A SENTINELONE-RÓL

A SentinelOne a végpontvédelmi megoldások piacán jelenlega leghatékonyabb és legátfogóbb megoldást kínáló szolgáltató.

Miért kapta meg a SentinelOne terméke az „ajánlott” minősítést az NSS Labstól az elmúlt két évben, és miért sorolta a Gartner a SentinelOne-t a „vizionáriusok” kategóriába az elmúlt három év során?

Dióhéjban: a SentinelOne a megfelelő technológia a megfelelő időben, melyet úgy alkottak meg, hogy mind ügyfeleink, mind partnereink számára egyszerűbbé tegye a végpontvédelmi folyamatokat, azaz a támadások megelőzését, észlelését és a támadásokra történő reagálást. A megfelelőség biztosítása érdekében a biztonsági iparág és az adott szakterületek képviselőivel való együttműködés eredménye, hogy a termék különböző vizsgálati intézmények ellenőrzésein (például AV-Test, AV-Comparatives, MRG Effitas, PCI-DSS, valamint HIPAA) is megfelelőnek bizonyult. A SentinelOne számára ügyfelei véleménye a legfontosabb hajtóerő. A szakterületükön globális vezető szerepet betöltő iparági szereplők rendre alapos vizsgálatnak vetik alá a gyártó termékeit, így választják jelenlegi és jövőbeli végpontvédelmi megoldásaik szállítójaként.

ELMOZDULÁS AZ AKTÍV EDR FELÉ

A napjaink kibertámadásaiban megtestesülő kihívások csak olyan átfogó végpontvédelmi megoldással kezelhetők, amely korszerű megelőzési és észlelési képességgel rendelkezik. Ezért a végpontok védelmét külön végpontvédelemre és elhárításra (EDR), valamint végpontvédelmi platformra (EPP – hagyományos vírus védelemi megoldás) bontó hagyományos szemléleten túllépve inkább az aktív EDR-megoldások számbavételén és lehetséges megvalósításán gondolkodunk. Az ActiveEDR a szervezet egészére kiterjedően skálázható, emellett az EDR- és EPP-megoldásokra egyaránt jellemző, jelentős munka- és teljesítménybeli terhelés nélkül teszi lehetővé a támadások valós idejű megelőzését, észlelését, illetve a támadásokra történő reagálást.

A SentinelOne megoldása

Az ActiveEDR működése a SentinelOne egyetlen software agent, egyetlen kódbázis és egyetlen konzol használatán alapuló architektúrájára épül. A SentinelOne szabadalmaztatott TrueContext technológiája – a hagyományos felfogás szerint külön víruskeresőből és EDR-ből álló megoldásokon túllépve – lehetővé teszi, hogy a kibertámadások során a biztonsági csoportok hamar átlássák a történések láncolatát, megtalálják a kiváltó okokat, és mindenféle felhőalapú erőforrástól függetlenül, önállóan reagáljanak. A TrueContext összefüggésbe hozza az eseményeket, és adott folyamatok csoportjához tartozó események egyedi azonosítójaként szolgál. Az ActiveEDR a biztonsági műveleti központok (SOC) szakértő elemzőitől kezdve a biztonsági csoportok kevésbé tapasztalt újoncaiig mindenki számára lehetővé teszi, hogy megjelenítse és egyből átlássa a támadás történetét anélkül, hogy órákat kellene vesződnie az események láncolatának manuális rekonstruálásával. A SentinelOne software agent arra is képes, hogy mindössze egyetlen gombra kattintva automatikusan megtisztíttassuk és helyreállíttassuk vele a rendszert, vagy visszavonassuk vele a támadások műveleteit, és ezzel visszaállítsuk a rendszert a fertőzést megelőző, megfelelő működési állapotába. A technológia lehetővé teszi a biztonsági csoportok számára, hogy a valóban fontos riasztásokra összpontosítsanak, és a technológiában rejlő lehetőségeket kiaknázva már csak asszisztálniuk kelljen a korábbiakban kizárólag ember által végezhető feladatokhoz.

VDI-k védelme

A SentinelOne software agent hatékony megoldás a virtuális gépeket, vékony klienseket, rétegelt alkalmazásokat és VDI-implementációkat magában foglaló virtuális infrastruktúra védelmére. Nem kell frissíteni, nem függ szignatúráktól, és a régebbi víruskeresőknél általában jellemző egyéb előfeltételt sem igényel. A SentinelOne VDI-khez kínált változata maradéktalanul magában foglalja a fizikai eszközöknél támogatott összes védelmi komponenst és funkciót.

A prediktív technológiák használata szükségtelenné teszi a napi/heti szignatúrafrissítéseket. Az írási/olvasási műveletek számának (disk IO lemezhasználat) csökkentésével és az egyidejűleg hirtelen fellépő terhelések (IO storms) megelőzésével javítani tudjuk a szervezetek virtuális infrastruktúrájának „VM density" mutatóját. A konzol automatikusan kiiktatja a már nem használt VDI-példányokat, ezzel mérsékli a rendszerfelügyeleti terheket, és megakadályozza, hogy kiiktatott „szellem végpontok" jelenjenek meg a felügyeleti konzolon. A SentinelOne egyaránt támogatja a perzisztens és a nem perzisztens működési módot, a kapcsolt klónok használatát és a felhőbeli üzemeltetést.

A szoftver a nagyvállalati licenchez kapcsolódó „Concurrent" (egyidejű munkamenetre szóló) licencelési konstrukció keretében használható. A SentinelOne házirendje natív módon menedzseli ezt, például automatikusan kiiktatja a software agenteket.

Deep Visibility

A SentinelOne és a Deep Visibility együtt hatékony és könnyen kezelhető megoldást nyújt a változó körülmények között. A Deep Visibility egyedülálló módon képes betekinteni a titkosított forgalomba, és felfedni az eseményeknek egészen a megfertőzésre tett próbálkozásokig terjedő láncolatát. A SentinelOne a Deep Visibility összetevővel együtt védelmet nyújt az adatokkal való visszaélésekkel szemben, monitorozza az adathalászatra irányuló próbálkozásokat, felismeri az adatszivárgást és rálátást nyújt több eszközre is. Mindezt úgy, hogy közben automatikusan mérsékli e próbálkozások negatív hatását az incidensek során. A Visibility a csatorna végén figyeli a forgalmat, ami lehetővé teszi, hogy egyedülálló módon, dekódolást nem igényelve és az adatátvitel megzavarása nélkül felügyelhesse a teljes forgalmat. Így a komponens egyrészt rejtve marad a tűzfal megkerülésére irányuló támadások elől, másrészt a felhasználói élményt is csak minimális mértékben befolyásolja.

A Deep Visibility teljeskörűen lehetővé teszi a fertőzöttségre utaló jelek keresését valamennyi végponti és hálózati tevékenységben, és olyan, információkban gazdag környezetet nyújt a fenyegetések felkutatásához, amelyben hatékony szűrők is használhatók, a fertőzött eszközök pedig elhatárolhatók. Mivel a Deep Visibility a SentinelOne EPP-platform szerves részét képezi, és nem igényel további software agentet, ezért ez az összetevő a kivizsgálási, kárenyhítési és reagálási képességekbe is teljesen integrálva van. A biztonsági csoportok így gyorsan el tudják intézni a Deep Visibilityn keresztül felfedezett fenyegetésekkel kapcsolatban szükséges teendőket: mélyreható vizsgálatot folytathatnak a folyamatokról, karanténba helyezhetik a fertőzött fájlokat és gépeket, illetve teljes körű, dinamikus helyre- és visszaállítást is végezhetnek.

A veszélyforrások menedzselt felismerése és menedzselt reagálása

A Vigilance a SentinelOne veszélyforrások menedzselt felismerésére és a menedzselt reagálásra (MDR) irányuló szolgáltatása, melyet egy magas szinten képzett kiberbiztonsági elemzőkből álló csoport nyújt. A szolgáltatás azzal lehet az informatikai/biztonsági műveleti központok segítségére, hogy az összetett kiberfenyegetések felismerésének, rangsorolásának és e fenyegetésekre történő reagálás folyamatának felgyorsításával csökkenti annak kockázatát, hogy a központok esetleg figyelmen kívül hagyjanak más, odafigyelést igénylő, kritikus riasztásokat. A Vigilance-csoport elemzői végignézik az összes riasztást, áttekintik a még feldolgozatlan fenyegetettségi adatokat, a folyamatok működését és a hálózati kapcsolatokat, és szükség esetén mintákat is elemeznek. A csoport tagjai váltott műszakban dolgoznak, de maga a csoport a hét minden napján, napi 24 órában rendelkezésre áll. A csoport a házirendek finomhangolásában, a kizárások kezelésben és a téves riasztások számának mérséklésében is tud segíteni. Választható „Monitor" és „Respond" szolgáltatáscsomag – előbbi a riasztások rangsorolása mellett javaslatokat foglal magában, utóbbi keretében pedig a szakértők az eseményekkel kapcsolatos intézkedésekkel tekintetében is segítenek.

SentinelOne-csomagok

SentinelOne Core: Azoknak a szervezeteknek ajánljuk, amelyek első osztályú védelmet igényelnek, ugyanakkor nem akarnak vesződni a komplex menedzseléssel együtt járó nehézségekkel, és jól képzett biztonsági elemzőkre sincs szükségük. A SentinelOne egyetlen software agentben egyesíti a kockázatmegelőzési, támadásészlelési és incidensekre való reagálási funkciókat, és ez az agent Windows, Mac és Linux rendszerek védelmére egyaránt alkalmas. A SentinelOne „Core" csomag képezi a platform alapját.

SentinelOne Control: Azoknak a szervezeteknek kínáljuk, amelyek a SentinelOne „Core" csomagba foglalt elsőrangú védelmen túl olyan biztonsági funkciókat is szeretnének, amelyekkel a kiterjedt végpontmenedzsment – például az eszközök felügyelete és a végpontok tűzfalas felügyelete is – egyszerűbbé tehető. Ez a csomag azzal is könnyíti az IT-csoportok munkáját, illetve egyedülálló végpont-felügyeleti lehetőségeket kínál, hogy távoli gépeken is szabadon meg lehet vele nyitni a parancssort.

SentinelOne Complete: Azoknak a szervezeteknek lesz tökéletes választás, amelyek a korszerű végpontvédelmen és felügyeleti funkciókon túl a fenyegetések felkutatásának lehetőségét is szeretnék megadni biztonsági műveleti központjuk számára. A SentinelOne „Complete" csomag a biztonsági adminisztrátorok, a biztonsági műveleti központok elemzői és az incidensekre reagálók igényeit is kielégíti. A legszigorúbb elvárásokat támasztó globális nagyvállalatok megalkuvást nem ismerő kiberbiztonsági igényeik miatt választják a SentinelOne „Complete" csomagot. Ebben a csomagban az alapmegoldás a Deep Visibility Threat Hunting modullal egészül ki, amellyel a vállalat biztonsági műveleti központjának tagjai, illetve a technológia iránt érdeklődő szakemberek alaposan feltérképezhetik a fenyegetéseket, remek rálátást kapnak az események láncolatára, és árnyalt reagálási képességek birtokába jutnak.

The next-gen suite of the future - born from the endpoint and orchestrated by AI

One Agent | Windows | Mac | Linux | On-prem | Cloud

EPP	EDR	Manageability	Services	Cloud Intel.
Static AI	Threat Hunting	Device Control	Vigilance MDR	Threat Feeds
Behavior AI	IOC Search	API and SDK		IP Reputation
Anti-Exploitation	Remediation	Application Inventory		Automated Analysis
Lateral Movement	Encrypted Traffic Visibility	File Integrity Monitoring		Shared Intelligence
Credential Theft Prevention	Containment and Rollback	Vulnerability & Patch Management		

USER ENDPOINT CLIENTS

Windows XP, 7, 8, 8.1, 10

Mac OSX 10.9.x, 10.10.x, 10.11x, macOS 10.12x macOS 10.13 (High Sierra), macOS 10.14 (Mojave), macOS 10.15.x (Catalina)

CentOS 6.5, 7.0, 7.1–7.7,7.8, 8.0, 8.1

Red Hat Enterprise Linux 6.5, 7.0, 7.1–7.7,7.8, 8.0, 8.1

Ubuntu 12.04, 14.04, 16.04, 16.10, 18.04, 19.04, 19.10, 20.04

openSUSE 42.2

SERVER ENDPOINT CLIENTS

Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, 2019

CentOS 6.5, 7.0, 7.1-7.7,7.8, 8.0, 8.1
Red Hat Enterprise Linux 6.5, 7.0, 7.1-7.7,7.8, 8.0, 8.1

Ubuntu 12.04, 14.04, 16.04, 16.10, 18.04, 19.04, 19.10, 20.04

SUSE Linux Enterprise Server 12.x, 15.x

Oracle Linux 6.5 - 6.9, 7.0+

Amazon Linux (AMI) 2016.09+, 2017.03+, 2018.03, AMI 2

VIRTUAL ENVIROMENTS

Citrix XenApp
Citrix XenDesktop
Oracle VirtualBox
VMware vSphere
VMware Workstation
VMware Fusion
VMware Horizon (Agent version 2.6.x)
Microsoft Hyper-V (requires the VHD file)

Gartner Visionary

SentinelOne

CLICO
sentinelone@clico.hu