Secure by Design in Public Sector Programs

BROUGHT TO YOU BY

FIERCE
SOFTWARE

Table of Contents

Secure by Design Sets a New Standard for Software

Secure by Design guidance is ratcheting up expectations for software manufacturers, and Enterprise Open Source companies like Red Hat and others are rising to the challenge. As the industry rises to the new benchmark, it is worth exploring how the Secure by Design expectations should be applied in public sector programs and how these programs approach their use of open source software.

The Cybersecurity & Infrastructure Security Agency (CISA) and other cyber centers are champions of Secure by Design. As an international effort to guide software manufacturers, Secure by Design takes the steps necessary to design, develop, and ship only products that are secure by design. CISA urges software manufacturers to build their products in a way that reasonably protects against malicious cyber actors exploiting vulnerabilities by baking in more risk mitigation and reducing the burden on customers.

SECURE BY DESIGN URGES MANUFACTURERS TO ADOPT THREE PRINCIPLES.

1. Take ownership of customer security outcomes and evolve the product accordingly so the burden of security does not fall solely on the customer.

2. Embrace radical transparency and accountability by sharing vulnerability information and making security a product differentiator.

3. Build organizational structure and leadership to achieve these goals internally and in partnership with customers.

While the Secure by Design principles and guidance are oriented toward commercial software manufacturers, the same general principles can and should apply to public sector technology programs. These programs are citizen-focused products, and users have the same high security expectations as any commercial product or service. It is incumbent on government leaders and their industry teams to act in alignment with the Secure by Design principles.

The Secure by Design principles may sound simple, but inherent in them is action, and none of this action is free. The cost to abide by these principles must be allocated somewhere in the supply chain.

The Challenge of Open Source-Only Public Sector Programs

Many public sector software programs are built by labor services teams using exclusively open source software. This is often done to limit short-term license costs. For these labor services team programs delivering purely open source software, consider the application of the Secure by Design principles.

There is significant interest in closely tracking the Software Bill of Materials (SBOM) for the components that make up public sector technology programs, but this is just the start of the challenge. When a vulnerability is identified, someone needs to DO something about it. For labor-only programs, this requirement to act falls solely on that program team. Since most teams are contracted, contractual constraints can become a choke point. Is there scope to do it? If there is flexibility in the contract to respond, the next question becomes that of priority. Do they fix it and sacrifice new features or take the risk? If the contract has no flexibility, as is common with legacy operations and maintenance contracts, a government-driven modification may be required to address the vulnerability. This often means shifting money from other priorities. It is easy to see how this challenge spans the principles of Secure by Design.

As with any product, the choice to action is a leadership challenge, and, in the case of the open source-only program, government leadership and that contracted product team are on their own. To properly take ownership of the security outcome, this team must rise to the challenge on its own merits; it must do the homework, become an expert, design an alternate solution, and implement it. The reality is that this is genuinely difficult, and there is a cost associated with it. Free software becomes very expensive very quickly. With the high complexity of today's Kubernetes-based software systems, too often, the team does not organically have the comprehensive domain expertise needed at the price point they bid to get the program to work. This forces a risk acceptance decision and technical debt in the program to build up.

Lean on Enterprise Tools to Make Programs Secure by Design

Fierce Software always advocates for public sector programs to lean on Enterprise Open Source providers. While there are many benefits to partnering with Enterprise tool providers, two benefits stand out in the context of Secure by Design. Leaning on Enterprise providers gives programs a secure baseline, associated configuration guidance, and access to expertise and best practices learned from across the customer base. It also provides programs with a dedicated security advocate and leadership partner who is sharing ownership of the program's security outcomes. This is a powerful backstop for public sector programs.

Secure by Design Should Be a Mosaic in Public Sector Programs

As Enterprise Open Source providers step up to meet the Secure by Design guidance, this gets passed on to public sector programs, who pass it on to their citizen customers. Supply chain security becomes a mosaic of Secure by Design components. A diverse vendor base becomes a force multiplier for vulnerability awareness. Each vendor looks at security issues from their own unique aperture and passes on this perspective to program leaders and delivery teams.

The cost of addressing vulnerabilities is never free, but when it is part of a commercial software item and that manufacturer has chosen to make security a differentiator, the burden is reduced. For programs that lean on Enterprise tool providers, if that software manufacturer follows the Secure by Design principles, the cost to address new vulnerabilities is already budgeted and committed. It's built into the subscription from the Enterprise Open Source providers. Government leaders don't need to modify contracts or sacrifice new functionality to address the issue. The bill is paid. For these programs, Secure by Design mosaic becomes a robust safety net that allows them to focus on new features and citizen outcomes. Instead of a small team being responsible for all the technical elements, the ownership of the customer security outcome is shared across a wide base of invested and committed partners.

Choose Partners Who See Security as a Differentiator

Red Hat is far from alone in stepping up to the new Secure by Design guidance, but it does stand out as a dependable starting point for public sector programs. Red Hat products are the benchmark for security, a product differentiator. With comprehensive security built into all the products, Red Hat was already a brand synonymous with security. The capabilities in line with the Secure by Design principles are no exception.

Red Hat Trusted Application Pipeline and Red Hat Advanced Cluster Security for Kubernetes are two halves of a full lifecycle approach to open source software security. Red Hat Trusted Application Pipeline focuses on the software build and component selection side of the equation, and Red Hat Advanced Cluster Security lives in the runtime environment.

Red Hat Trusted Application Pipeline is a hosted and managed service to securely build and assemble next generation cloud-native applications and deploy them to target environments. It is designed from the ground up to be both extensible and rigidly enforced and to provide maximum secure oversight during the build process, including digital audit assets and SBOM to temporally stamp and guarantee build source integrity. It provides a much-needed and necessary toolset for building, securing, and deploying applications to Red Hat OpenShift.

Red Hat Advanced Cluster Security for Kubernetes operates at the object and image level, providing runtime security of clusters, tracking misconfigurations, policy noncompliance, runtime threats, and images at risk. DevSecOps works best when Ops prompts Dev to take action, and Dev allows no new issues forward into Ops. As vulnerabilities are identified by Advanced Cluster Security and development teams take action, instead of starting from zero, they can simply lean on the built-in warnings and alternative component recommendations in the Trusted Application Pipeline to point them in the right direction.

To aid development teams further, Red Hat Trusted Content has curated builds and hardened open source libraries that have been verified and attested with provenance checks by Red Hat – OpenShift customers can draw upon these when building their apps. Contrast this with the lonely reality of an open source-only program where this responsibility falls solely on a small development team.

FIERCE SOFTWARE IS YOUR INNOVATION RESOURCE

The Secure by Design paradigm is essential for mitigating cybersecurity risks in an increasingly interconnected world, and it needs to be practiced by both commercial software manufacturers and public sector programs alike. In the public sector, program leaders must make informed decisions regarding resource allocation, recognizing that commercial products offer a cost-effective and secure alternative to purely open-source-based custom solutions.

Fierce Software is standing by to help public sector-focused teams assemble an enterprise-ready, Secure by Design, mosaicked approach to delivering better security outcomes for citizens. Our team makes the connections between market-leading vendors and government requirements. We are your Innovation Broker. Contact **sales@fiercesw.com** to get started.

FIERCE
SOFTWARE

SALES@FIERCESW.COM
888-576-1572
FIERCESW.COM