VMWARE WORKSPACE ONE TRUST NETWORK

Zabezpečení pro vyvíjející se digitální pracovní prostředí

STRUČNÝ PŘEHLED

Řešení VMware Workspace ONE™ Trust Network™ poskytuje organizacím ucelený a moderní přístup k podnikovému zabezpečení, který zajišťuje bezpečnost zaměstnanců, aplikací, koncových bodů a sítí. Díky schopnostem chránit se před současnými moderními hrozbami, odhalovat je a odstraňovat rozšiřuje řešení Workspace ONE Trust Network základní funkce zabezpečení platformy Workspace ONE, která je založená na inteligentní analýze, pomocí bohatého ekosystému integrovaných partnerských řešení, která zajišťují nepřetržité monitorování rizik a rychlou reakci zmírňující rizika v celém digitálním pracovním prostředí.

KLÍČOVÉ VÝHODY

Řešení Workspace ONE Trust Network zjednodušuje zabezpečení a správu prostřednictvím rámce založeného na důvěře a ověřování. Řešení Workspace ONE Trust Network umožňuje oddělením IT:

- Odstraňovat izolovanost řešení zabezpečení pomocí rámce založeného na akcích, který poskytuje souhrnný pohled a snižuje složitost v celém digitálním pracovním prostředí.
- Kombinovat jedinečným způsobem zabezpečení a správu přístupu, zařízení a aplikací s poznatky a automatizací za účelem zmírnění rizik v celém výpočetním ekosystému pro koncové uživatele.
- Využívat otevřený a důvěryhodný ekosystém partnerů a nadále používat stávající investice, a tím snižovat náklady.

Zabezpečení – největší překážka pro strategii moderního digitálního pracovního prostředí

Digitální pracovní prostředí může až 5×[1] zvýšit produktivitu zaměstnanců tím, že jim poskytne jednoduchý a zabezpečený přístup k aplikacím a datům ze zařízení podle jejich vlastního výběru. Stále další a další organizace se vydávají cestou digitální transformace, a proto se ekosystém digitálního pracovního prostředí zaměstnanců, aplikací, koncových bodů a sítí nadále rozrůstá a vyvíjí i mimo tradiční hranice vnitřního prostředí. Projevují se přitom obecné trendy, jako je používání vlastních zařízení a konzumerizace informačních technologií. A jak tyto tradiční hranice mizí, začínají se objevovat pokročilé kybernetické hrozby, jako jsou útoky nultého dne, útoky pomocí prostředníka (MiTM), phishingové útoky, roboti a ransomware.

Zabezpečení představuje hlavní prioritu pro investice do mobility a digitálního pracovního prostředí[2], nicméně stávající nástroje zabezpečení poskytují oddělením IT jen omezený přehled, protože se zaměřují pouze na izolované prostředky zabezpečení poskytující zastaralé funkce. Výsledkem je přístup, který zakrývá příznaky, aniž by řešil vlastní problém, a způsobuje organizacím vysoké náklady, protože zajistit zabezpečení digitálního pracovního prostředí je složité a vyžaduje ruční provádění úloh. Zabezpečení se tak stalo největší překážkou pro strategii moderního digitálního pracovního prostředí.

Komplexní a prediktivní zabezpečení v organizaci bez hranic

Uspokojení potřeb zabezpečení bez dopadu na možnosti uživatelů není možné bez splnění nové sady požadavků:

1. Pokud chtějí organizace získat souhrnný pohled, musejí použít rámec k nastolení důvěry mezi součástmi, které zabezpečují jejich ekosystém.
2. Aby mohly nepřetržitě snižovat rizika, musejí být organizace navíc schopné ze svého prostředí získávat poznatky, což jim umožní dosáhnout prediktivního a automatizovaného rozhodování ve vztahu k zabezpečení digitálního pracovního prostředí.

Řešení Workspace ONE Trust Network nabízí organizacím ucelený a moderní přístup k podnikovému zabezpečení, který zajišťuje bezpečnost zaměstnanců, aplikací, koncových bodů a sítí. Poskytuje sadu schopností pro ochranu, odhalování a odstraňování hrozeb v celém vyvíjejícím se digitálním pracovním prostředí, vycházejí z rámce, který je založen na důvěře a ověřování. Výsledkem vybudování důvěry v celém digitálním pracovním prostředí je vzájemně propojený systém s nejnižšími možnými oprávněními, který posiluje možnosti zaměstnanců tím, že zajišťuje jejich bezpečnost, kdekoli jsou. Řešení Workspace ONE Trust Network kombinuje informace z platformy Workspace ONE založené na inteligentní analýze s důvěryhodnými partnerskými řešeními zabezpečení, aby mohlo poskytovat prediktivní a automatizované zabezpečení v digitálním pracovním prostředí, a zajistilo tak správu rizik týkajících se dnešních moderních kybernetických hrozeb.

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

2 Průzkum subjektů kupujících mobilní technologie, CCS Insights, prosinec 2017

Ochrana, odhalování a náprava

Otázka dnes nezní, zda bude organizace vystavena kybernetickému útoku, ale kdy. Když budou týmy zajišťující provoz a zabezpečení IT takové útoky očekávat, dokážou spravovat rizika pro kybernetické zabezpečení tak, že zjednoduší mapování funkcí zabezpečení, například pomocí rámce, jako je NIST Cybersecurity Framework, na možnosti poskytované řešením Workspace ONE Trust Network:

- Možnosti zabezpečení začínají ochranou digitálního pracovního prostředí, která zahrnuje obranu před malwarem pomocí strojového učení, předcházení exfiltraci dat z podnikových cloudových aplikací a obranu před pokročilými trvalými hrozbami (APT) pomocí mikrosegmentace sítí.
- Když hrozby proniknou do digitálního pracovního prostředí, mohou být odhaleny pomocí nepřetržitého a adaptivního monitorování, které týmům zajišťujícím provoz a zabezpečení IT umožňuje odhalovat hrozby v mobilních a desktopových koncových bodech a aplikacích.
- Po zjištění hrozeb může řešení Workspace ONE Trust Network automatizovat nápravu s využitím výkonného rozhodovacího modulu. Když je odhalen útok na základě anomálií v chování, mohou být aktivovány automatizované zásady, které zablokují přístup k podnikovým datům.

Sjednocení zabezpečení a správy přístupu, zařízení a aplikací pomocí analýzy

Řešení Workspace ONE Trust Network kombinuje základní schopnosti zabezpečení platformy Workspace ONE založené na inteligentní analýze, které zahrnují zabezpečení a správu přístupu, zařízení a aplikací, s analytickými nástroji, aby dokázalo jedinečným způsobem přemostit izolované prostředky správy vytvořené řešeními zabezpečení. Služba Workspace ONE Intelligence využívá analytické nástroje na platformě Workspace ONE a nabízí agregaci a korelaci dat pracovního prostředí a doporučení týkající se těchto dat k poskytování integrovaných poznatků a automatizace. Integrace schopností řešení Workspace ONE Trust Network se službou Intelligence umožňuje organizacím průběžně monitorovat bezpečnostní rizika a zajistit rychlou reakci zmírňující rizika v dnešním světě bez jasně vymezených hranic.

Rozhodovací modul pomáhá uvádět informace, například o podnikových zařízeních, která nejsou připojena k síti, do vzájemného vztahu s chováním uživatelů, a tím umožňuje odhalovat hrozby a automatizovat nápravu prostřednictvím zásad pro přístup. Integrované poznatky získané z dat o hrozbách a podrobných informací o stavu shody zařízení nabízejí snadný způsob, jak identifikovat a zmírňovat problémy zabezpečení v reálném čase, a tím zdokonalovat zabezpečení digitálního pracovního prostředí. Rozhodovací modul umožňuje oddělením IT vytvářet pravidla pro automatizaci a optimalizaci běžných úloh, jako je zjednání nápravy u ohrožených koncových bodů se systémem Windows 10 pomocí instalace kritické opravy nebo nastavení kontrolních mechanismů podmíněného přístupu pro aplikace a služby na úrovni skupin či jednotlivců.

Využívání bohatého ekosystému řešení od důvěryhodných partnerů

K dosažení komplexního zabezpečení v celém digitálním pracovním prostředí je potřeba vybudovat důvěru mezi součástmi, které zajišťují bezpečnost rostoucího a vyvíjejícího se digitálního pracovního prostředí. Řešení Workspace ONE Trust Network poskytuje rámec důvěry využíváním rozhraní API založených na platformě Workspace ONE. Tato rozhraní API umožňují bohatému ekosystému řešení zabezpečení komunikovat s platformou Workspace ONE a v konečném důsledku poskytovat souhrnný pohled, který správci potřebují ke zjednodušení zabezpečení a správy. Díky propojení izolovaných řešení zabezpečení mohou zákazníci s využitím svých stávajících investic exponenciálně vylepšovat nepřetržité monitorování a analýzu rizik za účelem zkrácení doby odezvy. Výsledkem je strategie prediktivního zabezpečení založená na trendech a vzorech, která podporuje škálování podle rozsahu zavádění.

DALŠÍ INFORMACE

Další informace o řešení Workspace ONE Trust Network získáte na adrese: www.vmware.com/cz/products/workspace-one/security

Bezplatnou praktickou ukázku k vyzkoušení najdete na adrese: https://www.vmware.com/go/workspace-hol

DALŠÍ INFORMACE NEBO ZAKOUPENÍ PRODUKTŮ SPOLEČNOSTI VMWARE

VOLEJTE NA ČÍSLO:
+420 255 725 410 (v Severní Americe 877-4-VMWARE)

NAVŠTIVTE STRÁNKU:
http://www.vmware.com/cz/products nebo na internetu vyhledejte autorizovaného prodejce.

Hlavní funkce

Následující kritické funkce zabezpečení poskytované řešením Workspace ONE Trust Network umožňují organizacím chránit se před vyvíjejícími se kybernetickými hrozbami a odhalovat a odstraňovat je.

FUNKCE	POPIS
Základní platforma digitálního pracovního prostředí, která propojuje řešení zabezpečení	Zjednodušuje zabezpečení a správu pomocí rámce důvěry, který využívá rozhraní API, aby umožnil otevřenému ekosystému zabezpečení komunikovat s platformou Workspace ONE.
Řízení přístupu, které zjednodušuje chod vaší firmy	Nabízí oddělením IT nové možnosti pro poskytování samoobslužného katalogu, zajišťování aplikací, vícefaktorového ověřování a jednotného přihlašování (SSO) pro všechny aplikace.
Optimalizace možností uživatelů a zabezpečení pomocí kontextových zásad	Řídí ověřování pomocí zásad podmíněného přístupu založených na stavu shody zařízení, síle ověřování uživatelů, citlivosti dat, poloze uživatelů a dalších parametrech.
Zásady ochrany před únikem dat (DLP) napomáhající zabránit úniku dat	Aktivuje zásady pro šifrování na úrovni zařízení, šifrování dat a zabezpečení hardwaru. Konfiguruje zásady, včetně seznamů zakázaných aplikací, párování zařízení, zabezpečení sítí Wi-Fi a vynucování protokolu TLS. Monitoruje výskyt malwarových hrozeb, škodlivých aplikací, útoků v paměti nebo zařízení s jailbreakem a automaticky zjednává nápravu pomocí vzdáleného uzamknutí, vymazání zařízení, blokování přístupu nebo přizpůsobitelných kontrolních mechanismů pro umístění zařízení do karantény.
Zabezpečení aplikací bez obětování možností uživatelů	Využívá kontrolní mechanismy zabezpečení v zabezpečených kancelářských aplikacích společnosti VMware, jako jsou VMware Boxer™, Browser™ a Content Locker™. Odhaluje hrozby a automatizuje nápravu pro všechny ostatní aplikace a cloudové služby.
Šifrování uložených a přenášených dat	Ověřuje a šifruje přenosy z aplikací v zařízeních do datového centra pomocí technologie VMware Tunnel. Zabezpečuje uložená a přenášená data aplikací pomocí šifrování podle standardu AES (Advanced Encryption Standard) s délkou klíče 256 bitů.
Mikrosegmentace pro automatizaci zabezpečení napříč sítěmi	Minimalizuje potenciální oblast útoku v datovém centru využitím možností poskytovaných mikrosegmentací prostřednictvím řešení VMware NSX®, a tím automatizuje zabezpečení v celé síti.
Integrované poznatky a automatizace podporující prediktivní zabezpečení	Identifikuje a zmírňuje problémy zabezpečení v reálném čase pomocí integrovaných poznatků získaných z dat o hrozbách a podrobných informací o stavu shody zařízení poskytovaných službou Workspace ONE Intelligence.

VMware, Inc., 3401 Hillview Avenue, Palo Alto CA 94304, USA, tel.: 877-486-9273, fax: 650-427-5001, www.vmware.com
VMware International Limited, Anděl Park Smíchov – Scott&Weber Office, Karla Engliše 3201/6, 150 00 Praha 5, Česká republika, tel.: +420 255 725 410, fax: +420 255 725 401, www.vmware.com/cz

Č. položky: 130019wf-vmw-fy19q1 euc launch-trust network-ds-a4-106
3/18