

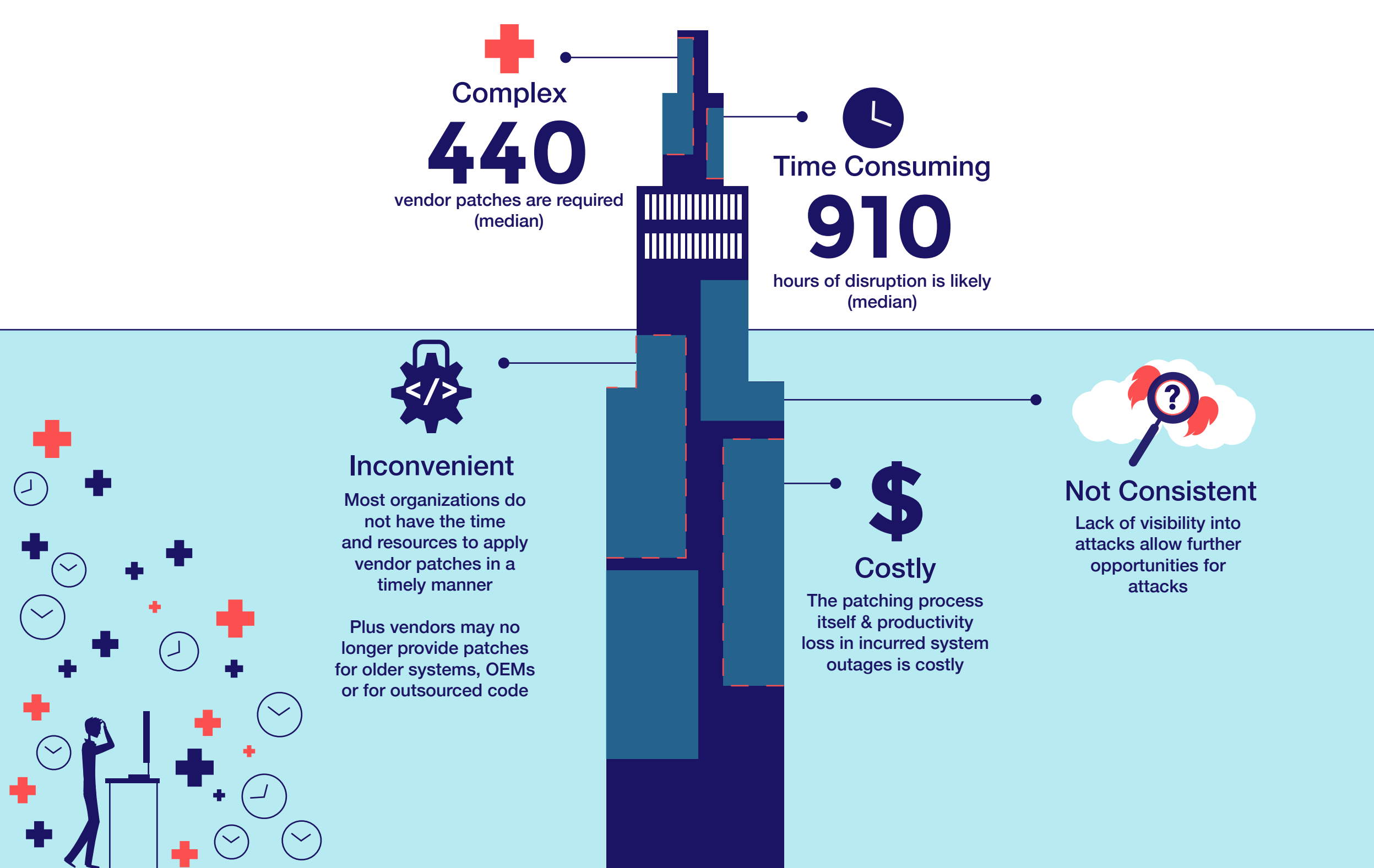
# The Case for Virtual Patching

## Reducing the Risk of Database and Application Vulnerabilities

In comparison to traditional vendor patching, virtual patching can be a highly effective strategy for addressing both the likelihood and business impact aspects of security-related risk. Here's why.

### PROBLEMS WITH VENDOR PATCHING

OVER 12 MONTHS, IN A \$100M COMPANY WITH 100 INSTANCES - VENDOR PATCHING IS FOUND TO BE:

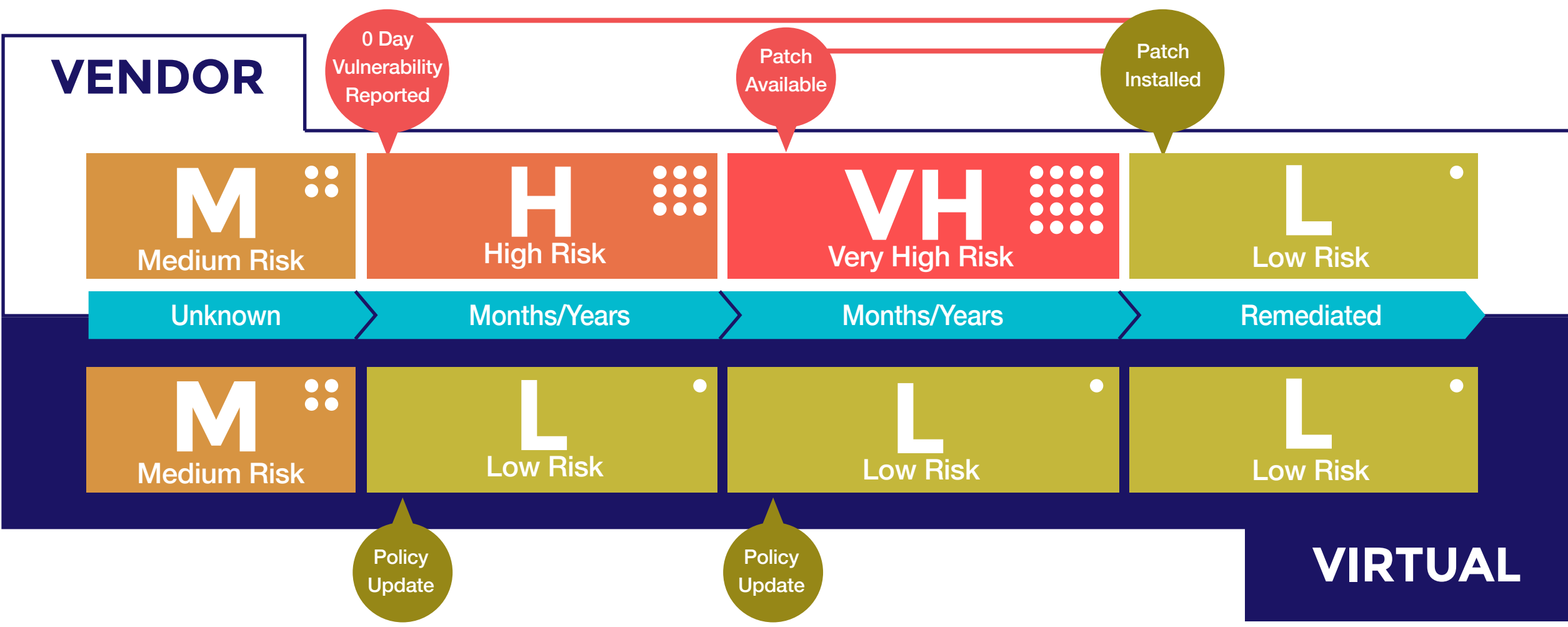


### VIRTUAL PATCHING REDUCES THE LIKELIHOOD OF RISK

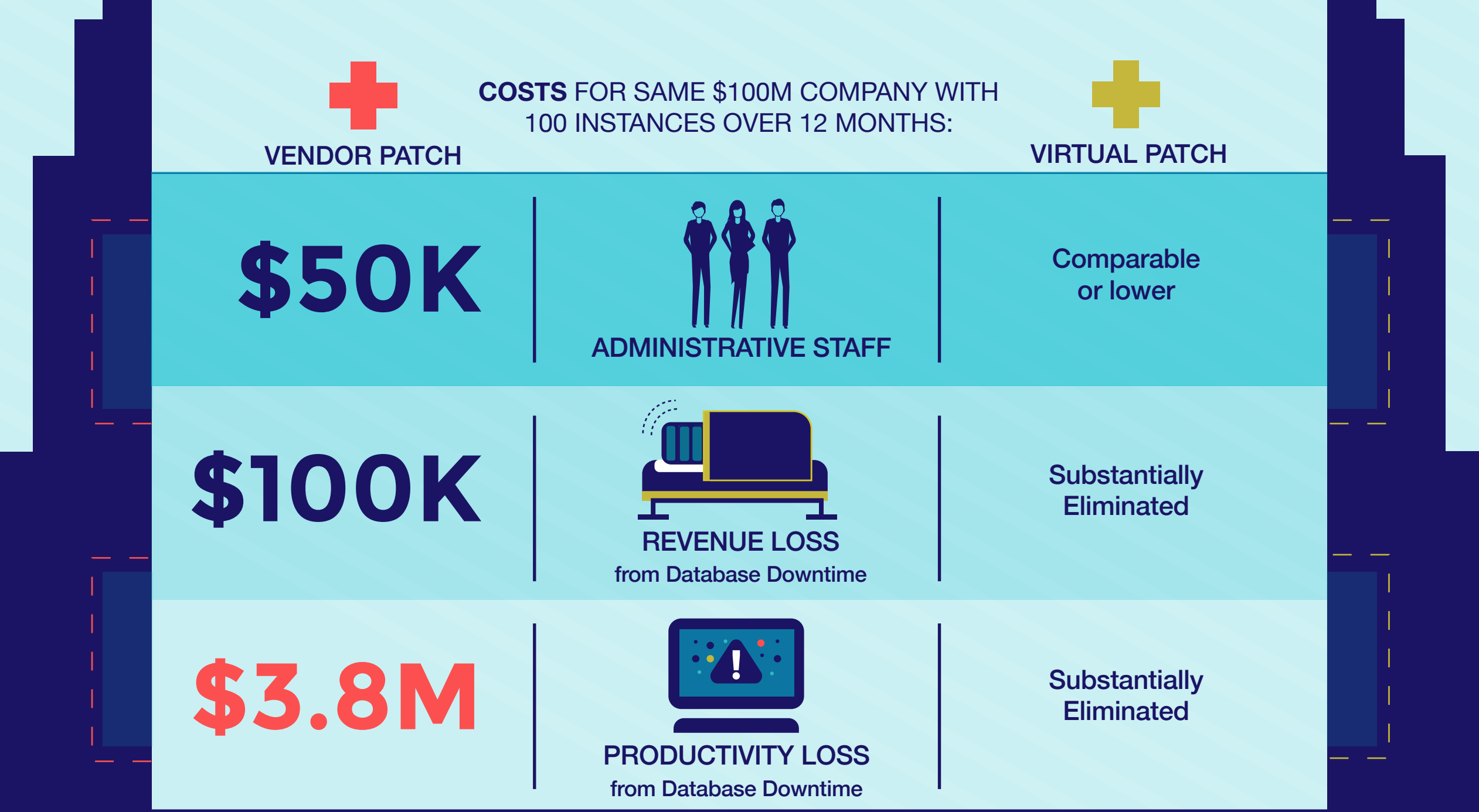


### CONTINUOUS SECURITY PROTECTION VS. VENDOR PATCHING

WINDOW OF VULNERABILITY IS DRASTICALLY REDUCED WITH VIRTUAL PATCHING



### VIRTUAL PATCHING REDUCES THE BUSINESS IMPACTS OF RISK



We can easily agree that our objective is to manage the risk of enterprise database and application vulnerabilities to an acceptable level. We just need to think more broadly about how best to achieve that objective – as in the case for Virtual Patching.

### To learn more,

[Read the Full Report](#)

All Aberdeen Group research is © 2016 by the Aberdeen Group. All rights reserved. All Aberdeen Group materials are licensed with Aberdeen Group's permission and in no way does the use of publication of Aberdeen Group research indicate Aberdeen Group's endorsement of Intel's products/or strategies.

Created by Aberdeen Group. Brought to you by Intel.