

General Purpose OS vs. TempestOS

The cost of building on the wrong foundation.

Executive Summary

Cybersecurity compliance is one of the most disruptive and consistently costly challenges in the path from development to deployment. For organizations building capabilities on general-purpose operating systems the compliance process arrives late and forces a retrofit of the already built system. Right when your team is ready for an exciting product launch your company faces a cost and delay black hole that often breaks what made your capability great. The result is expanded timelines, compromised product functionality, and wasted resources on a recurring operational burden.

This is the cyber compliance valley of death. The gap between a product that works and a product that can be sold to the government has swallowed entire programs and driven thousands of companies out of the defense market entirely.

TempestOS is built to eliminate that burden at the source. 92% STIG-compliant out of the box on average, TempestOS makes cybersecurity compliance a property of the infrastructure your capability runs on, rather than configurations made to the capability software after the fact. For engineering teams that need to stay focused on capability development, that starts with a cyber foundation that handles compliance at the infrastructure level, not as an afterthought. **TempestOS is that foundation.**

■ THE PROBLEM

Cybersecurity Valley of Death in Product Deployment Lifecycle



Building a capability for a Navy or DoW customer means navigating a complex acquisition environment. Your team is managing timelines, budgets, and the technical complexity of building something that works. Somewhere between build and deployment, cybersecurity compliance enters the picture and the forward movement stops.

Compliance doesn't fit the timeline. Government cybersecurity requirements do not slot cleanly into a development timeline. It arrives as a checklist of hundreds of controls that must be applied to a system that was already built. Your engineering team is now working backwards through that system to satisfy compliance requirements. Achieving baseline compliance typically takes 6 to 12 months, and for organizations starting from scratch, that window can extend to 18 months or more.

General-purpose operating systems like RHEL, Ubuntu, and Windows 11 were not designed for the operational and security demands of a warfighting system. The gap between what those systems are and what government compliance requires is measured in hundreds of controls (STIGs), months of engineering time, and a list of integration barriers that grows every time a CVE announces a new vulnerability.

The cost compounds across the entire program. While the cybersecurity team works through compliance requirements, the engineering team is on standby. When cyber inevitably changes something in the system, engineers go back to fix anything that breaks. Two teams, two disrupted workloads, and a program (and warfighters) absorbs the delay. Every iteration of that cycle is wasted money, measured in personnel hours, stalled programs, and opportunities that didn't move forward. Industry research consistently shows that addressing security as a retrofit rather than a foundational property results in significantly higher lifecycle costs and compounding rework.

■ THE SOLUTION

The Cyber-Hardened OS

TempestOS is an operating system built from the ground up for the defense environment, which means cybersecurity is a property of the foundation itself. When a program builds on TempestOS, it starts from a baseline that arrives approximately 92% STIG-compliant out-of-the-box, with the operating system having already handled the bulk of compliance requirements upfront. This is achieved through a secure-by-removal approach, where unnecessary components, services, and packages are stripped out at the build level rather than disabled or patched after the fact. **If a component doesn't exist in the system, it can't be exploited.**

CopyFail (CVE-2026-31431), a critical Linux kernel vulnerability discovered in April 2026, illustrates what that means in practice. TempestOS's debloated architecture had already removed the affected component at the build level, meaning teams running TempestOS had no exposure or interruption.

Operating System	STIG Compliance Out-of-Box
Ubuntu (22.04, latest STIG-profiled version)	23%
AlmaLinux	36%
RHEL 9	37%
TempestOS	92%

STIG compliance percentages based on internal assessment conducted by Caliburn Technologies against applicable DISA STIG benchmarks.

Building on a compliant foundation changes the trajectory of a program. Cybersecurity compliance is no longer an unpredictable variable in the path to deployment. Engineers stay focused on the capability cybersecurity teams get out of remediation mode, shifting compliance from operational expense to capital investment.

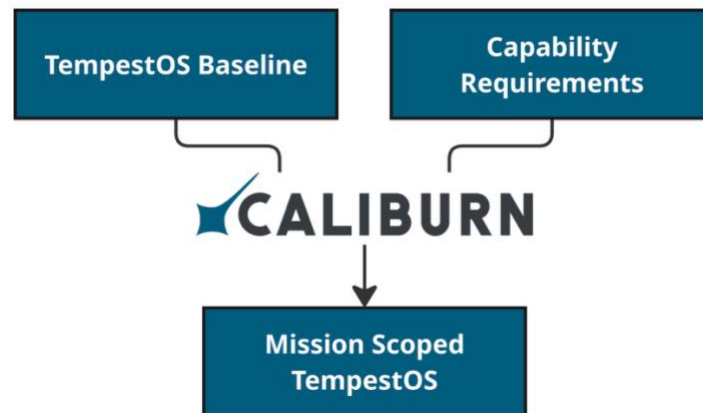
■ HOW

Secure by Design

TempestOS originated from AlmaLinux and has been systematically debloated into its own hardened tactical Platform as a Service. TempestOS is not a commercial OS adapted for defense use, it is developed by applying decades of DARPA and DISA guidance on what a hardened government system requires at the operating system level.

General-purpose operating systems ship with an enormous volume of code, services, and packages that most users will never need. In a defense context, that excess is a liability. Every unnecessary component is unnecessary attack surface. STIG compliance checklists exist to address that liability, requiring teams to disable or configure components that are largely not applicable to their use case. TempestOS removes them at the build level. If a vulnerability does not exist in the system, it cannot be exploited.

How TempestOS Works for You



TempestOS is configured specifically for the system it will run on, meaning the compliance foundation and the operational capability are built together from the start rather so there are fewer tradeoffs needed after the fact.

Caliburn leads that configuration process end to end. It begins with an assessment of the user's needs. Those components are then integrated into the TempestOS baseline as a container, producing a version of TempestOS scoped to that exact mission. The customer receives a cyber-hardened, compliant operating system built specifically for what they need to do.