Once upon a time, your custom software probably fit like a glove. But technology moves quickly, if your company has been around for a while, then it could pose a serious threat to your company and customers.

‘Unsupported (or end-of-life) software’ ranks first place in the Cybersecurity and Infrastructure Security Agency (CISA)’s list of security bad practices, while over half of IT professionals in critical industries say that legacy systems represent their biggest security challenge.

Legacy software exposes vulnerabilities and blindspots that cyber attackers can exploit to damage your company. Here are the main security risks of legacy software, and why, as a result more businesses are now migrating away from their legacy software to cloud-based environments.

What is legacy software?

It can be hard to work out whether your software has really depreciated, which is why so many companies struggle to know when and why they need to upgrade. Generally, however, legacy software can be split into two camps:

Dead software

This is software that’s no longer used, perhaps because it was replaced or became redundant. Either way, if this software is still tied into your services or provides access to your network, it poses a serious security risk.

Dying software

If your software is no longer useful, cost-effective, or agile enough to keep pace with your business, and most importantly – if it’s no longer being updated – then it’s legacy.

Why do companies hold on to legacy software?

The short answer is a fear of change. Software is the backbone of your company. Your employees use it every day (and probably know how to work around its flaws), it’s likely deeply embedded in your products, services, and day-to-day operations. What’s more, it may have been particularly expensive or complex to set up in the first place, meaning that upgrades can require a complete system overhaul and significant downtime. Ripping out your backbone in this way doesn’t appeal to anyone, and it’s why many companies delay important software upgrades and migration plans.

Unfortunately, the debt builds up in one way or another. More than half of chief information officers say that they spend up to 60% of their time managing legacy technology. And when the average cost of a data breach is over $4.5 million, the benefits of investing in modernisation become devastatingly clear.

What are the security risks of legacy software?

Over 20,000 vulnerabilities have been discovered in 2024 so far – a figure set to be the highest ever recorded. Attackers are finding increasingly sophisticated ways to breach systems using tools and techniques such as ransomware, malware, phishing scams, and authentication flaws, and legacy software makes their lives a lot easier. Here's why:

1. Legacy software **is no longer supported**

Legacy software eventually stops receiving support from the original developers, vendors, or manufacturers. While your teams may continue using it, you won't receive official updates or bug fixes that protect you against new and evolving cyber threats.

The longer you hold on to legacy software, the more the documentation goes out of date, making it harder to understand your system's vulnerabilities, and the harder it is to find professionals skilled enough to work with it. Even informal communities built around solving legacy problems dwindle as times change, and the only remaining support will likely be expensive and no guarantee of safety. All of this is a perfect storm of confusion that stops your current and future employees from being able to fully protect or even understand your software. It's in these blind spots that attackers catch your scent and exploit the vulnerabilities left unpatched.

2. Legacy software **lacks modern security controls**

In just the past few years, the cyber threat landscape has evolved dramatically. To keep pace with the latest attack methods, your software needs to include several security controls – at minimum. These include:

- **Multi-factor authentication (MFA)**
  - Designed to protect your sign-in processes and digital identities.
- **Zero trust model**
  - Continuously verifies identities and enforces strict session and access controls.
- **Modern encryption algorithms and secure communication protocols**
  - Helps prevent eavesdropping and data theft or manipulation.
- **Monitoring and reporting tools**
  - Such as behavioural analysis, intrusion detection, and antivirus software.

Security controls like these help prevent attackers accessing your network, escalating their privileges, and reaching critical data and resources. Unfortunately, legacy software is often designed to work independently – lacking compatibility with modern tools, networks, or mobile applications. This prevents you from backing up or recovering your systems and devices, and makes it easy for attackers to infiltrate your network without raising suspicion.

3. Legacy software **creates blindspots**

Visibility is key to good cybersecurity. If you can't see what's going on inside your network, how can you expect to spot suspicious behaviour? Legacy software is often home to users, privileges, applications, and third parties that IT teams can't see or have forgotten about, and it's through these unmonitored access points that attackers can infiltrate your network. As opposed to leaner cloud alternatives, for example, legacy software is usually monolithic too, which helps to hide any discrepancies within.

If your software is making life difficult for your teams, they're more likely to leave things exposed. After all, employees grappling with the day-to-day issues of legacy software may not be vigilant of phishing attempts, good password hygiene, or safe remote working practices, while admins and security teams may lack the tools to audit their network environment and assign the correct access permissions to users. To make matters worse, legacy software often lacks backup options or recovery processes. This means that if you're attacked, you could lose everything.

Case studies

Legacy accounts that aren't protected by authentication controls such as MFA or monitored by administrators are prime targets for attackers. Recent incidents such as the Change Healthcare ransomware attack and Russia-linked Microsoft hack are key examples.

4. Legacy software **opens the door to insider threats**

Legacy software can also be damaged from within by your own employees. These insider threats, as they're known, are often far quicker and more devastating than attacks coming from outside. In 2023, insider threat incidents cost companies an average $16.2 million.

Insider threats have privileged access to networks, systems, and data. This makes it easier for them to deploy malware, for instance, into the heart of your software without alerting security teams – especially if software lacks the proper security controls or architecture to recognise suspicious behaviour.

Here's a twist: insider threats aren't always malicious. If your software is causing confusion, employees can accidentally alter critical system controls, exploit unpatched vulnerabilities, or leak personal and business data – inadvertently damaging your system from within and opening the door to attackers.

Case studies

Malicious: In 2023, two former staff members at Tesla breached the sensitive information of nearly 76,000 employees and shared it with a German newspaper.

Accidental: An employee at Verizon accidentally leaked the personal information of more than 63,000 people (mostly Verizon employees). The incident wasn't discovered for three months.

5. Legacy software **leads to non-compliance**

Leaving these security holes exposed can have serious legal, financial, and reputational consequences. This is because most companies – especially those in sensitive industries such as healthcare, manufacturing, and finance – are subject to data privacy and security regulations including:

- General Data Protection Regulation (GDPR)
- Sarbanes–Oxley Act (SOX)
- California Consumer Privacy Act (CCPA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- And more

These regulations have been growing stricter in recent times as cyber threats grow more sophisticated. have been known to reach (billions?) and data security is a top concern for customers and suppliers today before deciding to trust a business. These regulations state that companies have a duty to protect their software to safeguard sensitive data – this may often involve modernizing and having up-to-date software. If legacy software is to blame for attacks and it shows up in audit logs, then companies will be penalised.

Now is the time to act

Strong cybersecurity requires fast, lean, and agile software that can scale with your company while fending off fast-evolving cyber threats. The gold standard today is a private, public (AWS, Google Cloud, Microsoft Azure), or hybrid cloud environment which includes security features such as:

- State-of-the-art encryption standards (such as TLS/SSL and ES-256)
- Strong authentication mechanisms (such as MFA, passwordless, and single sign-on)
- Behavioural detection and analysis tools
- Regular (and automated) security patches and bug fixes
- Detailed audit logs and compliance monitoring
- Digital identity protection
- Zero trust architecture
- Incident response and reporting measures

Ultimately, your employees and customers are relying on the security of your software. If you think you're running legacy software, it's crucial to review your security posture as soon as possible. Undiagnosed vulnerabilities in your system can have devastating consequences.

How Genolis can help

At Genolis, we offer a **free security assessment** to see whether your software is putting you at risk, and how you can modernise it to gain full protection and peace of mind. **Get in touch** for a free consultation today.

About us

Modernising your software doesn't have to be difficult or expensive. At Genolis, we have over 20 years of experience in building innovative, scalable, and secure custom products that help companies – especially those in industries with tight security requirements such as healthcare, finance, and manufacturing – to innovate and grow. With expertise in web services, cloud solutions, desktop and mobile apps, and more, we support you every step of the way on your journey to modernisation.