Windows Server 2012 and Windows Server 2012 R2 End Of Life

Windows Server 2012 and **Windows Server 2012 R2** will end on October 10, 2023. After this date, these products will no longer receive security updates, non-security updates, bug fixes, technical support, or online technical content updates.

Business Implications

When organizations are still using Windows Server 2012, they will face the following business implications as below:

1. Compliance

If your organization maintains compliance with PCI, HIPAA, or any other compliance agencies, then all application and infrastructure workloads must maintain a vendor supported state. For operating systems such as when Window Server support ends, you automatically become noncompliant if you have unsupported workloads in your environment or are running applications that are no longer in scope for compliance regulations. If you're running end-of-life workloads, your insurance premiums increase – along with your exposure to a security attack.

2. Loss of Supportability / Delays in Case of Event

When support ends for Windows Server 2012 in October 2023, organizations will lose supportability in the event of an issue or security threat. Without a reliable vendor to provide support, organizations will be vulnerable to disruption (or worse). If that happens, you won't be able to call someone to get immediate help. Instead, you would have to get a quote and then pay an invoice before you can get help. There's a significant delay in the case of an event.

3. Targeted Attacks and Increased Risk of Exposure

Bad actors are waiting with their fingers on the trigger for software to go out of life. If you wait until the last minute to migrate or upgrade your end-of-life software, then you may not have a secure solution in place by the time support ends. Not protecting your organization can lead to loss of revenue, loss of reputation, and targeted attack exposure risk.

a. Loss of Revenue

If your systems aren't operating correctly and you're in a time-sensitive industry, then any downtime caused by either loss of features, loss of support, or an attack could lead to revenue loss.

b. Loss of Reputation

Your reputation is also impacted because many security attacks hit the news. Clients become wary of organizations who aren't savvy enough to protect themselves or their clients' data from exposure.

4. Inability to Take Advantage of Newer Features and Functionality

Every new version of Windows introduces newer capabilities that improve the functionality and user experience. Therefore, being able to remain current allows you to take advantage of such improvements faster and sooner – improving your level of service to your organization.