Snort43, Snort44, Snort45, Snort46, Snort47, Snort48, Snort49, Snort50, Snort51, Snort52, Snort53, Snort54, Snort55, Snort56, Snort57, Snort58, Snort59, Snort60, Snort61, Snort62, Snort63, Snort64, Snort65, Snort66, Snort67, Snort68, Snort69, Snort70, Snort71, Snort72, Snort73, Snort74, Snort75, Snort76, Snort77, Snort78, Snort79, Snort80, Snort81, Snort82, Snort83, Snort84, Snort85, Snort86, Snort87, Snort88, Snort89, Snort90, Snort91, Snort92, Snort93, Snort94, Snort95, Snort96, Snort97, Snort98, Snort99, Snort100.

Network Monitoring
 Blue Coat, Cisco, Xixia, StillSecure, Bradford, LogRhythm, Juniper, DeepNines, Palo Alto Networks, Riverbed, Lancope, ForeScout, NetScout, EMC, RSA.

Intrusion Prevention Systems
 IBM, Cisco, Corefo, Snort, Radware, McAfee, DeepNines, Airtight, FireEye, Extreme, Juniper, Palo Alto Networks, Sophos, Fortinet, Check Point.

Unified Threat Management
 Fortinet, Dell, Juniper, Aker, Cyberteam, Check Point, WatchGuard, Palo Alto Networks, Hillstone, FireEye, Cisco, Stormshield, FortiGuard, Gateprotect.

Endpoint 보안

Endpoint Protection & Anti-Virus
 McAfee, LANDesk, CSBT, P-Safe, F-Secure, Kaspersky, Barkly, Lumension Security, ThreatTrack, Stormshield, SentinelOne, Panda, Microsoft, BitDefender, AVG, Confer, Trend, Emsisoft, Webroot, Malwarebytes, Symantec.

Endpoint Detection & Response
 Red Canary, Certego, Hexatec, ZoneFox, Morphisec, Hexadite, Fluency, Outlier, Tanium, Hexis, Bromium, CounterTack, Guidance, LightCyber, Confer, Cisco, Ziften, Invincea, SentinelOne, EMC, RSA, BitD + Black, Cybereason, Lastline, Digital Guardian, Nextthink, Hexis, Endgame.

메시징 보안
 Proofpoint, Websense, Microsoft, EdgeWave, FireEye, Trustwave, Morphic, Symantec, Cloudmark, Gwava, WatchGuard, Bar Systems, Cyren, Spamina, Fortinet, McAfee, Apprivo, Clear Swift, Agari, Sophos, Trend, Dell, Mimecast.

애플리케이션 보안

WAF & Application Security
 Pentasec, Sucuri, Qualys, Alertlogic, SH-PE, Trustwave, Denyall, Arxan, Fireblade, Akamai, Zenedge, Citrix, Ergon, SOHA, DBAppSecurity, Fortinet, Radware, Positive Technologies, Imperva.

Vulnerability Assessment
 Hackerone, WhiteHat, Rapid7, Checkmarx, SRC:CLR, Secunia, Flexera, RandomStorm, CoreSecurity, Nccgroup, Bugcrowd, IBM, Apprivo, Veracode, Digital, Outpost24, Qualys, Arxan.

웹 보안
 Blue Coat, Distil, Cisco, Sophos, Trustwave, Cloudflare, SH-PE, Zscaler, FireEye, Apprivo, Comenkeeper, Check Point, Easy Solutions, Juniper, Bluecat, Cyren, Websense, Webroot, Symantec, Trend, Gwava, Iboss, Sangfor, Venafi, Spinnaker.

IoT 보안

Mocana, Cryptosoft, Bastille, ZingBox, Webroot, Endian, Argus, Rubicon, Riscure, Avtron, ARM, SecuriThings, Imubit, Bayshore, Device Authority, Icon Labs, Cloudwear, Infineon, IOActive.

보안 운영 및 사고 대응

SIEM
 IBM, LogRhythm, Logentrics, EventTracker, Splunk, Alertlogic, Tenable, EMC, RSA, Trustwave, Swimlane, Netlogic, Netio, Tibco, Logscape, Netmonstry, Acelops, Hewlett Packard Enterprise, Coralogic, Fluency, BlackStratus, Logpoint, PhantomCyber, Hexadite, Invotas, Proofpoint, Resilient, Cyberason, Raytheon, Rapid7, Demisto, Click, CyberTriage, Lynceur, Expects, CyberResponse, Hexis, Swimlane.

Security Incident Response
 Hexadite, Invotas, Proofpoint, Resilient, Raytheon, Rapid7, Demisto, Click, CyberTriage, Lynceur, Expects, CyberResponse, Hexis, Swimlane.

트랜잭션 보안

Feedzai, Ethoca, Forter, Sift Science, Early Warnings, ThreatMetrix, Riskified, Acculynk, Jumio, Nu Data Security, Kount, iProterior, Socure, IdenTrust, AU1, TIX, Signifyd, MaxMind, Guardian Analytics.

리스크 및 규정 준수

RedSeal, Firemon, Agilience, R-sam, RSA, Archer, Cytegit, Brinqa, SecurityScorecard, Tufin.

보안 위협 인텔리전스

BrightPoint, DomainTools, Threat Connect, ThreatStream, VirusBlok, PhishLabs, ZeroFox, Security, JID, Webroot, ThreatMetrix, Recorded Future, Blueiv, OpenDNS, Digital Shadow, Norse, Surveo, Bitsight, SurfWatch, LookingGlass, Securonix, Proofpoint, ThreatQuotient.

전문화된 위협 분석 및 보호

IronNet CyberSecurity, Fortscale, Bay Dynamics, Invincea, TrapX Security, Exabeam, LightCyber, Damballa, Vectra, Palantir, Sqrrl, Prelet, Avecto, Cymmetria, Area 1, Protectwise, Securonix, Spkps, Reglass, Seculert, Darktrace, Novetta, Endgame, Cyllance, Bromium, DataVisor, Menlo, Cyphort, Gladius, Ironic, Esentire, Illusive, Light Security.

모바일 보안

Lookout, MobileIron, Wandera, Mocana, Airwatch, Nuro, Silent Circle, Auth, TigerText, Check Point, Bitglass, Kaspersky, AVG, Trustlook, IBM, Vikey, SnoopWall, Trend, Apprivo, Airtight, Qeioslab, Trend, Koolspan, Apprivo, NowSecure, Good, Pindrop, P-Safe, Zimperium, Sophos.

데이터 보안

Hewlett Packard Enterprise, Vermetric, Harvest.ai, Nuro, Digital Guardian, Eniso, Venafi, Wicr, Privitar, VERA, Security, Venafi, Winalago, Somansa, CyberCloud, BlueTalon, THIN AIR.

ID 및 액세스 관리

Covisint, CLEF, Nok Nok, PingIdentity, Okta, EMC, RSA, SailPoint, Forgerock, Microsoft, Onelogin, Trulioo, BeyondTrust, Simeio, Secure Key, Welcome, Verato, Tascent, Avecto, IBM, Pirean, SecureAuth, CyberArk, Centrify, Iantus.

클라우드 보안

Ilumio, Sookasa, CloudPassage, CATO, Elastic, Panda, Adallom, Bitglass, Zscaler, Evident.io, ManageMethods, Code42, Whitehat, SOHA, Cloudway, Covata, Threat Stack, Vaultive, Harvest.ai, Polera, CloudLock, FireLayers, MyTrust, FortiCloud, Dome, Guardtime, ClearData, Qualys, WARMOUR, Skyhigh, Netskope, BetterCloud, Securix, PanspecSys, CyberCloud.

또한 이런 정책들은 사용자의 만족도를 저하 시킵니다

인프라 보안

Endpoint 보안

클라우드 보안

Network Firewall

Network Monitoring

Endpoint Protection & Anti-Virus

Intrusion Prevention Systems

Endpoint Detection & Response

Unified Threat Management

IoT 보안

오류!

잘못된 암호!

액세스 거부!

Band Aid

Limited Visibility

High Costs

기존 IT 환경은 업무 생산성 향상에 적합 한가요?

Mobile Team



iOS / MAC

- iTunes
- Apple ID
- App Store
- iWork
- iCloud



ANDROID / CHROME

- Gmail Account
- Google Play
- G Suite
- Google Drive



Desktop Team



WINDOWS

- Microsoft ID
- AD/Azure AD
- Office 365
- Windows Store Update Service



LOB



SaaS APPS

- Salesforce 1
- Concur
- Workday
- Slack
- Dropbox
- DocuSign



Digital Workspace는 통합된 정책이 필요합니다



End-User Services Team



iOS / MAC

- iTunes
- Apple ID
- App Store
- iWork



ANDROID / CHROME

- Gmail Account
- Google Play
- G Suite
- Google Drive



WINDOWS

- Microsoft ID
- AD/Azure AD
- Office 365
- Windows Store



SaaS APPS

- Salesforce 1
- Concur
- Workday
- Slack

Digital Workspace Platform



Connected
Things
(Rugged / IoT)

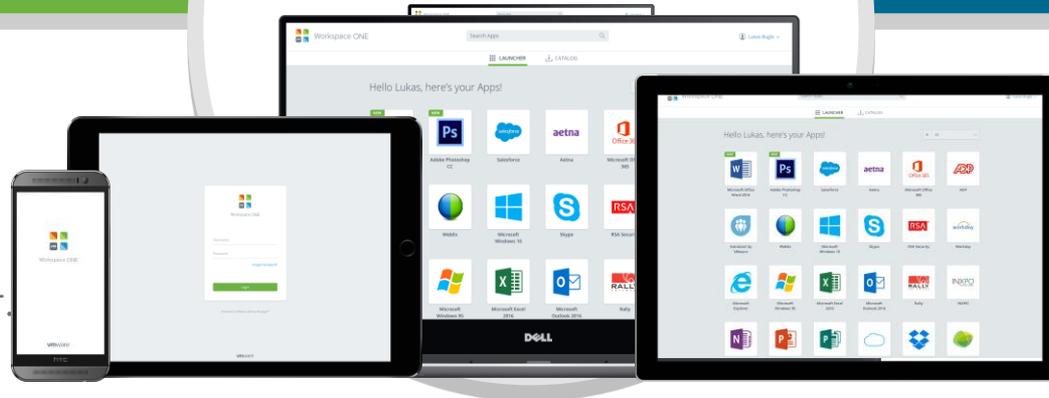
VMware는 완벽한 Digital Workspace를 제공합니다.

CONSUMER
SIMPLE

vmware®
Workspace™ ONE™

ENTERPRISE
SECURE

회사의 업무 환경이
변하지 않으면
비즈니스 목표 달성이
어려워 질수 있습니다.



업무환경의 보안을
희생할 필요는
없습니다.

VMware는 업계 최초의 디지털 워크스페이스 플랫폼을 구축했습니다.



Workspace ONE™



사용자
편의성



모든
애플리케이션



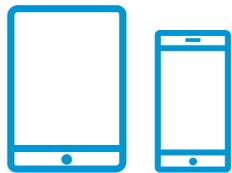
최신 방식의
관리



중앙집중
모니터링



자동화



iOS/Android



Windows
10/Mac/Chromebook



러기드/커넥티드 사물

업무환경의 클라우드 / 모바일 전의



Workspace ONE 통합 단말 관리 (UEM)

현재의 모든 연결 단말에 대한 관리 및 보안성 보장

Workspace ONE UEM

Lifecycle Management

Security

User Experience

어떠한 단말이라도

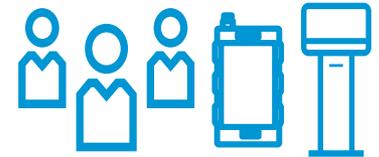
Desktops, Laptops,
Mobile Devices, IoT



플랫폼에 제약 없이



BYO



Corporate-Owned,
Purpose-Built

모든 사용 환경에 적용 가능

단일 플랫폼 지원 – All Employees, All Use Cases

관리되지 않는 환경



필요에 따라 어느곳에서도
어플리케이션 실행 지원

관리되는 환경

One-touch SSO를 통한 email &
Wi-Fi 등이 자동구성

UEM을 통한 관리환경

정해진 규칙에 따라 전체 구성이 적용된 경우



Not Your Device
(Browser Access)



Bring Your
Own Device



“Choose Your Own”
You Manage



“Choose Your Own”
Corporate Managed



“Corporate
Issued”



Locked Down



Ruggedized

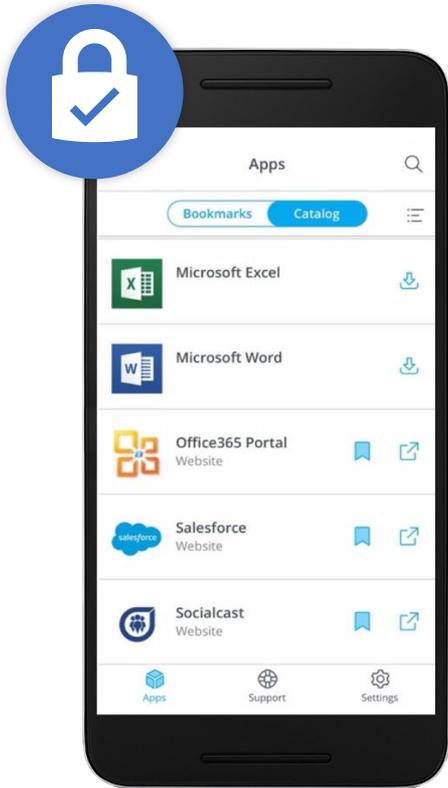


경우에 따라 앱 접근 여부 판단
(허용된 네트워크에서
적절한 인증을 거친 경우)

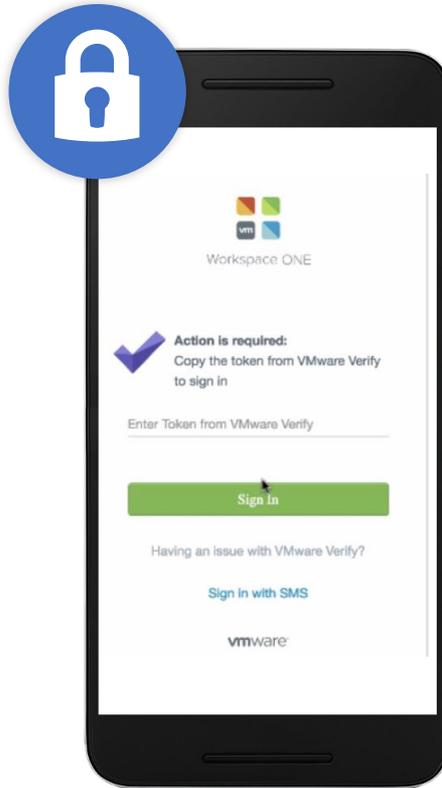
기본적인 규율 준수를 통해
강제적으로 한당되는
어플리케이션 수준의 데이터,
DLP, 제거 정책 제공 (MAM)

기기 전체에 강제적으로 적용된 장치수준 데이터,
DLP, 제거 정책, 자동 복구 등 지원

보안이 필요한 데이터에 조건부 접근 제공



관리되는 기기가
허가된 네트워크를 통한 접근



관리되는 기기가
원격지에서 접근하는 경우



해킹된 기기 (Jail Broken) 이거나
허가받지않은 네트워크를 통한 접근

업계 유일한 통합 관리 플랫폼

모바일



DEP, VPP, and Apple School Manager와 같은 최고수준의 iOS 지원



심도있는 기술을 통한 Android Enterprise 와 Samsung Knox 지원.

데스크톱



Win10 MDM 뿐만 아니라, PCLM 전문야를 지원 (정책, 패치, 보안, 소프트웨어 배포)



macOS High Sierra 기반의 MDM + Apple DEP 을 바탕으로 향상된 관리기능 지원



Google과의 파트너십을 통한 Chrome OS 의 특별한 장치관리 지원device

엔드



러기지, 웨어러블, 계측기, 키오스크 및 IoT 장치들의 손쉬운 관리 제공

모든 종류의 디바이스 모든 종류의 OS 지원



탁월한 확장성,
경계없는 클라우드 지원,
multi-tenant architecture



17 개 이상의 언어 지원,
24/7 전세계 지원망

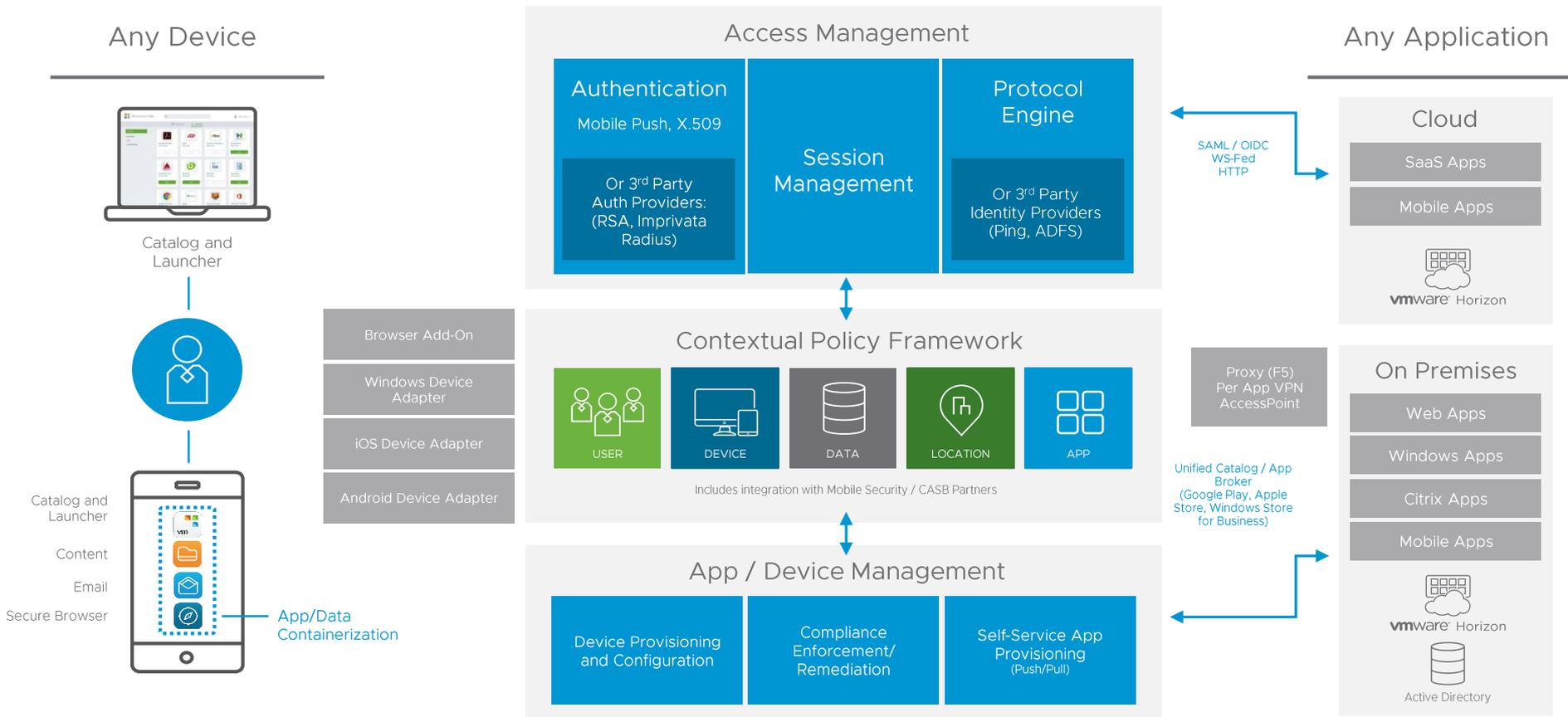


내장된 Workspace ONE
identity-defined 어플리케이션
카타로그



대규모 시장 점유율을 가지는
EMM/UEM 선도자

Workspace ONE 아키텍처



디지털 트랜스포메이션을 통한
비즈니스 혁신과 4차 산업혁명 대응을 위한

GIT 솔루션즈 데이

감사합니다.
