OPERATING SYSTEM MONITORING

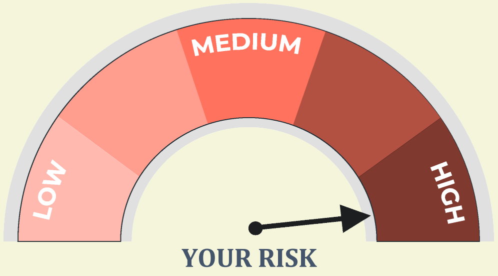
FOR YOUR ASSESSMENT REPORTS

Outdated Operating System Report

The presence of outdated operating systems (OSes) in a business environment represents a gap in security because the company who built the software, commonly Microsoft, no longer provides security updates or ongoing support. Cybercriminals thus have unlimited time to discover vulnerabilities and their exploits can end up encrypting sensitive business data. Cybercriminals may then demand payment from compromised businesses through ransomware.

During our assessment of your environment, we analyzed the OSes present among your servers and workstations and found the following:

Outdated Operating System	Servers and Workstations
Windows 2000 Server	PROIT30-WS
Windows 7 Enterprise	BO-SANDBOX EXCH-GW USER-PC23
Windows 7 Professional	CONFERENCE-ROOM ROSS-HP PGARFUNK-WIN7TEST
Windows Server 2003 R2	ISA1
Windows Server 2008 R2 Datacenter	W2K8R2-A
Windows Server 2008 R2 Enterprise	PTO1 STORAGE01



Why is this important?

According to a 2017 report on operating system usage by BitSight [1], 20% of computers from a pool of 300,000 analyzed were using operating systems that did not have security patches available before the “WannaCry” attacks occurred.

WannaCry is an infamous ransomware attack that served as a wakeup call for security teams, revealing the larger number of organizations that use outdated systems and ignore critical updates.

Reference Link:
1.https://www.bitsight.com/blog/latest-bitsight-insights-explores-growing-risk-frequently-ignored-critical-updates