

# Hardened Backup Purpose Built for 'No Internet' Environments

A tested & trusted point solution for the US public sector's most sensitive networks



## WHAT MAKES OUR HARDENED SOLUTION UNIQUE?

Acronis SCS Cyber Backup 12.5 Hardened Edition is specifically designed to meet the unique backup and disaster recovery needs of US government air gapped environments – a traditionally underserved market. This game-changing solution is the only full disk image backup and disaster recovery point solution available on the Department of Defense Information Network Approved Products List (DoDIN APL). Four key elements set our product apart to keep your critical systems safe:

**Zero-connectivity.** Our hardened product requires zero integration or outbound connections to online services. That means no kill switches or callbacks for activation or licensing. Our licenses are *only* validated locally. As a result, our product radically reduces your environment's attack surface, while minimizing the time your IT staff must spend wading through false alerts and failed outbound communications – common pitfalls of using a non-hardened solution in an air gapped environment.

**Encryption.** Our hardened product incorporates FIPS 140-2 validated encryption and RSA key generation. It also uses the Intel-pioneered, hardware-based random number generation method to ensure our encryption is seeded with maximum entropy.

**Security.** Our hardened product has undergone extensive penetration testing by third-party "red teams" and our own internal security department. In addition, users can enjoy the security benefits of our built-in, AI-based anti-ransomware tool, called Active Protection, and our US-based product support (available for *all* our products).

**Certification.** Our hardened solution is [certified and officially listed](#) on the DoDIN APL. It is in process for FIPS 140-2 and Common Criteria, with both certifications slated to finalize in 2020.

## Why Certification Matters?

**DoDIN APL (certified)** ensures our hardened product is recognized as a military/DoD lab- tested and trusted solution for purchase within DoD. Customers can now choose the only approved full disk image backup and disaster recovery point solution available.

**FIPS Certification** (in process) verifies our backup communication and archives are protected with military-grade encryption and have been reviewed by government labs for use in environments that contain sensitive information.

**Common Criteria** (in process) provides assurance that our specification, implementation, and evaluation processes were conducted in a thorough and standard manner.

These standards, which satisfy information assurance and supply chain requirements in the United States and are managed by the National Security Agency, are also accepted by thirty+ countries.

## THE RIGHT FIT FOR YOUR ENVIRONMENT

### Federal & Defense

Our hardened backup solution is a game-changer for DoD, other federal agencies, and Federal Systems Integrators (FSIs) that operate in air gapped environments containing sensitive and/or classified information. Within one streamlined interface, organizations can easily build, test, deploy, and protect their complex integrated systems. This is critical for FSIs looking for a protection application that easily integrates into larger platforms supporting unique and sensitive DoD environments.

Our hardened product meets the unique backup and imaging needs for these environments, including deployed 'no internet' tactical elements (like ships, planes, and land vehicles) and warfighters stationed on Forward Operating Bases across the globe. In an emergency situation, our solution's bootable media component can seamlessly and quickly restore standardized and unique images to toughbooks and field laptops from one command.

Our product also has specialized utility for defense training simulators for unmanned aircraft/vehicles. In just one hardened solution, you can protect both the stack running your training programs and all the highly sensitive data generated from these activities.

### SCADA Systems & Development Centers

With mission critical and sensitive operations to protect, development centers and Supervisory Control and Data Acquisition (SCADA) systems need a resilient and secure backup solution. Our hardened product is your answer.

SCADA-centric environments that maintain electricity, water, and other utilities for municipalities across the United States require critical infrastructure protection they can count on. Our hardened solution minimizes recovery times for mission critical systems.

### THE BOTTOM LINE

Performing repetitive yet crucial tasks on sensitive systems – like full disk image and file-level backup – is a daily reality for technical personnel across all levels of the US government, the education/nonprofit sectors, and beyond. Let our hardened backup solution make your job easier and your systems more resilient to attack. No unnecessary complexity and outbound connection points that expand your organization's attack surface. No third parties touching your interface and accessing backend protocols for integration or license maintenance. Just one cost-effective, flexible, and state-of-the-art solution that seamlessly supports all your disk imaging, backup, and disaster recovery needs.

Users can immediately restore an image of a working version of a device and capture reliable backups prior to applying system security updates and patches.

For development centers that create and test systems and applications in a lab before migrating to production, our hardened product meets your unique needs. With one single imaging product and interface, development centers can build, test, deploy, and protect their complex integrated systems with ease. Your IT staff can easily perform flexible backup and restore functions on both legacy and newer systems, in dissimilar computing environments, and on all types of platforms, from physical to virtual, virtual to virtual, and virtual to physical.

### SLED & Nonprofits

Our hardened product's unmatched security features enable SLED and nonprofits to safeguard constituent and student PII and ensure operational continuity. Our product is easy-to-implement and cost-effective, making it ideal for limited IT staff and cybersecurity budgets. With the ability to restore to dissimilar environments – across both legacy and newer systems – you can rest easy that *all* your devices are protected, whether your network is air gapped or not.

As recent headlines make clear, SLED targets are fixed in ransomware attackers' sights. Our built-in, AI-based module called Active Protection keeps your data virtually impervious to their efforts.

### Other Non-Air Gapped Environments

Even if your organization's environment is not air gapped, our hardened product offers a user-friendly solution to keep your data accessible yet secure. With no outbound connections and AI-based anti-ransomware protection built in, our hardened product reduces your vulnerability to outside attack and keeps your devices up and running.