blancco

CERTIFIED DATA ERASURE

# Data Erasure Solutions for Data Center and Cloud Computing Security

Blancco White Paper
Published 23 October 2012
Second Edition

# Table of contents

# Abstract

Ongoing regulatory, consolidation, environmental and cloud computing developments mean that data centers need reliable, fast and flexible tools like certified data erasure to secure growing amounts of customer data. Data centers are complex hardware environments, with equally complex data erasure needs. Certified data erasure addresses these needs with automated data removal for a variety of scenarios, from targeted erasure of files for PCI DSS purposes to removal of data from logical units, servers, loose drives and storage arrays.

By removing all information and providing auditable proof of data removal at vulnerable hardware transition points, certified data erasure offers data centers the ability to:

- Answer demands for sustainable data center operations through equipment reuse.
- Attract customers in regulated industries like retail, healthcare and finance.
- Create a secure and cost-effective cloud computing environment with sound data removal processes.
- Develop additional revenue streams with safe remarketing of equipment.
- Maximize use of assets internally through secure reassignment of hardware.
- Respond to consolidation requirements with safe equipment transition processes.

This white paper explores major industry trends impacting data centers, with direct implications for the necessity of certified data erasure. It also describes certified data erasure solutions for a variety of mass storage hardware and configurations commonly found in data centers and cloud computing infrastructures.

# The data explosion and information security

By 2020, IDC predicts that the amount of digital information created and replicated in the world will grow to almost 40 trillion gigabytes – or more than 40 times what exists today.[1] At some point, much of this information will reside in data centers, managed either by businesses or external storage providers, especially with the growth in cloud computing environments. In 2012, Gartner predicts that worldwide data center spending for hardware – including servers, storage and networking equipment – will total $106.4 billion, and will surpass $126.2 billion by 2015.[2]

A large portion of the information residing on data center hardware is sensitive and subject to protection under a growing number of industry standards and regulations like the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley. Because of this, data center asset managers need a way to secure information at vulnerable transition points, while extending the lifecycle of enterprise storage systems.

Removing data is a critical measure to protect against data at rest inadvertently becoming data in transit. Protecting data in transit typically focuses only on data traveling across wire, not on data that travels within large data center equipment, which might be the case when a data center moves to another physical location or simply when data center hardware changes hands.

The explosion of digital information, proliferation of data centers, new regulations mandating data security and other industry trends necessitate a secure solution for removing data such as certified data erasure software. Certified data erasure software addresses requirements for tighter data center security with automated erasure processes for a variety of common mass storage hardware and configurations. It is certified to all major international erasure standards, protecting sensitive customer information while also enabling compliance with regulations. Certified data erasure is a safe, cost-effective technology that supports either the reuse of costly and complex enterprise storage systems, or their secure retirement at end of life.

*The explosion of digital information, proliferation of data centers, new regulations mandating data security and other industry trends necessitate a secure solution for removing data such as certified data erasure software.*

# Data center trends and erasure needs

With the growth of data and regulations in the last 10 years has come a variety of changes and challenges for data centers. Currently, there are several major trends impacting data centers that have direct implications for the necessity of certified data erasure, including demands for green operations, the increase in information security standards and regulations, the growth of cloud computing and consolidation of data centers.

**Green operations**

Customer demands for sustainability have fueled an ongoing emphasis on green operations at data centers. While power-saving technologies like server virtualization have resulted in less equipment for the same task and a slower growth in energy consumption, there are other important considerations for staying sustainable, such as reduction of e-waste, including computers, servers and smartphones, through effective asset management.

E-waste is a major component of data center material flow and represents the fastest growing municipal waste flow in the U.S. (and likely around the world), with reports indicating an 8.6 percent growth rate. In 2007 alone, over 41 million computers were discarded in the U.S. – with only 18 percent being properly recycled.[3] Certified data erasure allows data centers to reduce e-waste by removing all data from equipment so it can be reused or resold, without worry that data

will end up in the wrong hands. For example, due to the amount of improperly disposed e-waste it receives, Ghana is one of the top sources of cybercrime in the world according to the U.S. State Department, and suffers from dangerous air, soil, and water contamination from the discarded electronics.[4]

*Advanced data erasure software offers an automated, auditable and targeted process for removing data from files, LUNs, disks, servers and storage systems that complies with all major government and industry standards.*

**Information security standards and regulations**

The growth in high profile data breaches has prompted increased efforts to secure sensitive data, with 75 countries now having data protection laws and numerous industries defining their own regulations. Many data centers and cloud service providers seek to serve industries with highly regulated data, such as retail, banking, government and healthcare. To attract these customers, compliance with industry standards, regulations and certifications like PCI DSS, HIPAA and Sarbanes-Oxley, respectively, is critical. Cloud providers in particular will differentiate and compete based on compliance support and effectiveness, but a key aspect for data centers will be the absorption of compliance cost in the form of automated processes.

Also, comprehensive regulations requiring data removal are under review in the US with the Consumer Privacy Bill of Rights and in Europe with EU legislation on data protection reform. The Consumer Privacy Bill of Rights addresses how to enable ongoing innovation in information technologies while offering strong privacy protection, including a requirement for data deletion. The EU legislation revisits rules that have been in place since 1995 to encompass technological advances like social networking sites, cloud computing and location based services. Currently under review by all EU member states. This legislation would require deletion of online data and use of auditable procedures for companies processing personal data. It also encourages the use of certified tools and processes. Companies with cloud services must comply with this legislation if they process data belonging to EU citizens, regardless of whether their servers are located in the EU or not.

Advanced data erasure software offers an automated, auditable and targeted process for removing data from files, LUNs, disks, servers and storage systems that complies with all major government and industry standards. A key aspect of compliance is the auditable erasure report, which proves data was thoroughly removed at critical transition points, such as for hardware reassignment or resale, disaster or back-up recovery tests, and facility relocation. The report provides specific hardware details, including serial number, number of server drives, size, and speed, as well as information about the erasure process, such as how long the process took and who performed it.

**Cloud computing**

Companies looking to avoid information technology (IT) investments due to a volatile economy, combined with a generation of employees accustomed to technology on demand, have fueled ongoing growth in the global market for cloud computing (services delivered over the Internet). Gartner predicts that cloud computing revenue will jump to $148.8 billion by 2014, while Forrester sees the number jumping to $241 billion in 2020.[5]

Virtualization is a key enabling technology for cloud computing environments. Segmenting physical drives for virtual machines (VMs) is a trend that is expected to continue, as it allows for more efficient and cost-effective use of hardware. By 2014, approximately 60% of server workloads will be virtualized, according to predictions from Gartner.[6] Erasure of VMs presents a challenge for data centers, because it must be accomplished in an active, on-line environment without impacting other VMs running on a particular piece of hardware.

*Data centers need an auditable report from a certified data erasure tool to prove that data was removed from equipment slated for retirement or transfer.*

Growth in the cloud computing market will continue to drive investment in data centers. With this increase in stored information and managed applications comes the requirement for data centers to secure not just the facility, but the valuable data residing on hardware. Also, while the focus was previously on pulling data into the cloud, growing attention is now given to securing this data when it exits, as with a change in service providers. Data erasure helps cloud and managed service providers achieve improved security by erasing data when equipment is reassigned, and can target specific information for erasure on a time or event driven basis, as required by standards like PCI DSS.

**Consolidation**

Mergers, acquisitions, right sizing and a host of other initiatives have lead to the consolidation of data centers. For example, the U.S. Federal Data Center Consolidation Initiative of 2010 includes plans to close 370-plus data centers through 2012 in an effort to reduce government costs and environmental footprint.[7]

While many data centers opt for hardware refreshes when contemplating a move, Gartner recommends leveraging contracts to negotiate for early availability of "swing gear" equipment at the new site.[8] Either way, data centers need an auditable report from a certified data erasure tool to prove that data was removed from equipment slated for retirement or transfer.

# Five levels of data erasure

Data erasure technology allows data centers to secure sensitive customer information, while complying with regulations and supporting productivity and green operations. These data erasure solutions are especially critical in protecting against data leaks at transition points in the hardware's chain of custody and use. To address requirements for tighter data center security, automated data erasure processes work for a variety of common mass storage hardware and configurations.

**1. File level erasure**

Data centers with high availability requirements save multiple copies of the same data file for redundancy purposes. Because standards like PCI DSS require deletion of file-level data at specific intervals, administrators need a centralized way to remotely execute erasure of targeted or duplicate files and folders on servers and in storage areas across the network.

In Windows distributed file system (DFS) environments, data erasure must occur concurrently across redundant and mirrored systems to preserve uptime, while producing an audit trail for proof of compliance. In most cases, the erasure tool is invisible at the server node level and is managed centrally by a systems administrator.

In a virtual environment, a VM may be configured with a virtual drive that is actually a single file on a storage area network (SAN), storage device or a local drive. Under certain scenarios, it may be important to erase the VM in a live environment, without interrupting activities on the host physical device.

**Example scenarios for erasing individual files include:**

**PCI DSS compliance**

Payment card information should not be stored more than five years under PCI DSS requirements. This indicates that data centers need an erasure product that targets specific files on a time or event basis.

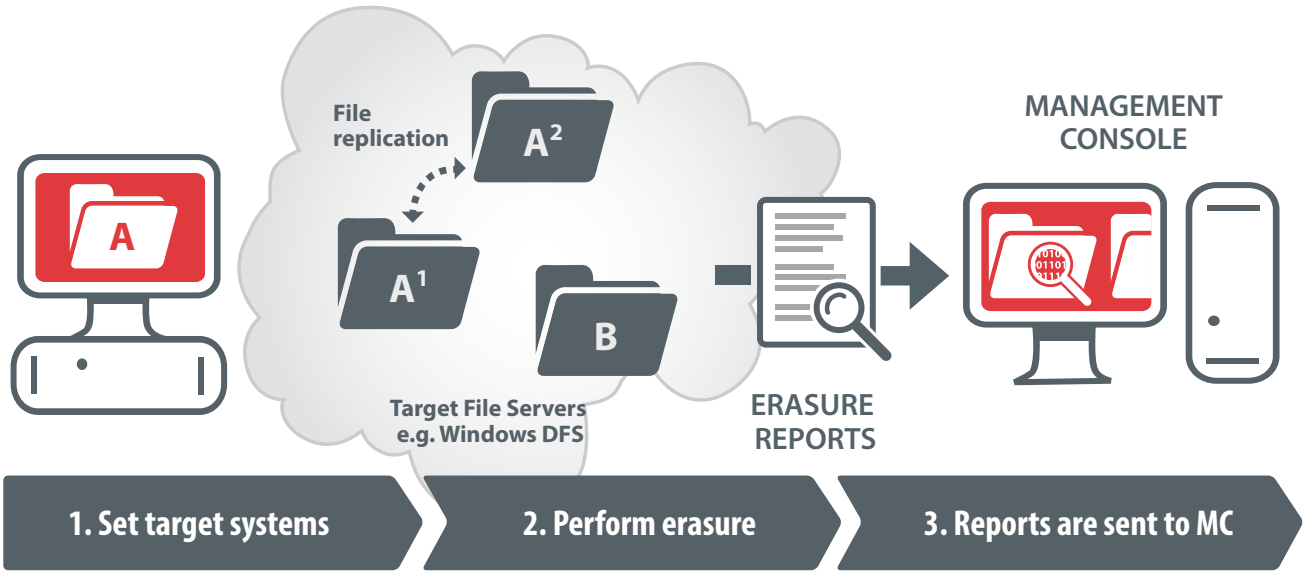


*Figure 1. File level secure erasure*

**Data housekeeping**

Erasure is part of an overall good data housekeeping practice so that too many copies of data are not stored in too many places unnecessarily, increasing the potential for data loss.

**Data spillage**

Occasionally, sensitive or confidential data gets copied to an unaccredited or unauthorized system or application. In other words, data is still in the organization's control, but was copied to the wrong place. Classified data must be erased, not just deleted from an unclassified system, for example.

**End-of-hosting for virtual drives**

Targeted erasure of a VM with a virtual drive residing on a storage system or local drive is necessary when a customer changes service providers or when the VM migrates location within a data center. This requires a tool that can accomplish the erasure without requiring a reboot of the host device. After erasure, the storage may be safely reused, without compromising the customer's data.

A professional data erasure tool destroys individual files on a time or event driven basis, or as flagged by the user or systems administrator. This tool can be set to replace all Windows delete commands with secure and targeted file shredding in real time, as Figure 1 shows. Administrators select what rules and storage areas apply from a central interface. No temporary files or "deleted" information is left behind as a source for potential data leakage. The solution can be monitored as a service for full control, and all file destruction operations are logged.

*A professional data erasure tool destroys individual files on a time or event driven basis, or as flagged by the user or systems administrator.*

In addition, data erasure software is compatible with Microsoft's Windows Server 2008 R2 file classification infrastructure (FCI), allowing the administrator to target and erase specific information, such as protected health information (PHI) or PCI DSS data, regardless of its location on the network. The tool's flexible back end also allows easy integration with internally developed file classification and management systems.

**2. LUN level erasure**

In today's cloud computing environment, data centers need secure, cost-effective options for reusing enterprise storage system configurations without rebuilding them. To safely achieve this, administrators need a centralized tool that can erase logical drives like LUNs in an active storage environment where the storage array cannot be taken offline.

This scenario encompasses VMs, which may be configured with dedicated storage of one or more LUNs in a SAN system.

An erasure tool should support compliance with a wide variety of policies, erasure standards and regulations like PCI DSS, HIPAA, and U.S. Department of Defense (DoD) standards. This includes providing auditable erasure reports to prove LUN erasure, while also offering ease of use and expedited data removal. LUN erasure is run from the application server, which has a view of the targeted LUN and supports simultaneous erasure of multiple units.

Secure erasure of LUNs can be critical to managed hosting and cloud computing providers with customers that do business with the U.S. Government, for example. Proof that all customer data has been

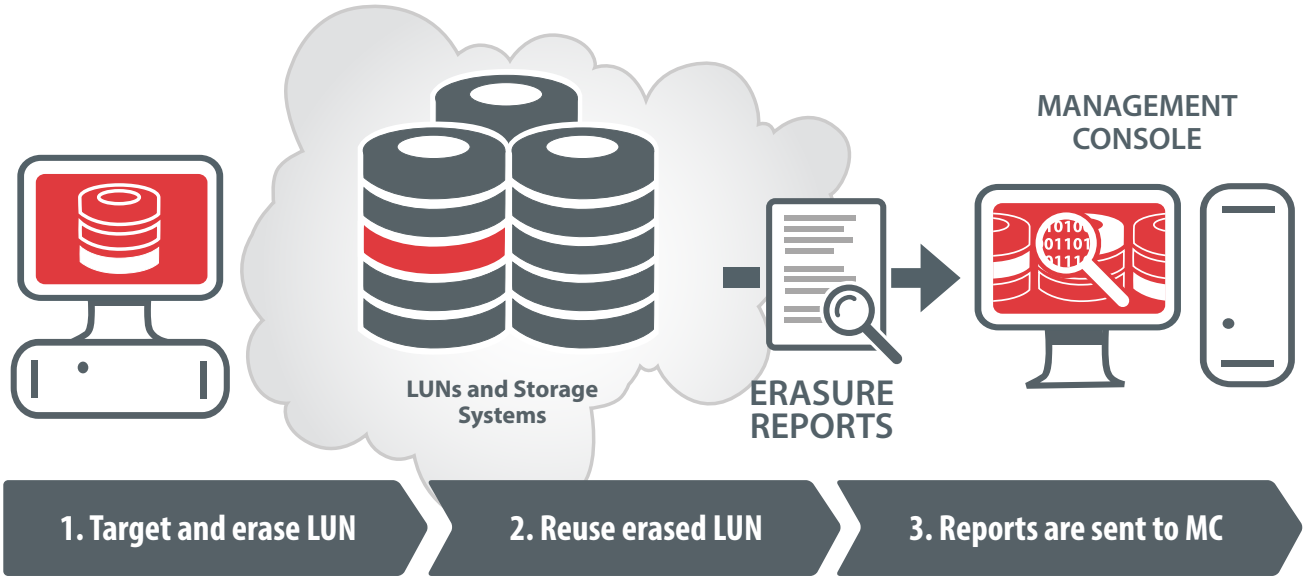


*Figure 2. LUN level erasure with live data.*

deleted to DoD standards is required if a customer changes service providers or changes platforms with the same service provider. Without a LUN eraser, which is compliant with DoD or other required standards, the service provider may have to take drastic steps to eliminate old customer data, such as taking an entire storage array offline to erase physical drives or quarantining old LUNs with customer data, which drives storage costs higher. With a LUN Eraser, that same service provider can now erase, to a DoD standard, an existing LUN – without affecting other users of the storage array in any way.

*Without a LUN eraser, which is compliant with DoD or other required standards, the service provider may have to take drastic steps to eliminate old customer data.*

**Example scenarios for LUN erasure include:**

**End-of-hosting subscription**

Erasure is necessary for LUN reuse in a hosted environment when a current customer leaves and a new user is assigned to an existing LUN. This scenario occurs for both physical servers using LUNs as storage and for VMs with dedicated storage on a particular LUN.

**Disaster recovery test**

After a disaster recovery test, multiple copies of LUN data exist and must be erased for security reasons.

**Back-up recovery test**

As with a disaster recovery test, a backup tape recovery test will easily produce terabytes of data on multiple copies of LUNs and servers, which should be erased for security reasons before the next client uses the same hardware.

Data erasure offers LUN versions that support simultaneous data destruction on 200+ units by starting parallel instances of the software, which can be started from a central administrative interface, as shown in Figure 2. The software can erase any unit (physical or logical) that a Windows, Unix, or Linux system can detect by overwriting the entire writeable area, sector by sector, on the logical disk or drive according to the erasure standard selected. Erasure reports are then available to support compliance needs.

**3. Disk level erasure**

Disk level erasure is necessary for sanitizing hard disks outside the original host, as with loose drives from storage area network (SAN) servers. Many of these are return material authorization (RMA) drives that need

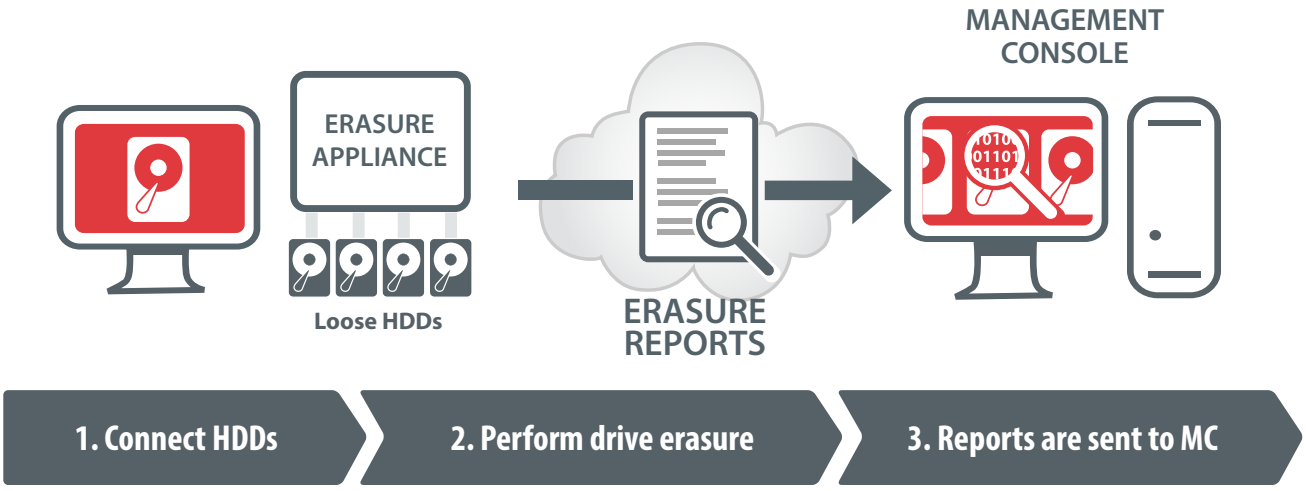


*Figure 3. Erasure of loose drives.*

erasure before returning to the original equipment manufacturer (OEM) under warranty.

Because of handling requirements and chain of custody concerns, local erasure of disks is necessary. Similar to full array erasure, erasing loose drives requires an external host/boot device and the correct connectivity between the drives to be erased and the erasure host device in question. Once erasure is in progress, an erasure tool should support monitoring and final erasure reporting across the network, when network connectivity can be leveraged.

**Example scenarios for erasing individual disks include:**

**Replacing RMA warranty drives**

On-site erasure of "failed" disks removes the disk content so that that the drive can be transported risk free to the OEM for warranty replacement, avoiding costly disk retention fees.

*Data erasure provides a tailored data erasure solution for the server environment that guarantees high-speed, simultaneous erasure of all connected hard disk drives (HDDs).*

**Drive backlog**

If secure end-of-life erasure processes were not used in the past, a data center may own a backlog of drives with sensitive data that need erasure to avoid risk of data loss.

**Drive swap for end-of-service servers**

Swapping and using loose drives as replacements is a common and fast process that expedites retirement of a server using pre-sanitized drives, but it generates loose drives with unsecured data intact.

Certified data erasure provides a tailored data erasure solution for the server environment that guarantees high-speed, simultaneous erasure of all connected hard disk drives (HDDs). It is run from an appliance for erasure at the disk level, as Figure 3 shows, to remove data from RMA drives as specified by the administrator, who can choose from a range of internationally supported erasure standards. RMA drives from servers or disk arrays are simply removed from their enclosure and attached to the erasure appliance, which is booted with data erasure software that recognizes drives intended for erasure.

With certified data erasure, SCSI, SAS, SATA, FC and even IDE drives may be erased simultaneously. When the erasure process is complete, taking one

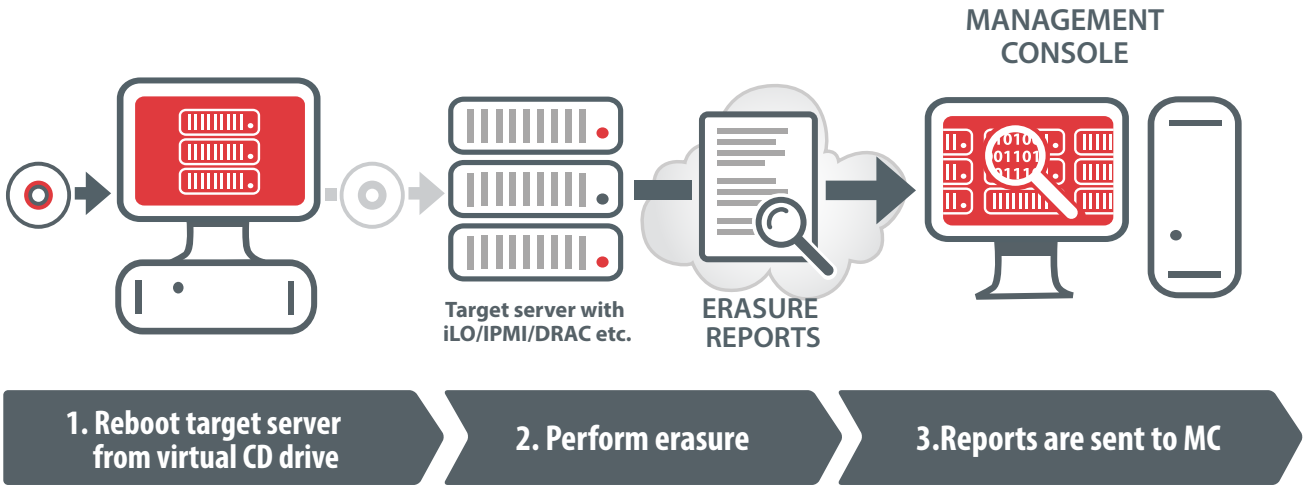


*Figure 4. Remote server erasure.*

gigabyte per minute on average, an erasure report is automatically generated and sent over the network to a management console or asset management database. The console validates the erasure report as genuine, verifies erasure is complete, and functions as a repository for erasure reports. Certified data erasure also supports erasure of the increasingly common solid state drives (SSDs) via an option to select flash based storage media standards.

**4. Server level erasure**

Full server erasure involves erasing all internal connected drives. Server level erasure can be performed either locally or remotely. For example, remote erasure is easily implemented with a virtual CD drive for servers with iLO/IPMI/DRAC capabilities. Auditable reports regarding hardware attributes and the data erasure process are necessary for customer security and requirements for PCI DSS and other regulations.

For complete security, data centers need erasure tools that detect protected areas of the disk and remapped sectors during the erasure process, flagging those that cannot be erased. Depending on policy and risk tolerance, data centers may refurbish or resell servers after data erasure has been performed. Either way, data erasure must occur before a server leaves the premises.

**Example scenarios for erasing entire servers include:**

**End-of-service**

At the end of a hardware refresh cycle, data centers must securely erase all information on servers to comply with regulations and protect customers. This allows resale and recycling of healthy disks, while creating a green data center environment and profit streams.

**End-of-hosting subscription**

Erasure is necessary for server reuse in a hosted environment when an existing customer terminates hosting services.

**Data center relocation**

Data centers frequently move or expand, requiring relocation of servers that, if not securely erased, could result in data loss during transport.

*For complete security, data centers need erasure tools that detect protected areas of the disk and remapped sectors during the erasure process, flagging those that cannot be erased.*

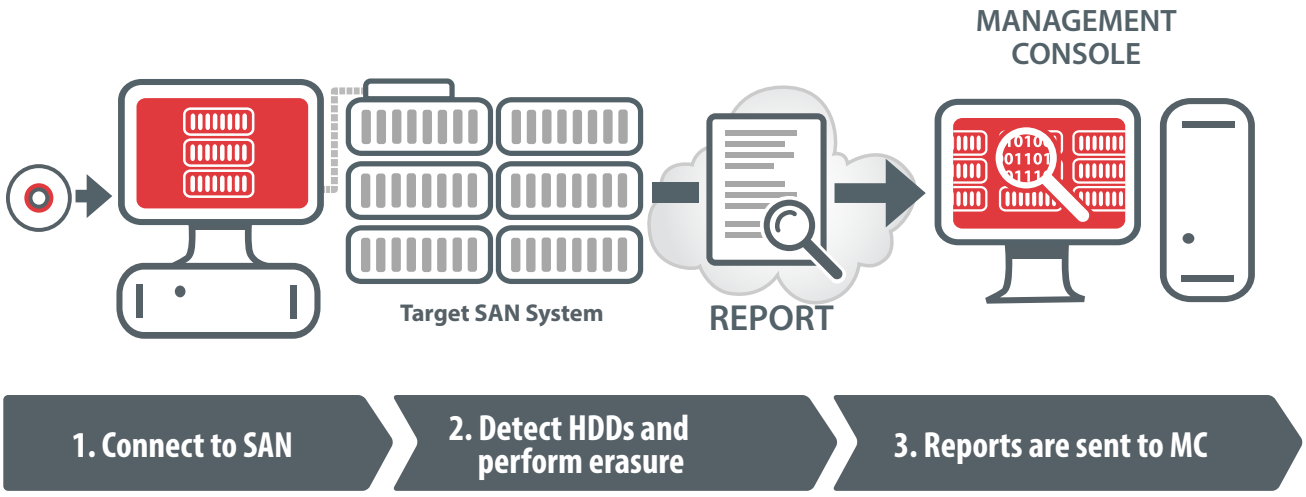


*Figure 5. Full array erasure.*

As with disk level erasure, certified data erasure is available for servers. As in Figure 4, the administrator boots the erasure software from a CD, USB, or through the network. The software then identifies the installed drives for erasure, performs the erasure, and sends the report to a management console, database, or USB memory stick.

X86 and x64 servers are erased with certified data erasure software. Also, certified data erasure can removed data from both RAID and non-RAID servers. For servers with an integrated RAID controller, the erasure software "breaks" the RAID and directly erases all internal hard drives to an erasure standard chosen by the administrator. As SPARC servers are typically used by data centers to support mass data needs for organizations like financial institutions, a version of certified data erasure software also works with the SPARC architecture from companies like ORACLE.

**5. Storage level erasure**

Data centers work with a broad range of complex storage configurations that can yield revenue upon retirement. SAN disks and other mass storage devices can be sold if data is securely removed as they are decommissioned.

To eliminate the need for multiple erasure products, data centers with high-end server and SAN environments need a tool that erases a broad range of hardware, such as Serial ATA, SAS, SCSI and Fiber Channel disks. Because of the scale of data centers, simultaneous erasure of multiple disks is a necessity.

**Example scenarios for erasing storage systems include:**

**End-of-lease**

At the end of a hardware refresh cycle, data must be erased before transporting storage systems back to the leasing company. Keeping the drives is cost prohibitive, as is physical destruction, because of heavy lease settlement fees if equipment is retained.

**Competitive hardware refresh**

At the end of a hardware refresh cycle, data centers must securely erase storage arrays to allow resale and recycling of healthy disks, while creating a green data center environment. The data center – not the OEM – owns the data and is responsible for its erasure to prevent data leaks.

**Data center relocation**

Data centers frequently move or expand, requiring relocation of storage systems that, if not securely erased, could result in data loss or breach during transport.

A data center version of certified data erasure software offers 100% secure data destruction for high-end storage arrays. The software runs on an externally attached x86 server that is not directly attached to SAN host ports, but instead attaches to the storage device access enclosure (DAE). Certain storage arrays enable direct access to multiple DAEs simultaneously via integrated loop switches, which are the preferred method of accessing drives for erasure because many additional drives may be erased concurrently. The externally attached boot server must be configured with the correct host bus adapter, as in SCSI or Fiber Channel, and the correct cable is required for optimal performance.

Once connected, an administrator launches the data erasure software from the external boot server. Capable of simultaneously detecting and erasing 250+ HDDs within the same array, the software can quickly remove data on ATA, SATA, SCSI, Fiber Channel and SAS hard drives. This version also provides remapped sector erasure for ATA/SATA/SCSI/Fiber Channel hard drives, and provides detailed hardware asset reports with hard drive health status indicators.

*To eliminate the need for multiple erasure products, data centers with high-end server and SAN environments need a tool that erases a broad range of hardware.*

## Certified data erasure for complex requirements

As the cloud computing market develops and data centers evolve to meet growing storage requirements, certified data erasure software is emerging as a practical, automated and auditable solution for efficient and secure operations. The software supports erasure of hardware and storage configurations throughout the data center, as well as targeted erasure of folders, files and logical units. To ensure minimal disruption and complete data security in the dynamic data center environment, administrators, users and customers can trust certified data erasure as a tool for now and for future requirements.

# References


[1] IDC Digital Universe Study, sponsored by EMC, December 2012

[2] Gartner, "Forecast: Data Centers, Worldwide, 2010-2015," October 2011

[3] Emerson Network Power, "Recycling Ratios: The Next Step for Data Center Sustainability"

[4] Newsweek, "Digital Dump," July 2011

[5] Wall Street Journal, "More Predictions on the Huge Growth of Cloud Computing," April 2011

[6] Cloud Computing, "5 Cloud Computing Statistics You May Find Surprising," http://cloudcomputingtopics.com/2011/11/5-cloud-computing-statistics-you-may-find-surprising/, November 2011

[7] Federal Data Center Consolidation Initiative (FDCCI) Data Center Closings 2010-2012, http://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37

[8] Gartner, "Data Center Consolidation: Top 10 Best Practices for Project Success," Research Note, May 2011



Portions of this white paper originally appeared in *ITAK* magazine, Vol. 6, Issue 8, published by the International Association of Information Technology Asset Managers.


---

*For further information, please visit*

www.blancco.com

blancco

**Blancco U.S.**
3901 Roswell Road, Suite 302
Marietta, GA 30062, UNITED STATES
sales-atl@blancco.com
Tel. (770) 971 9770
Fax. (770) 485 7530
www.blancco.com