

TELJES KÖRŰ LÁTHATÓSÁG NÉLKÜL NINCS FELHŐ

# A csomagok soha nem hazudnak

A felhő jó dolog, de a felhőbe költözni és ott céges infrastruktúrát működtetni már korántsem olyan egyszerű. Az egyik alapfeltétel, hogy a vállalat teljes egészében lássa át hálózata működését, a felhőben és a földön is.



MESTER SÁNDOR, SZEMES TIBOR, VÁRALJAI KRISTÓF, PALÁSTI PÉTER ÉS LIPCSEI ATTILA

„Nemcsak a világon, de Magyarországon is egyre inkább kezdik belátni a szervezetek, hogy a jövőt a hibrid felhős infrastruktúra jelenti. Sokáig lehet sorolni egy ilyen rendszer előnyeit, de ettől még számos kihívással kell szembenéznie annak a vállalatnak, amelyik elhatározza: legalább részben a felhőbe költözteti infrastruktúráját”, kezdte előadását Szemes Tibor, az Exclusive Networks üzletfejlesztési menedzsere a januári ITBUSINESS Clubon.

## Elkerülni a vakfoltokat

Az első felmerülő kérdés technikai: a saját adatközpontban működő szoftvereket, eszközöket, adatokat a felhőben is elérhetővé kell tenni. Sok esetben erre nincsenek kész programok, megoldások, ezért fejleszteni kell ilyeneket, ami plusz időt és költséget jelent.

A következő nagy kihívás a biztonság megteremtése. A hibrid felhős környezetek összetettsége megnöveli a „vakfoltok” kialakulásának veszélyét. A vakfoltok azok a rendszerek, adatforrások, kapcsolatok, amelyekre a szervezetnek nincs igazi rálátása – emiatt viszont ideális terepet jelentenek minden támadó

számára, akik az esetleges sérülékenységeket kihasználva észrevétlenül kompromittálhatják az infrastruktúra egyes elemeit.

Végül pedig mindeközben figyelni kell arra is, hogy a költségek ne szálljanak az egekbe. A várható kiadásokkal viszont csak akkor lehet legalább elfogadható pontossággal kalkulálni, ha a vállalat előre tudja, hogy mennyi adatot akar mozgatni a felhő és a saját infrastruktúra között, milyen sávszélességre, mekkora tár- és processzorkapacitásra lesz szükség. Ha az infrastruktúrában ott rejtőznek a már említett vakfoltok, akkor kiszámíthatatlan rejtett és felesleges költségekkel kell számolni.

## Minden adat ott, ahol kell

„A gond igazából nem azzal van, hogy az infrastruktúrát menedzselő mérnökök számára ne állna rendelkezésre megfelelő mennyiségű adat; sokkal inkább az a baj, hogy túl sok adat érkezik túl gyorsan a hálózati eszközökből”, vette át a szót Lipcsei Attila, az Exclusive Networks presales tanácsadója. Az ellentmondás látszólag feloldhatatlan: egyszerre kellene figyelni mindent a hálózaton, miközben meg kell óvni az elemzőeszközöket a túlterheléstől. A hagyományos infrastruktúrákban az úgynevezett „észak-déli”

(azaz a hálózatba be- és onnan kilépő) forgalom figyelhető meg könnyen, a „kelet-nyugati” (vagyis az egyes hálózati eszközök közötti) adatforgalom jórészt láthatatlan.

Itt jön a képbe a Gigamon Hawk Deep Observability Pipeline. A megoldás lényege, hogy amolyan csővezetéként (innen a neve is) összeköttetést biztosít a saját adatközpontban, a virtualizált környezetekben vagy a felhőben futó munkafolyamatok, valamint az ezek kezelésére szolgáló hálózati, biztonsági és teljesítményelosztó eszközök között. A forgalom úgynevezett packet brokerekre megy keresztül: ezek olyan moduláris eszközök, amelyek különféle szabályok alapján osztják szét az adatcsomagokat a passzív hálózati eszközöknek.

A nagy varázslat abban áll, hogy a packet brokerek a továbbítás mellett számos más műveletre is képesek. Így elvégzik a deduplikációt (nem küldik kétszer ugyanazt az adatot); szűrést hajtanak végre (nem küldenek minden adatot minden eszközre); és az adatcsomagokat is fel tudják szeletelni, hogy az egyes eszközök ténylegesen csak azokat az adatdarabkákat kapják meg, amelyekre szükségük van – a teljesítménymenedzser (APM) csak a fejleceket, a VoIP-elemző csak a VoIP-adatokat. Mindezek révén az infrastruktúra üzemeltetői úgy férhetnek hozzá a hibrid infrastruktúra teljes forgalmához, hogy közben a ténylegesen átvitt adatmennyiség (és ezáltal a szükséges sávszélesség) nagymértékben csökken, magyarázta el a működés lényegét Lipcsei Attila.

## Nincs egymásra mutogatás

Arról, hogy mindez milyen kézzelfogható előnyöket jelent a gyakorlatban, az Exclusive Networks két partnerétől hallhattuk az ITBUSINESS Club vendégei. *Váraljai Kristóf*, a Schoeller Network Control Hungary hálózati szakértője egy kis visszatekintéssel kezdte. Mint mondta, tevékenységük már évtizedekkel ezelőtt a hálózati forgalom elemzésére irányult. Eleinte az volt a probléma, hogy nem jutottak hozzá elég adathoz az eszközökből, anélkül pedig nehéz volt a magasabb szinten jelentkező problémák gyökereit felderíteni.

Az első generációs forgalomaggregátorok megoldották ezt a kérdést: akár forgalomelemzés, akár biztonsági vizsgálat szempontjából volt szükség az információra, átfogó képet kaphattak a hálózatról. Az infrastruktúrák bővülésével azonban az áthaladó adatmennyisége olyan mértékben nőtt meg, hogy az már nehezítette az elemzést. A Gigamon eszközei ezen segítettek fejlett funkcióikkal.

### Mit kínál a Gigamon Deep Observability Pipeline?

- Megszünteti a vakfoltokat az on-premise és a felhős hálózati környezetekben.
- Teljes körű láthatóságot biztosít virtuális és felhős környezetben is.
- Növeli a biztonságot, mert minden biztonsági eszközt megkapja a releváns adatokat.
- 50-80 százalékkal csökkenti az adatforgalmat, ezzel optimalizálja a költségeket, feleslegessé tehet bővítéseket.
- Felderíti a nem kívánt folyamatokat, tevékenységeket, például a kriptobányászatot.



FORRÁS: ITBUSINESS

„Ha valamiért akadoznak az alkalmazások, minden üzemeltetési csapat hajlamos a többiekre mutogatni, hogy náluk van a hiba. És tényleg lehet, hogy mindenkinél hibahatáron belül vannak a teljesítményértékek, de a végeredmény mégis katasztrofális. Ilyenkor jön nagyon jól a Gigamon és a mélységi hálózatelemzés, mert a csomagok soha nem hazudnak”, mondta *Váraljai Kristóf*.

## Pár nap alatt eredmény

*Palásti Péter*, az NTT Magyarország hálózati rendszermérnöke pontosan erre hozott példát. Az egyik nagy magyar vállalatnál akadozott az internetes értékesítési rendszer, rendkívül lassan működött a webes felület. Összetett architektúráról volt szó, a webes frontend mögött terheléselosztó rendszerek működtek, azokon keresztül futottak be a kérések az alkalmazásba és a mögöttes adatbázisba. Itt is az volt a helyzet, hogy az egyes területek monitoring rendszere nem jelzett hibás működést, a szolgáltatás mégis lassú volt.

Beállították a hálózatba egy Gigamon-eszközt, amely egyben tudta monitorozni és elemezni az összes hálózati adatot. Alig néhány nap alatt kiderült az akadozás oka: a terheléselosztó infrastruktúrában egy hibás beállítás miatt a négy eszközből mindig egy kapta meg a teljes forgalom 80 százalékát, a maradék 20 oszlott meg a három másik között. Átlagos tranzakciószám mellett ez nem okozott gondot, de csúcsidőben az az egy terheléselosztó már nem birkózott meg a kérésekkel. Innentől kezdve már könnyen lehetett orvosolni a problémát, és helyreállt a szolgáltatás.

Szemes Tibor szerint is tipikus ez a forgatókönyv. Az ügyfelek rendszerint nem úgy keresik meg őket, hogy valamilyen Gigamon eszközt szeretnének vásárolni, hanem problémájuk van a hálózat teljesítményével vagy biztonságával. Amikor aztán megmutatják, hogy miként oldják meg az adott problémát, általában a többi funkció is felkelti a figyelmet. „Rájönnek, hogy mennyi mindent meg tudnak oldani, amit eddig nem, az eszköz pedig szinte eladja magát”, fogalmazott az Exclusive Networks menedzsere. ■