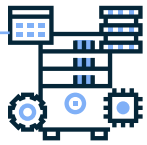
VIRSEC

FIVE REASONS
EDR AND EPP SOLUTIONS CANNOT PROTECT APPLICATION WORKLOADS

There are five key areas where EDR and EPP technology isn't suited to analyze behavior in applications, on servers or processes that occur during runtime.

1



Applications on Server/ Workloads are fundamentally different than those running on devices.

Applications running on your servers and workloads and those running on devices and laptops are fundamentally different. Users, purposes and performance requirements for these applications are also different and therefore require different means of protection.

2

Exploits targeting servers and workloads are also fundamentally different.

Given the above, it stands to reason that attackers would use different methods in going after applications and workloads. Their methods are stealthier and have no trouble getting by endpoint tools – i.e., the same tools designed to protect endpoints are not equipped to handle exploits that target applications and workloads.

3

The blacklisting model is old and doesn't scale.

Blacklisting has been around for a long time but it's become obsolete because it can no longer keep up with today's threats. In the infinite universe of potential malware, finding everything bad and blocking it before an attack happens is not realistically possible. It's an approach that by definition always runs behind current threats.

4

Reactive security models always fall behind.

Most security tools operate in reactive mode. When EDR tools see something suspicious, they might run some algorithms to try to analyze the activity. If external analysis determines that the activity is bad, the hope is next time the tools will be able to stop it. But that is too slow for organizations. It puts them always in reactive mode – too little, too late. Aware they are always being tracked, attackers are constantly morphing and changing their techniques to escape detection.

5

Advanced exploits today bypass EDR security tools.

All of these areas together demonstrate the ways in which EDR solutions cannot protect applications and systems from the kinds of obfuscated code used in advanced attacks. The failure to address this risk can be catastrophic, as we recently saw in the December 2020 SolarWinds attack.