

security<sup>®</sup>  
quotient.

# HOW TO PREVENT FILELESS ATTACKS?

# 1

## **Monitor system tools**

Regularly monitor for unauthorized user privileges, remote command executions, unfamiliar processes in memory, and suspicious registry modifications.

# 2

## **Use behavior analysis**

Establish normal behavior patterns and identify deviations, like unusual database access or logins, to detect potential fileless attacks.

# 3

## **Regularly update & patch systems**

Regularly update and patch systems to close vulnerabilities and reduce entry points for fileless attackers.



**Change human cyber  
security behavior with**

**security<sup>®</sup>  
quotient.**

Singapore | India | Malaysia