ÜGYNÖKMENTES VIRTUÁLIS JAVÍTÁS

A védelem és a teljesítmény optimalizálása a VMware és a Trend Micro segítségével

Miért kihívás a javítókészletek kezelése

Ma a vállalatokat szinte elsodorja a sebezhetőségek áradata, amelyek ellen akár napi hét kritikusan fontos javítókészletet kapnak. Ez a végeláthatatlan „pecselés" rengeteg pénzt és időt von el hasznosabb informatikai feladatoktól. Ennek ellenére szinte elérhetetlen a naprakész védelem. Egy nemrég készült felmérés szerint a vállalatok harmada jelezte, hogy aránytalanul sok időt és munkaórát fordít a javítókészletek kezelésére – az informatika biztonsági feladatai közül ez jelenti számukra a legnagyobb terhet. Ugyanakkor csak 22 százalékuk nagyon eredményes a javítókészletek kezelésében1.

Tetézi a bajt, hogy a virtualizálás fokozza a biztonsági gondokat: virtuális környezetek hagyományos javítása egyszerre ronthatja a védelmet és a teljesítményt. A virtuális javítás ügynökmentes biztonsági megközelítése azonban az ismert és potenciális sebezhetőségek leárnyékolásával jól kiegészíti a meglevő javítókészlet-kezelési folyamatokat, a virtuális környezetek teljesítményének rontása nélkül.

Hol vannak a sebezhetőségek?

A vállalatok a kritikusan fontos alkalmazások és rendszerek széles körében szembesülnek árnyékolást igénylő ismert és ismeretlen sebezhetőségekkel.

- Vállalati alkalmazások: Évente többezer kritikus szoftversebezhetőségre derül fény operációs rendszerekben, adatbázisokban, kiszolgálókban és alkalmazásokban. Ezek javítása zavarhatja a normális munkavégzést. Ha történetesen rendelkezésre is állnak a javítókészletek, hetek vagy akár hónapok telhetnek el teljeskörű telepítésükig.
- Régebbi webes alkalmazások A rekordokba való sikeres behatolások többsége mögött az eredendően nyitott és a támadók számára elérhető webes alkalmazások elleni SQL injektálásos támadások állnak. A peremvédelem nem árnyékolja le ezeket a rendszereket, és a programkódok javításához nehéz felkészült szakembert találni.
- Nem támogatott operációs rendszerek és alkalmazások: Az életciklusuk végére ért operációs rendszerekhez és alkalmazásokhoz már nem készülnek javítókészletek. Az ilyen és egyéb nem támogatott rendszerek költséghatékony védelmére gyakran a virtuális javítás az egyetlen lehetséges megoldás.
- Zárolt rendszerek: A 24x7-es időbeosztásban futó kritikusan fontos rendszerek nem pecselhetők, mert ez bevétel- vagy termeléskiesést okozna.

Miért érinti ez a virtuális környezeteket?

A virtualizált asztali gépeket és adatközpontokat ugyanúgy kellene árnyékolni virtuális javítással, mint fizikai megfelelőiket a fizikai pecseléssel. A hagyományos, ügynök-alapú megoldások azonban nem a virtuális környezetekre készültek, és jelentős működésbiztonsági gondokat okozhatnak.

- Erőforrásigény: A hagyományos biztonsági ügynökök, pl. virtuális javítók, még üresjáratban is jelentős memóriát kötnek le egy-egy VM virtuális gépen, különösen akkor, ha egyidejűleg több ilyen biztonsági ügynök is fut a gépen, különféle védelmekhez. Ez rontja a konszolidálási hányadot, és a CAPEX és OPEX mutatókat is.
- A hálózat rontása: A hagyományos biztonsági termékek nem hatékonyak a virtuális környezetekben, mert itt a VM-ek között minden forgalmat központi célgépen kell átfolyatni az ellenőrzéshez. A hálózati forgalom ilyen átirányítása megfelelőségi problémákat okozhat, ronthatja a hálózat teljesítményét, és torlódást idézhet elő.
- Gyors ki-be kapcsolás: A gyors egymásutánban ki- és bekapcsolt VM-ek nehezen pecselhetők egyöntetűen és tarthatók naprakészen folyamatosan. A szunnyadó, javítatlan VM-ek hatalmas biztonsági sebezhetőséget idézhetnek elő, amikor bekapcsolják őket.
- Többletmunka: A rendszergazdáknak gondoskodniuk kell arról, hogy minden VM megkapja a legújabb javítókészletet. A VM-ek mozgatása és állapotváltozásai miatt a következetes javítás nagyon időigényes, és ennek ellenére sem szüntet meg minden biztonsági rést.

Az ügynökmentes virtuális javítás előnyei

A VMware és a Trend Micro együtt ügynökmentes sebezhetőség-árnyékolást biztosít a virtualizált adatközpontoknak, a következő előnyökkel:

- Nagyobb konszolidálási hányad a virtuális javítás átterhelésével az egyes VM-ekről az egy-egy vSphere hoszton futó egyetlen virtuális biztonsági célgépre.
- Gyorsabb működés az egyidejű javítások miatti biztonsági „viharok" és erőforráslekötés semlegesítésével.
- Jobb kezelhetőség a virtuális javítást végző ügynökök megszüntetésével, és ezzel konfigurálásuk/frissítésük szükségtelenné tételével.
- Erősebb biztonság az új VM-ek azonnal működő védelmével, amit a biztonsági célgép koordinál.

Az ügynökmentes virtuális javítás a teljesítmény rontása nélkül árnyékolja a sebezhetőségeket

A VMware és a Trend Micro partnerkapcsolatának célja a virtualizált asztali gépek és adatközpontok virtuális javítását lehetővé tevő ügynökmentes biztonsági megoldás forgalmazása. A közös megoldás minimálisra csökkenti a VM-ek teljesítménycsökkenését és az erőforrásvetélkedési problémákat, a következő két kölcsönösen függő megoldás egymást erősítő hatásával:

- A **VMware vsphere** optimalizálja a biztonságot azzal, hogy a VM ügynök-alapú hagyományos biztonságkezelést átterheli a VMware partnerek által szállított megerősített biztonságú virtuális hosztgépekre.
- A **Trend Micro™ Deep Security** adja megerősített biztonságú virtuális gépet, amely az integrált VMware API felületekkel kombinálva a VMware virtuális gépek ügynökmentes virtuális javítását végzi (és további ügynökmentes biztonsági lehetőségekkel ruházza fel őket).

Trend Micro Deep Security

A Trend Micro Deep Security leárnyékolja a kritikusan fontos rendszerek sebezhetőségét új javítás megérkezéséig és telepítéséig, vagy „holnapután kiskedden" várható javítások helyett. A Deep Security virtuális célgépként telepíthető VMware ESX kiszolgálóra, ahol ügynökmentes védelmet nyújt a vendég VM gépeknek. A VMware VM-ek ügynökmentes virtuális javításával naprakészen és költséghatékonyan kiegészítheti a hagyományos javítási folyamatokat, s ezáltal jelentős költségcsökkentést érhet el, kevésbé zavarja az üzemmenetet, és jobban kézben tarthatja a javítások ütemezését. További előny, hogy kritikusan fontos vállalati rendszerei és alkalmazásai jobban lesznek védve adatszivárgás ellen, és csökkennek a megfeleléssel kapcsolatos ráfordításai.

Vmware vSphere

A VMware vSphere segítségével biztonsági célgépre terhelhetők át a főbb biztonsági funkciók, mint például a virtuális javítás, amivel felszabadítható a biztonsági ügynök által elfoglalt hely a virtuális gépeken. Ez a kifinomult architektúra rendszererőforrásokat szabadít fel, javítja a futásteljesítményt, és megszünteti a biztonsági „viharok" kockázatát.

A Trend Micro illetéktelen hozzáférés ellen megerősítve védett virtuális célgépével a vSphere teherbíró és biztonságos hipervizor önvizsgálati képességet biztosít a védelem kompromittálásának megelőzésére. A megfelelés bizonyítását és az ellenőrök követelményeinek teljesítését a tevékenységeknek a biztonsági szolgálatban indított részletes naplózása teszi lehetővé.

Így működik az ügynökmentes virtuális javítás

1. A VMware vCloud Networking and Security ügynökmentes VM önvizsgálatot biztosít, valamint figyeli az aktuális, új és újraaktivált VM-eket, gondoskodva ezzel a legújabb sebezhetőségek elleni naprakész védelmükről.
2. A VMware vCloud Networking and Security lehetővé teszi a Trend Micro Deep Security számára a kommunikálást a vendég VM-ekkel a virtuális javítások elvégzéséhez.
3. A Trend Micro Deep Security a VMware vShield API felületekkel integrált megerősített biztonságú virtuális célgéppel gondoskodik az ügynökmentes biztonságról.
4. Ez a megközelítés a vendégeken telepített biztonsági ügynökök nélkül teszi lehetővé a sebezhetőségek árnyékolását.

> "A Deep Security védi egészségügyi rendszerünket azzal, hogy proaktívan árnyékolja elektronikus nyilvántartórendszerünk webes alkalmazásainak és operációs rendszereinknek a sebezhetőségeit a célzott támadások elől a javítókészletek telepítése között."
>
> Bill Gillis,
> **Beth Israel Deaconess Gyógyászati Központ**

Az ügynökmentes virtuális javítás jellemzői

- A behatolásészlelő és -megelőző (IDS/IPS) szabályok védelmet nyújtanak az ismert – például a Microsoft által kedden nyilvánosságra hozott – sebezhetőségek kihasználása ellen, és alapállapotukban több mint 100 alkalmazást védenek, köztük adatbázisokat, valamint web, e-mail és FTP kiszolgálókat. Az IDS/IPS szabályok zero-day védelmet nyújtanak javítókészlettel nem lefedett ismert sebezhetőségek és ismeretlen sebezhetőségek ellen is.
- A Recommendation Scanning hatékonyabbá teszi a biztonsági frissítések kezelését és tovább egyszerűsíti a javítást azzal, hogy automatikusan javasolja, mely szabályokat kell telepíteni adott rendszer védelmére. A Deep Security a rendszer vizsgálatával, az operációs rendszer, a szervizcsomag, a javítási szint és a telepített alkalmazások alapján azonosítja, hogy mely IDS/IPS szabályokat kell telepíteni a védelem optimalizálásához. A Deep Security emellett automatikusan javasolja, hogy a kiszolgáló környezetének változása és a javítókészletek telepítése eredményeként mely szabályok törölhetők erőforrások felszabadításához.
- A vállalati szintű, kétirányú, állapot-nyilvántartó tűzfal átengedi a kommunikációt a kiszolgáló helyes működéséhez szükséges portokon és protokollokon, és letilt minden más portot és protokollt. Ez csökkenti a kiszolgáló illetéktelen hozzáférésének kockázatát.
- A webes alkalmazások védelmi szabályai védelmet nyújtanak a SQL injektálásos támadások, site-ok közti scriptelés (XSS), és egyéb webalkalmazás-sebezhetőségek ellen, amelyeket a programjavítások telepítéséig leárnyékolnak.
- A VM-ek közti védelem egyetlen virtuális célgéppel nyújt hoszt-alapú védelmet több VM-nek. Ezzel a VM-gépenkénti irányelvek feláldozása nélkül figyelhető a VM-ek közötti forgalom.
- A sebezhetőségekre vonatkozó információk folyamatos figyelésére, valamint az új releváns fenyegetések és sebezhetőségek azonosítására és korrelálására szakosodott biztonsági szakembercsapattól származó biztonsági frissítések naprakészen tartják a védelmet. A Trend Micro részt vesz a Microsoft Active Protections Programjában is, a kezdeti stádiumban levő fenyegetések elővételezése és a védelem naprakészebbé tétele érdekében.
- A fizikai, virtualizált és felhős számítástechnikai környezetek védelme gondoskodik a sebezhetőségek leárnyékolásáról, függetlenül a hosztok telepítési módjától. Vendég-alapú védelem biztosítása mellett a Deep Security a VMware API felületek útján is gondoskodik a virtualizálást figyelembe vevő védelemről, ami fokozza a telepítési rugalmasságot.

Válassza a megfelelő megoldást a sebezhetőségek leárnyékolására

A VMware erős API felületeket fejlesztett ki a biztonság javítására. A Trend Micro pedig a virtuális javítási megoldások terén vezető. A vállalatok igényeire szabott élenjáró virtualizációs platformjával és biztonságával a VMware / Trend Micro páros segít önnek védelme maximalizálásában, a komplexitás minimalizálása mellett. További információk webhelyünkön találhatók: www.trendmicro.com/virtualpatching

TREND MICRO™

Securing Your Journey to the Cloud