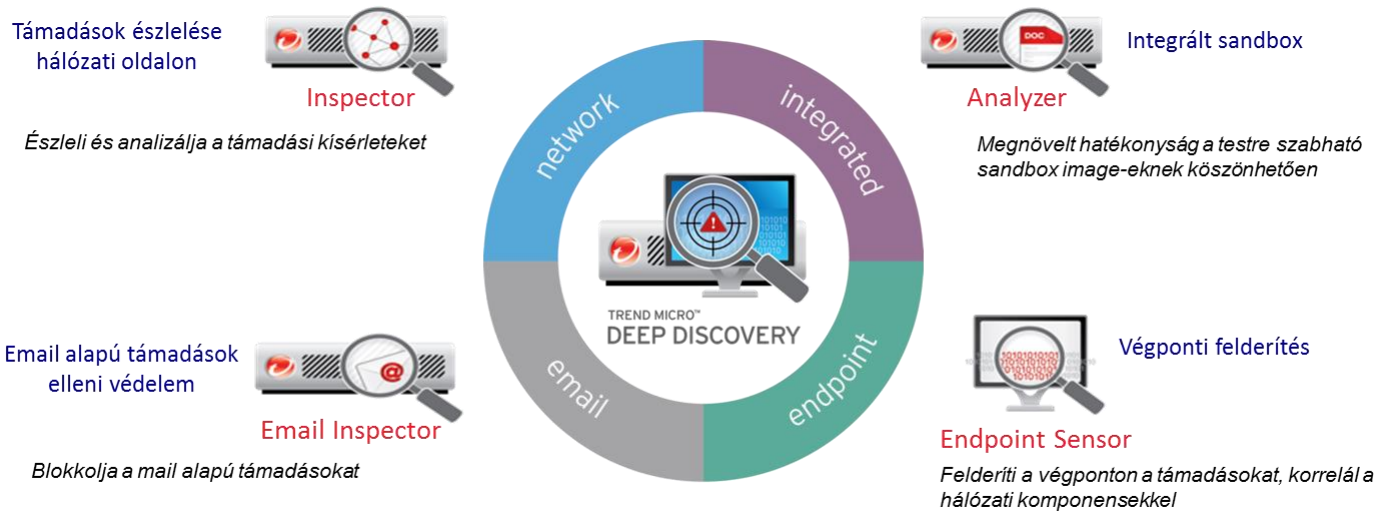
Trend Micro™ DEEP DISCOVERY

Magasszintű védelem a célzott támadások ellen

A Trend Micro Deep Discovery egy magasszintű védelmi platform, ami lehetővé teszi a rejtett, célzott támadások észlelését, elemzését és a megfelelő válaszadást. Specializált észlelő motorja, az ügyfél teljes környezetét modellező virtuális emulátor (sandboxing) és a Trend Micro™ Smart Protection Network™ által szolgáltatott globális fenyegetettségi infromációk segítségével védelmet nyújt a hagyományos biztonsági eszközök számára láthatatlan támadások ellen. Akár önállóan, akár valamilyen integrált megoldás részeként telepítve a Deep Discovery hálózati-, email-, végponti- és beépített moduljai ott nyújtanak kiemelkedő védelmet a célzott fenyegetések ellen, ahol a vállalatnak a leginkább szüksége van rá.



A Deep Discovery platform legfontosabb tulajdonságai

- **Fejlett fenyegetés felderítés:** specializált keresőmotorjával, korrelációs szabályokkal és az ügyfél teljes környezetét modellező virtuális emulátor (sandboxing) segítségével azonosítja a hálózati támadásokat
- **Egyedi virtuális emulátor (sandboxing):** olyan egyedi virtuális környezet hozható létre segítségével, ami teljes mértékben megegyezik az ügyfél rendszerbeállításaival így észlelve a specializált támadási kísérleteket
- **Smart Protection Network™ intelligencia:** valós idejű, felhő alapú biztonsági intelligencia információk a fenyegetések felderítésére és a részletekbe menő vizsgálathoz
- **Más rendszerekkel való integráció:** IOC (Indicator of Compromise) információk megosztása más Trend Micro vagy egyéb gyártók biztonsági megoldásaival a további támadások megakadályozására

Támadások észlelése hálózati oldalon

Trend Micro Deep Discovery Inspector hálózati eszköz, mely figyeli több mint 80 protokoll és alkalmazás átmenő forgalmat. Specializált keresőmotorjával és egyedi virtuális emulátor (sandboxing) képességével azonosítja a rosszindulatú programokat, C&C és egyéb aktivitásokat, melyek támadást jelezhetnek. A felderítési intelligencia segít a gyors válaszadásban és automatikusan megosztásra kerül más biztonsági termékekkel a további támadások blokkolására.

Email alapú támadások elleni védelem

Trend Micro Deep Discovery Email Inspector email biztonsági eszköz, mely fejlett kártékony program felderítési képességével, és virtuális emulátor (sandboxing) moduljával azonosítja és blokkolja az adathalász leveleket, melyek jellemző kezdeti lépései a legtöbb célzott támadásnak. Olyan transzparens vizsgálati szintet kínál, ami felfedezi a káros tartalmakat, csatolmányokat és URL linkeket, melyek észrevétlenül átjutnak a hagyományos email biztonsági megoldásokon.

Végponti felderítés

Trend Micro Deep Discovery Endpoint Sensor tartalomfüggő végponti biztonsági monitorozó megoldás, mely részletes rendszeraktivitást rögzít és riportol, hogy az elemzők gyorsan felmérhessék egy támadás természetét és kiterjedését. A Deep Discovery vagy más eszközöktől származó IOC intelligencia adatok felhasználhatók a végpontok szkennelésére a beszivárgás megerősítésére és a támadás teljes idősíkjának és tartalmának felderítésére.

Integrált sandbox

Trend Micro Deep Discovery Analyzer nyílt, egyedi virtuális emulátor (sandbox) analízis szerver, ami megnöveli a kártékony programok észlelésének képességét. Az Analyzer natív integrációs lehetőséget kínál számos egyéb Trend Micro megoldással, manuális vagy nyílt Web Services interface alapú file feltöltésre, hogy más termékek vagy folyamatok is hozzáférjenek az elemzés eredményéhez.

Központi menedzsment és vizsgálat

A **Deep Discovery Threat Intelligence Center** központi menedzsment és riportolási funkciókat biztosít az összes komponens számára. A legtöbb modul integrálható a Trend Micro Control Manager™-rel csakúgy, mint a népszerű SIEM megoldásokkal (IBM QRadar, HP ArcSight, Splunk) az egész vállalatra kiterjedő vizsgálatok és riportolás érdekében

Bővebb információ:

http://www.trendmicro.co.uk/products/deep-discovery/index.html