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 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.

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

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

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

Certifications

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 140-2 (in process)
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.

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 30+ countries.

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.

FULL DISK IMAGE BACKUP AND DISASTER RECOVERY

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 battlefield and beyond by:

- Minimizing recovery times for mission critical systems following a cyberattack or failure
- Providing the flexibility to seamlessly restore standardized and unique 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 user-friendly 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 DoDIN APL certification in April 2020, with FIPS 140-2 and Common Criteria expected to finalize in 2020 as well. Our solution meets or exceeds more than 45 Common Criteria-specified security controls & more than 70 DoDIN APL-specified security controls.

Ours 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 2019, 2016, 2012, 2012 R2, 2008/2008 R2
- Windows 10, 8.1, 8, 7
- Linux x86_64 with kernel from 2.6.18 to 4.15 and glibc 2.3.4 or later

Microsoft Windows

- Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2, 2008, 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 10, 8.1, 8, 7, Vista,
- Windows XP Professional SP2 (x86, x64), SP3 (x86, x64)

Linux

- Linux with kernel from 2.6.9 to 4.15 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–7.6
  - Ubuntu 9.10–17.10, 18.04, 18.10
  - Fedora 11–29
  - SUSE Linux Enterprise Server 10–12*
  - Debian 4–9.6
  - CentOS 5.x–7.5
  - CloudLinux 7, 7.1
  - ClearOS 5.x, 6.x, 7, 7.4
  - Oracle Linux 5.x–7.5 (including UEK)

Applications

- Microsoft Exchange Server 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
- SAP HANA

Storage

- Local disks – SATA, SCSI, IDE, RAID
- Networked storage devices – SMB, NFS, iSCSI, FC
- Removable media – ZIP, Rev, RDX, etc.
- External HDDs and SSDs – USB 3.0/2.0/1.1and IEEE1394 (Firewire)

Hypervisors

- VMware vSphere ESX(i) 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 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
- Nutanix AHV from 20160925.x to 20180425.x
- Proxmox Virtual Environment 5.3-8

File Systems

- FAT16/32 NTFS HPFS
- Ext2/Ext3/Ext4 ReFS * ReiserFS3 *
- ReiserFS4 * XFS * JFS *
- Linux SWAP

*some limitations may apply