virsec™

5 Reasons

Why EDR and EPP Solutions Cannot Fully Protect Application Workloads on Servers

> Security teams are dealing with challenges from too many alerts and too many missed attacks that rely on detection and response methodologies.
>
> Here are **5 Key Reasons** why EDR and EPP technologies are not well-suited to protecting applications and processes running on servers.

5 Key Reasons Why EDR and EPP are Not Enough

1 

Servers and End-user Endpoints are Fundamentally Different

Applications on server workloads are fundamentally different than those running on end-user endpoints. Endpoints are operated directly by human beings and therefore, are soft spots for adversaries to take advantage of—workloads don't get spear phished; users do.

2 

Easy to Bypass

Traditional EDR and EPP approaches focus on detection and response of host attacks by comparing the sequence of system processes against a set of processes known to be used by attackers. Attackers can easily bypass EDR and EPP systems by using out of the norm attack processes with no known signatures.

3

The Denylist Model Doesn't Work

Denylists force users to make decisions in real time on whether a given code is malicious or not. One wrong decision and the workload can be compromised. Tens of thousands of new malware are created daily and users are not able to adapt and scale to maintain protection.

4

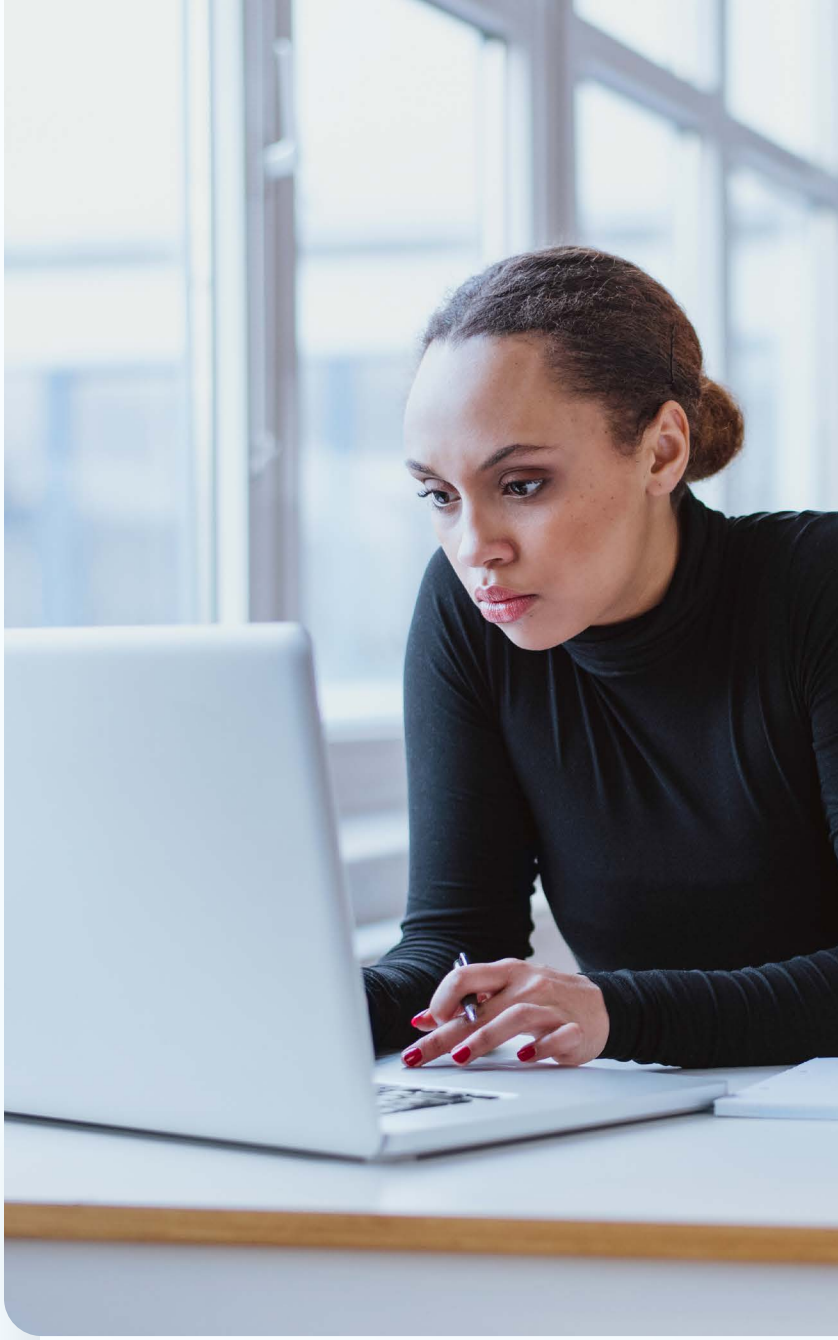
No Protection from Unknown Attacks

Using the detect and respond model, EDR or EPP alone cannot protect against unknown attacks. This leaves organizations exposed to stealth attacks that can exfiltrate sensitive data.

5

Operational Complexity

EDR and EPP rely on large teams of highly skilled security analysts to triage alerts. Spending hours analyzing false positives, these analysts come at an additional cost.



Learn more

To learn more about Deterministic Protection Platform by Virsec, visit us here: www.Virsec.com or contact us for a personalized demonstration