blancco
technology group

WHITE PAPER

Cloud & Data Center Erasure: Why Delete Doesn't Suffice

Data Deletion Doesn't Suffice

There are many cases when your organization must delete sensitive data from corporate servers or other IT infrastructure. But is the deleted data truly gone, or can it still be accessed by cyber attackers? It isn't gone forever. That's where certified data erasure becomes a vital asset for your business – it safeguards the integrity of your most sensitive, confidential data and prevents it from falling into the wrong hands.

After Sony lost 100 terabytes of data to a cyber attack in November 2014, the company was widely criticized for lax records management. The most damaging files included tens of thousands of emails between studio executives that exposed the inner workings of Sony Pictures and led to serious backlash among the public and the media. Had emails regularly been deleted from corporate servers, it's safe to say that the film studio would not have born the brunt of such negative publicity and a severely damaged corporate reputation.

Or would it? Typical file-deletion commands don't truly delete data; they simply remove pointers to the disk sectors where the data resides. Such "deleted" data can easily be recovered with common software tools. So while most CIOs and IT professionals are aware of the security dangers that lie ahead, they're still not always taking the right precautionary measures.

Vast amounts of sensitive data are stored in both data center and cloud environments, including employee records, customer information, intellectual property, just to name a few. So it's not a question of *if* a data breach will occur; it's a matter of *when*. This is quite apparent when you look at the number of retailers, healthcare providers, financial institutions and even government agencies that have fallen prey, including eBay, Target, Home Depot, Texas Health and Human Services. And let's not forget the latest breach of 800 million social security numbers from the U.S. government's Office of Personnel Management (OPM). Across jurisdictions, state lines and country borders, regulators are increasing both oversight and penalties for security breaches. And customers—from consumers to businesses to government agencies—are paying closer attention to how organizations manage data.

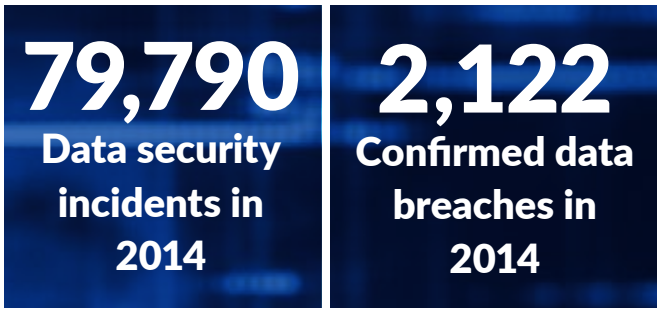
As you can see, mere data deletion is no longer enough. What's needed is certified data erasure, achieved through enterprise-class software that can truly erase, and verify the erasure of, sensitive information. Certified data erasure meets the growing requirements for strong enterprise security—whether your organization operates its own data center, stores its data in a public cloud, or provides cloud-based data storage to other firms.

But effective data erasure management (DEM) requires a well-planned, automated approach – one that leverages trusted DEM software, fits into an overall IT security strategy and helps protect your data *and* your brand. Here's how.

Racing Toward Erasure

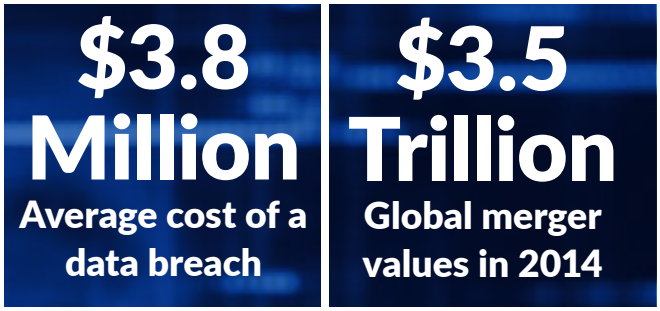
Many organizations have long been aware of the need for data erasure in certain situations. But some have overlooked Data Erasure Management – or DEM, as we call it – as an integral component of their overall IT infrastructure and data security policy. That's beginning to change, thanks to several converging trends that we outline below.

Cyber Attacks: It doesn't matter what you do or where you look, data breaches are on the rise. In fact, there were 79,790 documented data security incidents and 2,122 confirmed data breaches in 2014, according to Verizon. What's more frightening is that those attacks are increasingly carried out by sophisticated players, with the North Korean government allegedly behind the Sony breach and the Chinese government blamed for stealing records of 4 million U.S. taxpayers from the U.S. Internal Revenue Service (IRS) in the spring of 2015.



Source: Verizon

At the same time, the financial burden of stolen data is rising. As Ponemon Institute reports, the average cost of a data breach was $3.8 million in 2014, or about $150 per record – that's up 23 percent from 2013. The root causes of that lost data come down to human error (25 percent), system glitches (29 percent) and criminal attacks (47 percent).



Source: Ponemon Institute

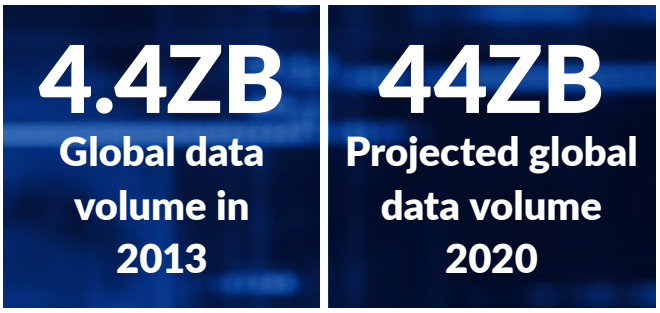
Regulations: In the face of data breaches, governments are ratcheting up regulations. At least 75 countries have data protection laws, as do U.S. states such as California and Massachusetts. Companies must now comply with both general and industry-specific regulations and guidelines, from Sarbanes-Oxley Information Security Standards and Health Insurance Portability and Accountability Act (HIPAA) to Payment Card Industry Data Security Standard (PCI DSS).

And now even more are on the way. The Obama Administration's Consumer Privacy Bill of Rights, proposed in 2015, would require industries to establish codes of conduct around data and create privacy boards overseen by the U.S. Federal Trade Commission (FTC). Also in 2015, the European Union (EU) expects to complete an overhaul of its 1995 Data Protection Directive. The new regulation will strengthen citizen rights such as the so-called "right to be forgotten," or erased from data records. More importantly, the rules would apply to companies with cloud services that process EU citizen data even if the servers were located outside the EU.

Other relevant guidelines include ISO/IEC 27001 and ISO/IEC 27040, which have been issued by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). These standards set out rules for how data is protected, including the overwriting of storage media prior to reuse or disposal. They can also underlie rules and accreditations for companies that want to participate in government procurement exchanges such as G-Cloud. Similar rules are in place for U.S. agencies that want to leverage cloud environments through the FedRAMP program.

Corporate Consolidation: Corporate acquisitions, divestitures and right sizing are also driving interest in data erasure. Global merger values topped $3.5 trillion in 2014, up 47 percent over 2013, according to Thompson Reuters. When companies merge, so do data centers. When this happens, it increases the need for auditable evidence that data is protected or erased when physical and virtual IT resources are moved or retired.

Data Growth: One the most significant factors driving the need for data erasure is simply the unprecedented explosion of data stores. The global volume of data will mushroom from 4.4 zettabytes (ZB) in 2013 to a staggering 44 ZB—that is, 44 trillion gigabytes—in 2020, predicts IDC. No small amount of that data resides in corporate clouds and data centers.



Source: IDC

Virtualization: Data growth and other factors are driving organizations to cloud and virtualization. More than three-quarters of server workloads will be processed in the cloud by 2018, according to Cisco. While overall data center workloads will nearly double from 2013 to 2018, cloud workloads will nearly triple in comparison. Reflecting a greater degree of virtualization, workloads per physical server in clouds will grow from 5.2 to 7.5.

As virtual machines (VMs) are migrated and retired, all associated data must be erased from the physical server or storage that hosted them. And while VMs require the same level of security as physical servers, their erasure presents unique challenges. For this reason, VM erasure must be accomplished in an active environment, without affecting other VMs running on the same hardware.

Now You See It, Now You Don't

While Data Erasure Management (DEM) is new to many organizations, it's really a common part of the overall life cycle of a data file: create, store, use, edit and erase. No enterprise business should create a data record without also considering how it will erase it. That applies to every place data is created and stored in the organization – be it on physical servers, virtual servers, physical disks, logical drives, and everything that accesses and stores that data, including PCs, laptops, tablets and smartphones.

Data erasure is necessary regardless of your IT infrastructure. That's true whether any of the following circumstances apply to your organization.

- Operate your own on-premise data center
- Outsource to an IT provider that handles your data center for you
- Outsource your physical equipment to a co-location provider
- Store your data offsite in a public cloud
- Manage a hybrid cloud, with some resources onsite and others external
- Maintain any combination of physical and virtual environment

There are five key situations where data erasure is necessary in both clouds and data centers. Here we outline each of them.

At Equipment End-of-Life: When a server, storage device or other IT asset is retired, it's either resold or discarded. In either case, any data it contains must be erased so that it doesn't fall into the wrong hands.

During Data Migration: Whenever data is moved from one location to another—from a retired server to a new server, from one virtual machine to another—the original data location must be erased.

At Data End-of-Life: Many organizations manage virtual machines that are used by a line of business for a particular project that covers a specific period of time. When the project is complete, the data should be not just deleted. Instead, it should be completely erased.

Cloud Providers and Data Erasure as a Service (DEaaS)

Organizations often turn over their IT environments to cloud providers and expect their cloud-based data to remain protected. But they need to feel confident not only that their active data is secure, but also that all of the retired data is fully erased from virtual environments.

To that end, don't be surprised if cloud providers begin to expand on their software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS) offerings with a new service: data erasure as a service (DEaaS).

For cloud providers using popular solutions such as VMware ESXi, vCenter Server or Microsoft Hyper-V, with the right data erasure management (DEM) software, when cloud customers delete a virtual machine (VM) or vApp, it's securely erased at the host level. For cloud providers grouping specific VMs into data stores, effective DEM software can erase the entire data store just as it would a logical unit number.

When Customers Demand It: In jurisdictions such as the EU, "right-to-be-forgotten" rules dictate that if consumers ask you to remove their data from your servers, you must comply. It's not enough to simply delete the record. Instead, it must be completely expunged without any possibility of coming back to haunt them. An audit trail with a certified report must exist to prove that the erasure occurred.

After Disaster Recovery: During major disasters, data is typically recovered at an offsite location. The same is true during disaster-recovery exercises, where real customer data is typically used in the test. Because of this, it's critical to erase the data from the secondary site. In either case, once production systems are restored, any data left on recovery disks should be erased.

Many organizations mistakenly believe that data erasure isn't necessary at these transition points because if data is

encrypted, it's protected. But while encryption can be effective at protecting data, encryption keys can still be stolen, allowing encrypted data to be exposed. Always remember that 'inside jobs' are a very real possibility. Data breaches can take weeks or months to discover. For payment card skimmers, 36 percent of breaches take days to find, while 18 percent take weeks and 9 percent take months, according to Verizon. This reiterates an important fact – the longer a breach goes undetected, the more encrypted data is at risk.

DEM, then, should be an integral part of a comprehensive, absolute line of defense approach to data security. With this approach, each security measure—be it firewall, antivirus, data encryption or data erasure —offers an added layer of protection. If an attack gets through your firewall, your antivirus software may catch it. If a malware payload evades your antivirus, encryption may prevent data exposure. But if you've employed effective data erasure to completely remove unneeded data, there's simply no data there for attackers to steal.

Finding the Right Data Erasure Management Solution

Just as deleting a file isn't the same as erasing it, not all data erasure management (DEM) software is created equal. An effective DEM solution should offer the following features and benefits.

Compliance: Your DEM solution should be certified to meet all major international government and industry standards for data erasure, both protecting sensitive data and ensuring regulatory compliance.

Reporting: Your solution should issue an auditable and digitally signed erasure report proving that data was thoroughly removed at critical transition points. The report should provide specific hardware details, such as serial numbers, virtual machine names, LUN IDs, as well as who performed the actual erasure process and how long it took.

Versatility: A good DEM solution should provide a targeted and auditable process for removing data from files, disks, logical unit numbers, servers, virtual machines and storage systems.

Automation: Finally, your chosen solution should provide a level of erasure automation that's right for your organization's needs. If an internal employee doing self-provisioning fails to erase a virtual machine or LUN, your data is vulnerable. If a busy IT administrator fails to erase a server correctly, your data is at risk. The more you automate, the more you can be sure erasure is truly protecting your information assets.

Disk Erasure

Disk erasure is necessary for sanitizing disks outside the host, as with loose drives from storage area networks (SANs). Because of chain-of-custody concerns, local erasure of disks is necessary. Erasing loose drives requires an external host/boot device and connectivity between the drives and the host. Scenarios include:

Return Material Authorization (RMA) Warranty Drives: Erasure of failed disks removes the content so the drive can be transported to the OEM for warranty replacement. The data center, not the OEM, is responsible for the data's erasure.

Drive Backlog: If end-of-life erasure hasn't been used before, your data center may have a backlog of drives that need erasure.

Drive Swap for End-of-Service Servers: Swapping loose drives is a common process that expedites retirement of a server using pre-sanitized drives. But it results in loose drives with intact data.

Effective data erasure software should allow high-speed, simultaneous erasure of all connected drives. It can be run from an erasure appliance at the disk level to remove data from RMA drives as specified by the administrator, who can choose from a range of erasure standards. (See Figure 1.)

The process should take about one minute per gigabyte to simultaneously erase SCSI, SAS, STAT, Fibre Channel (FC)

and IDE/ATA drives. It should optionally include solid state drives. The erasure software automatically sends an erasure report to a management console or asset management database. The console then validates the report, verifies erasure and stores the report.

Server Erasure

Server erasure involves erasing all internal connected drives. You can perform it locally or remotely. Your erasure solution should issue auditable reports on hardware attributes and data erasure. It should also detect protected areas of the desk and remapped sectors, flagging those that can't be erased. And it should handle a broad range of hardware such as serial ATA, SAS, SCSI and FC disks. Scenarios include:

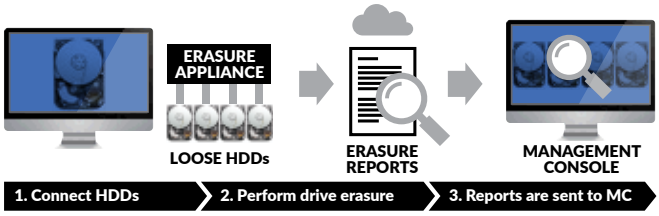


Figure 1. Erasure of loose drives.

End of Service: At the end of a hardware refresh, data centers must securely erase all information on servers and storage arrays to protect data and comply with regulations. This enables recycling or resale of healthy disks, promoting both "green" operations 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.

End of lease: At the end of a hardware refresh, data must be erased before transporting storage systems back to the leasing company.

In server erasure, the administrator boots the erasure software from a CD or USB, or over the network. (See Figure 2.) The software identifies the drives, performs the erasure and sends a report to a management console, database or memory stick.

Your chosen erasure solution should be capable of erasing x86 and x64 servers, as well as RAID and non-RAID servers. For servers with an integrated RAID controller, the software should "break" the RAID and erase all internal drives to the erasure standard chosen by the administrator. It should also work with the SPARC architecture.

File Erasure

Many data centers save multiple copies of the same data for redundancy purposes. Because standards like PCI DSS require deletion of file-level data at specific intervals, you need a centralized way to erase targeted or duplicate files across the network. In Windows Distributed File System (DFS) environments, data erasure must occur concurrently across redundant and mirrored systems to preserve uptime. In most cases, the erasure tool should be invisible at the server-node level. File-erasure scenarios include:

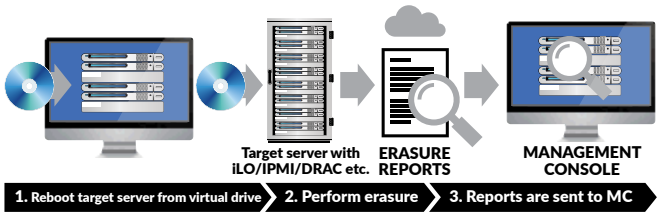


Figure 2. Remote server erasure.

PCI DSS Compliance: Payment card information shouldn't be stored more than five years under PCI DSS. In this case, you need an erasure solution that targets specific files on a time or event basis.

Data Housekeeping: File erasure is part of overall data maintenance, ensuring that redundant data isn't stored unnecessarily, which can increase IT costs and the potential for data theft.

Data Spillage: Sensitive data can be inadvertently copied to an unauthorized system or application. That data should not just be deleted, but thoroughly erased.

An effective data erasure solution can destroy files on a time or event basis, or as flagged by an administrator. (See Figure 3.) The administrator selects which rules and storage areas to apply from a central interface. The tool should allow monitoring as a service for full control, and it should log all erasure activities. It should also be able to replace all

Windows or UNIX delete commands. And it should be compatible with Microsoft's Windows Server File Classification Infrastructure (FCI) and other document management systems, allowing the administrator to erase specific files regardless of their location on the network.

LUN Erasure

Data centers must be able to securely reuse virtual storage system configurations without rebuilding them. To achieve this, you need a centralized tool that can erase logical drives such as logical unit numbers (LUNs) in an active environment where the storage array can't be taken offline. Because LUN erasure occurs in a live environment, there is no downtime necessary. How, you might ask? While one LUN is erasing, the rest of the system is operational and live. As a result, the erasures do not disturb data center productivity.

LUN erasure is run from the operating system from where the LUNs are configured or from an externally connected server, which has a view of the targeted LUN and can simultaneously erase multiple units. LUN erasure can be crucial for companies doing business with government agencies such as the U.S. Department of Defense. Lacking the ability to erase LUNs, you may have to take an entire storage array offline to erase physical drives. Scenarios for LUN erasure include:

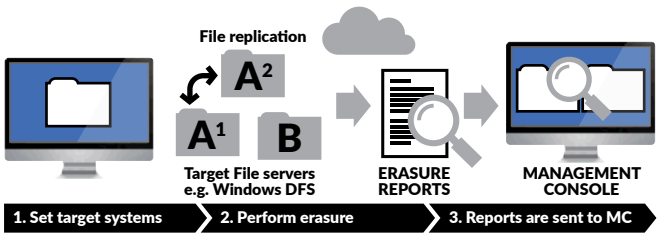


Figure 3. File level secure erasure.

End of Hosting, Deletion or Migration of LUNs: Erasure is necessary for LUN reuse in a hosted environment when a user migrates to a larger LUN or leaves the cloud, so that the LUN can be safely reassigned to a new user. This is true for both physical servers using LUNs as storage and for VMs with dedicated storage on a particular LUN.

Disaster-Recovery Tests: After a disaster recovery test, duplicate copies of LUN data must be erased.

Your data erasure solution should support simultaneous destruction of multiple LUNs by starting parallel instances of the software from a central interface. (See Figure 4.) The software should erase any physical or logical unit that a Windows, UNIX or Linux system can detect by overwriting the entire writeable area, sector by sector, on the logical disk or drive.

Virtual-Environment Erasure

As big data multiplies and migrates, it calls for data erasure in virtualization environments such as VMware vSphere, Citrix XenServer and Microsoft Hyper-V. Your data erasure solution should overwrite data without affecting data center operations or business activities. It should also be able to erase VMs in a live environment without interrupting other VMs or activities on the physical host. (See Figure 5.) Scenarios include:

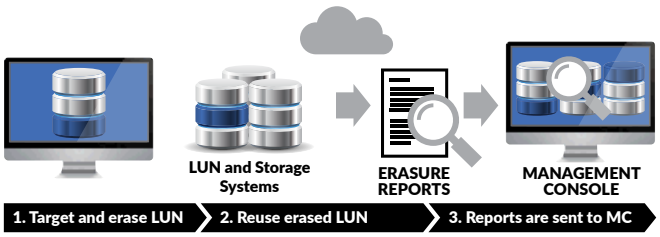


Figure 4. LUN level erasure with live data.

Integration with VMware vCenter Server: VMware vCenter Server is the standard tool for managing both physical host servers and VMs in a VMware-powered data center. Your erasure solution should integrate with vCenter so that the administrator can simply right-click a virtual machine to erase it from the data store.

End of Hosting, Deletion or Migration of VMs on VMware ESXi Platforms: Targeted erasure of a VM is necessary when the VM is deleted or changes location in the data center. You should be able to achieve this without rebooting the host. By installing the erasure solution at the VMware ESXi level, you can manually erase VMs in VMware vSphere. All files associated with the targeted VMs should be erased, including VMDK, VMSD, VMX and VMXF.

End-of-Hosting, Deletion or Migration of VMs on VMware vCloud Director: VMs accessed through VMware vCloud Director are often deleted or migrated within the

data center. Seamless integration and access through the vCloud Director user interface lets you use the "delete" command to destroy all data on VMs or vApps in active systems.

Erasure from an In-House, Developed Portal: Users running VMware ESXi hosts often deploy VMs with an in-house-developed portal instead of vCloud Director. In this situation, data erasure software can be installed on the ESXi hosts and executed from the in-house-developed portal.

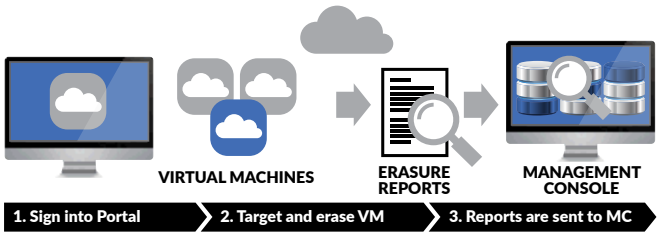


Figure 5. Erasure in virtual environments.

Final Thoughts

The advantages of data erasure management are self-evident. For one, effective data erasure lets you better manage proliferating virtual and cloud environments, ensure compliance with multiplying government regulations, better protect customer information and intellectual property, and mitigate the potential cost and legal risk of data exposure.

Additionally, the organizations benefitting from data erasure are wide-ranging. A global wireless distributor turned to data erasure to ensure effective retirement of VMs. A major U.S. telecom provider deployed an erasure solution to retain business-critical contracts with the federal government. And a leading European data center provider leverages data erasure as a competitive differentiator to win new customers. Meanwhile, a major U.S. IT provider took advantage of data erasure to secure IT infrastructure for an aerospace leader.

All these organizations have embraced what a growing number of market leaders are discovering: that changing outlooks for cyber-security, IT infrastructure management, government regulations and customer expectations place a new onus on protecting corporate data. And data-erasure management is an integral part of data security—protecting your information assets, safeguarding your brand and positioning your organization for business success.