certero.

2020 Micropocalypse Now:

Say Goodbye to Windows 7, Office 2010 and Server 2008

Version 3

Executive Summary

In 2020, Microsoft is initiating end-of-support procedures for Windows 7, Office 2010 and Windows Server 2008, which means no more security updates and patches to keep your IT ecosystem protected from threats of hacking, viruses and malware.

While end-of-support for Microsoft products is nothing new, the current decision to end support for these Operating Systems and applications will have a significant impact on organizations.

According to recent estimates, around 39% of users are running Windows 7, Office 2010 is still widely used and millions of apps still run on Windows Server 2008. All of these Operating Systems and applications will become exposed to potentially serious risks within less than 12 months, which can cause catastrophic damage to mission critical business systems – just like the WannaCry attack.

So, when is all of this happening, why is it such a problem and what can be done to protect your organization?

Back

Next

When is the Micropocalypse?

According to Microsoft, end-of-support will happen on the following dates:

- Windows SQL Server 2008 - July 9th 2019
- Windows 7 - January 4th, 2020
- Windows Server 2008 - January 4th, 2020
- Office 2010 - October 13th, 2020

ack

Next

What’s the big deal?

You may be wondering what the big deal is. After all, you can simply apply the latest patches to these Operating Systems and applications, accept the risk and upgrade at some future point, right?

Wrong! End-of-support for these Operating Systems and applications means they are:

- no longer maintained and;
- no longer receive security patches.

What’s more, when something goes wrong you have nobody to call. Basically, you are on your own.

Due to widespread use of Windows 7, Windows Server 2008 and Office 2010, many are predicting a new world-wide cyber-attack similar to WannaCry.

WannaCry was a global ransomware attack that was launched in May 2017. The attack targeted computers running outdated Microsoft Windows Operating Systems. While Microsoft had released patches prior to the attack, much of WannaCry's spread was from organizations that had not applied these updates, ***or were using older Windows systems that were past their end-of-support.***

Back

Four-step plan for Microsoft end-of-support

1) Discovery and inventory
2) Understand your options
3) Build your plan
4) Execute your plan and track its progress

Next

On the coming pages, we'll look at each of these options and what you need to consider when evaluating and comparing them.

We'll outline some of the pros and cons of each approach and try to help you identify and avoid some of the potential gotchas that could create unexpected costs, resource demands or time delays.

Back

1. Discovery and inventory

To protect your organization and its mission critical systems, you need to identify all instances of these Operating Systems and applications right across your IT ecosystem. For this you will need advanced IT Asset Management (ITAM) and Software Asset Management (SAM) capability.

While many SAM tools claim to be able to discover all your Operating Systems and applications, most lack effective discovery and will leave gaps across your network. Similarly, a lack ITAM data will make it harder to identify devices that can be upgraded rather than replaced. Without a complete dataset you cannot perform a full risk assessment and plan your mitigation actions. At best you will protect a portion of your IT ecosystem, but leave other areas exposed. For a WannaCry-style attack to succeed, malware only needs one entry point – all loose ends must be tied off.

Certero can help you gather all the data you need to make better, informed decisions and formulate a more robust action plan. Our tools for ITAM (Certero for Enterprise ITAM) and SAM (Certero for Enterprise SAM) work holistically as one unified solution, developed specifically to address your Microsoft challenges.

Next

2. Understand your options

So, you've implemented an ITAM and SAM solution and now have a complete view of all your Microsoft assets, across all your devices (from Mobile to Mainframe to Cloud). You can locate all of your instances of Windows 7, Windows Server 2008 and Office 2010. What next?

Well, it may surprise you to learn that you have a few options, but most of these are short-term, temporary fixes.

Windows SQL Server 2008 and Windows Server 2008

For Windows SQL Server 2008 and Windows Server 2008, you can:

- Purchase extended support updates
- Migrate to Microsoft Azure or
- Upgrade to a supported version

Back

Next

While Microsoft is ending support for these Operating Systems, you will be able to purchase extended support updates until 2023. The updates you receive will not be as frequent, which may still result in exposure to risk. It is not a long-term solution and should only be viewed as a band aid to buy you some time while you upgrade or migrate Operating Systems.

Migrating to Azure is another option, although this is not always possible. While hosting these Operating Systems in Azure will entitle you to free support, maintenance updates and security patches, this too will end in 2023 and should not be seen as a long-term solution.

Your long-term solution is upgrading to a supported version of these Operating Systems. This will enable you to remove potential risks and continue receiving maintenance updates, security patches and support from Microsoft. Depending on whether or not you have a cloud migration strategy, you may wish to take this opportunity to migrate and upgrade simultaneously.

Windows 7

Windows 7 offers broadly similar options:

- Purchase extended support updates
- Migrate to virtual desktops in Microsoft Azure
- Upgrade to a supported version

Again, purchasing extended updates is a short-term fix, which will buy you some time until 2023 to get this Operating System fully removed from your IT ecosystem. Prices are per device and increasing year-on-year, ending completely in 2023.

Similarly, migrating to virtual desktops in Azure will grant you access to free support, maintenance updates and security patches, but only until 2023. This is not a long -term solution.

To fully protect your organization, you need to upgrade to a supported version, which means applying Windows 10 to all your affected devices. This can be done in parallel with a migration to Azure, if this is within the scope of your organization's cloud strategy.

Back

Next

Office 2010

Office 2010 is slightly different to the others. Here you will not be able to access extended support updates, which means your options are:

- Migration
- Upgrade

Microsoft is keen to move customers on to its Office 365 subscription service, so it is no surprise migrating to this is a long-term option.

Upgrading also offers a long-term solution. Identifying all devices running Office 2010 will enable you to upgrade them to Office 2013, 2016 or 2019. However, these will also be subject to end-of-support procedures in the future, as Microsoft continues its roll out of Office 365.

With all migrations and upgrades, you will need comprehensive ITAM and SAM data for all your devices and users. This is the only way to fully scope out your requirements and plan your migration program, with complete costings.

3. Build your plan

Now you know what your options are for each of these Operating Systems and applications, you need to build a plan.

What plan do you want to build?

With the data provided by your ITAM and SAM tools you will be able to identify all assets that pose a threat and scope out what you need to mitigate those risks. What you choose to do will largely depend on the availability of resources and budget.

What resources do you need?

You can start by identifying the ideal scenario, then working back from there. For example, you may wish to upgrade and migrate all your Operating Systems and applications, but do not have the resources or budget to do so?

If this is your long-term goal, how can you get there through incremental steps and maintain your IT security?

What are manageable targets?

Once you have determined what you want to build, the resources and costs needed and the phases of development you will implement, you need to set clear manageable targets. These targets are likely to focus on time and cost of delivery, but may also extend to other key metrics.

What does success look like?

Finally, you will want to set out what success looks like. This will drive your project forward, give you a clearly defined end -goal and shape how you report progress and success to other stakeholders.

Back

Next

4. Execute your plan and track its progress

Armed with you action plan, you can now begin its implementation and start driving the necessary changes to protect your IT ecosystem.

Create a timeline

In your plan you will have determined your phases of development and when these should be completed. To keep you on course, you will need to flesh these plans out with a more detailed timeline of tasks and milestones, and who is responsible for delivering them.

Track progress

Once you know what has to be delivered, by whom and when, you can track progress against your project plan. This will help you maintain momentum and, where possible, accelerate the project. Outside your project plan you can track progress by using insights from your ITAM and SAM tools. From this, you can see which Operating Systems and applications are still present in your IT ecosystem and the resolutions you have successfully implemented.

Report success

At key milestones during your project, you may need to report progress to various stakeholders. In addition, you may also need to provide regular updates to show your progress against your 'vision of success'. This is likely to include the milestones you have achieved, costs incurred vs budget, whether resolutions have been successfully implemented and so on. For more technical insights, you can generate reports from your ITAM and SAM tools that can be shared automatically with key stakeholders on a daily, weekly or monthly basis.

Finalize project

Once the project has been completed you can review all assets and Operating Systems and applications in your ITAM and SAM tools. Here you will be able to identify whether or not any instances of these outdated systems are still present. If they have all been removed, you can close the project and report its success.

Back

Next

Back

Help and support is available

If you are concerned about the end-of-support scheduling of Windows 7, Windows Server 2008 or Office 2010, and would like to discuss this with one of our Microsoft experts, you can request a call back from our team.