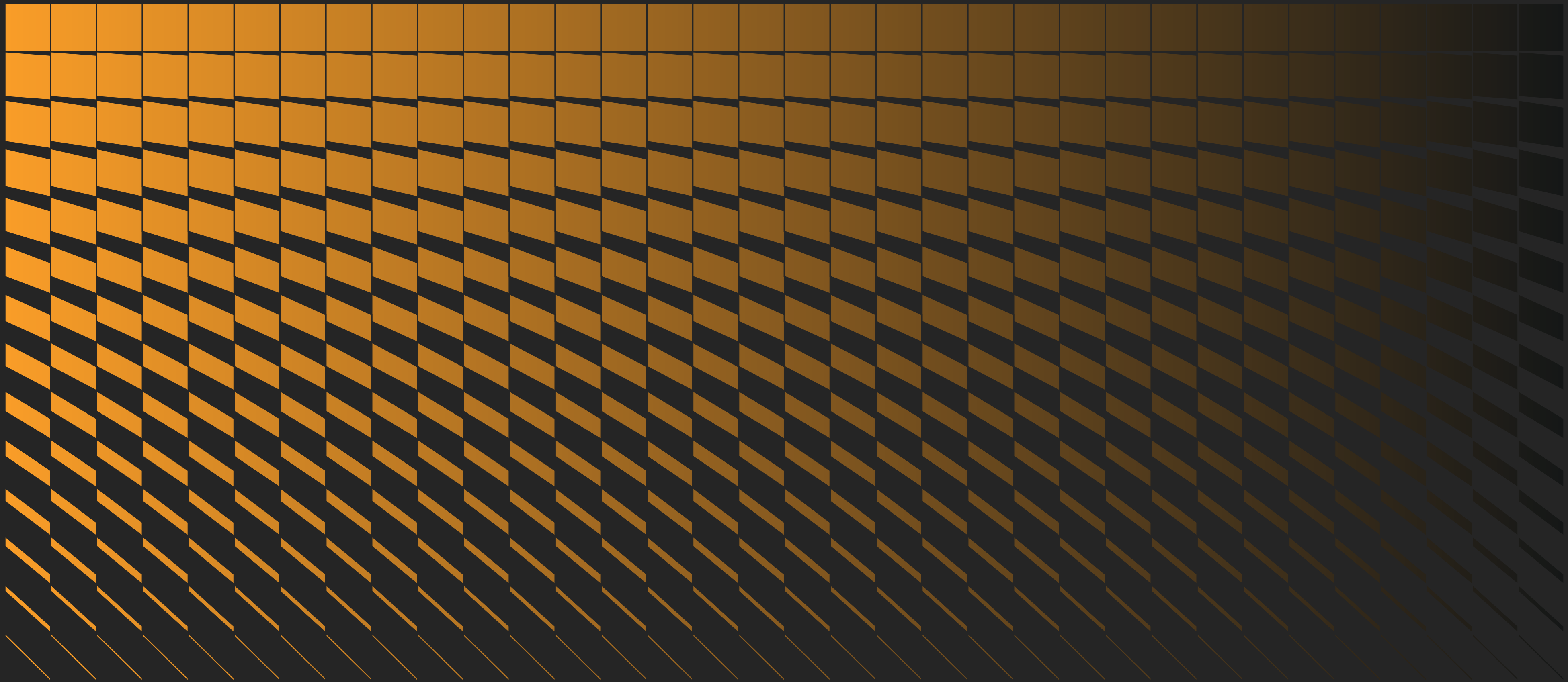
extech cloud

Beyond the Deadline:

Upgrading End-of-Life Microsoft Software in the Cloud Era



Introduction:
Are you Running on Borrowed Time?

Once software, such as Windows Server or SQL Server, is released by a vendor, it requires ongoing maintenance. This includes technical support, quality-of-life improvements and security patches. When vendors stop maintaining the software, it reaches end-of-life (EOL) status.

If businesses continue to use the software past this point it creates a plethora of risks, ranging from loss of productivity to security gaps that are impossible to plug without upgrading the software to a new version.

Running any EOL software is never advised, but it is even more dangerous to run an unsupported operating system on a server, as there is a high risk of falling victim to an entirely avoidable cyberattack.

Whilst this may seem obvious, many small and medium businesses are using end-of-life server operating systems, such as Windows Server 2012 or SQL Server 2014. In the next 3 years Windows Server 2016 and SQL Server 2016 and 2017 will reach end-of-life and many SMBs have not planned for this.

Some businesses are simply unaware of the fact that this software has reached end-of-life, whereas others are using this software as a cost-saving measure. Whatever the reason, running end-of-life software is a ticking time bomb.

In this guide, we will explain the risks of EOL software, the ins and outs of Microsoft's software lifecycle, how to tell if your business is at risk, and how you can mitigate this risk by migrating to Microsoft Azure.

The Real Business Risks of **End-of-Life Software**

Cybersecurity Risks

There is a constant battle between cyber criminals and software vendors, such as Microsoft. Whenever Microsoft releases an application or operating system, cybercriminals quickly look for weak points, and Microsoft races to close them before they're exploited. Microsoft also invests billions into finding and patching these vulnerabilities before hackers find them to keep businesses safe.

But what happens when software reaches the end of life?

If a cybercriminal finds a vulnerability in an older operating system Microsoft will not patch it. This means that every other device running the same operating system is at risk, with no hope of a fix.

Every month after software reaches the end of life, more vulnerabilities are found, and businesses running this software are increasing the likelihood of falling victim to an avoidable cyberattack.

The most noteworthy real-world example of this risk materialising was the 2017 WannaCry ransomware attacks on Britain's NHS.

There was a known vulnerability in Windows Server 2003, 2008, 2012 and 2016, which Microsoft had patched in May of 2017. However, the NHS was running Windows Server 2003, which had reached end-of-life in 2015.

The hackers exploited that known flaw, taking down hundreds of GP practices and costing the NHS over £92 million in disruption and damages.

Compliance Risks

Across the UK and EU, there are many regulatory frameworks and standards that either discourage or prohibit the use of end-of-life software due to the associated security and compliance risks.

Some of these frameworks include the UK Cyber Governance Code of Practice, GDPR, Cyber Essentials and Cyber Essentials Plus, NIS 2 as well as multiple ISOs, including 27001, 27002 and 9001.

An example of an indirect reference is in GDPR, which mandates that "appropriate technical and organisational measures" are in place to protect personal data. It is highly likely that if personal data was breached using EOL software as the entry point, the organisation would be liable for this, as they did not meet the appropriate technical measures to protect the data.

The National Cyber Security Centre's Cyber Essentials explicitly states that "All software on in-scope devices must be licensed and supported." Therefore, any organisation running end-of-life software would not be eligible for a Cyber Essentials certification.

Operational Risks

The security and compliance risks are enough to show the danger of running end-of-life software, but there is an ongoing operational risk outside of this. There are three ways that this can manifest.

Support Problems: Most software vendors, including Microsoft, will not provide support to customers who are using end-of-life software, or if they do, they will charge significantly more for the services. This means that if something goes wrong, it is up to your business to fix it. Most of the time, businesses will not have the appropriate expertise in-house, or if they do, it will take a significant amount of time to fix minor issues.

Poor Performance: Windows Server and SQL Server have a mainstream lifespan of 5 years, with security updates being provided for an additional 5 years. If your organisation purchases a server at the start of the lifecycle, by the time the software reaches the end of life, the hardware will likely be at the point that it feels like it is slowing down and is more prone to hardware failure. In real terms, this means that the users who rely on the server, either your employees or your customers, will have a worse experience.

Temporary Fixes and Knowledge Loss: Whilst it is possible to run software past its expiry date, it often results in a patchwork of internal fixes which is a poor use of IT resources. It also means that your organisation is the only group with knowledge of the solution and if employees leave the organisation that knowledge also leaves.

Understanding Microsoft End of Life

Unlike software, such as Microsoft 365 which is evergreen, Microsoft has a defined lifecycle for all their server software, including Windows Server and SQL Server. This lifecycle is divided into four stages.

Mainstream Support

Approximately 5 years

After a product is released, it enters the first stage of the product lifecycle. During mainstream support, you will receive incident support, security updates, the ability to request non-security updates and quality-of-life updates.

For example, Windows Server 2019 was released in late 2018 and up until 2024 there were over 60 updates that improved performance for Hyper-V, improved Admin Center compatibility, and more, alongside over 1,000 security patches.

Extended Support

Approximately 5 years

Once the software leaves the mainstream support stage, it enters extended support. During this period, you will receive security updates, but no new features. This is considered a grace period, to give you time to move to a new version.

Windows Server 2019 reached extended support on January 9th, 2024. Since then, it has still received 13 updates, which have patched approximately 250 vulnerabilities.

Extended Security Updates

Approximately 5 years

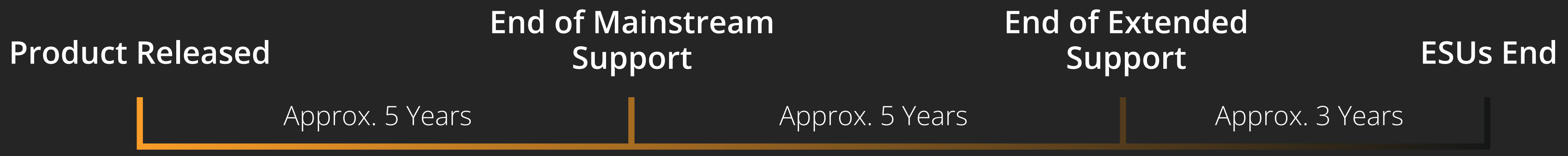
In certain extenuating circumstances, it is possible to purchase an additional three years of security updates. These can be purchased for on-premises infrastructure or included free of charge for eligible customers that have servers hosted in Azure but only include critical security patches.

This should not be relied upon for on-premises servers, ESUs are expensive and many businesses do not qualify for them unless they migrate workloads into Azure.

Post Support

For most organisations, extended support is the true end-of-support date. From this point, there are no updates, and your business is at risk of operational challenges and having known vulnerabilities exploited.

Product	Mainstream Support	Extended Support	Extended Security Updates - Year 3
Windows Server 2012 and R2	~~October 9, 2018~~	~~October 10, 2023~~	October 13, 2026
Windows Server 2016	~~January 11, 2022~~	January 12, 2027	January 2030
Windows Server 2019	~~January 9, 2024~~	January 9, 2029	January 2032
Windows Server 2022	October 13, 2026	October 14, 2031	October 2034
SQL Server 2012	~~July 11, 2017~~	~~July 12, 2022~~	July 8, 2025
SQL Server 2014	~~July 9, 2019~~	~~July 9, 2024~~	July 8 2027
SQL Server 2016	~~July 13, 2021~~	July 14, 2026	July 2029
SQL Server 2017	~~October 11, 2022~~	October 12, 2027	October 2030
SQL Server 2019	~~February 28, 2025~~	January 8, 2030	January 2033



Product Released

End of Mainstream Support

End of Extended Support

ESUs End

Approx. 5 Years

Approx. 5 Years

Approx. 3 Years

How to Tell if Your Business is at Risk

In some organisations, there may be noticeable signs when you are using software that has recently reached the end of life. These may include slower speeds when accessing resources, or an increase in time for support tickets to be closed.

But most of the time, at least shortly after the end-of-life date, there are systems that "just work" but have not been updated and are a risk.

In theory, all businesses should have a central repository of assets and what software each device is running, which can be cross-referenced against a list of end-of-life products. In practice, this is often not the case.

The easiest and most accurate way to find out if your business is at risk is by working with a managed service provider, like us, to run an initial software audit. This will not only let you know what has reached end-of-life, but what is reaching EOL in the coming years, so you have time to plan.

What are Your Options?

If, after a software audit, you find that you have an instance of Windows Server or SQL Server that is no longer receiving updates, or will not receive updates for much longer, you have two options, either to upgrade your hardware or migrate to Azure. There is the option of Extended Security Updates, but most organisations do not qualify for these.

Upgrade Server

To upgrade Windows Server or SQL Server, it is technically possible to update the operating system without replacing the hardware, but in practice, this is not feasible. The average on-premises server has a lifespan of 5-10 years, and it is rare to continue to use a server after 7 years.

This means that to update the operating system, you will need to purchase a new server. From the end user's perspective, likely your employees, this will maintain the status quo, with potentially increased productivity from the more modern hardware.

From a commercial perspective, this will require capital expenditure for the new server, as well as costs involved with the migration process and physically removing the old server.

When considering this option, it is important to note that when you buy a server it has a set resource capacity, so you need to have enough computing resources to function smoothly during your busiest period. For most organisations, this means that for the vast majority of the server's lifespan, it is not being used to its full potential.

Migrate to Azure

There are many options available when migrating your server to Azure. Simply put, the migration will extend the life of many operating systems, as they will receive free Extended Security Updates, which buys more time to upgrade to a newer operating system. It is also possible to start fresh with the latest operating system as part of the Azure migration.

What is Azure?

Microsoft Azure is a cloud computing platform offering a vast array of services, from computing power and storage to AI and analytics. Businesses use it to build, deploy, and manage applications across Microsoft's global network of data centres.

Whether you need virtual machines, databases, or even machine learning tools, Azure provides a scalable and secure environment to meet diverse needs.

For Windows Server, you can use a virtual machine, which can be accessed from anywhere. As the server is in the cloud, you never need to worry about upgrading the hardware to update the operating system, but you still have full control over everything, just like your on-premises server.

For SQL Server, you can either use a virtual machine running the SQL Server operating system or move to a managed platform. By using a fully managed Azure SQL Database, you eliminate the burden of operating systems maintenance and knowledge, reducing the reliance on in-house expertise.

Working with a managed service provider can remove your dependency on EOL systems entirely, and protect you against future deadlines. Whilst there will be a cost involved with the migration and disposal of the old server, however, there is no capital expenditure, as Azure has monthly billing.

Why Microsoft Azure Works for Small and Mid-Sized Businesses

Historically, there has been a misconception that cloud infrastructure is reserved for large enterprises, but most small and medium businesses can achieve the same benefits as their larger counterparts by migrating to the cloud.

CAPEX to OPEX

As mentioned previously, when migrating to Azure, there is no capital expenditure on computing hardware, cooling, power or physical infrastructure like uninterruptable power supplies (UPS) or space for the server. With Microsoft Azure, you have a simple monthly bill, which includes your resource utilisation for the previous month.

This works particularly well for small and medium businesses as it means you don't need to allocate cash or open a line of credit to purchase a new server every 5-10 years. There are also fewer costs associated with maintenance, as there is no physical hardware.

Security and Resilience

Microsoft Azure comes packed full of security controls included with every environment. A managed service provider can set these up for you, enabling you to have a strong baseline of security and you are less likely to fall victim to a cyberattack.

On top of this, there are many other security options available in Azure, including:

Azure Firewall is a cloud-based security system that helps protect your business by controlling and monitoring incoming and outgoing network traffic.

Azure DDoS Protection automatically shields your online services from large-scale attacks that try to overwhelm and shut them down.

Microsoft Sentinel is a cloud-based tool that helps you detect, investigate, and respond to security threats across your entire IT environment.

Defender for Cloud continuously checks your systems for vulnerabilities and gives you recommendations to keep your data and apps secure.

With all of the data being stored in the cloud, there is an additional layer of redundancy as it is all offsite. Even if there is a power outage or natural disaster in your office, your data is safe and accessible.

Scalability

Many SMBs rely on on-premises hardware for line of business applications, custom apps and data storage. Whilst there are methods to allow your employees to access these resources remotely, such as VPNs, it is often laborious and prone to issues.

With Microsoft Azure, your employees can securely access company resources from any device, at any time. This makes it easier for staff in different geographies and scale your business.

Azure also makes it easy to start small and scale up. As you only pay for what you use, during quiet periods your monthly bill will be low, but can be quickly, and even automatically, scaled up to meet your demands.

Opportunity for Innovation

One of the lesser-talked-about benefits of cloud computing for SMBs is the opportunity for innovation. Once you're on the Azure platform, it becomes easier to start making use of the advanced products and features only available with the cloud.

This may include using Microsoft Fabric for analytics and business intelligence, ingesting data sources from your Azure environment, all the way to Azure AI services, where you can innovate with the latest AI models from OpenAI, Meta, Perplexity and more.

Working with Azure gives you access to this innovation and working with a managed service provider gives you insights into where to invest to grow your business through innovative use of technology.

What’s Right for Your Business?

Choosing the right solution when facing software end-of-life ultimately depends on your unique needs, goals, and resources. For most businesses, leveraging the scalability and innovation offered by Microsoft Azure presents a significant advantage and it is an investment that pays dividends for years to come.

However, it is essential to evaluate factors such as your existing infrastructure, budget, and technological expertise before making a decision.

For those with legacy systems and limited IT support, working with managed service providers can simplify the migration process and highlight areas where cloud technology can generate the greatest impact. The right option is one that aligns with both your current operational demands and your long-term vision for growth, ensuring that technology evolves in step with your business objectives.

Quick Reference:
End-of-Life Readiness Checklist

- Are you unsure of which versions of operating systems or applications are in use at your business?
- Are any of them over 5 years old?
- Is your server or key software version no longer supported?
- Are your employees complaining about slow systems?

If you answered yes to any of these questions, you may be at risk. We strongly recommend you speak to our helpful team of IT experts to create a plan to confidently move away from end-of-life software.

Time is Not On Your Side

End-of-life software isn't just a technical inconvenience. It poses serious risks that span cybersecurity, compliance, operational reliability, and ultimately, your reputation. As cyber threats become more advanced and regulatory standards more stringent, ignoring the support status of your infrastructure is a gamble few businesses can afford to take.

With Windows Server 2012 and SQL Server 2014 already out of support, and future dates fast approaching for other versions, the time to act is now. Whether you've inherited technical debt from the past or are just becoming aware of these looming deadlines, this guide has shown that there are practical, forward-thinking solutions available today.

Microsoft Azure provides a secure, scalable, and cost-effective way for small and medium businesses to leave legacy software behind. From enabling secure remote access to automating updates to supporting innovation and AI integrations, Azure isn't just a way to eliminate risk, it's a leap toward a more resilient and agile future.

How Extech Can Help

We specialise in helping small and midsize businesses identify these risks early, and migrate to modern, secure, and scalable platforms like Microsoft Azure with minimal disruption.

We start by conducting a full software audit of your current environment. This helps us identify unsupported operating systems, legacy applications, and other vulnerabilities that may be putting your business at risk.

From there, we'll build a bespoke migration plan that aligns with your specific needs, whether that means upgrading to a new server or moving your workloads to Azure virtual machines or managed databases. Our certified team handles the entire transition, from architectural design to implementation, ensuring security best practices at every step.

But our support doesn't stop there. We work with you long-term to optimise your Azure environment, reduce unnecessary costs, and unlock capabilities that drive future growth.

With us, you get a trusted technology partner who understands the challenges you face today and helps you prepare for the opportunities of tomorrow.

Let's modernise your infrastructure before it becomes a liability and turn that investment into a competitive advantage.

extech cloud

01444 443200 | **www.extechcloud.com** | info@extech.co.uk