comtegra

Digital Workspace VMware

Przewodnik wraz z odpowiedziami na najczęściej zadawane pytania

Zintegrowany cyfrowy obszar roboczy, który spełnia unikalne wymagania biznesowe i przypadki jego zastosowania?

W dzisiejszych czasach coraz powszechniejszym modelem pracy stała się praca na odległość. W tej sytuacji należy sobie zadać pytanie w jaki sposób pracodawca powinien zapewnić swoim pracownikom bezpieczne stanowisko pracy z dostępem do wszystkich niezbędnych zasobów firmy.

Mając na uwadze przyszłość, przedsiębiorstwa będą nieustannie rozwijać model pracy na odległość. Już teraz firmy przechodzą od zwykłego wspierania pracy zdalnej do modelu prawdziwie rozproszonych organizacji, pracujących z dowolnego miejsca. Ponieważ firmy zastanawiają się, gdzie pracują zespoły, jak pracują i jak wspierają klientów, inwestycje w technologię i długoterminową strategię odgrywają ogromną rolę w tworzeniu silniejszej, bardziej skoncentrowanej i odpornej organizacji.

Cyfrowa przestrzeń robocza powinna umożliwiać pracownikom wydajną pracę z dowolnego miejsca, przy użyciu dowolnego urządzenia, aby zapewnić bezpieczny dostęp do potrzebnych aplikacji. Stworzenie odpowiedniej infrastruktury nie tylko zapewnia im możliwość wykonywania pracy, ale daje swobodę i zwiększa efektywność wykonywanych działań oraz wprowadza zupełnie nowy sposób i spojrzenie na prowadzenie działalności.

Odpowiedzią na potrzeby współczesnego biznesu może być Digital Workspace będący platformą komputerową dla użytkowników końcowych, zapewniającą bezpieczny dostęp w dowolnym czasie i miejscu do wszystkich aplikacji, usług i zasobów na wszystkich urządzeniach. Rozwiązanie obejmuje analitykę na potrzeby operacyjne i minimalizuje koszty poprzez konsolidację i zarządzanie natywne w chmurze prywatnej lub publicznej. Zmiany te zwiększają szybkość reakcji i wydajność IT, jednocześnie rozbijając silosy, zmniejszając złożoność IT i całkowity koszt posiadania.

Co należy wziąć pod uwagę, aby zapewnić produktywną i bezpieczną cyfrową przestrzeń roboczą? Jaka jest właściwa kolejność kroków potrzebnych do wdrożenia? W dalszej części poradnika odpowiemy na te pytania.

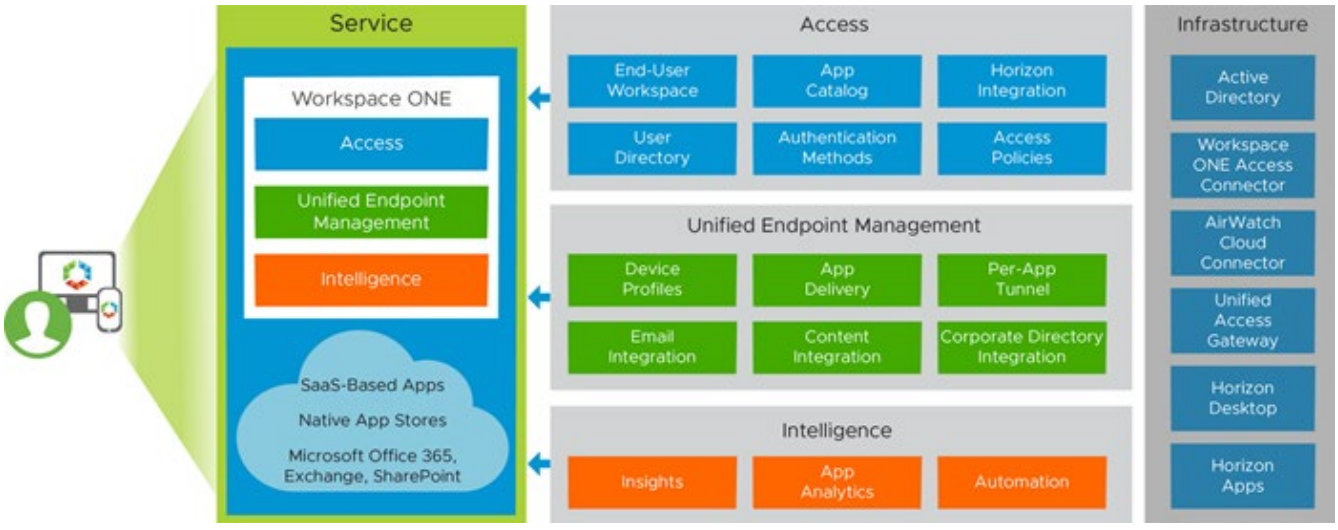
VMware Digital Workspace

W ramach portfolio VMware oferowane są produkty, których celem jest dostarczenie cyfrowej przestrzeni roboczej w organizacji. Główne z nich to pakiet komponentów Workspace ONE oraz Horizon, zapewniające centralizację zarządzania urządzeniami końcowymi użytkowników oraz zabezpieczenie przetwarzanych przez użytkowników danych biznesowych, poprzez przeniesienie środowiska ich pracy do wirtualnych pulpitów zlokalizowanych w centrach danych. W przypadku dostępu zdalnego, bezpieczeństwo staje się kluczową kwestią, która realizowana jest poprzez dostęp użytkowników do danych wewnętrznych z urządzeń roboczych konfigurowanych w modelu Zero Trust Security. Wykorzystanie zwirtualizowanych pulpitów umieszczonych w DataCenter umożliwia konsolidację zasobów oraz bezpieczeństwo przetwarzanych danych, jak również wydłużenie cyklu życia urządzeń, z których użytkownicy łączą się do swojej przestrzeni roboczej.

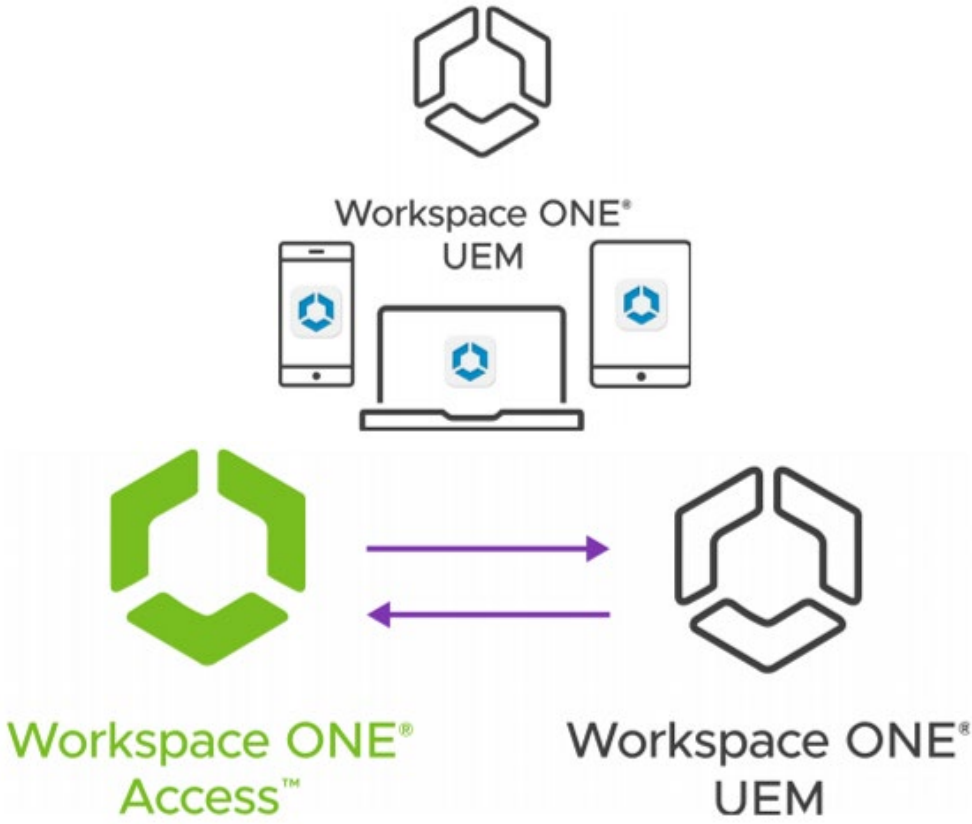
WORKSPACE ONE

VMware Workspace ONE to prosta i bezpieczna platforma korporacyjna, która dostarcza i zarządza dowolną aplikacją na dowolnym urządzeniu. Workspace ONE integruje zarządzanie tożsamością, aplikacjami i mobilnością w organizacji, zapewniając bezproblemowy i bezpieczny dostęp do wszystkich aplikacji i danych, których pracownicy potrzebują do wykonywania swojej pracy. Platforma dostępna jest jako usługa w chmurze lub do wdrożenia lokalnego. Składa się z kilku komponentów m.in. VMware Workspace ONE Unified Endpoint Management (UEM) i VMware Workspace ONE Access (wcześniej nazywanego VMware Identity Manager) oraz aplikacji zwiększających produktywność Workspace ONE, które są obsługiwane na większości popularnych platform mobilnych.

Ponadto Workspace ONE integruje się z wirtualnymi pulpitami VMware Horizon i opublikowanymi aplikacjami dostarczanymi za pośrednictwem Horizon i Horizon Cloud w Microsoft Azure. Ta integracja zapewnia szybki dostęp z wykorzystaniem logowania pojedynczego (SSO) do wirtualnego pulpitu lub aplikacji.



Workspace ONE UEM to komponent platformy służący do zarządzania mobilnością w przedsiębiorstwie. Umożliwia rejestrację urządzeń i używa profili do wymuszania ustawień konfiguracji i zarządzania urządzeniami użytkowników. Umożliwia również katalogowi aplikacji mobilnych publikowanie publicznych i wewnętrznie opracowanych aplikacji dla użytkowników końcowych.



Platforma Workspace ONE zapewnia następujące funkcjonalności klasy korporacyjnej dla użytkowników końcowych:

- Dostarczanie i automatyzacja aplikacji w czasie rzeczywistym. Korzystając z nowych możliwości systemu Windows, Workspace ONE umożliwia administratorom komputerów stacjonarnych automatyzację dystrybucji i aktualizacji aplikacji. Ta automatyzacja, w połączeniu z technologią wirtualizacji, pomaga zapewnić dostęp do aplikacji, a także poprawić bezpieczeństwo i zgodność.
- Samoobsługowy dostęp do aplikacji. Gdy użytkownicy końcowi zostaną uwierzytelnieni za pomocą aplikacji VMware Workspace ONE Intelligent Hub, mogą natychmiast uzyskać dostęp do aplikacji mobilnych, chmurowych i Windows za pomocą pojedynczego logowania (SSO).
- Wybór dowolnego urządzenia. Administratorzy mogą umożliwić użytkownikom wykorzystanie formuły BYOD (Bring Your Own Device), oddając wybór urządzeń w ręce użytkowników końcowych.
- Rejestracja urządzeń. Proces rejestracji umożliwia zarządzanie urządzeniem w środowisku Workspace ONE UEM, dzięki czemu profile urządzeń i aplikacje mogą być dystrybuowane, a zawartość może być dostarczana lub usuwana. Rejestracja umożliwia również obszerne raportowanie na podstawie zaewidencjonowania urządzenia w usłudze Workspace ONE UEM.
- Zarządzanie adaptacyjne. Dla niektórych aplikacji użytkownicy końcowi mogą logować się do Workspace ONE i uzyskiwać do nich dostęp bez uprzedniego rejestrowania urządzenia. W przypadku innych aplikacji wymagana jest rejestracja urządzenia, a aplikacja Workspace ONE może monitować użytkownika o zainicjowaniu rejestracji.
- Dostęp warunkowy. Zarówno Workspace ONE Access, jak i Workspace ONE UEM mają mechanizmy oceny zgodności. Gdy użytkownicy rejestrują swoje urządzenia w Workspace ONE, próbki danych z urządzenia są wysyłane do usługi w chmurze Workspace ONE UEM zgodnie z harmonogramem w celu oceny zgodności. Ta regularna ocena zapewnia, że urządzenie spełnia reguły zgodności określone przez administratora w konsoli Workspace ONE UEM. Jeśli urządzenie nie będzie zgodne, zostaną wykonane odpowiednie akcje skonfigurowane w konsoli Workspace ONE UEM Console.

Workspace ONE Access zawiera składniki związane z tożsamością rozwiązania. Działa jako punkt dostępu użytkownika do zasobów i oparty jest o warunki tego dostępu, które administratorzy mogą skonfigurować w celu sprawdzenia urządzenia oraz użytkownika, który loguje się do platformy.

Reguły oraz odpowiadające im akcje mogą być konfigurowane na podstawie sieci, w której znajdują się użytkownicy używanej platformy oraz aplikacji, do których uzyskują dostęp. Oprócz sprawdzania zgodności urządzenia w Workspace ONE UEM, możliwa jest ocena zgodności na podstawie zasięgu sieci urządzenia, typu urządzenia, systemu operacyjnego i poświadczeń.

Workspace ONE Access dostarcza następujące funkcjonalności:

- Ujednolicony katalog aplikacji. Katalogi aplikacji Workspace ONE Access i Workspace ONE UEM są łączone i prezentowane w przeglądarkowym portalu Workspace ONE lub w aplikacji VMware Workspace ONE Intelligent Hub.
- Bezpieczne aplikacje zwiększające produktywność: VMware Workspace ONE Boxer, Web, Content, Notebook, People, Verify i PIV-D Manager. Użytkownicy końcowi mogą korzystać z dołączonych funkcji poczty, kalendarza, kontaktów, przeglądarki, zawartości, organizacji i uwierzytelniania, a oparte na zasadach bezpieczeństwa środki chronią organizację przed wyciekiem danych, ograniczając sposoby edytowania i udostępniania załączników i plików.
- Mobilne logowanie pojedyncze (SSO). Technologia SSO jest dostępna dla wszystkich obsługiwanych platform. Implementacja opiera się na funkcjach dostarczanych przez podstawowy system operacyjny.
- Uwierzytelnianie wieloskładnikowe. Workspace ONE Access pozwala na integrację z narzędziami dostarczającymi uwierzytelnianie wieloskładnikowe dla użytkowników (MFA).
- Dostęp warunkowy. Każdy proces logowania do Workspace ONE Access podlega regułom dostępu, w których zdefiniowane są warunki jakie użytkownik/urządzenie muszą spełnić, aby uzyskać dostęp do platformy.
- Bezpieczne przeglądanie. Korzystanie z VMware Workspace ONE Web zamiast natywnej przeglądarki lub przeglądarki innej firmy zapewnia, że dostęp do poufnych treści internetowych jest bezpieczny i łatwiejszy w zarządzaniu.
- Zapobieganie utracie danych (DLP). Funkcja wymusza otwieranie dokumentów lub adresów URL tylko w zatwierdzonych aplikacjach, aby zapobiec przypadkowemu lub celowemu rozpowszechnianiu poufnych informacji.
- Typy zasobów. Workspace ONE obsługuje różne aplikacje udostępniane za pośrednictwem katalogów Workspace ONE Access i Workspace ONE UEM, w tym aplikacje SAML oparte na modelu SaaS, aplikacje i pulpity VMware Horizon, wirtualne aplikacje i pulpity Citrix, aplikacje pakowane VMware ThinApp dostarczane za pośrednictwem Workspace ONE Access oraz natywne aplikacje mobilne dostarczane za pośrednictwem Workspace ONE UEM.

HORIZON

VMware Horizon oferuje prostotę, bezpieczeństwo, szybkość i skalowalność w dostarczaniu lokalnych wirtualnych pulpitów i aplikacji z ekonomią chmurową i elastycznością skali, dostarczając poniższe funkcjonalności:

- Just-in-Time (JIT) Delivery. Prostota zarządzania w przygotowaniu w pełni gotowych i odpowiednio skonfigurowanych, personalizowanych przestrzeni roboczych dla użytkowników, z wykorzystaniem kluczowych elementów platformy Horizon:
  - Technologia VMware Instant Clone pozwalająca na tworzenie wirtualnych pulpitów na żądanie w szybki i zautomatyzowany sposób
  - VMware AppVolumes – usługa zapewniająca dostarczanie aplikacji w czasie rzeczywistym
  - VMware Dynamic Environment Manager - odpowiadający za personalizację oraz konfigurację zasad.
- Topologię hybrydową lub multi-cloud . Możliwość konfigurowania i zarządzania wirtualnymi pulpitami oraz aplikacjami w chmurze prywatnej lub chmurach publicznych, m.in. Microsoft Azure, VMware Cloud on AWS, Google Cloud.
- Wsparcie dla różnych systemów operacyjnych. VMware Horizon wspiera możliwość udostępniania wirtualnych pulpitów opartych o systemy Windows oraz Linux.
- Zasady dostępu. Możliwość uproszczenia uwierzytelniania użytkownika we wszystkich usługach pulpitu poprzez wykorzystanie True SSO.
- Optymalizację strumieni Audio/Video – zwiększając komfort pracy użytkownika oraz jego produktywność poprzez wsparcie optymalizacji aplikacji takich jak Microsoft Teams, Zoom oraz Cisco Webex.
- Integrację z innymi produktami Vmware. VMware Horizon zakłada integrację z innymi produktami z portfolio VMware, rozszerzając swoje możliwości np. w kierunku infrastruktury hiperkonwergentnej (vSAN), wirtualizacji sieci (NSX) oraz platform chmury hybrydowej (VMware Cloud Foundation).

Dzięki rozwiązaniom Workspace ONE i Horizon, można efektywnie tworzyć usługi z kilku składników wielokrotnego użytku. To modułowe, powtarzalne podejście do projektowania łączy komponenty i usługi, aby dostosować środowisko użytkownika końcowego bez konieczności stosowania specjalnych konfiguracji dla poszczególnych użytkowników. Powstałe środowisko i usługi można łatwo dostosować do zmian w biznesie i wymagań dotyczących przypadków użycia.

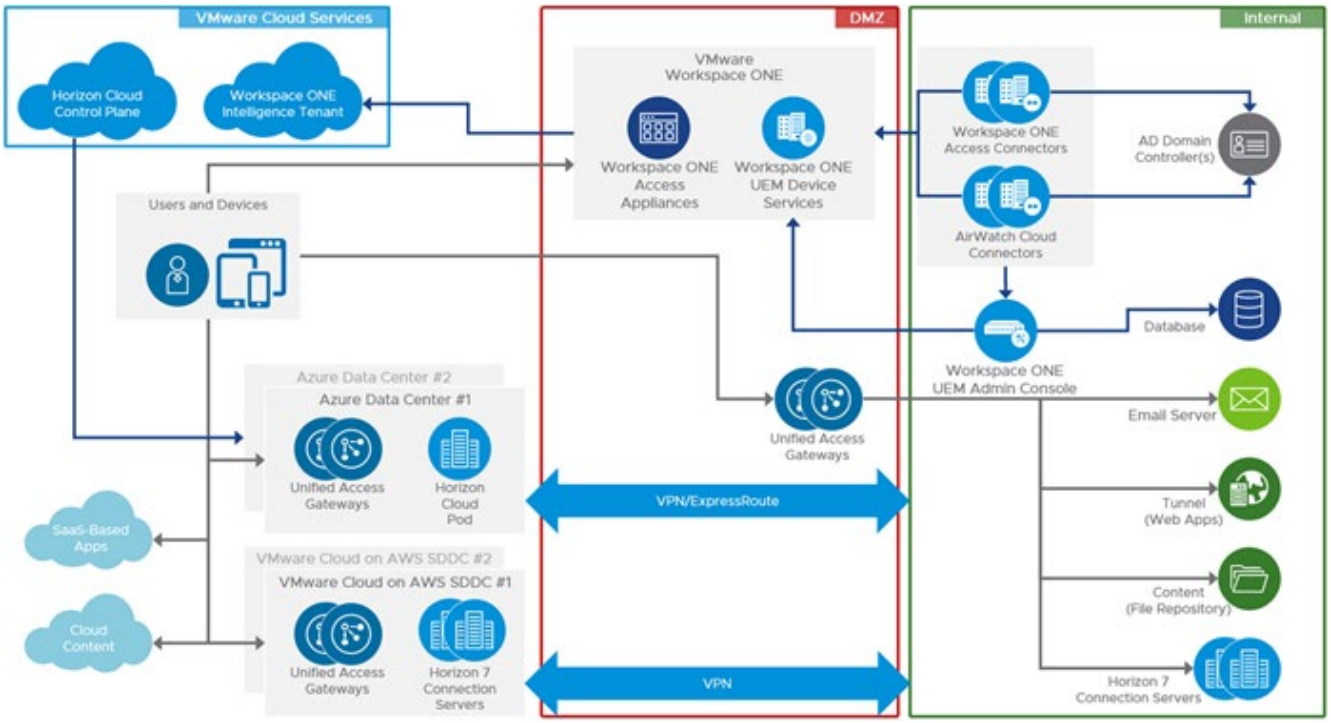
Platforma Workspace ONE oraz Horizon

Platforma Workspace ONE składa się z Workspace ONE Access i Workspace ONE UEM. Chociaż każdy produkt może działać niezależnie, integracja między nimi umożliwia działanie platformy Workspace ONE. Ponadto integrując się z VMware Horizon pozwalają na dostęp użytkowników do wirtualnych pulpitów zlokalizowanych w centrum danych.

Workspace ONE Access i Workspace ONE UEM są podstawowymi składnikami we wdrożeniu Workspace ONE, jednak można wdrożyć wiele innych składników, w zależności od przypadków użycia biznesowego. Na przykład, jak pokazano na rysunku poniżej można użyć VMware Unified Access Gateway aby zapewnić VMware Workspace ONE Tunnel lub dostęp oparty na VPN do zasobów lokalnych.
Architektura logiczna

Dzięki lokalnemu wdrożeniu Workspace ONE zarówno Workspace ONE UEM, jak i Workspace ONE Access są wdrażane w centrach danych. Usługi te mogą być również wdrożone w chmurze publicznej.

- VMware Workspace ONE UEM – składa się z kilku podstawowych komponentów, które można zainstalować na jednym serwerze. Workspace ONE UEM działa jako platforma MDM, MCM i MAM.
- Workspace ONE Access – Działa jako dostawca tożsamości, synchronizując się z Active Directory w celu zapewnienia logowania jednokrotnego w aplikacjach opartych na SAML, aplikacjach i pulpitach opartych na VMware Horizon oraz aplikacjach spakowanych VMware ThinApp. Workspace ONE Access jest również odpowiedzialny za wymuszanie zasad uwierzytelniania opartych na sieciach, aplikacjach lub platformach.



Wiele opcjonalnych składników we wdrożeniu Workspace ONE jest wspólnych zarówno dla wdrożenia chmurowego, jak i lokalnego.

- AirWatch Cloud Connector (ACC). Działa w sieci wewnętrznej, działając jako serwer proxy, który bezpiecznie przesyła żądania z Workspace ONE UEM do krytycznych składników infrastruktury korporacyjnej organizacji. Organizacje mogą korzystać z zalet Workspace ONE UEM, integrującego się z istniejącymi systemami LDAP, urzędem certyfikacji, pocztą e-mail i innymi systemami wewnętrznymi.
- Workspace ONE Access Connector. Umożliwia synchronizację katalogów i uwierzytelnianie między lokalną usługą Active Directory a usługą Workspace ONE Access.
- VMware Unified Access Gateway. Zapewnia bezpieczne usługi brzegowe i umożliwia zewnętrzny dostęp do zasobów wewnętrznych.

Zarówno Horizon, jak i Horizon Cloud Service można połączyć i zintegrować z wdrożeniem Workspace ONE, niezależnie od tego, czy jest to wdrożenie lokalne czy chmurowe. Zintegrowana platforma Horizon pozwala na bezpieczne połączenie użytkowników do wirtualnego pulpitu i zasobów wewnętrznych organizacji.

Najczęściej zadawane pytania

Czym jest VDI?

Virtual Desktop Infrastructure (VDI) to technologia, która pozwala na hostowanie wielu sesji wirtualnych pulpitów na serwerach fizycznych, oraz udostępnianie zdalnego dostępu użytkowników do tych pulpitów z różnych urządzeń i lokalizacji. VDI może być wykorzystywane jako alternatywa dla tradycyjnej infrastruktury (gdzie wykorzystywane są rzeczywiste fizyczne komputery stacjonarne).

Co to jest VMware Horizon i kiedy można go używać?

Horizon to rozwiązanie stworzone do wdrażania infrastruktury pulpitów wirtualnych. VMware Horizon zapewnia użytkownikom końcowym wirtualne pulpity i aplikacje dostępne za pośrednictwem jednej platformy.

VMware Horizon bazuje na VMware vSphere i wykorzystuje środowisko vSphere do hostowania wirtualnych pulpitów. Pulpity użytkowników to maszyny wirtualne działające na hostach ESXi, dlatego dostępne są funkcje vSphere, takie jak migawki, vMotion, High Availability, Distributed Resource Scheduler i inne. Rozwiązanie VMware Horizon VDI zapewnia większą elastyczność i bezpieczeństwo niż usługi terminalowe. Wirtualne pulpity pracują jako tymczasowe, a po wylogowaniu zostają usunięte i powołane przy połączeniu nowej sesji, a dane zgromadzone podczas sesji są zapisywane na udziałach sieciowych. Użytkownicy mogą łączyć się z wirtualnymi pulpitami za pośrednictwem komputerów osobistych (PC), tabletów PC, smartfonów.

Jakie korzyści może uzyskać organizacja dzięki VMware Horizon?

VMware Horizon zapewnia ujednoliconą cyfrową przestrzeń roboczą dzięki wydajnemu dostarczaniu wirtualnych pulpitów i aplikacji, które zapewniają pracownikom środowisko pracy w dowolnym miejscu, o każdej porze i na dowolnym urządzeniu. Dzięki głębokiej integracji z ekosystemem technologii VMware, platforma oferuje sprawną podstawę gotową do pracy w chmurze, nowoczesne, najlepsze w swojej klasie zarządzanie oraz kompleksowe zabezpieczenia, które wzmacniają dzisiejsze Anywhere Workspace.

Jakie opcje wdrażania są dostępne dla Horizon?

VMware Horizon można wdrożyć w następujących środowiskach:

- Wdrażanie lokalne - VMware Horizon można wdrożyć w infrastrukturze lokalnej lub w chmurze prywatnej. Istnieje możliwość użycia licencji wieczystej do wdrożenia lokalnego lub opcjonalnie zakupu licencji subskrypcyjnej Horizon, która zapewni dostęp do płaszczyzny kontroli Horizon i powiązanych usług.
- Wdrożenie hostowane w chmurze - VMware Horizon można wdrożyć w chmurze publicznej, takiej jak VMware Cloud on AWS lub Azure VMware Solutions. Do wdrożenia w chmurze publicznej wymagane jest użycie licencji subskrypcyjnej.
- Wdrożenie hybrydowe - wdrożenia VMware Horizon zarówno lokalnie, jak i w środowiskach hostowanych w chmurze.

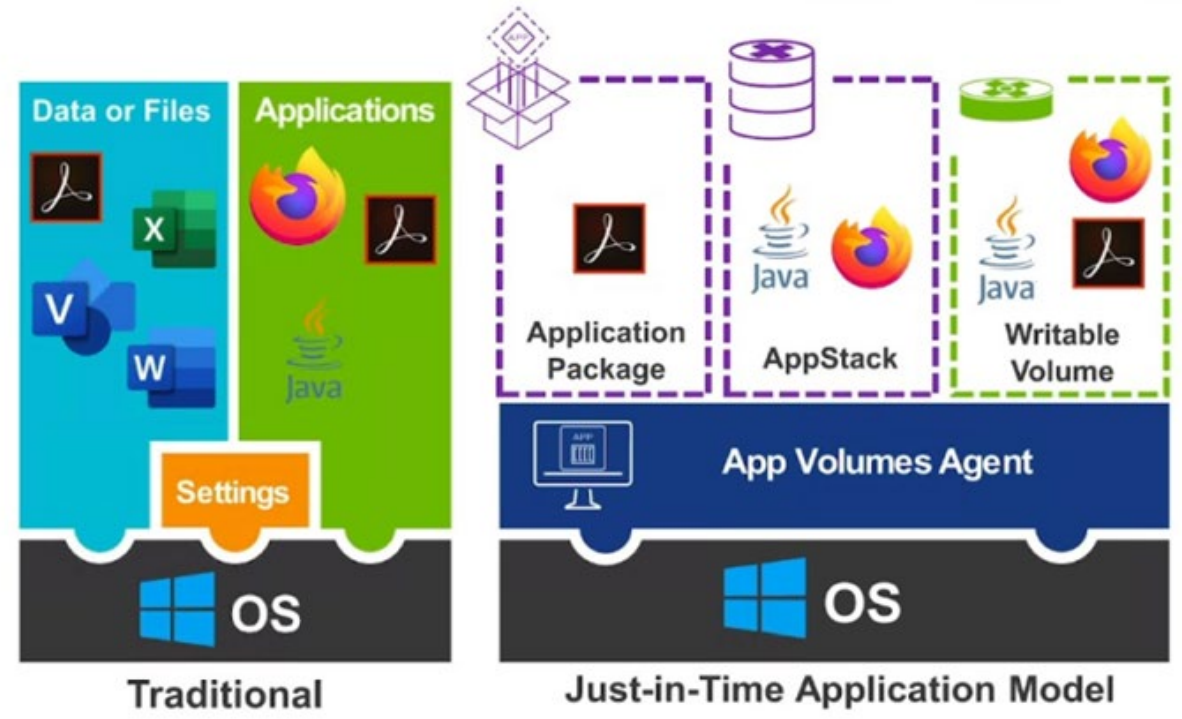
Czym jest technologia Instant Clones?

Instant Clone to technologia klonowania oparta na vSphere, która służy do udostępniania tysięcy nietrwałych wirtualnych pulpitów z jednego obrazu wzorcowego. Dzięki technologii Instant Clone uruchomiona nadrzędna maszyna wirtualna może zostać zatrzymana i „sklonowana na gorąco”, aby szybko utworzyć

podrzędne maszyny wirtualne. Wykorzystując ten sam dysk i pamięć nadrzędnej maszyny wirtualnej, klon startuje w już uruchomionym stanie. Ten proces omija wielokrotne cykle zasilania i wywołania rekonfiguracji wykonane przy użyciu tradycyjnego klonowania. Łącząc technologię Instant Clone z VMware App Volumes i Dynamic Environment Manager, uzyskujemy desktopy, które zachowują personalizację użytkownika z sesji na sesję, a jednocześnie mogą być szybko udostępniane, nawet jeśli pulpit jest niszczony po wylogowaniu użytkownika.

Co to jest VMware App Volumes ?

VMware App Volumes to zintegrowany i ujednolicony system dostarczania aplikacji i zarządzania użytkownikami dla VMware Horizon i innych środowisk wirtualnych.



Co to jest VMware Dynamic Environment Manager (VMware DEM)?

VMware Dynamic Environment Manager oferuje personalizację i dynamiczną konfigurację zasad w dowolnym środowisku wirtualnym, fizycznym i chmurowym. Zapewnia dynamiczną konfigurację środowiska, taką jak mapowanie dysków lub drukarek, gdy użytkownik uruchamia aplikację.

Czym jest Blast Extreme?

Blast Extreme to protokół wyświetlania stworzony przez VMware, aby zapewnić bogate w funkcje doświadczenie użytkownikom końcowym na różnych urządzeniach, lokalizacjach, mediach i połączeniach sieciowych.

Blast Extreme zapewnia:

- dostęp do swoich spersonalizowanych wirtualnych pulpitów lub aplikacji zdalnych z firmowego laptopa, komputera domowego, tabletu lub smartfona;
- spójne środowisko użytkownika na różnych urządzeniach i lokalizacjach przy zachowaniu zgodności danych firmowych i bezpiecznego przechowywania w centrum danych;

- możliwość spełnienia wymagań wydajnościowych dla wymagających wizualnie aplikacji w przypadku korzystania z akceleracji sprzętowej opartej na procesorze graficznym NVIDIA Tesla na hoście;
- szeroką obsługę klientów, w tym klientów Windows, Linux, macOS, Android, iOS, Chrome i internetowych (dostęp HTML);
- możliwość korzystania z transportu sieciowego TCP lub UDP.

Czy VMware Horizon obsługuje SSO?

Pojedyncze logowanie (SSO) umożliwia użytkownikowi używanie jednego zestawu poświadczeń logowania do uwierzytelniania i uzyskiwania dostępu do różnych aplikacji. W ramach VMware Workspace ONE Access użytkownicy końcowi mogą używać SSO do uzyskiwania dostępu do aplikacji internetowych i SaaS za pośrednictwem przeglądarki Intelligent Hub lub katalogu aplikacji Workspace ONE. Ponadto True SSO, funkcja Horizon, usprawnia logowanie do wirtualnych pulpitów i aplikacji. Użytkownicy końcowi omijają Active Directory za pomocą automatycznie generowanego krótkotrwałego certyfikatu.

Czy VDI VMware Horizon jest w stanie sprostać wymaganiom graficznym projektantów, inżynierów i naukowców?

Tak, VMware wspólnie z firmą NVIDIA dostarcza technologię sprzętowej akceleracji grafiki.

Przeniesienie sprzętu do akceleracji grafiki ze stacji roboczej na serwer to kluczowa innowacja architektoniczna. Ta zmiana zmienia metaforę obliczeniową przetwarzania grafiki, udostępniając użytkownikowi dodatkowe zalety centrum danych w zakresie mocy obliczeniowej, pamięci, sieci i bezpieczeństwa, dzięki czemu można uzyskać dostęp do złożonych modeli i bardzo dużych zestawów danych. Dzięki odpowiedniej przepustowości sieci i odpowiednim zdalnym urządzeniom klienckim, IT może teraz zaoferować najbardziej zaawansowanym użytkownikom akcelerację grafiki 3D.

Oprócz obsługi najbardziej wymagających obciążeń graficznych akceleracja sprzętowa może również zmniejszyć użycie procesora w przypadku mniej wymagającego użycia podstawowego pulpitu lub opublikowanych aplikacji oraz kodowania lub dekodowania wideo, które obejmuje domyślny protokół zdalnego wyświetlania Blast Extreme.

Jak jest licencjonowany VMware Horizon?

Horizon jest dostępny w dwóch modelach licencji:

- Nazwany użytkownik (NU),
- Użytkownik równoczesnego połączenia (CCU).

Jakie opcje licencjonowania są dostępne dla Horizon?

VMware Horizon jest dostępny w kilku wariantach w zależności od funkcjonalności i komponentów zawartych w licencji:

- Horizon Standard
- Horizon Advanced
- Horizon Enterprise
- Horizon Apps Standard
- Horizon Apps Advanced

Które elementy zestawu Horizon można kupić osobno?

Jako licencję samodzielną można zakupić następujące elementy: ThinApp, App Volumes, Dynamic Environment Manager, vSphere for Desktop i Horizon for Linux.

W jaki sposób Workspace ONE sprawdza poprawność konfiguracji urządzenia końcowego, tożsamości użytkownika i zabezpieczeń połączenia aplikacji przed zezwoleniem na dostęp?

Zero Trust to model warunkowej kontroli dostępu, który wymaga weryfikacji zaufania przed zezwoleniem na dostęp do aplikacji, a po przyznaniu tego dostępu ma on najmniejsze uprawnienia. Zasada najmniejszego uprzywilejowania oznacza przyznanie tylko wymaganego dostępu do aplikacji, aby użytkownik miał możliwość wykonać swoją pracę i nic więcej. Zero Trust chroni dane i aplikacje nie tylko na początku sesji, ale także poprzez ciągłą weryfikację użytkowników i urządzeń końcowych w trakcie sesji aplikacji.

Jakie są wymagania architektury Zero Trust?

- Ciągła weryfikacja zgodności punktów końcowych — aby dostęp został przyznany, punkty końcowe muszą być stale weryfikowane pod kątem zgodności z zasadami zabezpieczeń organizacji.
- Warunkowa kontrola dostępu do wszystkich aplikacji — aby użytkownik uzyskał dostęp do aplikacji, musi udowodnić swoją tożsamość.
- Zmniejszenie powierzchni ataku — aby chronić aplikacje i dane organizacji, każdy użytkownik musi mieć przyznany dostęp z najniższymi wymaganymi uprawnieniami.

W jaki sposób Workspace ONE zabezpiecza dostęp do danych firmowych z urządzeń mobilnych?

Niektóre funkcje zabezpieczeń Workspace ONE obejmują:

- Szyfrowanie - uwierzytelnianie i szyfrowanie ruchu z aplikacji na urządzeniach do centrum danych. Zabezpieczanie danych aplikacji w spoczynku i w tranzycie dzięki 256-bitowemu szyfrowaniu AES.
- Zarządzanie dostępem - dostarczanie obsługi administracyjnej aplikacji, katalogu samoobsługowego, uwierzytelniania wieloskładnikowego i logowania pojedynczego (SSO) dla wszystkich aplikacji.
- Zasady kontekstowe — kontrola uwierzytelniania za pomocą zasad dostępu warunkowego na podstawie stanu zgodności urządzenia, siły uwierzytelniania użytkowników, wrażliwości danych, lokalizacji użytkownika i innych.
- Zasady zapobiegania utracie danych (DLP) — konfiguracja zasad z nowoczesnym zarządzaniem, w tym szyfrowaniem danych na poziomie urządzenia, blokowaniem aplikacji i zabezpieczeniami sieci Wi-Fi.

W jaki sposób Workspace ONE UEM zapewnia zapobieganie utracie danych (DLP) na różnych typach urządzeń i systemach operacyjnych?

Aplikacje zbudowane przy użyciu zestawu Workspace ONE SDK lub przygotowane w Workspace ONE UEM można zintegrować z ustawieniami zestawu SDK w konsoli Workspace ONE UEM w celu stosowania zasad, kontrolowania zabezpieczeń i zachowania użytkowników oraz pobierania danych dla określonych aplikacji mobilnych bez zmieniania samej aplikacji.

Czy Workspace ONE UEM obsługuje uwierzytelnianie wieloskładnikowe (MFA)?

Tak, jest możliwość użycia wbudowanego uwierzytelniania wieloskładnikowego dla Workspace ONE UEM poprzez włączenie funkcji VMware Verify w konsoli Workspace ONE Access.

Workspace ONE integruje się również z dostawcami uwierzytelniania wieloskładnikowego, aby zapewnić szereg funkcji mobilnej usługi MFA, w tym powiadomienia push, kod TOTP i SMS. Rozwiązanie obsługuje uwierzytelnianie wieloskładnikowe za pośrednictwem Okta Verify, Duo, PingID, RADIUS, RSA SecurID i RSA SecurID Access oraz uwierzytelnianie oparte na certyfikatach.

W jaki sposób Workspace ONE UEM grupuje urządzenia i użytkowników na potrzeby zarządzania i przypisania?

Workspace ONE UEM używa kilku różnych typów grup do zarządzania użytkownikami, urządzeniami, aplikacjami, zawartością i nie tylko. Strategię ujednoliconego zarządzania punktami końcowymi można zoptymalizować, korzystając z kombinacji grup organizacyjnych, grup inteligentnych i grup użytkowników w celu usprawnienia przypisywania i zarządzania.

Czy Workspace ONE UEM może wymusić zatwierdzoną wersję oprogramowania na urządzeniu przed przyznaniem dostępu użytkownikowi?

Tak, można ustawić ograniczenia, aby wymagać zatwierdzonych wersji systemu operacyjnego oraz aplikacji przed udzieleniem urządzeniom dostępu do danych wewnętrznych w organizacji.

Czy Workspace ONE UEM może wykonać zdalne czyszczenie urządzenia?

Tak, w konsoli administracyjnej Workspace ONE UEM można wykonać zdalne czyszczenie na żądanie lub na podstawie zasad zgodności. Administratorzy mogą dołączyć notatkę dla użytkowników podczas czyszczenia urządzenia.

Istnieją główne opcje:

- Enterprise Wipe - usuwa wszystkie połączenia firmowe, aplikacje i zawartość. Workspace ONE Intelligent Hub pozostaje na urządzeniu w celu łatwej ponownej rejestracji.
- Full Wipe - urządzenia powoduje „przywrócenie ustawień fabrycznych" w celu usunięcia wszystkich danych urządzenia (dostępne tylko na żądanie). Workspace ONE Intelligent Hub nie jest już na urządzeniu.
- Enterprise Reset — resetowanie w przedsiębiorstwie przywraca urządzenie do stanu gotowości do pracy, gdy urządzenie jest uszkodzone lub ma nieprawidłowo działające aplikacje. Ponownie instaluje system operacyjny Windows, zachowując dane użytkowników, konta użytkowników i zarządzane aplikacje. Urządzenie ponownie zsynchronizuje automatycznie wdrożone ustawienia, zasady i aplikacje przedsiębiorstwa po zresetowaniu, pozostając zarządzane przez Workspace ONE.

Jak wygląda integracja Workspace ONE UEM z innymi systemami Enterprise w organizacji?

Wiele istniejących składników przedsiębiorstwa można zintegrować z wdrożeniem Workspace ONE. Na przykład można bezpiecznie zintegrować z usługą AD/LDAP, urzędami certyfikacji, pocztą e-mail i innymi systemami przedsiębiorstwa zarówno w modelu wdrażania w chmurze, jak i lokalnie.

Z poziomu konsoli administracyjnej Workspace ONE UEM można skonfigurować następujące składniki:

- Usługi katalogowe — integracja z usługą AD/LDAP w celu uwierzytelniania i członkostwa w grupach, co pomaga zapewnić użytkownikom odpowiednie profile oraz dostęp do aplikacji i zawartości.
- Certyfikaty i infrastruktura PKI — integracja z dostawcami usług certyfikatów Microsoft CA, CA lub SCEP, takimi jak MSCEP i VeriSign.
- Infrastruktura poczty e-mail.
- Proxy – Microsoft Exchange 2010/2013/2016/2019, IBM Domino z Lotus Notes, Novell GroupWise (z EAS), Google Apps for Work Beehive
- PowerShell — Exchange 2010/2013/2016/2019, Office 365/BPOS.
- Google – Google Apps dla Firm.
- Usługi UEM Edge Services na VMware Unified Access Gateway umożliwiające bezpieczny zdalny dostęp z sieci zewnętrznej do różnych zasobów wewnętrznych. Unified Access Gateway obsługuje następujące przypadki użycia Workspace ONE UEM:
- Tunelowanie aplikacji natywnych i internetowych na platformach mobilnych i stacjonarnych w celu zabezpieczenia dostępu do zasobów wewnętrznych za pośrednictwem usługi VMware Tunnel.
- Lokalna infrastruktura poczty e-mail, która udziela dostępu tylko autoryzowanym urządzeniom, użytkownikom i aplikacjom poczty e-mail na podstawie zarządzanych zasad. Ta funkcja wykorzystuje usługę Secure Email Gateway zintegrowaną z Workspace ONE UEM.
- Odwrotne proxy aplikacji internetowych.
- Mostkowanie tożsamości na potrzeby uwierzytelniania w starszych aplikacjach lokalnych, które używają protokołu Kerberos lub uwierzytelniania opartego na nagłówku.

Czy mogę zintegrować interfejsy API REST Workspace ONE UEM z istniejącą infrastrukturą i aplikacjami innych firm?

Tak. Workspace ONE UEM zawiera zbiór interfejsów API, które umożliwiają programom zewnętrznym korzystanie z podstawowych funkcji produktu poprzez integrację interfejsów API z istniejącą infrastrukturą IT i aplikacjami innych firm.

Czy Workspace ONE UEM obsługuje ręczne tworzenie użytkowników?

Tak, jeśli Workspace ONE UEM nie zostanie zintegrowany z usługami katalogowymi, można ręcznie dodać podstawowe konta użytkowników. Są one przydatne do testowania, mogą być też używane w przypadku dowolnej metody wdrażania i nie wymagają infrastruktury przedsiębiorstwa.

Czy Workspace ONE zawiera wbudowane funkcje raportowania?

Tak, Workspace ONE zawiera niezawodne funkcje raportowania, które umożliwiają administratorom centralne monitorowanie flot urządzeń przy użyciu następujących metod:

- Wbudowane raporty Workspace ONE UEM.
- Raporty Workspace ONE Intelligence
- Interaktywne pulpity nawigacyjne Workspace ONE Intelligence.
- Workspace ONE Access User Engagement Dashboard.

W jaki sposób Workspace ONE UEM realizowana jest kontrola dostępu administratorów platformy na podstawie ról?

Role wbudowane i niestandardowe definiują grupy urządzeń, do których administrator IT może uzyskiwać dostęp i którymi może zarządzać, oraz ograniczają szczegółowość informacji i funkcji zarządzania urządzeniami dostępnymi dla każdego użytkownika konsoli, np.: udzielenie ograniczonego dostępu w konsoli administratorom pomocy technicznej i przyznanie większego zakresu uprawnień menedżerowi IT.
Ponad 1 000 unikatowych uprawnień zabezpieczeń pozwala zdefiniować role niestandardowe, dzięki czemu można ustawić uprawnienia tylko do odczytu, zapisu lub aktualizowania systemu.

Czy Workspace ONE obsługuje RBAC administratora dla funkcji takich jak odzyskiwanie kluczy funkcji BitLocker, dystrybucja aplikacji i polecenia zdalne?

Tak. Portal administracyjny Workspace ONE UEM używa kontroli dostępu opartej na rolach (RBAC), aby wyświetlać administratorom tylko wstępnie zatwierdzone urządzenia/użytkowników/informacje. Na przykład administratorzy pomocy technicznej w przedsiębiorstwie mogą mieć ograniczony dostęp w konsoli, podczas gdy menedżer IT ma większy zakres uprawnień.

Czy Workspace ONE UEM obsługuje zasady GPO dla systemu Windows 10?

Tak. Można utworzyć zasady GPO dla systemu Windows 10 w konsoli Workspace ONE UEM, tworząc odpowiedni profil natywny. Administratorzy mogą również używać niestandardowych zasad GPO lub CIS. LGPO.exe musi znajdować się we właściwym miejscu, aby można było zastosować plany bazowe.

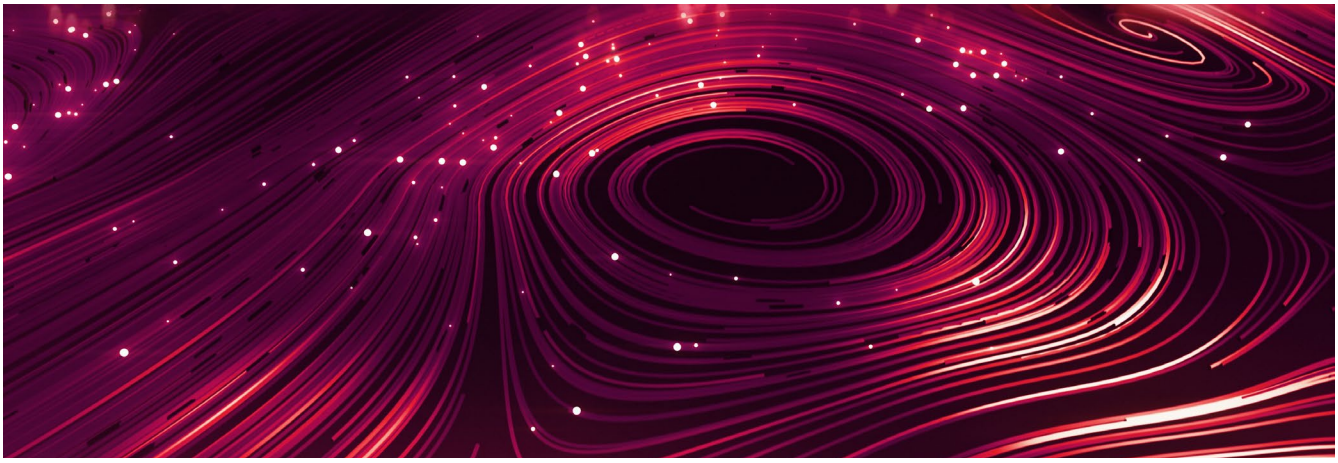
Jakie typy plików Windows mogą być dystrybuowane za pośrednictwem Workspace ONE UEM?

Workspace ONE UEM obsługuje dostarczanie pakietów MSI, EXE i ZIP do urządzeń. Dzięki skryptom i czujnikom skrypty programu PowerShell mogą wysyłać zapytania o atrybuty na urządzeniu lub uruchamiać skrypty.

Czy Workspace ONE UEM może zarządzać zarówno zabezpieczeniami urządzeń, jak i dostępem do aplikacji?

Tak. W przypadku aplikacji Workspace ONE Intelligent Hub dla systemu Windows są zapewnione ujednolicone powiadomienia, stany instalacji aplikacji i pełne ujednolicone środowisko katalogu aplikacji w Internecie, systemie Windows 10, macOS, na telefonie iPhone i iPad oraz na platformach Android dla wszystkich użytkowników. Workspace ONE może również wymuszać listy dozwolonych i niedozwolonych aplikacji dla wszystkich platform.

VMware Workspace Security zapewnia najbardziej zaawansowane zabezpieczenia urządzeń końcowych w połączeniu z ich zintegrowanymi analizami i analizą aplikacji. Ta integracja rozwiązania wykorzystuje głęboką telemetrię punktów końcowych i alerty o podejrzanym lub złośliwym zachowaniu z Carbon Black oraz koreluje te dane z innymi natywnymi i zewnętrznymi źródłami danych Workspace ONE.



W jaki sposób Workspace ONE UEM obsługuje wdrażanie poprawek systemu Windows na dużej flocie urządzeń?

Workspace ONE UEM pozwala na utworzenie profilu z konfiguracją usługi Windows Update, aby stosować aktualizacje automatyczne lub na żądanie dla grup urządzeń.

Workspace ONE UEM wykorzystuje nowoczesne, oparte na chmurze podejście do zarządzania poprawkami systemu Windows. Usługa Zarządzanie usługą Windows Update przy użyciu programu Workspace ONE dostarcza aktualizacje często i dynamicznie. Dzięki temu użytkownicy końcowi zawsze mają dostęp do aktualnych funkcji systemu operacyjnego.

W jaki sposób Workspace ONE UEM ustawia zasady konfiguracji i zarządza nimi na urządzeniach z systemem Windows?

Workspace ONE UEM łączy w sobie najlepsze zestawy narzędzi do zarządzania tradycyjnego (PCLM) i EMM (MDM), aby zapewnić zasady konfiguracji dla urządzeń z systemem Windows. Workspace ONE może oddzielać zasady według własności urządzenia, co oznacza, że gdy urządzenie jest rozwijane, dane użytkownika pozostają nienaruszone.

Zasady są dostarczane na dwa sposoby:

- Workspace ONE UEM Baselines - Korzystanie z zasad GPO zabezpieczeń systemu Microsoft Windows 10 lub CIS Microsoft Windows Desktop Benchmark albo niestandardowych GPO opartych na kopii zapasowej obiektu zasad grupy.
- Zasady MDM lub dostawcy usług konfiguracji (CSP) — ten mechanizm jest natywnie wbudowany w system operacyjny i stosowany za pośrednictwem istniejących profili systemu Windows 10 lub przy użyciu profilu ustawień niestandardowych.

Czy komputery z systemem Windows 10 muszą być przyłączone do domeny lokalnej, aby otrzymywać aktualizacje zasad?

Tradycyjne narzędzia do zarządzania cyklem życia komputera wymagają, aby urządzenia z systemem Windows 10 były przyłączone do domeny znajdującej się w organizacji lokalnie, aby zasady grupy i ustawienia zabezpieczeń były stosowane. Jeśli użytkownicy pracują zdalnie, zazwyczaj używa się sieci VPN do uzyskiwania komunikacji z kontrolerem domeny w celu zaktualizowania tych ustawień zasad grupy. Dzięki Workspace ONE Baselines urządzenia z systemem Windows 10 mogą być członkami domeny, grupy roboczej, a nawet usługi Azure AD, eliminując złożone wymagania dotyczące narzędzi PCLM.

Korzyści jakie płyną z tego rozwiązania to:

- Brak gpupdate /force
- VPN nie jest wymagany
- Wyniki zapytań uzyskiwane „w locie”.

Dzięki nowoczesnemu zarządzaniu wszystkie urządzenia potrzebują połączenia z Internetem, aby ponownie zameldować się na serwerze Workspace ONE UEM. Zasady zgodności można ustawić, aby zapewnić meldowanie urządzeń w określonych odstępach czasu. Jeśli urządzenie nie zaewidencjonuje się ponownie w określonych odstępach czasu, można podjąć kroki naprawcze.

Czy użytkownik końcowy może wykonać odzyskiwanie klucza szyfrowania (na przykład funkcją BitLocker)?

Użytkownicy końcowi mogą zalogować się do portalu samoobsługowego w celu pobrania klucza odzyskiwania usługi BitLocker. Tę funkcję można wyłączyć za pomocą RBAC dla klientów portalu samoobsługowego. W przypadku korzystania z szyfrowania funkcją BitLocker z Workspace ONE należy skonfigurować samoobsługowy adres URL podczas uruchamiania systemu Windows w funkcji odzyskiwania funkcji BitLocker.

W jaki sposób Workspace ONE wykorzystuje nowoczesne zarządzanie systemem Windows 10?

Workspace ONE łączy w sobie kompletne, oparte na chmurze, nowoczesne zarządzanie systemem Windows 10 z inteligentną automatyzacją, aby wzmocnić pozycję użytkowników, wzmocnić zabezpieczenia i uprościć procesy w organizacji. Workspace ONE współistnieje również z tradycyjnymi narzędziami do zarządzania klientami.

Workspace ONE wykorzystuje bazujący na EMM projekt systemu Windows 10, aby umożliwić skoncentrowaną na mobilności strategię zarządzania. Rozwiązanie współpracuje z wbudowanymi narzędziami systemu Windows 10, aby usprawnić cykl życia urządzenia, dostarczanie aplikacji i kompleksowe zabezpieczenia w celu zarządzania urządzeniami.

W jaki sposób Workspace ONE obsługuje urządzenia z systemem Windows 10, które nie są przyłączone do domeny lub nie należą do organizacji?

Jeśli urządzenie z systemem Windows 10 jest zarządzane przez inne narzędzie do zarządzania lub urządzenie nie jest własnością organizacji, użytkownicy mają dwie opcje:

- Rejestracja w BYOD — jeśli urządzenie jest własnością prywatną, użytkownik może pobrać i zainstalować IntelilgentHub dla systemu Windows 10, odwiedzając stronę getwsone.com i rejestrując się. Workspace ONE ma solidną kontrolę prywatności, aby zapewnić, że dane osobowe pozostają na urządzeniu podczas offboardingu, a wszelkie zasady lub aplikacje mogą być stosowane dla BYOD lub urządzeń należących do firmy.
- Przypadek użycia określany jako Kontrahent, który oznacza, że urządzenie kontrahenta może być nadal zarządzane przez inny system, ale użytkownik końcowy może uzyskać dostęp do zasobów oraz pojedynczego logowania do web-aplikacji, aplikacji wirtualnych i wirtualnych desktopów za pośrednictwem Internetu.

W jaki sposób Workspace ONE wymusza warunkowy dostęp do aplikacji i zasobów na podstawie kondycji urządzenia końcowego i sieci?

Workspace ONE UEM umożliwia administratorom definiowanie „zgodnego” stanu urządzenia i ocenę zgodności na podstawie jednego z najbardziej niezawodnych zestawów punktów danych. Workspace ONE Access może wykorzystać telemetrię urządzeń z Workspace ONE UEM do agregowania danych o zachowaniu urządzeń, aplikacji i użytkowników z wielu źródeł wewnętrznych i zewnętrznych. Workspace ONE Intelligence wykorzystuje modele uczenia maszynowego do obliczania oceny ryzyka użytkownika i włączania dostępu warunkowego na podstawie kontekstu urządzenia, ryzyka logowania i zachowania użytkownika.

Jakie platformy i typy aplikacji obsługuje Workspace ONE UEM?

W poniższej tabeli przedstawiono typy aplikacji i obsługiwane platformy systemu operacyjnego.

Typ aplikacji	Android	ChromeOS	macOS	iOS	tvOS	Windows 10
Aplikacje wewnętrzne	✔		✔	✔	✔	✔
Aplikacje publiczne (bezpłatne i płatne przez użytkownika)	✔	✔		✔		✔
Aplikacje zakupione zbiorczo (VPP)			✔	✔	✔	
Aplikacje niestandardowe (B2B oparte na Sklepie)				✔		
Łącza internetowe	✔		✔	✔		✔
Aplikacje SaaS z uwierzytelnianiem federacyjnym	✔	✔	✔	✔		✔

Źródło:
https://techzone.vmware.com/

vmware® Principal Partner
Data Center Virtualization

vmware® Principal Partner
Network and Security

Chcesz dowiedzieć się jeszcze więcej – skontaktuj się z nami!

Comtegra S.A.
Ul. Puławska 474, 02-884 Warszawa
tel.: +48 22 311 18 00
info@comtegra.pl
www.comtegra.pl

Partner publikacji

vmware®