SentinelOne är först med att använda endpoint-säkerhet för att kartlägga och kontrollera IoT.

SentinelOnes nya mjukvara Ranger använder befintliga klienter och servrar för att kartlägga, kontrollera och skydda varje IoT-ansluten enhet i nätverket.

Stockholm den 24 maj 2019: Säkerhetsföretaget SentinelOne, ledande inom Endpoint detection, har lanserat SentinelOne Ranger – där varje enskild skyddad slutpunkt fungerar som detekteringsenhet med kapacitet att identifiera och styra alla IoT-enheter som finna anslutna i nätverket. SentinelOne är med detta den första och enda cybersäkerhetsleverantör som konvergerar EPP och EDR till en unik lösning som nu även omfattar IoT.

“Nästa nivå för alla cybersäkerhetsprogram är möjligheten att upptäcka och skydda IoT-enheter. SentinelOne Ranger-lösning är den första av sitt slag och gör stor skillnad när det gäller att hjälpa företag att säkra sina ständigt växande nätverk,” säger Les Correia, chef för global informationssäkerhet, arkitektur, teknik och verksamhet på Estée Lauder. Han fortsätter:
”Vid 2030 förväntas det finnas mer än 125 miljarder anslutna IoT-enheter, många med obefintlig eller ingen inbyggd säkerhetsfunktion. Dessutom blir enheter som adderas till företagsnätverk allt mer intelligenta, från TV till brödrostar till kroppsnära teknik, så kallade wearables. Resultatet är att mer kod körs på allt fler enheter, vilket dramatiskt ökar antalet potentiella sårbarheter för en angripare att rikta in sig på. För närvarande saknar företagens säkerhetsteam möjligheten att distribuera programvara på dessa fragmenterade enheter, vilket resulterar i en total brist på insikt i företagsmiljön och förmåga att kunna inventera företagsnätverken med precision. Att uppnå en sådan medvetenhet och inventering genom manuella processer är helt enkelt omöjligt.”

SentinelOne Ranger löser detta kritiska problem genom att ge maskiner möjlighet att upptäcka och skydda andra maskiner, så att de kan detektera miljön och avvärja attacker från varandra utan mänsklig inblandning. Med hjälp av AI som övervakar och styr åtkomst till varje IoT-enhet, möjliggör SentinelOne att maskiner löser ett problem som tidigare varit omöjligt att adressera. Tekniken kan inte bara peka ut och profilera enheter som SentinelOne-agenten upptäcker, vilket möjliggör fullständig transparens, utan kan även identifiera om någon aspekt av miljön är farlig. SentinelOnes Ranger-teknik är branschens första lösning som gör att maskiner autonomt kan skydda och underrätta säkerhetsansvariga om svagheter, oseriösa enheter och avvikande beteende.

”Företagen kan ha tusentals nya enheter anslutna till sina nätverk, ofta utan att ens veta om det. Med IoT finns det ingen möjlighet att distribuera programvara eller

tillhandahålla den manuellt, vilket skapar en enormt sårbar miljö som riskerar att angripas," säger Tomer Weingarten, VD och medgrundare, SentinelOne.

"Ranger är i frontlinjen när det gäller ändpunktsskydd. SentinelOne-agenten gör inte bara en kartläggning av varje enskild slutpunkts försvar, vem eller vad som kan anslutas till det och varifrån den kan anslutas. Den kompletterar även synligheten till det omgivande nätverket, identifierar närliggande IoT-enheter i nätverket och förhindrar högriskenheter att ansluta till dem. Dessutom segmenterar det effektivt ut oönskade anslutningar och reducerar onödig attackyta. Vi är övertygade om att det här är revolutionerande för marknaden och för våra kunder," säger Tomer Weingarten.

Om SentinelOne

SentinelOne levererar autonomt ändpunktsskydd genom en enda agent som automatiskt förhindrar, detekterar och spårar alla attacker. SentinelOne plattformen är konstruerad så den är extremt enkel att använda och sparar tid för kunder genom att tillämpa AI som automatiskt eliminerar hot i realtid både lokalt och i molnet och är den enda lösningen som ger fullständig synlighet över nätverk direkt från slutpunkten. För mer information besök sentinelone.com eller följ oss på @SentinelOne, LinkedIn eller Facebook.

Presskontakt:
Susan Rose, tel. 073 300 3010. E-post susan@susanrose.se