5 Keys to Protecting Legacy Applications

It is time to break free from *the older the code, the more vulnerabilities* and embrace ***security that leaves no applications behind.***

Following are the five key challenge areas to protecting legacy applications that can be solved with deterministic protection:

1 Understand the Software

For many reasons, detecting unusual behavior by legacy applications while they're running is extremely difficult for any organization or agency.

Solution: Protection that determines what an application is supposed to do and immediately stops anything it should not—before an attack happens.

2 Make Age Inconsequential

Legacy applications may be years to decades old and no longer supported. Often patches are no longer available, and finding individuals with expertise to address vulnerabilities is difficult—technology has advanced & developers of the original source code have moved on.

Solution: Protection despite no prior knowledge or access to code — making age inconsequential.

3 Keep the Uptime Promise

Ensuring the resilience of the application in the face of an attack is challenging for vulnerable legacy applications. Many are so outdated and remain exposed to risk without proper protection in place.

Solution: Software is protected while it is running, wherever it is running—with no downtime.

4 Mitigate Risk of Third-Party Code

Most enterprises rely heavily on commercial off-the-shelf applications & third-party software components that have an increasing number of vulnerabilities which you cannot fully resolve yourself.

Solution: An approach that fully protects your software—bugs and all.

5 Reach For the Clouds

Legacy applications are often deployed in hybrid-cloud environments or ported to containers.

Solution: Workloads that have the same level of protection wherever they are running, regardless of the platform.