

Open Source, Security & the Future of Digital Experience

Why Enterprises Can Have Both with Umbraco



Executive Summary

For years, open-source software has carried a reputation for being “less secure” than proprietary platforms. Many enterprises assumed that transparency created risk and that “closed doors” meant safety.

This perception is outdated. Today, enterprises already run the bulk of their mission-critical infrastructure on open source – from Linux to Kubernetes to MySQL. Security isn’t about whether software is open or closed; it’s about implementation, governance, and transparency.

This paper examines why **open source and security are not opposites but allies**, and why Umbraco CMS is a prime example of how enterprises can achieve flexibility, innovation, and compliance without compromise.

The Persistent Myths of Open Source Security

Security concerns remain a top priority for enterprises in 2025, as digital experiences become increasingly complex and tightly regulated. At the same time, open-source adoption has surged across every layer of enterprise infrastructure.

Far from being a fringe option, open source now powers the operating systems, databases, and container technologies relied on by the world's largest organizations. Yet myths persist that open source is inherently less secure.

- **Myth 1: Open source is insecure.** If the code is visible, vulnerabilities must be too.
- **Myth 2: Proprietary means safer.** Vendors control visibility, so threats must be lower.
- **Myth 3: Communities are unreliable.** With “too many cooks,” the risk of bad actors is greater.





These beliefs are rooted in outdated views of open source projects and don't reflect how modern enterprise software ecosystems operate.

“I came into the industry with the idea that you couldn't really use open source software if security was a concern... I was deeply concerned about the transparency. I was concerned about the hive mind aspect... But, you know, little me, 10 years ago, had no idea really that some of the things that I believed were just myths.”

– Emma Burstow, VP Developer Relations, Umbraco

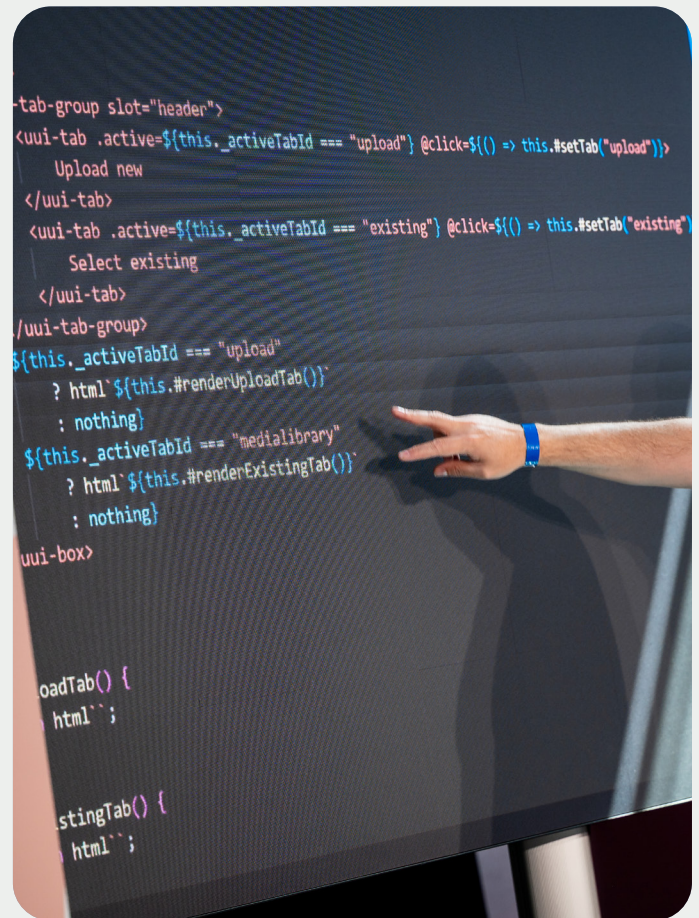
The Reality: Open Source is Already Everywhere

Enterprises trust open source for the foundations of their digital infrastructure:

- **Operating Systems:** Linux (Ubuntu, CentOS).
- **Containerization:** Docker, Kubernetes.
- **Databases:** MySQL, PostgreSQL.

If open source is trusted for the most sensitive enterprise systems, why not content management?

The challenge is not open source itself, but how it is implemented and governed.



“I would say that 90–95% of actual enterprise companies find open source software strategically important. If you think about operating systems – Linux, whether it’s Ubuntu or CentOS – that’s open source. All the containerization products we’re using, Docker, Kubernetes... that’s all open source. Even databases like MySQL. They’re already comfortable with open source in their infrastructure.”

– Chris Osterhout, SVP Strategy, Diagram

Transparency and Community as Security Assets

In proprietary systems, enterprises depend on vendors to disclose vulnerabilities – sometimes weeks or months after discovery. In open source, transparency enables:

- **Rapid discovery of vulnerabilities.** Issues are found and reported by the community.
- **Faster patching.** Fixes are often delivered by contributors before the vendor is even aware.
- **Shared accountability.** A global developer community contributes to a stronger, more innovative platform.

Umbraco's Security and Privacy Community Team, which consists of global security experts, developers, and digital agencies, works proactively to identify risks, share best practices, and innovate on security features.

It's also important to note that while Umbraco is proudly open-source, Umbraco HQ is the main contributor to the core CMS and is committed to maintenance and management of the project. This means enterprises benefit from the innovation and transparency of the community, while also relying on a dedicated, professional team that takes full responsibility for security and quality.





“When you are able to discover vulnerability rapidly and patch it also rapidly, it means you have a short process. In some cases, vendors take longer than open source. That’s why transparency and community are really important.”

– Zoja Antuchevic, *CEO & Partner, SolutionLab*

“If everything’s transparent and in the open, then yes, people can spot vulnerabilities and report them and fix them.”

– Emma Burstow, *VP Developer Relations, Umbraco*

Enterprise Alignment: Why Umbraco Fits

Umbraco is not just open source – it is enterprise-ready.

- **Release Cadence:** Aligned with Microsoft .NET's six-month cycle, ensuring predictable, secure updates.
- **Composability:** Easily fits into enterprise infrastructures – marketing websites in Umbraco Cloud, sensitive data in HIPAA- or PCI-compliant portals.
- **Security by Design:** Built on ASP.NET Identity, enabling MFA, Azure AD, and enterprise-grade authentication integrations.
- **Scalability:** Powers everything from corporate websites to multi-site, multi-language enterprise platforms.

Behind this, Umbraco HQ ensures that the platform's core is actively maintained, reviewed, and improved by full-time experts, giving enterprises confidence that the CMS is professionally governed while still benefiting from the openness of the wider ecosystem.



Education as a Superpower

Procurement teams often arrive with rigid checklists that are sometimes copied from unrelated use cases.

Examples:

- Demanding PCI compliance for a simple marketing website.
- Insisting on custom in-house development rules for SaaS platforms.

The real opportunity lies in asking the right questions:

- Why do you need this?
- What risk are you trying to mitigate?
- What business goal is behind the requirement?



Enterprises that partner with solution providers who take this approach gain more trust and achieve smarter, more flexible solutions.

“Most of the time, there’s an educational process that goes along with it. Once you start to peel back the layers on their request, you find out things aren’t what they seem... If you raise the right questions, they’ll then say, ‘okay, this is an exemption for this request’, because it doesn’t make sense.”

– Chris Osterhout, SVP Strategy, Diagram

Balancing Freedom and Security

Enterprises are drawn to open source for developer freedom, but does freedom compromise security?

The answer: **No.**

- **Freedom fuels innovation.** Developers can build exactly what is needed, not wait years for vendor approval.
- **Security is a team sport.** Infrastructure, governance, and community contributions all strengthen the system.
- **ROI improves.** Faster fixes, faster innovation, and faster time-to-value create direct business benefits.

With Umbraco, enterprises don't choose between agility and safety. They achieve both.





“When you don’t have security through obscurity, and you have transparency, it creates a scenario where developers have more flexibility. And in doing so, it accelerates fixes and it accelerates innovation.”

– Chris Osterhout, SVP Strategy, Diagram

“Freedom and security are complementary. With collective accountability, you can prioritize what you will do first, without sacrificing trust in your product.”

– Zoja Antuchevic, CEO & Partner, SolutionLab

Practical Considerations for Enterprises

Enterprises evaluating CMS security should focus on real-world implementation scenarios rather than theoretical risks. Consider the following:

- **Multi-tier infrastructure requirements:** Modern CMSs like Umbraco can operate securely in highly regulated environments (e.g., finance, healthcare, government) using headless configurations, APIs, and composable infrastructure strategies.
- **Authentication:** By leveraging ASP.NET Identity, enterprises gain enterprise-grade login capabilities, with support for MFA, Azure AD, and other identity management integrations.
- **Extensions and marketplace packages:** As with any software ecosystem, governance matters. Enterprises should apply their own risk tolerance, auditing, and testing to ensure packages meet compliance needs, while benefiting from a strong, active community review process.



“From my perspective, security is a team sport. There’s infrastructure, governance, and then the actual code. And that’s where the community comes in so great, because we’re talking about it openly.”

– Chris Osterhout, SVP Strategy, Diagram



Conclusion: You Can Have It All

The choice between open source and security is a false dilemma. With Umbraco, enterprises gain:

- **Transparency and Trust:** Security through openness, not obscurity.
- **Predictability and Control:** Microsoft-aligned release cadence and enterprise-ready compliance.
- **Flexibility and Innovation:** Community-driven enhancements and rapid adaptation to new needs.
- **Lower Total Cost of Ownership:** No license fees and modular architecture ensure unmatched ROI.

Enterprises don't need to choose between freedom and security. They can have both. And with Umbraco, they can have it all.

Ready to explore how Umbraco can support your enterprise security, compliance, and digital experience goals? Schedule a discovery call with us and get a tailored assessment of how Umbraco fits your security requirements.



“You can have it all. There’s an illusion of security with proprietary software, security through obscurity. Working in the open means we’re better equipped to innovate, to fix vulnerabilities, and to build solutions that are as safe as they can be.”

– Emma Burstow, VP Developer Relations, Umbraco



umbraco