

# Why **PATCHING** Will Never Be Enough



## **TOO SLOW**

Hackers exploit vulnerabilities in hours; patches take weeks or months.

## **TOO FRAGILE**

Legacy and embedded systems can't always be updated without disruption.



## **TOO REACTIVE**

New zero-days appear faster than patches can be developed.

## **ELIMINATE AN ENTIRE CLASS OF VULNERABILITY**

Protect critical systems before patches exist. Runtime code protection neutralizes buffer overflows, use-after-free attacks, and other memory exploits.



## **BUILD RESILIENCE BEFORE THE NEXT PATCH CYCLE**

Protect embedded devices across critical infrastructure. RunSafe Protect delivers memory safety **without the wait for patches.**

[LEARN MORE](#)