

# 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:

**Complex**  
**440**  
vendor patches are required (median)

**Time Consuming**  
**910**  
hours of disruption is likely (median)



#### Inconvenient

Most organizations do not have the time and resources to apply vendor patches in a timely manner

Plus vendors may no longer provide patches for older systems, OEMs or for outsourced code



#### Costly

The patching process itself & productivity loss in incurred system outages is costly



#### Not Consistent

Lack of visibility into attacks allow further opportunities for attacks

### VIRTUAL PATCHING REDUCES THE LIKELIHOOD OF RISK

Virtual Patching is:



#### Simple

Need for emergency patches or workarounds is reduced



#### Efficient

Enterprises can choose to avoid the hassle of vendor patches



#### Convenient

Libraries & support code files are unchanged, preventing disruption of critical applications & databases

### CONTINUOUS SECURITY PROTECTION VS. VENDOR PATCHING

WINDOW OF VULNERABILITY IS DRASTICALLY REDUCED WITH VIRTUAL PATCHING

VENDOR

0 Day Vulnerability Reported

Patch Available

Patch Installed

**M**

Medium Risk

**H**

High Risk

**VH**

Very High Risk

**L**

Low Risk

Unknown

Months/Years

Months/Years

Remediated

**M**

Medium Risk

**L**

Low Risk

**L**

Low Risk

**L**

Low Risk

Policy Update

Policy Update

VIRTUAL

### VIRTUAL PATCHING REDUCES THE BUSINESS IMPACTS OF RISK

**VENDOR PATCH**

**\$50K**

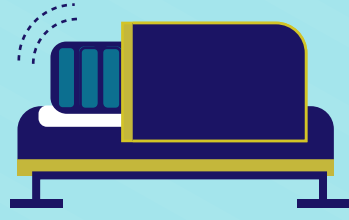


ADMINISTRATIVE STAFF

**VIRTUAL PATCH**

Comparable or lower

**\$100K**



REVENUE LOSS from Database Downtime

Substantially Eliminated

**\$3.8M**



PRODUCTIVITY LOSS from Database Downtime

Substantially Eliminated

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.

ABERDEEN GROUP

McAfee