VMWARE WORKSPACE ONE TRUST NETWORK

Bezpieczeństwo cyfrowego miejsca pracy podlegającego ciągłym przemianom

PODSTAWOWE INFORMACJE

VMware Workspace ONE™ Trust Network™ zapewnia organizacjom kompleksowe i nowoczesne podejście do bezpieczeństwa korporacyjnego, zabezpieczając pracowników, aplikacje, urządzenia końcowe i sieci. Dzięki funkcjom wykrywania i usuwania zagrożeń oraz ochrony przed nimi rozszerza wbudowane funkcje zabezpieczające opartej na analizie biznesowej platformy Workspace ONE o bogaty ekosystem zintegrowanych rozwiązań partnerskich. Umożliwiają one ciągłe monitorowanie ryzyka i szybkie łagodzenie zagrożeń w całym cyfrowym miejscu pracy.

GŁÓWNE KORZYŚCI

Workspace ONE Trust Network upraszcza zabezpieczanie i zarządzanie przez zastosowanie infrastruktury opartej na zaufaniu i weryfikacji. Dzięki Workspace ONE Trust Network pracownicy działów IT mogą:

- zlikwidować silosy rozwiązań zabezpieczeń za pomocą infrastruktury opartej na działaniach, która zapewnia zagregowany widok danych i redukuje złożoność w obrębie cyfrowego miejsca pracy;
- w unikatowy sposób łączyć zabezpieczenia dostępu, urządzeń i aplikacji oraz zarządzanie nimi z analizą i automatyzacją, by usuwać zagrożenia w ekosystemie rozwiązań klasy End-User Computing;
- korzystać z otwartej i zaufanej sieci partnerów oraz kontynuować eksploatację istniejących inwestycji, by obniżyć koszty.

Zabezpieczenie — największa bariera nowoczesnej strategii cyfrowego miejsca pracy

Cyfrowe miejsce pracy może 5-krotnie[1] zwiększyć wydajność pracowników, pozwalając na prosty i zabezpieczony dostęp do aplikacji i danych na wybranym urządzeniu. W miarę jak organizacja podąża drogą cyfrowej transformacji biznesu, ekosystem cyfrowego miejsca pracy obejmujący pracowników, aplikacje, urządzenia końcowe i sieci ciągle się rozrasta i wykracza poza tradycyjne granice. Ten efekt wzmacniają popularne trendy, takie jak model BYOD i konsumeryzacja infrastruktury IT. Wraz z zanikaniem tradycyjnych granic zaczynają pojawiać się zaawansowane zagrożenia cybernetyczne, takie jak ataki typu „zero day" i „Man-in-the-Middle" (MiTM), wyłudzanie informacji, boty i oprogramowanie wymuszające okup.

Zapewnienie bezpieczeństwa to najwyższy priorytet w przypadku inwestycji w obszarze mobilności i cyfrowego miejsca pracy[2]. Istniejące narzędzia zabezpieczeń zapewniają jednak działom IT tylko ograniczony wgląd w dane, koncentrując się wyłącznie na silosach zabezpieczeń oferujących zbiór funkcji starszego typu. W efekcie powoduje to przyjęcie podejścia polegającego na punktowym usuwaniu problemów, które z powodu złożoności i wymogów zadań wykonywanych ręcznie w celu zabezpieczenia cyfrowego miejsca pracy pociąga za sobą wysokie koszty dla organizacji. Bezpieczeństwo staje się zatem największą barierą stojącą przed nowoczesną strategią cyfrowego miejsca pracy.

Kompleksowe i predykcyjne zabezpieczenia w organizacji bez granic

Zaspokojenie potrzeb w zakresie zabezpieczeń bez pogarszania komfortu użytkowania wiąże się z koniecznością spełnienia nowego zestawu wymogów:

1. Aby uzyskać zagregowany widok danych, organizacje potrzebują infrastruktury, która ustanowi relacje zaufania między elementami zabezpieczającymi ekosystem.
2. Aby stale ograniczać czynniki ryzyka, organizacje muszą być w stanie pozyskiwać informacje ze środowiska w celu podejmowania predykcyjnych i zautomatyzowanych decyzji w zakresie zabezpieczenia cyfrowego miejsca pracy.

Workspace ONE Trust Network zapewnia organizacjom kompleksowe i nowoczesne podejście do bezpieczeństwa korporacyjnego, zabezpieczając pracowników, aplikacje, urządzenia końcowe i sieci. Oferuje zestaw funkcji do wykrywania i usuwania zagrożeń w zmieniającym się cyfrowym miejscu pracy oraz zapewniania jego ochrony, opierając się na infrastrukturze zaufania i weryfikacji. Efektem ustanowienia relacji zaufania w cyfrowym miejscu pracy jest połączony system o najniższym poziomie uprzywilejowania, który zwiększa możliwości pracowników dzięki zabezpieczeniom, które podążają ich śladem. W celu zarządzania ryzykiem związanym z nowoczesnymi zagrożeniami cybernetycznymi rozwiązanie Workspace ONE Trust Network łączy dane z opartej na analizie biznesowej platformy Workspace ONE z zaufanymi partnerskimi rozwiązaniami bezpieczeństwa. Dzięki temu może dostarczać predykcyjne i zautomatyzowane zabezpieczenia w cyfrowym miejscu pracy.

1 Źródło: https://www.vmware.com/radius/impact-digital-workforce/

2 CCS Insights Mobile Technology Buyer Survey, grudzień 2017 r.

Ochrona, wykrywanie i usuwanie problemów

To, kiedy organizacja padnie ofiarą cyberataku, jest jedynie kwestią czasu. Mając tego świadomość, zespoły ds. operacji IT i bezpieczeństwa mogą zarządzać zagrożeniami cybernetycznymi przez uproszczenie odwzorowania funkcji zabezpieczeń, na przykład przy użyciu infrastruktury, takiej jak NIST Cybersecurity Framework, do funkcji obsługiwanych przez rozwiązanie Workspace ONE Trust Network:

- Funkcje zabezpieczeń rozpoczynają działanie od ochrony cyfrowego miejsca pracy, co obejmuje uniemożliwienie złośliwemu oprogramowaniu wykorzystania funkcji uczenia maszynowego, zapobieganie odfiltrowywaniu danych z firmowych aplikacji opartych na chmurze oraz mikrosegmentację sieci w celu przeciwdziałania zaawansowanym długotrwałym zagrożeniom (APT).
- Gdy zagrożenia dotrą do cyfrowego miejsca pracy, można je zidentyfikować dzięki ciągłemu adaptacyjnemu monitorowaniu, które umożliwia zespołom ds. operacji IT i bezpieczeństwa wykrywanie czynników ryzyka na przenośnych i stacjonarnych urządzeniach końcowych oraz w aplikacjach mobilnych i komputerowych.
- Po wykryciu zagrożeń rozwiązanie Workspace ONE Trust Network automatyzuje usuwanie problemów, wykorzystując zaawansowany mechanizm decyzyjny. Jeśli atak został wykryty na podstawie anomalii zachowania, można zainicjować zautomatyzowany zbiór reguł blokujący dostęp do danych korporacyjnych.

Ujednolicenie zabezpieczeń dostępu, urządzeń i aplikacji oraz zarządzania nimi dzięki analityce

Workspace ONE Trust Network łączy wbudowane funkcje zabezpieczeń oparte na analizie biznesowej platformy Workspace ONE — w tym zabezpieczenia dostępu, urządzeń i aplikacji oraz zarządzanie nimi — z funkcjami analitycznymi. Pozwala tym samym w wyjątkowy sposób łączyć silosy tworzone przez rozwiązania zabezpieczające. Usługa Workspace ONE Intelligence obsługuje funkcje analityczne na platformie Workspace ONE, realizując agregację i korelację danych obszaru roboczego oraz dostarczając zalecenia na temat korzystania ze zintegrowanych informacji i automatyzacji. Dzięki integracji funkcji rozwiązania Workspace ONE Trust Network z usługą Intelligence organizacje mogą zapewnić ciągłe monitorowanie ryzyka i szybkie łagodzenie zagrożeń w dzisiejszym świecie bez granic.

Mechanizm decyzyjny usprawnia korelację informacji, na przykład danych dotyczących firmowych urządzeń znajdujących się poza siecią oraz danych o zachowaniu użytkowników, do celów wykrywania zagrożeń i automatyzowania środków naprawczych za pomocą zbioru reguł dostępu. Zintegrowany wgląd w dane o zagrożeniach i szczegółowe informacje o stanie zgodności urządzeń z zasadami stanowi łatwy sposób identyfikowania i usuwania w czasie rzeczywistym problemów z zabezpieczeniami. W efekcie zapewnia wyższy poziom bezpieczeństwa w cyfrowym miejscu pracy. Mechanizm decyzyjny daje działom IT możliwość tworzenia reguł w celu automatyzacji i optymalizacji popularnych zadań, takich jak poprawa bezpieczeństwa podatnych na zagrożenia urządzeń końcowych z systemem Windows 10 za pomocą ważnych poprawek czy konfigurowanie kontroli dostępu warunkowego do aplikacji i usług na poziomie grupy lub jednostki.

Wykorzystanie bogatego ekosystemu rozwiązań zaufanych partnerów

Wdrożenie kompleksowego zabezpieczenia w rozrastającym się i ewoluującym cyfrowym miejscu pracy wymaga ustanowienia relacji zaufania między elementami zabezpieczającymi. Workspace ONE Trust Network zapewnia infrastrukturę zaufania, wykorzystując interfejsy API oparte na platformie Workspace ONE. Te interfejsy programistyczne umożliwiają komunikację między bogatym ekosystemem rozwiązań zabezpieczeń a platformą Workspace ONE i w rezultacie zapewniają administratorom zagregowany wgląd w dane, który jest niezbędny do uproszczenia działań w obszarach bezpieczeństwa i zarządzania. Łącząc silosy rozwiązań zabezpieczeń, klienci mogą wykorzystać aktualne inwestycje, by znacząco poprawić ciągłe monitorowanie i analizę ryzyka oraz skrócić czas reakcji. W efekcie otrzymują predykcyjną strategię bezpieczeństwa opartą na trendach i wzorcach, która daje możliwość skalowania wraz z wdrożeniem.

WIĘCEJ INFORMACJI

Więcej informacji o rozwiązaniu Workspace ONE Trust Network można znaleźć na stronie: www.vmware.com/products/workspace-one/security

Weź udział w bezpłatnych zajęciach praktycznych: https://www.vmware.com/go/workspace-hol

WIĘCEJ INFORMACJI O PRODUKTACH FIRMY VMWARE I MOŻLIWOŚCIACH ICH ZAKUPU MOŻNA UZYSKAĆ

TELEFONICZNIE
877-4-VMWARE (lub +1-650-427-5000 dla klientów spoza Ameryki Północnej)

W INTERNECIE
http://www.vmware.com/pl/products lub zapoznając się z ofertą u autoryzowanego sprzedawcy.

Najważniejsze funkcje

Organizacje mogą korzystać z następujących krytycznych funkcji zabezpieczeń rozwiązania Workspace ONE Trust Network do ochrony, wykrywania i usuwania problemów związanych z powiększającą się różnorodnością ataków cybernetycznych.

FUNKCJA	OPIS
Podstawowa platforma cyfrowego miejsca pracy łącząca rozwiązania zabezpieczeń	Uproszczenie działania w zakresie bezpieczeństwa i zarządzania dzięki infrastrukturze zaufania, która wykorzystuje interfejsy API do komunikacji między otwartym ekosystemem zabezpieczeń a platformą Workspace ONE.
Zarządzanie dostępem, które upraszcza działalność biznesową	Rozszerzenie możliwości działów IT o obsługę przydzielania zasobów, samoobsługowego katalogu, uwierzytelniania wieloskładnikowego i rejestracji jednokrotnej (SSO) w odniesieniu do wszystkich aplikacji.
Zapewnienie komfortu użytkownikom i optymalizacja zabezpieczeń za pomocą reguł kontekstowych	Kontrola uwierzytelniania przy użyciu zbioru reguł dostępu warunkowego opartych na stanie zgodności urządzenia, stopniu złożoności uwierzytelniania użytkownika, wrażliwości danych, lokalizacji użytkownika i innych czynnikach.
Reguły zapobiegania utracie danych (DLP), które uniemożliwiają wyciek informacji	Obsługa szyfrowania na poziomie urządzenia, szyfrowania danych i sprzętowych reguł dotyczących zabezpieczeń. Konfigurowanie reguł, w tym czarnych list aplikacji, parowania urządzeń, zabezpieczeń sieci Wi-Fi i egzekwowania TLS. Monitorowanie zagrożeń stwarzanych przez złośliwe oprogramowanie i aplikacje, ataki w pamięci i urządzenia z odblokowanym dostępem na poziomie administratora oraz automatyczne eliminowanie problemów za pomocą blokady zdalnej, wymazania danych na urządzeniu, blokady dostępu lub konfigurowalnych środków kontroli inicjujących kwarantannę urządzenia.
Zabezpieczanie aplikacji bez pogarszania komfortu pracy	Zastosowanie środków kontroli bezpieczeństwa w bezpiecznych aplikacjach firmy VMware zwiększających produktywność — VMware Boxer™, Browser™ i Content Locker™. Wykrywanie zagrożeń i automatyzacja usuwania problemów dla wszystkich pozostałych aplikacji i usług w chmurze.
Szyfrowanie danych w klastrze i danych przesyłanych	Uwierzytelnianie i szyfrowanie ruchu z aplikacji na urządzeniach do centrum przetwarzania danych przy użyciu rozwiązania VMware Tunnel. Zabezpieczanie danych aplikacji w klastrze i danych przesyłanych przez zastosowanie 256-bitowego szyfrowania AES.
Automatyzacja zabezpieczeń w obrębie sieci za pomocą mikrosegmentacji	Ograniczanie obszaru ataków w centrum przetwarzania danych za pomocą funkcji mikrosegmentacji z użyciem platformy VMware NSX® umożliwia automatyzację zabezpieczeń w obrębie sieci.
Zabezpieczenia predykcyjne dzięki zintegrowanej analizie danych i automatyzacji	Identyfikowanie i łagodzenie w czasie rzeczywistym problemów bezpieczeństwa dzięki zintegrowanej analizie danych o zagrożeniach i szczegółowym informacjom o stanie zgodności urządzeń z regułami dostarczanymi przez rozwiązanie Workspace ONE Intelligence.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Faks 650-427-5001 www.vmware.com/pl
 Pozycja nr: 130019wf-vmw-fy19q1 euc launch-trust network-ds-a4-106
3/18