ComputerWeekly.com

Managing risk after support for Windows Server 2003 ends

With Microsoft due to end support for Windows Server 2003 in July 2015, we look at best practice for migration

Carl Claunch

In recent months, Gartner has seen an increasing volume of inquiries around continuing to use systems that run on Microsoft Windows Server 2003, which will be unsupported after 14 July 2015. For quite a few clients, it is becoming apparent these systems will not be migrated in time to new supported versions of the operating system.

In these calls, the companies are looking for advice, new ideas, best practices and information on how similar organisations are addressing this issue. First, Gartner generally talks through the consequences and risks they will face after the extended support period expires in 2015. With that as a basis for assessing the situation using business risk-management principles, the discussion then moves on to cover techniques, tools, strategies and actions that have worked for others.

A surprising number of organisations will be operating those unsupported systems in 2015 and beyond – they range from medium-scale up to the largest enterprise IT organisations. Both technically adept and less sophisticated shops find themselves without sufficient time and budget to completely migrate all workloads.

No simple, single system exists to fully manage the risks – rather, the best practice in this area is the application of choices from a large pool of options. The particular approach selected for each system is dependent on characteristics of that application and of the risk.

Security and operational risks after support ends

Microsoft's support programme for both Windows Server 2003 and Windows Server 2003 R2 is currently in the extended support phase, which is scheduled to cease on 14 July 2015. After that date, if a new security vulnerability is discovered in the code, there is no commitment that a fix will be produced

and released by Microsoft, nor will it address non-security defects or assist customers that encounter problems in operation.

Further, it is not just the operating system that should concern clients. Third parties that sell and support software, including business applications, may tie the support of their code to the status of the underlying operating system. Therefore, running the third-party software on Windows Server 2003 will constitute an unsupported environment.

If a security exposure is discovered and exploited by outsiders, clients could have the operation of applications disrupted, data could be stolen or tampered with, and the compromised system may be the launching pad for eavesdropping and active attacks against other systems in the datacentre.

In addition to security risks, it is possible an IT system running on Windows Server 2003 may cease to operate correctly because of some latent defect that has been triggered by changes in the client's use. There is no assurance that a correction will be possible, rendering that IT system suddenly unable to fulfil its purpose, in part or totally. Even if the problem encountered does not require code changes to solve, it may need expert assistance from Microsoft to diagnose the root cause, but those resources may no longer be available.

Regulatory and compliance obligations may pertain as well, requiring all production systems to have support available from the product providers. Thus, continuing to use software running on Windows Server 2003 after support ends could violate the compliance or regulatory obligations of an organisation.

Microsoft is open to negotiating a custom support agreement to provide fixes for security vulnerabilities for Windows Server 2003 after it reaches the end of the extended support phase in 2015. However, this is not a full solution, even if the relatively high cost is acceptable. These agreements are not open-ended – they are signed in the context of a plan with a fixed end date for migration of the remaining systems to a supported version of Windows Server. They do nothing to address Windows Server 2003 as an unsupported environment for its product, and the client's custom support agreement with Microsoft doesn't help.

How to manage security and operational risks

Among all possible security and operational risks, some may be solvable by one or more tools. Other risks require different tools or complex custom development of systems, or they may not be amenable

to a fix at all. For example, a tool that manages database access may be the resolution if a security vulnerability is discovered in structured query language (SQL), but not so helpful if the issue affects Microsoft's Internet Information Services (IIS) or the business application itself. A firewall and intrusion-monitoring tools may be sufficient to address possible compromise of some of the systems, while other exposures may involve the business rules themselves, demanding a change to the core logic of the application.

Prioritise affected systems

Although a risk is identified, it may never occur. Further, the effects are not the same, and the means of mitigating or resolving different risks may vary significantly. It may be imprudent to spend large amounts of time and money to offset a very low-probability event when the corresponding impact is light. On the other hand, some regulated industries may not be permitted to run certain applications if the system is unsupported.

The systems running under Windows Server 2003 may have been in successful operation for almost a decade – what is the risk a new problem will arise that impairs the system's operation? Security exposures in this operating system version have been frequently detected and patched – how often have the systems been the target of attacks? For some IT systems being assessed, the business has alternative means at hand if the application were to be unavailable for an extended period. This may already have been studied as part of an impact assessment for disaster recovery planning – take advantage of that work to speed the analysis of the future risks.

Continuing to operate on Windows Server 2003

If a means exists to survive without the software, even if it is more cumbersome or expensive for the business users, the impact is controlled. The client may continue to operate the system, while watching for the occurrence of the risk scenarios, at which point the impaired system can be rapidly shut down. The best practice involves setting up a means to watch for the risk events and the creation of a process to follow in that scenario.

Risk management is a discipline that seeks the appropriate balance between risks and mitigation activities. Some risks are worth taking, with an impact that is less than the costs of eliminating the risk.

Some actions can be deferred, given the low odds that a given event will occur in the coming years. If the action can be applied quickly to cap the impact of a possible event, this may be a better decision than to launch an immediate high-resource effort to migrate or replace the system.

Identify and prepare for broad class of issues

Since a company need not eliminate every risk, particularly if the mitigation can be readily applied in the future if the risk materialises, the best practice is to develop broad classes of potential issues and to identify the appropriate response for each. Organisations prioritise and begin activities only for the systems with very high impacts or facing situations highly likely to happen.

Additional software products could be installed and used to block security exposures or overcome operational problems in the event these arise in the future. For the most part, these are specific solutions to narrow classes of problems.

The concept of a demilitarised zone (DMZ) has been frequently used to isolate systems that are accessible by outsiders. This is to minimise what they could do to the rest of the datacentre if they become compromised. Further, much tighter control can be placed on which other systems they are permitted to contact and the types of access allowed. This may reduce the usability of a system, but it may be better than the alternative of losing all use if a new vulnerability becomes known.

Carl Claunch is a vice-president and analyst at Gartner

This article is from ComputerWeekly.com and was first published November 2014