blancco
technology group

WHITE PAPER

Enterprise Data Erasure: Your Last Line of Defense

Your organization invests significant resources in data security. But are you overlooking data erasure? Here's why you need it and how to implement this final fortification in your data security defenses.

How much does your organization spend on data security? If you're like most mid-size and large enterprises, the answer is likely a hefty sum, and growing.

Worldwide spending on information security is set to exceed $77 billion in 2015, an annual jump of 8 percent, according to Gartner.[1] The area clocking the fastest growth is data loss prevention, at 19 percent. In fact, two-thirds of U.S. tech CFOs—people who don't shell out dollars unless they have to—increased spending on cyber security in 2014, reports accountancy network BDO.[2]

Yet with all that budget going to data safeguards, many organizations overlook a simple, effective and cost-efficient measure in safeguarding information: data erasure. Across your enterprise – from data center to mobile devices – all assets require thorough and verifiable data erasure through their entire life cycle. This includes everything from daily file-level erasure all the way to full decommissioning at the end-of-life. Here's why you need data erasure and how to leverage it to strengthen your overall information security posture.

Trending Threats

Smart organizations have long been aware of the need for data erasure in certain situations. But many have overlooked it as an integral element of overall information security. That's beginning to change, thanks to several converging trends.

Cyber Attacks: Data theft is on the rise, as news headlines testify. There were 79,790 documented data security incidents and 2,122 confirmed data breaches in 2014, according to Verizon.[3] Those attacks are increasingly carried out by sophisticated, well-financed players such as organized crime groups and rogue governments.

At the same time, the financial burden of stolen data is rising. The average cost to companies for a data breach was $3.8 million in 2014, or about $150 per record, which is up 23 percent from 2013, Ponemon reports. The root causes of lost data come down to human error (25 percent), system glitches (29 percent) and criminal attacks (47 percent).[4]

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

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). On December 15, 2015, the European Commission, the European Parliament and the European Council reached an agreement on the General Data Protection Regulation (GDPR). The new regulation would strengthen citizen rights such as the so-called "right to be forgotten," or erased from data records. The rules would apply to companies with cloud services that process EU citizen data even if the servers were located outside the EU.

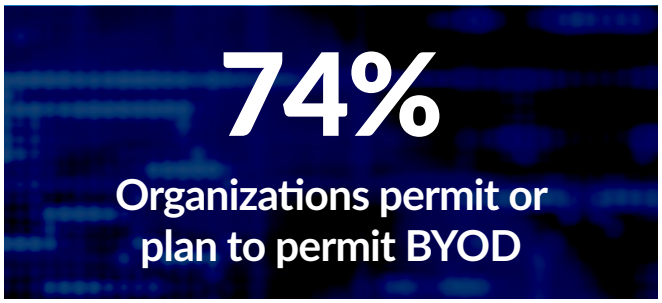
1 "Forecast: Information Security Worldwide, 2012-2018, 2Q14 Update," Gartner, August 2014
2 "Tech CFOs Counter Cyber-Security Threats," BDO USA, March 2015
3 "2015 Data Breach Investigations Report," Verizon, May 2015
4 "2015 Cost of Data Breach Study," Ponemon, May 2015

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.[5] No small amount of that data resides in data centers, corporate clouds and mobile devices used for work.

More Mobile Devices: Smartphone and tablet use in the workplace has exploded. A growing proportion of that equipment is BYOD. Some 1.6 billion BYOD devices were projected to be in use by 2014, according to Gartner.[6] Today 74 percent of organizations permit or plan to permit BYOD, says Tech Pro Research.[7] By 2018, employee-owned devices will outnumber company- issued devices by two to one, Gartner reports.[8] All those smartphones and tablets have rapid life cycles and all will require data erasure at their end-of-life.

Virtualization: Data growth and other factors are driving organizations to cloud and virtualization. More than three quarters of server workloads will be processed in clouds by 2018, according to Cisco. While overall data center workloads will nearly double from 2013 to 2018, cloud workloads will nearly triple. Reflecting a greater degree of virtualization, workloads per physical server in clouds will grow from 5.2 to 7.5.[9]

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



When Delete Falls Short

Many organizations mistakenly assume they can prevent data loss at end-of-equipment-life by simply deleting the data. But typical file deletion commands don't truly erase data; they simply remove pointers to the disk sectors where the data resides. Such "deleted" data can easily be recovered with common software tools. And while most CIOs and IT pros are aware of this fact, many organizations are just waking up to the security implications.

Other approaches exist, including physical destruction of devices, degaussing, encryption, re-formatting, simple overwriting and factory resets. But each has its drawbacks.

Destruction and Degaussing: Physical destruction and degaussing render disk drives inoperable, precluding the opportunity to recover value through reuse or resale of devices. It's also possible to recover data from shards of destroyed media. And because costly equipment is required to destroy devices, the activity typically is outsourced, thus increasing the chance of data loss during equipment transportation.

Encryption: Encryption of inactive equipment is a time consuming, processor intensive operation that doesn't provide a completely safe or verifiable method of data security. Cryptographic erasure at end-of-life includes no verification mechanism or audit trial. And both active and inactive systems that use encryption are subject to attack if not continually updated. Malware penetrations can remain hidden for months, during which they can exploit implementation weaknesses, steal encryption keys and crack the encryption.

6 "Bring Your Own Device: The Facts and the Future," Gartner, May 2013
7 "Wearables, BYOD and IoT: Current and Future Plans in the Enterprise," Tech Pro Research, January 2015
8 "Gartner Says Tablets Are the Sweet Spot of BYOD Programs," Gartner, November 2014
9 "Global Cloud Index," Cisco, October 2014

Reformatting and Simple Overwriting: Reformatting disks still leaves data intact. Less than comprehensive overwriting technology many not perform enough overwriting passes or provide erasure reports to meet regulatory obligations. Overwriting freeware fails to deliver a detailed, auditable report and the software's effectiveness hasn't been independently verified.

Factory Resets: For mobile devices, using the internal factory reset command isn't enough to secure data. Factory reset simply removes pointers to the data while leaving the data itself intact. The "deleted" data that remains on mobile devices, as well as on external SD cards, can quickly and easily be recovered using readily available software.

Life Cycle Approach

To truly protect your employee records, customer information, intellectual property and other mission-critical data, you need comprehensive, certified data erasure. Certified data erasure can be achieved only through enterprise-class software that truly erases and verifies the erasure of sensitive information.

Effective data erasure also requires a life cycle mindset that aligns data erasure with your business needs. Such an approach enables you to strategize, budget, target, standardize and report on your enterprise data erasure. (See Figure 1.)

Enterprise data erasure calls for a life cycle approach – from establishing data erasure policies to automating the process to reporting on results.

Figure 1: Data Erasure Life-Cycle

Strategize

Data loss can have a significant impact on your organization's reputation and bottom line. The costs for incident response and remediation can be high and the legal and regulatory penalties can be severe. So it's important that your approach to data erasure reflects the realities of your industry and your business.

A key consideration is whether you should outsource data erasure or handle it in-house. In the European Union, where regulations have been in place longer and data erasure strategies in general have been more mature, organizations are more likely to handle data erasure in-house. To date, U.S. companies have been more inclined to outsource this capability.

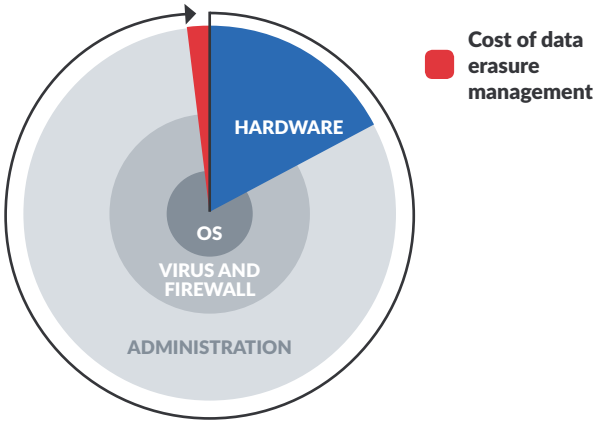
In-house data erasure is more secure because it ensures that sensitive data never leaves the enterprise. If you elect to outsource data erasure, make sure you choose a service provider that follows the most secure erasure processes. In either case, you need complete and customizable reporting so that you always have an audit trail. The International Association of IT Asset Managers has recommended a combined approach of in-house data erasure before transfer to a third-party erasure provider.

Budget

As organizations spend more on cyber security, a large portion of that expenditure is going specifically to protecting data. The average Fortune 1000 company now spends $2.4 million a year on data privacy, says the IAPP.[10] And 40 percent of those firms say privacy spending will increase "significantly" this year.

As spending to prevent data loss increases, it's important to consider how much of that investment should address data erasure. One way to approach the question is to track what you spend to secure IT equipment during its lifetime. That includes antivirus, firewalls, patch management, device control and so on, as well as the policies and procedures to implement those measures. Data erasure represents only a small fraction of that overall expenditure. (See Figure 2.) And while only a small percentage of devices are lost or stolen during their usable lifetimes, virtually all IT equipment leaves the enterprise at end-of-life.

10 "Benchmarking Privacy Management and Investments of the Fortune 1,000," Int'l Assn. of Privacy Professionals, September 2014



The investment to achieve effective data erasure represents only a small fraction of the overall costs for enterprise data security.

Figure 2: Data Erasure Costs

Target

Part of strategizing and budgeting includes determining exactly where you will apply data erasure. It's imperative to target all places data exists in the enterprise. That involves all relevant equipment in your data center, from servers to storage devices. It covers cloud environments, including both physical and virtualized systems. And it extends to all endpoints, from PCs and laptops to smartphones and tablets. All these devices and environments can store sensitive information and all must be targeted for data erasure.

You also need to determine when you will erase data. There are several key times when data erasure is necessary.

At Equipment End-of-Life: When a server, storage device, mobile device or other piece of IT equipment is retired, it's resold, repurposed or discarded. In any of those cases, any data it contains must be erased so that it doesn't fall into the wrong hands. This obviously also pertains to equipment returned at the end of a leasing period too.

During Data Migration: Whenever data is moved from one location to another, either from a retired server to a new server or from one virtual drive to another, the original data location must be expunged.

At Data End-of-Life: Many organizations manage LUNs 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 not just be deleted; it should be completely overwritten.

When Equipment is Serviced: If equipment is serviced in-house, it remains in a secure environment and there's no need to erase its data. But if the device will be serviced by an external entity such as a mobile device store, you should be sure any sensitive data is removed before servicing takes place.

When Loaner Devices are Returned: Mobile users who have their equipment serviced at a repair center are often given loaner devices. If these devices are used to access corporate systems, they should be erased before they're returned to the servicer. Additionally, large storage equipment such as SANs are oftentimes rented from leasing companies. Before they are returned at the end of the leasing period, they should be securely erased of all user data.

When Equipment is Repurposed: When many corporate users replace their BYOD devices, they retain their old equipment or give it to their children or to other family members to use. Any corporate data that remains on the device is vulnerable and should be erased.

When Customer 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. Failure to comply could result in a fine of up to 4 percent of a company's annual turnover, or €20 million, whichever is higher.

Standardize

Data erasure must become a standardized process so that all data is being securely removed from all devices at key transition points. To that end, you need to document your erasure processes and assign roles and responsibilities to make sure erasure is properly carried out. Include details such as what data erasure steps must take place when an employee leaves the company, for example.

Where possible, automate erasure procedures so they aren't overlooked. Define parameters such as specific data, file types, locations or events that initiate data erasure. Leverage capabilities you already have in place, such as Windows scheduling and patch management tools that can push erasure solutions to target machines.

When performing erasure at end-of-equipment-life, consider what other issues you should address at the same time. For example, you might document that when laptops reach end-of-life, access to corporate systems must also be removed. Or you might specify that after data erasure, the service provider that removes the equipment must verify that USB key locks or other hardware is no longer attached to the device.

Report

Finally, you need detailed reporting and certification to verify that erasure took place. Your report should be customizable to include relevant details such as:

- Hardware serial numbers
- Hardware specs, such as storage capacity
- Software license details
- Why the data was erased
- When the data was erased
- How the erasure was performed
- Who performed the erasure
- Authentication of who has rights to erase data
- Other end-of-life actions performed along with erasure

The report should be digitally signed and stored as a tamper-proof electronic file. It should be managed by IT but shared with HR, Legal, Risk Management and other relevant functions as appropriate. Most importantly, the report should include an audit trail that preserves the original report and maintains a log of any changes, documenting who made the change, when it was made and why it was made. Such an audit trail is vital for regulatory compliance and legal protection.

Comprehensive Solution

Just as deleting a file isn't the same as erasing it, not all data erasure software is created equal. An effective solution should offer these features.

Compliance: Your erasure solution should be certified by 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 erasure report proving that data was thoroughly removed at critical transition points. Reporting should include relevant serial numbers and asset tags, software details for license harvesting and how and by whom the erasure was performed.

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

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

Broad Platform Support: For mobile erasure, the software should be able to communicate directly with all major mobile operating systems, including iOS, Android and Windows mobile devices. It should also be able to detect and simultaneously erase data from a wide range of devices, regardless of the specific erasure requirements for each device.

High-Volume Erasure: Finally, your erasure solution should allow you to execute and automate erasure of multiple devices, regardless of the environment. This could include multiple HDDs and SSDs, smartphones and tablets, files and folders, virtual machines and LUNs. The automated erasure capability should be quick and easy to use and it should allow you to erase large numbers of devices in a single day.

Comprehensive, verifiable data erasure has emerged as a crucial component of enterprise data protection. As organizations spend more on cyber security, they need to ensure they're achieving optimum return on those expenditures. An advanced data erasure solution is an effective, cost-efficient investment in data security. Combined with a life cycle approach, such a solution can ensure that data erasure is protecting your mission-critical information and your business.