Security | Networking | Management

CLICO

Rövidítések a Cloud Securityben 2023

Az IT biztonságban különösen igaz, hogy a mozaikszavak, rövidítések, beépülnek a mindennapi kommunikációba, de ez csak akkor jelent segítséget, ha mindenki jól ismeri a mögöttes jelentést. Tapasztalataink szerint a felhőbiztonsági megoldások tekintetében különösen eltérnek vagy félreértelmezettek egyes rövidítések, ráadásul a terület itthon újdonságnak számít, ezért szeretnénk útmutatást nyújtani, hogy ebben a labirintusban kicsit könnyebb legyen eligazodni. Sorravesszük, hogyan jöttek létre ezek a felhőbiztonsági rövidítések, mit jelentenek egyenként, és vizsgáljuk meg, hogyan illeszkedik a CNAPP a felhőbiztonsági stratégiába.

A 2000-es évek elején a nagyvállalatok lehetőségeket kerestek a túlterhelt on-premise (földi) környezetük helyett, így elkezdődött az IT infrastruktúra nagy arányú virtualizációja, és ezzel egyidőben az üzemeltetés kiszervezése is előtérbe kerül. Egyre profibbak, átfogóbbak lettek az IT szolgáltatók. Így a felhőbiztonsági megoldások szükségszerűen születtek meg, leginkább az új felhős (akkor még szimplán csak kiszervezett hipeskálázható virtuális) környezetek átláthatósága és védelme érdekében.

Rövidítések a Cloud Securityben

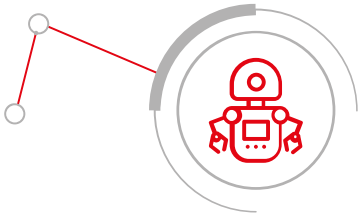
Ezeket a biztonsági szolgáltatásokat azonban valahogy definiálni kellett. A Gartner, mint technológiai kutató- és elemző cég, - egyben az iparág hárombetűs rövidítéseinek keresztapja-által elsőként meghatározott kategória a **CWPP (Cloud Workload Protection Platform)** volt. A CWPP megoldások a kezdeti virtuális gépek és konténerek védelmére lettek megalkotva, azaz a földi, hagyományos végpontvédelmi megoldások felhőbeli megfelelőjeként érdemes rájuk gondolni. Ahogy az onprem datacenterben is használunk a szervereinken akár host alapú IDS/IPS-t és a vállalat egyéb végpontjaival közös végpontvédelmi megoldást, ugyanúgy a felhős végpontjainkon is szükség van ezekre. Viszont a felhős „szervereink", a workloadok amilyen dinamikusan létrejönnek, úgy el is tűnnek pillanatok alatt a szükségeink szerint, ezért itt végpontvédelemre is hasonló dinamikára képes megoldást célszerű használni, ez a CWPP.

2014 környékén kezdődött el a nagy felhőszolgáltatók népszerűségének növekedése, leginkább az általuk kínált **IaaS (Infrastructure-as-a-Service)** megoldásuk miatt, ami már nemcsak hiperskálázható virtualizáció volt, hanem komplett virtuális infra, hálózattal, dedikált tárolással, felhasználókezeléssel, mindennel. Ez azt eredményezte, hogy a Gartner ismét kitalált egy új kategóriát, a **CSPM-et (Cloud Security Posture Management)**. Ennek a technológiának a segítségével a szervezetek megfelelően konfigurált felhős környezeteket üzemeltethetnek, azaz egy előre definiált biztonsági szabályrendszer alapján jönnek létre ad-hoc a szükséges erőforráscsomagok, template-ek alapján, egyenszilárdságú biztonsági szinttel

A következő években rengeteg innováció zajlott le a felhős világban, ami egy újabb fogalmi kategória létrehozásához vezetett. Az új kategória a **CIEM (Cloud Infrastructure Entitlements Management)**. A CIEM segítségével képesek vagyunk automatikusan szkennelni, hogy a felhasználóknak, vagy ami talán még fontosabb, hogy az egyes automatizációknak milyen jogosultságai vannak, mikre képesek a hozzáféréseik által, hogyan férnek hozzá egyes a felhőben futó szolgáltatáshoz és hogyan képesek ezeket módosítani.

Mostanáig a legfrissebb Gartner által alkotott rövidítés a **CNAPP**, azaz **Cloud Application Protection Platfor**m, amely a felhőalapú alkalmazások komplex védelmét jelenti. A CNAPP biztosítja az alkalmazás teljes fejlesztési életciklusának védelmét a kódtól a termelésig. Egyetlen platformon belül képes helyettesíteni az olyan eszközöket, mint a **CSPM (Cloud Security Posture Management)**, a **CWPP (Cloud Workload Protection Platform)**, és a **CIEM (Cloud Infrastructure Entitlement Management)**.

ÉS AKKOR ÍME A SZÁRAZ DEFINÍCIÓK:



Mit nevezünk CWPP-nek?

A Gartner definíciója szerint a CWPP egy workload-központú biztonsági megoldás, amely kielégíti a speciális követelményeket egy részben felhőben, részben pedig on-prem környezetben futtatott infrastruktúra esetében. A CWPP feladata, hogy szerver szintű munkafolyamatokat biztonságossá tegyen a public cloudban (AWS, Azure, GCP, Oracle, stb.). Képes feltérképezni a public cloudban futtatott munkafolyamatokat, amelyekre ajánlásokat tesz a jobb átláthatóság érdekében, így könnyebben felismerjük a sérülékenységeket vagy helytelen konfigurációkat ezzel biztonságosabbá téve az infrastruktúrát. Viszont ez nem egy teljeskörű biztonsági megoldás, ugyanis hiányoznak belőle azok a funkciók, amelyekkel képesek vagyunk követni a munkafolyamatok közötti kapcsolatokat és kommunikációt, így a munkafolyamatokat futtató infrastruktúráról sem kapunk széleskörű átláthatóságot. Kifejezetten a munkaterhelések védelmére összpontosít, függetlenül a típusuktól vagy helyüktől. Egy jól kialakított CWPP megoldás zökkenőmentesen együttműködik egy CSPM megoldással is.

MIÉRT FONTOS?

Az átmenet a hagyományos rendszerekről a felhőalapú alkalmazásokra nem egy automatikus folyamat. A vállalatok általában nem tudják (és a legtöbbször nem is érdemes) „lift and shift" módszerrel a felhőbe migrálni azt az alkalmazást, amely jelenleg on-premise fut. A legtöbb vállalatnak olyan örökölt alkalmazásai és infrastruktúrája van, amelyek megakadályozzák a funkciók teljes áthelyezését a felhőbe.

Sok szervezet szándékosan több felhőszolgáltatót használ, a konkrét igényeiknek megfelelően. Ennek eredményeként a vállalatok körülmények vagy tervezés szerint hibrid, többfelhős környezetben dolgoznak. Ez nehezíti a biztonsági szakemberek számára az átláthatóságot.

A fejlesztők sok esetben külső forrásból beszerzett kódokat használnak, például Githubon tároltakat. A kódok sokszor ellenőrizetlenül, egyből a CI/CD folyamatba kerülnek, ezáltal potenciális veszélyforrásokká alakulnak. A CWPP segítségével ellenőrizhetjük ezeket, így kiküszöbölve olyan sérülékenységeket vagy részleteket egy kódban, amelyek által sebezhetővé tesszük környezetünket.

Mit nevezünk CSPM-nek?

A Cloud Security Posture Management egy olyan megoldáshalmaz, ahol olyan eszközöket találunk, amelyek feladata a hibás konfigurációk és a megfelelőségi (compliance) kockázatok felismerése. További fontos tulajdonsága a CSPM eszközöknek, hogy folyamatosan monitorozzák az átfogó cloud környezetet, felismerik a hiányosságokat a policy-enforcementben (irányelvek végrehajtása kapcsán).

A CSPM platformokon automatizáható a kockázatok azonosítása, bizonyos esetekben ezeknek a javítása is a cloud környezetekben. Ez periodikus lekérdezések segítségével történik (periodical queries), aminek eredményeként riasztásokat (alerts) kapunk a biztonsági szabályok megsértéséről, bevált gyakorlatoktól (best-practice) való eltérésekről egy adott konfigurációban. A CSPM platformok segítségével a szervezetek központosított átláthatóságot és kockázatértékelést kapnak a teljes általuk üzemeltetett felhőinfrastruktúráról. Ezek lehetnek multi-cloud környezetek, ahol több felhőszolgáltatónál is üzemeltetnek erőforrásokat.

MIÉRT FONTOS?

A CSPM segítségével ellenőrizhetjük és azonosíthatjuk a compliance és konfigurációs problémákat. Ezáltal megszüntethetjük a biztonsági réseket (black hole) és széles körű átláthatóságot biztosíthatunk a hibrid és többfelhős környezetekben. A CSPM továbbá lehetővé teszi a hibás konfigurációk észlelését és javítását. Proaktívan azonosítja a felhőben található hibás konfigurációkat, például egy felhőben futó virtuális gépet, amely publikus IP címmel van ellátva, vagy egy hibásan konfigurált virtuális hálózatot. Ez segít megelőzni a biztonsági incidenseket és minimalizálni a kockázatokat.

A CSPM megoldások alkalmazkodnak az általános iparági előírásokhoz, például a HIPAA-hoz, a PCI DSS-hez, a GDPR-hez és az Azure benchmarkhoz. Emellett képesek segíteni a belső irányelvek betartását is, például az ISO 27001-es szabványban foglaltakat a kockázatkezelési folyamatok során.

Mit nevezünk CIEM-nek?

A Cloud Infrastructure Entiltements Management egy olyan megoldás, amely azonosítja az anomáliákat a fiókok jogosultságaiban. A CIEM platformokat a felhőinfrastruktúrában azonosítások és jogosultságok kezelésére használják. A legkisebb jogosultság elve alapján alkalmazzák, ezzel segítve a magasabb jogosultságok, hozzáférések engedélyezésének kiküszöbölését olyan esetekben, amikor erre nincsen szükség, így csökkentve az adatsértések kockázatát.

Nagyon hatékonyan megszüntethetőek vele a már meglévő olyan jogosultságok, amelyek egyáltalán nem – lettek használva, valamint a hibásan konfigurált jogosultságokat is felismeri. Ezzel a módszerrel megakadályozhatjuk a támadók behatolását felhőkörnyezetünkbe.

A CIEM használatával a security csapatok könnyebben tudják kezelni a hozzáféréseket a felhős környezetben, és hatékonyabban képesek nyomon követni az automatizációk hozzáféréseit is a szolgáltatásokhoz vagy infrastruktúrához.

MIÉRT FONTOS?

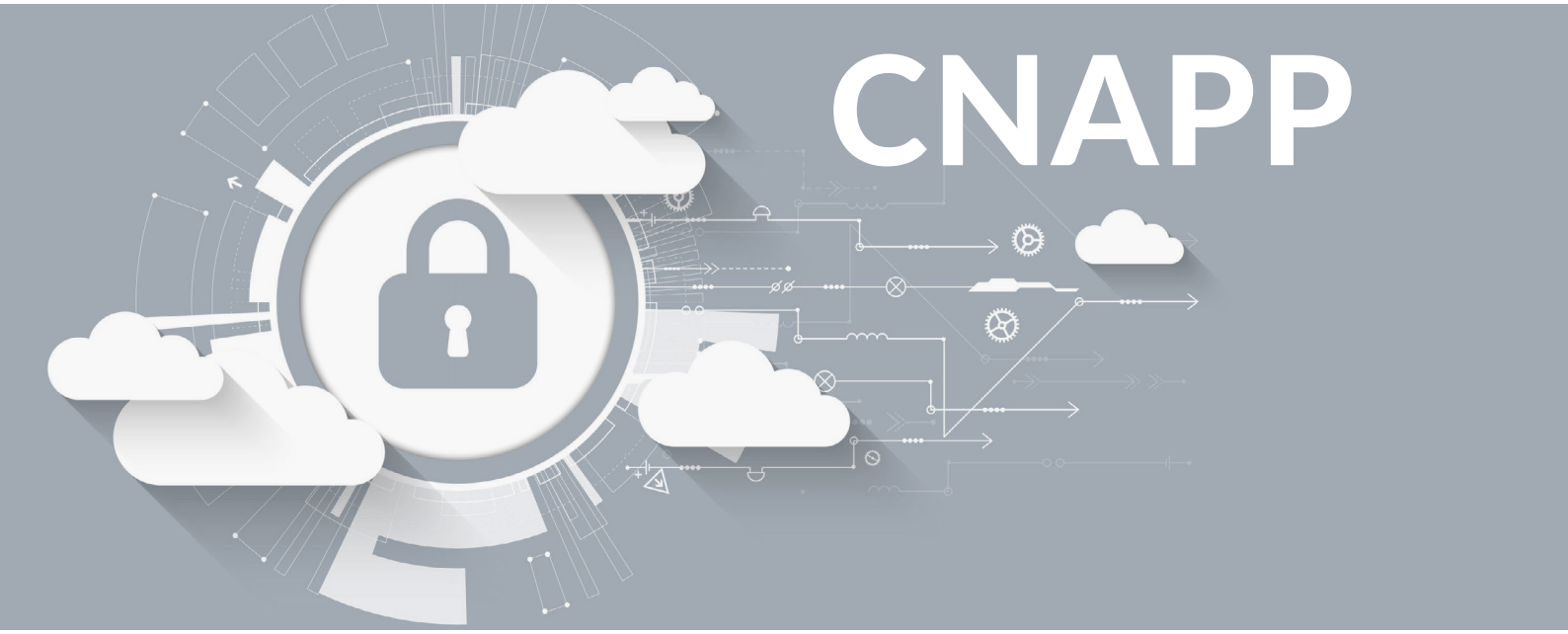
A CIEM megoldás kitölti a szervezetek felhőbiztonságában fennálló hozzáféréskezelési hiányosságait, biztosítva a hozzáférések egységes és megfelelő kezelését az összes erőforrás tekintetében.

Mit nevezünk CNAPP-nek?

A Cloud-Native Application Protection Platform teljeskörű képet nyújt a felhőbiztonsági kockázatokról. Több biztonsági megoldást integrál, többek között az összes eddig bemutatottat: ezek a CIEM, CSPM, CWPP, Compliance and risk Assessment.

Ahelyett, hogy az összes szegmenst elszigetelten vizsgáljuk, a CNAPP teljeskörű lefedettséget biztosít a felhőkörnyezetben. Képes azonosítani a kockázatokat a komplett technológiai környezetben, többek között a helytelenül konfigurált erőforrásokat, alkalmazásokat, hozzáféréseket (Identity and Access Managementet). A shift-left beépített képességének köszönhetően már az erőforrás létrehozásának szakaszában képes felismerni a sérülékenységeket és a félrekonfigurációkat. Erre egy jó példa amikor a szervezet IaC (Infrastructure as a Code) formában, Terraform használatával hoz létre automatizáltan környezeteket a felhőinfrastruktúrájában. A CNAPP ilyenkor képes már a forráskódban felismerni a hibákat, ezekről figyelmeztet és javítási lehetőséget kínál fel. Néhány CNAPP képes felhőtámadási útvonal-elemzéseket készíteni (attack-path analysis), ezzel megmutatva az alacsony kockázatúként besorolt sérülékenységek valós kockázatait.

Összefoglalva tehát, az említett technológiák már valamilyen formában a vállalatok életének részét képezik, de a közeljövőben mind az igények, mind a megfelelési kényszerek tekintetében ugrásszerű növekedésre kell számítanunk. Jól mutatja a felhő előretörését az is, hogy már a „mezei” IT biztonsági pozíciókon belül is az egyik, ha a nem legkeresettebb szaktudás a cloud és a leggyakoribb rövidítések érdemi ismerete, köszönhetően a rendkívül komplex implementációs és integrációs lehetőségeknek.



clico.hu

Security | Networking | Management

Clico Hungary Kft. • H-1134 Budapest, Dévai utca, 26-28. • +36 1 612 1309 • sales@clico.hu