LE VIOLAZIONI NON FANNO ECCEZIONI

Tre motivi per cui è importante una soluzione EDR per dispositivi mobili

In passato il tuo obiettivo era proteggere l'endpoint. Oggi invece vuoi proteggere i dati, perché i cybercriminali possono attaccarli ovunque siano, su computer desktop o dispositivi mobili. Ecco tre motivi per cui è importante una soluzione di rilevamento endpoint e risposta (Endpoint Detection and Response, EDR) per dispositivi mobili.

Tutti i dipendenti hanno un dispositivo mobile.

Se la tua soluzione EDR copre solo gli endpoint tradizionali, non potrai contrastare gli attacchi provenienti da dispositivi mobili, ritrovandoti con una grave falla di sicurezza.

La protezione da sola non basta.

Avere un sistema di protezione degli endpoint è un buon punto di partenza, ma non tutti gli attacchi sono generati da file dannosi. Devi essere in grado di rilevare gli attacchi file-less, qualunque sia l'endpoint di provenienza.

L'EDR tradizionale non è efficace con i dispositivi mobili.

I sistemi operativi dei dispositivi mobili non hanno mai consentito l'accesso al kernel e hanno sempre imposto alle applicazioni di operare in modo isolato. L'approccio tradizionale basato sul perimetro di rete e l'analisi dei contenuti non funziona più.

Come funziona una soluzione EDR per dispositivi mobili?

Una soluzione EDR avanzata per dispositivi mobili ti permette di capire se un attacco ha preso di mira i dispositivi mobili, dove si trova l'aggressore e cosa fa, anche se non c'è un malware. In più ti consente di rilevare e isolare gli incidenti sul dispositivo e avere indicazioni su come risolvere il problema in autonomia.

Stai cercando una soluzione EDR per dispositivi mobili?
Visita lookout.com per saperne di più.

Lookout®