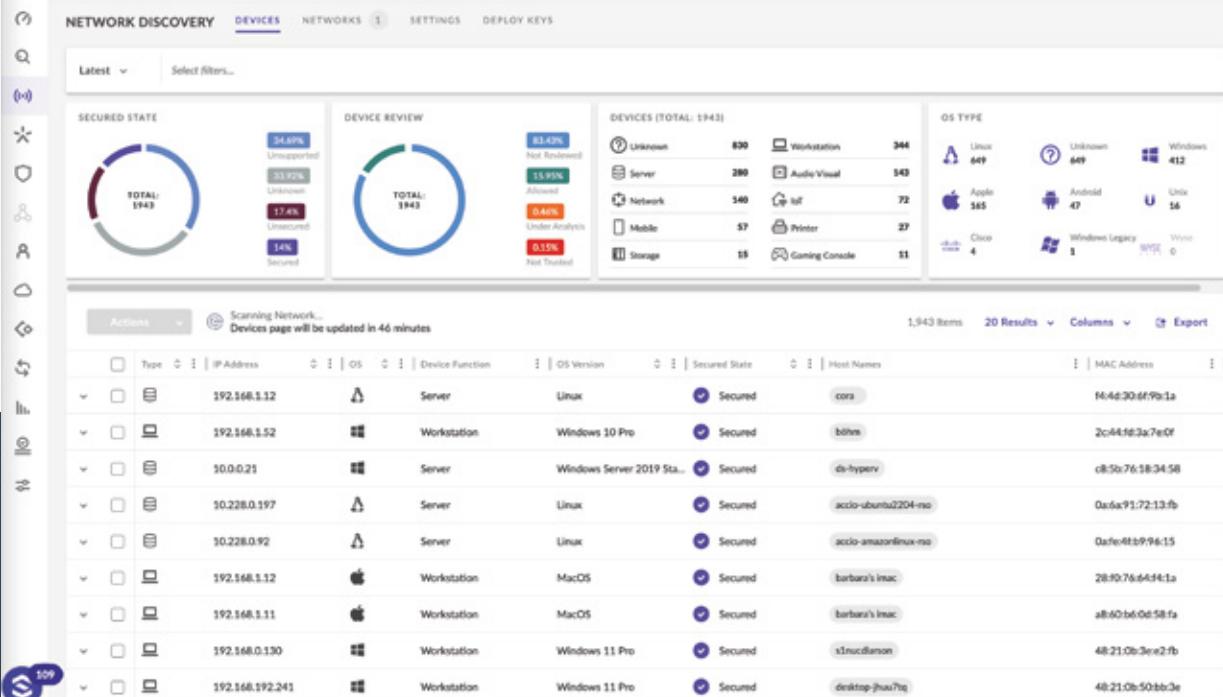


# Ochráňte svoje dátá, podnikanie a ľudí

## Všetko prehľadne v jednej konzole, alebo konzola podľa zákazníka

Podporujeme Windows, macOS, Linux, Android a iOS a cloud platformy AWS, Azure a Google.

Kompletný prehľad o pripojených počítačoch s možnosťou správy na diaľku, inštalovania aplikácií, púšťania scriptov, správy súborov a procesov. Súčasťou riešenia je prehľadný reporting.

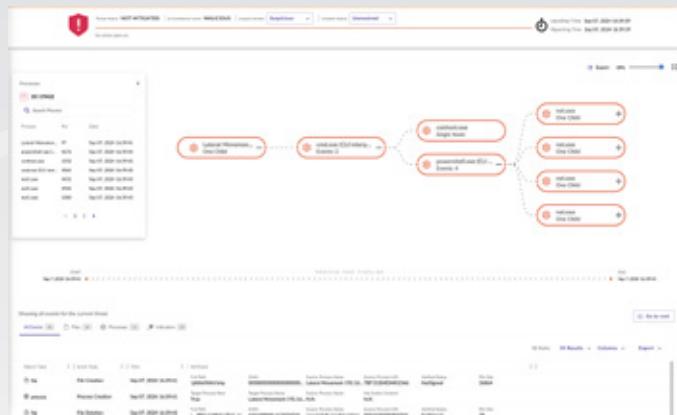
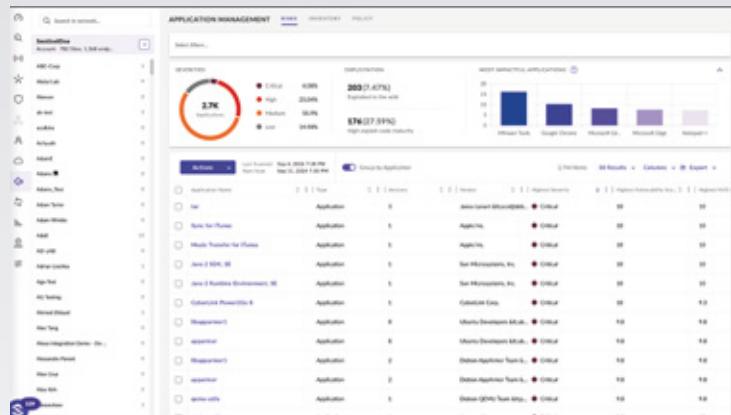


The screenshot displays the SentinelOne Network Discovery interface. At the top, there are four main sections: SECURED STATE (showing 1943 total devices with 34.6% unsupported, 33.9% unknown, 17.4% unsecured, and 14% secured), DEVICE REVIEW (showing 81.83% not reviewed, 15.95% allowed, 0.46% under analysis, and 0.55% not trusted), and two tables for DEVICES (total 1943) and OS TYPE. The DEVICES table includes columns for icon, name, count, and type (e.g., Workstation, Server, Network, Mobile, Storage, Gaming Console). The OS TYPE table shows counts for Unknown, Linux, Apple, Android, Unix, Cisco, Windows Legacy, and WINE. Below these is a large table listing 1,943 items, with columns for Actions, IP Address, Device Function, OS Version, Secured State, Host Names, and MAC Address. The table lists various devices including servers, workstations, and gaming consoles running Linux, Windows, and macOS, along with their respective MAC addresses.



# PREHĽAD O NAINŠTALOVANÝCH APLIKÁCIÁCH A ICH ZRANITEĽNOSTIACH

# ANALÝZA "CAUSALITY CHAIN" V PRÍPADE BEZPEČNOSTNÉHO INCIDENTU



# RIEŠENIE PATRÍ MEDZI ŠPIČKU NA TRHU V OBLASTI ENDPOINT PROTECTION PLATFORM, ČO DOKAZUJE UMIESTNENIE MEDZI LEADRAMI V RENOMOVANOM MAGIC QUADRANTE OD SPOLOČNOSTI GARTNER.



**KONCOVÁ  
CENA  
OD 5€  
/mesiac**

Cena je bez DPH



 +421 905 727 605

 bezpecnost@asenti.sk



[www.asenti.sk](http://www.asenti.sk)

# BEZPEČNOSTNÉ FUNKCIE

## Inventár aplikácií

Agent je chránený proti neoprávnenej manipulácii

Analýza incidentov (MITRE ATT&CK®, časová os, prieskumník, anotácie tímu)

Karanténa zariadenia zo siete

Autonómna odozva na vrátenie / 1 kliknutie, žiadne skriptovanie (Win)

Autonómna odpoveď na nápravu / 1 kliknutie, žiadne skriptovanie (Win, Mac)

Autonómna reakcia na hrozbu / zabitie, karanténa (Win, Mac, Linux)

Behaviorálna detekcia útokov AI fileless

Statická AI a SentinelOne Cloud ochrana pred útokmi file-based

Autonómny nástroj Sentinel Agent Storyline

Zraniteľnosť aplikácie (Win, Mac)

Rouge Device Discovery

Ovládanie Bluetooth / BLE (Win, Mac)

Ovládanie OS Firewall so znalosťou polohy (Win, Mac, Linux)

Secure Remote Shell

**Vstavaná statická AI a behaviorálna analýza AI zabraňuje a detektuje širokú škálu útokov v reálnom čase skôr, ako spôsobia poškodenie. SentinelOne chráni pred známym a neznámym malvérom, Trójskymi koňmi, hackerskými nástrojmi, ransomvérom, zneužitím pamäte, zneužitím scriptov, škodlivými makrami a ďalšie.**

- ✓ Sentinely sú autonómne, čo znamená, že uplatňujú prevenciu a detekčnú technológiu s cloudovým pripojením alebo bez neho a spustia ochranné reakcie v reálnom čase.
- ✓ Obnova je rýchla a používateľov dostane späť k práci v priebehu niekoľkých minút bez reinštalácie počítača a bez písania scriptov. Akékoľvek neoprávnené zmeny, ktoré sa vyskytnú počas útoku, možno zvrátiť pomocou 1-Click remediation a 1-Click Rollback pre PC s Windows.
- ✓ Analýza incidentov s integráciou MITRE ATT&CK®, a ďalšie.
- ✓ Firewall Control pre kontrolu sietového pripojenia do a zo zariadení vrátane povedomia o polohe
- ✓ Device Control pre ovládanie USB zariadení a Bluetooth/BLE periférií
- ✓ Rogue visibility na odhalenie zariadení v sieti, ktoré potrebujú ochranu Sentinelovým agentom
- ✓ Správa zraniteľností, okrem toho aj pre prehľad o aplikáciách tretích strán, ktoré obsahujú známe zraniteľnosti mapované do databázy MITRE CVE

