Acronis SCS Cyber Backup 12.5 Hardened Edition

Hardened backup purpose built for “no internet” environments

Acronis SCS Cyber Backup 12.5 Hardened Edition is a full disk image backup and disaster recovery point solution specifically designed to keep systems up- and-running in the US public sector’s most sensitive environments: air gapped, “no internet” networks, including Department of Defense weapons testing sites, development labs / centers, training simulators, deployed tactical elements and warfighters, public utility supervisory control and data acquisition (SCADA) systems, and more.

Maximum operational assurance and data security through complete asset protection

- Minimize or eliminate downtime to ensure access to mission critical data and systems.
- Immediately restore a full-disk image of a working version of a device.
- Easily build, test, deploy, and protect complex integrated systems with one interface.
- Keep DoD and other government agency systems up and running in the face of attack or failure.
- Recover a full system image from the network or optical drive without deploying an agent.

ZERO CONNECTIVITY

- Requires zero integration or outbound connections to online services
- No kill switches or callbacks for activation or licensing
- Licenses are only validated locally

HIGH GRADE ENCRYPTION

- FIPS validated encryption
- RSA key generation for encryption
- Uses Intel-pioneered hardware random number generation for maximum entropy

KEY SPECS

- Uses OS keychains for secure storage of credentials
- Exclusive use of TLS v1.2 for transport-level security. This is the most up to date certified, encrypted communication protocol
- Uses highest levels of public key infrastructure (PKI) validation throughout the entire certificate chain, with emphasis on revocation checking

SECURITY

- Extensively reviewed and tested as part of certification processes
- Built in, AI-based ransomware protection
- US based support - no customer information leaves US soil

Certifications & Compliance

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.

Common Criteria (certified)

The Common Criteria Certification ensures our product’s specification, implementation, and evaluation processes were developed throughly and comprehensively.

FIPS 140-2 (validated)

Verifies our backup communication and archives are protected with high grade encryption and have been reviewed by government labs for use in environments that contain sensitive information.

Cyber Security Maturity Model Certification 2.O (CMMC 2.0) Level 1

Acronis SCS demonstrates effective cyber security practices and safeguards for sensitive information through CMMC 2.0 level 1 compliance, achieved by completing a Self-Attestation and obtaining a letter of Affirmation from a C3PAO.

VPAT Section 508 (Validated)

The Voluntary Product Accessibility Template (VPAT) evaluates how accessible a particular product, in our case software, is according to Section 508 Standards of Rehabilitation Act.

Acronis SCS Cyber Backup 12.5 Hardened Edition is the only full disk image backup and disaster recovery point solution available on the DoDIN APL.

FFull Disk Image Backup Disaster Recovery Point Solution

Maximize security, keep systems operational in the face of crisis, and maintain overall peace of mind.

Radically Reduces Attack Surface While Enhancing Usability

Acronis SCS Cyber Backup 12.5 Hardened Edition requires zero integration or outbound connections to online services. No kill switches, no callbacks, and no unnecessary points of potential vulnerability in your network. Hear the shouts of joy as your IT staff reclaims the hours normally spent wading through the false alerts and failed outbound connections generated by non-hardened solutions.

In addition, Acronis SCS Cyber Backup 12.5 Hardened Edition uses only the highest grade encryption methods, including RSA key generation and Intel-pioneered random number generation for maximum entropy, and our AI-based anti-ransomware module keeps systems virtually impervious to attacks with award-winning technology that has caught every strain of ransomware since notPetya.

Keeps Critical Systems Operational

Acronis SCS Cyber Backup 12.5 Hardened Edition ensures operational assurance and preserves timely decision -making on the battefield and beyond by:

- Minimizing recovery times for mission critical systems following a cyberattack or failure
- Providing the flexibility to seamlessly restore standardized and uniqe imaged to devices out in the field via our bootable media feature
- Ensuring you can build, test, deploy, and protect complex integrated systems from one management console

Delivers the Highest Standard of Security

Acronis SCS Cyber Backup 12.5 Hardened Edition has been rigorously tested as part of in-depth FIPS 140-2, Common Criteria, and DoDIN APL certification processes. The product earned DoDaIN APL certification in April 2020, Common Criteria-certified under server and agent protection profiles in August 2020, FIPS 140-2 validation in December 2020 and CMMC 2.0 Level 1 Compliance in March 2023. Not only does our solution meet or exceed more than 45 Common Criteria & 70 DoDIN APL specified security controls, it is the only full disk image backup and disaster recovery point solution available on the DoDIN APL - providing you peace of mind that your DoD or other government systems and data are protected with the absolute highest security standards.

Supported systems

On-Premises Console

- Windows Server 2022, 2019, 2016, 2012, 2012 R2, 2008/2008 R2
- Windows 11, 10, 8.1, 8, 7, Vista
- Linux x86_64 with kernel from 2.6.18 to 5.14 and glibc 2.3.4 or later

Microsoft Windows*

- Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2, 2003 R2, 2003
- Windows Small Business Server 2011, 2008, 2003 R2, 2003
- Windows MultiPoint Server 2012, 2011, 2010
- Windows Storage Server 2016, 2012, 2012 R2, 2008 R2, 2008, 2003
- Windows 11, 10, 8.1, 7, Vista
- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)

Linux*

- Linux with kernel from 2.6.9 to 4.18 and glibc 2.3.4 or later
- Various 32-bit (x86) and 64-bit (x86_64) Linux distributions including:
- Red Hat Enterprise Linux 4.x–8.2
- Ubuntu 9.10–17.1, 18.04, 18.1, 19.04, 20.04
- Oracle Linux 5.x–8.2 (including UEK)

Applications

- Microsoft Exchange Server 2022, 2019, 2016, 2013, 2010, 2007
- Microsoft SQL Server 2016, 2014, 2012, 2008 R2, 2008, 2005
- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2

Hypervisors

- VMware vSphere ESX(i) 7.0, 6.7, 6.5, 6.0, including vSphere Hypervisor (Free ESXi)**
- Microsoft Hyper-V Server 2019, 2016, 2012, 2012 R2, 2008 R2, 2008
- Microsoft Windows Server 2022, 2019, 2016, 2012, 2012 R2, 2008 R2, 2008 with Hyper-V
- Microsoft Windows 10, 8.1, 8 (x64) with Hyper-V
- Citrix XenServer® 4.1 -7.6**
- Red Hat® Virtualization 2.2–4.1
- Linux KVM
- Oracle VM Server 3.0-3.3
- Oracle VM VirtualBox 4.x

Storage

- Local disks – SATA, SCSI, IDE, RAID, ATA, SSA, NVME
- Networked storage devices – SMB, NFS, iSCSI, FC, SAS, ATA, ATAPI

File Systems

- FAT16/32 NFTS HPFS ReFS** exFAT

*** Older versions supported by our bootable media ISO. Please see user guide for full list.**
**** Some limitations may apply.**