



# Microsoft® OS patching

An essential component of Philips Software Evolution Services\*

## Security by design

At Philips, we take an end-to-end approach to security. Infusing security principles begins with product design and development, and extends through testing and deployment. We follow-up on your system's safety with robust policies and procedures for monitoring, updating and managing incident responses, when needed.

## Connectivity matters

Philips Software Evolution Services are designed for connectivity to accelerate an appropriate response.

Automated connectivity for seamless protection is a built-in feature of your Software Evolution Services including:

- Microsoft OS patching
- PIC iX application patching (\*fixes)

## The impact of cybercrime is astounding

**Healthcare is primary target**  
A healthcare record lost or stolen could cost as much as

**\$363**

per record to remediate<sup>1</sup>



**The cost of cybercrime**  
**2 trillion**  
by 2019<sup>2</sup>



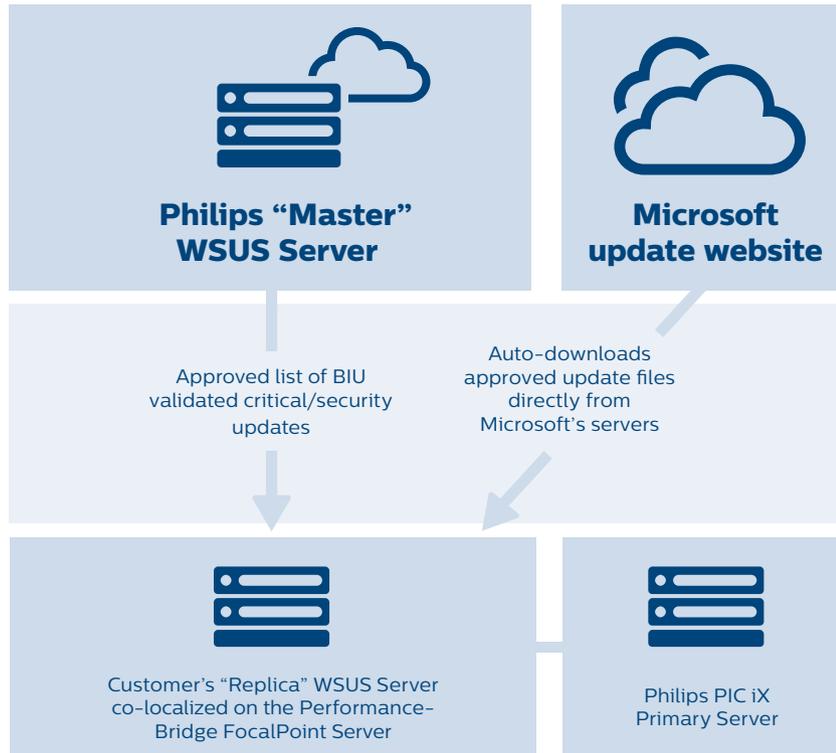
\*This offering is available to purchase as a stand alone service.

<sup>1</sup> IBM X-Force Threat Intelligence Report 2016

<sup>2</sup> Juniper Research. <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#26eda0143a91>. Accessed Dec 2018.

## WSUS enablement

- Software Evolution Services customers get Philips-enabled Windows Server Update Services (WSUS) co-localized on the PerformanceBridge Focal Point server
- You can choose the frequency and the timing to apply the validated patches based on their risk profile
- Microsoft OS patching bolsters your security



## Philips delivers

- Testing and validation of Microsoft patching
- Support in patch delivery mechanisms
- Project management and field resource support for onsite coordination\*
- Dedicated Philips team, technology and service to drive success\*

\* With purchase of additional support services

Philips next generation Software Evolution Services keep you one step ahead every step of the curve in **managing IT risk (cybersecurity via security patching)**, ensuring staff preparedness in managing life-and mission-critical platforms. With Philips, you can standardize on quality patient monitoring and protecting your investments.



Security



Reliability



Compliant

## Optional services\*

### Proactive patching

- Philips informs customer that the latest validated patches are available
- Onsite Philips resources are scheduled to support application of Microsoft OS critical updates and application patching for PIC iX
- Coordinated change management with hospital staff to limit downtimes
- Reporting/documentation on file of patches applied
- Onsite support services, up to 4 times a year

### Responsive patching

- Additionally, two event-based (emergency patching) at no additional cost
- Coordinated PIC iX application patching for "fixes"

\* Additional costs for optional services.

© 2019 Koninklijke Philips N.V. All rights reserved. Specifications are subject to change without notice. Trademarks are the property of Koninklijke Philips N.V. (Royal Philips) or their respective owners.

[www.philips.com](http://www.philips.com)

45229 914 6151 \* FEB 2019



To learn how Philips can help you protect your system, call  
**+1 888 647-4285.**