BitRaser®

BITRASER DATA ERASURE & DIAGNOSTICS SOFTWARE

AN INNOVATION FROM

stellar®
DATA CARE EXPERTS

SECURE | CERTIFIED | COMPLIANT

www.bitraser.com

BitRaser®

A managed & certified
data erasure & diagnostics software
that fulfils internal & external audit
requirements for government, enterprises,
ITADs, MSPs & SMBs.

BitRaser guarantees
wiping of sensitive data permanently
from hard drives, SSDs, desktops, laptops,
servers and mobile devices; safeguarding
privacy and preventing data leakage.

www.bitraser.com

TABLE OF CONTENTS

THREAT LANDSCAPE

BITRASER SECURE & RELIABLE DATA ERASURE SOFTWARE

BITRASER VARIANTS & CERTIFICATIONS

DATA: AN EVER GROWING EPIDEMIC

The Rising Data Security Risks

Unsecure device disposal, increases the chances of data privacy breach; for both individuals & organizations.

While individuals face the risks of identity theft, financial fraud and criminal act, for businesses & government organizations, unsafe device disposal poses the risk of facing penalties, lawsuits and reputation loss on failing to meet obligatory compliance with various privacy and data protection regulations like GDPR, HIPAA, GLBA, SOX.

Failure to comply with EU-GDPR provisions, for instance, can result in fine of up to € 20 Million or 4% of annual global turnover, whichever is more.

175 Zettabytes Projected In 2025 From Current 33 Zettabytes

Today, data is growing at a phenomenal rate. Every day, vast amount of information is created, transmitted, stored and collected across the globe. More than 3.7 billion people use internet. Worldwide 5 billion searches are done everyday.

As per Forbes 2018, ˝There are 2.5 quintillion bytes of data created each day at our current pace, but that pace is only accelerating with the growth of the Internet of Things (IoT).”

IDC predicts that the collective sum of the world’s data will grow from 33 zettabytes in 2018 to 175 zettabytes by 2025, at a compound annual growth rate of 61 percent.

2.3 Billion Computing & Mobile Devices Sold Each Year

Since 2016, each year 2.3 billion computing & mobile devices were shipped to help people manage their data.

In a globally connected world, multiple instances of data gets stored across geographies, adding to data volume and increased compliance demands. With the digital transformation of societies and organizations, and more and more economic & social activities moving online, each is generating exponential demand for more computing devices.

Rise of 'digital social' culture, high-speed internet, technologies such as IoT, AI & resultant industry shifts such as digital transformation underpin this stupendous growth of data & storage devices.

03 Years Is The Average Refresh Cycle Rate For IT Assets

The rapid technological evolution, aspirational needs of consumers and the ever stretching performance demands to process business data faster have led to shortened device lifespan. As a result there is a huge amount of devices that are traded in the second hand market, leading to a thriving re-use economy.

Organizations constantly replace outdated computers, servers, laptops, copiers and countless other types of electronic devices to keep up with technology. The average refresh cycle of a computing device is under three years. With this sprint to upgrade, a challenge of data security is on the rise at the time of refresh cycle, retiring or decommissioning of IT assets.

DATA SECURITY

End-of-Life of IT Assets : The Most Overlooked Part

Most organizations worldwide take data security seriously during the active lifespan of the IT assets by spending billions of dollars on measures including firewalls, network monitoring, encryption, etc. Secure data destruction when retiring IT assets remains a serious concern due to lack of awareness, concrete policies, procedures, budget and resources. Data breaches, identity theft, corporate espionage and dumpster diving have equally been a rapidly growing concern.

Disposing Old IT Assets

Returning Leased IT Assets

Donating To Meet CSR Obligations

Today, disposed IT devices are considered by business espionage professionals as the single most lucrative source of business insider information and personally identifiable data to fulfil malafide intentions. Establishments that discard storage devices at the end of device lifecycle without sanitization are vulnerable to data breaches & risks. The only means of mitigating risk of data leakage is by having a secure process of information destruction.

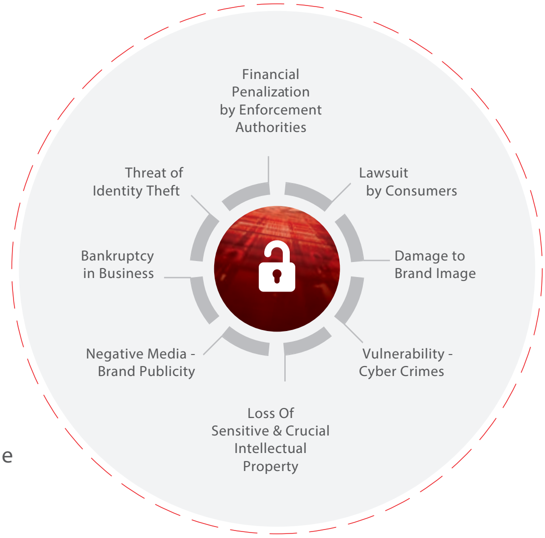
DUMPSTER DIVING HAS BEEN
AN EVER GROWING CONCERN AT LARGE

RISK IMPLICATIONS

High Stakes: Organizations & Individuals

Improper disposition of IT assets can put an organization at risk of data breaches & misuse of business-critical information.

These data breach scenarios put businesses at an immense risk of financial loss, legal proceedings, brand damage and embarrassment, all of which are unpleasant and damaging to the reputation of a company.


Financial Penalization by Enforcement Authorities
Threat of Identity Theft
Lawsuit by Consumers
Bankruptcy in Business
Damage to Brand Image
Negative Media - Brand Publicity
Vulnerability - Cyber Crimes
Loss Of Sensitive & Crucial Intellectual Property

POTENTIAL DATA BREACH TYPES

Due to Unsafe IT Asset Disposition

ENTERPRISE & GOVERNMENT BODIES

For organizations, securing data is of top most priority. The ambit of data threat extends beyond PII to include theft & misuse of business-critical information such as intellectual property, financial reports, business intelligence, trade secrets, etc. Today, secure IT asset disposition is a paramount need to prevent data breach, meet compliance with statutory regulations, and safeguard businesses from financial penalties, lawsuits and brand damage.

Financial Data	Intellectual Property	Business Intelligence	Trade Related Details
Customer Invoices	Patent/ Formula Misuse	Marketing Action Plans	Client Contact Details
Business Contracts	Innovation Leakage	Sales Strategies	Sourcing Information
Bank Account Details	Technology Breach	Trade Secrets	Purchase Records

INDIVIDUALS & HOME USERS

Individuals need to secure their used devices before disposing of to secondary markets, to ensure their data doesn't fall into wrong hands. The goal is to protect their sensitive information, prevent misuse & safeguard against identity theft, fraudulent transactions & exploitation of credit histories.

User Identity Thefts	User Privacy Issues	Financial Frauds	Risk to New Owners
Biometric Information	Photos & Videos	Bank Accounts	Possess Illegal Data
National Identity Card	Address Book	Banking Passwords	Risk of Litigation
Voters Card	Text & Messages	Credit Card Details	Reputation Loss
Social Security Number	Emails & Chats	Business Contracts	Embarrassment
Passport & Visa	Web Browsing History	Invoices	

DID YOU KNOW

A recent study by Stellar, on the world's largest known sample of 311 devices revealed that 7 out of 10 used devices were at risk of data breach. This lab study was based on the second-hand device study principles defined by National Association for Information Destruction (NAID), an international watchdog for the secure data destruction industry, outlines the threat landscape of residual data in used devices.

COMPLIANCE VIOLATION

Financial Penalties & Imprisonment

To protect privacy of citizens, data security laws have been framed in EU, USA and more than 100 countries in the world that levy penalties and legal actions on data breaches & non-compliance. All businesses have to comply with multiple national & international laws and regulations.

Stringent laws like EU-GDPR, PCi-DSS, HIPAA, GLBA, SOX etc. govern the data privacy of citizens and ensures organizations operate responsibly and take measures to mitigate data breach incident that may pose threat to any individual, organization or even country. In an event of data compromise, the organization and its officers have to face severe financial penalties and imprisonment.

EU-GDPR Violation

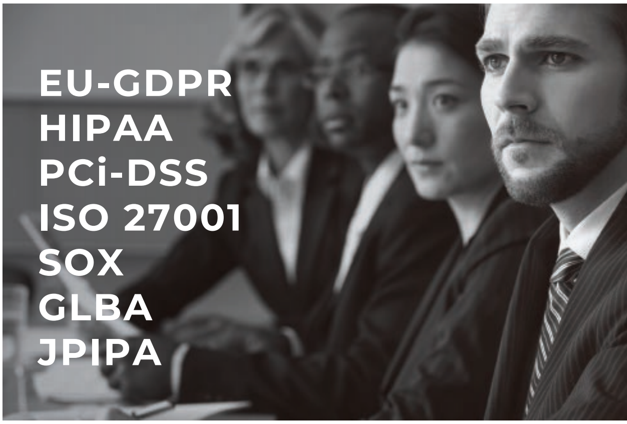
A more serious violation can result in a fine of €20 Million, or 4% of the violator's annual revenue, whichever is higher. Individuals can also face fines for GDPR violations if they use other parties' personal data for anything other than personal purposes. EU-GDPR applies to all European citizens residing anywhere in the world.

HIPAA Penalty

HIPPA violation could result in fines of up to $50,000 per violation for willful neglect, with maximum USD1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in imprisonment.

GLBA Violation

The US Attorney General enforces GLBA (Gramm-Leach-Bliley Act). It has provision for fines of up to $100,000 for the financial institution for each violation and civil penalty of up to $10,000 for the officers & directors of an organization. Imprisonment of up to 5 years may also happen.



PCi-DSS

Non compliance leads to fines ranging from $5,000 to $500,000 per month depending on the nature of violation.

SOX 906

Penalty can be up to $5,000,000 in fines & up to 20 years imprisonment.

DID YOU KNOW

Fresenius Medical Care North America paid a $3,500,000 settlement fine for risk analysis failures, an ePHI disclosure; lack of policies covering electronic devices; lack of encryption; inadequate security policies; & physical safeguards.

DATA PROTECTION LAWS & ACTS

The US Laws Matrix & Navigating the Maze

While there is no single principal federal data protection legislation in United States, there are multitude of sector specific laws that focus on particular data type like FTCA [Federal Trade Comission Act], DPPA [Driver Privacy Protection Act], COPPA [Children's Online Privacy Protection Act].

Today, over 600 federal and state laws exist that protect the privacy of an individual. State level inititative to implement comprehensive privacy bills is at an all time high in 2020 and many are inspired by EU-GDPR, considered the gold standard for privacy protection. While the provisions of the approved acts and some pending bills are expansive in nature, a noteworthy area is to grant consumers the right to request deletion of personal data and PII.

> Grant a consumer the right to request deletion of personal information and require the business to delete information upon receipt of a verified request
>
> ***California Consumer Privacy Act***
> *effective January 2020*

Timeline of Data Privacy Laws and Acts in USA	
US Privacy Act . 1974	US Privacy Act of 1974- Maintains restrictions on data held by government agencies
HIPAA, 1996	Health Insurance Portability and Accountability Act– Protects sensitive patient health information
COPPA, 1998	Children's Online Privacy Protection Act– Protects data of children under the age of 13
GLBA, 1999	Gramm-Leach-Billey Act– Protects financial non-public personal information
SOX, 2002	Sarbanes-Oxley Act– Protects investors from fraudulent financial reporting by corporations
H. B. 1493, 2017	Washington Biometric Privacy Law– Governs collection, use, and storage of "biometric identifiers"
NPL, 2019	Nevada Privacy Law– Governs the collection of personally Identifiable Information (PII) by websites
CCPA, 2020	California Consumer Privacy Act– Provides consumers more control over their personal information
Maine Privacy Law, 2020	Maine Broadband Privacy Laws of 2020– Protects the privacy of online customer information
CDPA, 2021	Virginia's Consumer Data Protection Act– Implements reasonable security practices to protect sensitive data

DATA DESTRUCTION STRATEGY

Key Pillars to Consider Before Choosing the Right One

Organizations must choose the right media sanitization strategy to safeguard data privacy at the time of IT asset disposal, minimize business risk & meet regulatory compliance. An ideal strategy would also help reduce e-waste and monetize the ‘residual value’ of used IT assets. There are 3 most prevalent techniques to destroy data for safe disposal of IT assets, namely Wiping, Degaussing & Shredding.

Degaussing is a demagnetizing process to erase magnetic hard drives rendering the data unrecoverable. Degaussing is an ineffective method to sanitize emerging magnetic storage media and flash memory based storage devices. As per NIST SP 800-88 Guideline, “existing degaussers may not have sufficient force to degauss evolving magnetic storage media and should never be solely relied upon for flash memory-based storage devices or magnetic storage devices that contain non-volatile non-magnetic storage”. Further, Degaussing renders the sanitized media unusable and results in toxic e-waste.

Shredding is a physical destruction technique that disintegrates storage media such as hard drive and USB flash drive into minute pieces to destroy data. However, Shredding and other physical destruction methods are not always feasible ‘On Site’ (i.e. on company premises) due to various logistic & financial constraints. The need to ship out storage media to off-site shredding facility for sanitization in such cases may pose threat of data leakage from the media while it is in-transit. Also, inventoried storage media lined up for shredding is at constant risk of theft & data leakage till the point it is ‘actually’ shredded. Further, Shredding destroys the storage hardware and generates toxic e-waste.

Data Wiping and Software Erasure is based on overwriting all the addressable storage locations & hidden areas on the media with binary pattern in order to secure the media from any kind of data leakage threats. Data erasure by using professional tools can provide immutable audit trails through verifiable reports & certificates for failsafe regulatory compliance. Erasure technique allows erased storage media to be reused resulting in zero e-waste generation. Additionally, the residual value of the asset can be monetized. A professional data erasure software can automate large media sanitization jobs at scale.

CHOOSE THE RIGHT METHOD

	DEGAUSSING	DATA WIPING	SHREDDING
Is It Secure ?	◐	🟢	🟢
Is It Trusted ?	🔴	🟢	◐
Is the Device Reusable ?	🔴	🟢	🔴
Is It Environmentally Safe ?	🔴	🟢	🔴
Is It 100% Audit Compliant ?	🔴	🟢	🔴
Is It Cost-Effective & lowers TCO ?	🔴	🟢	🔴

COMPLIANCE IS PARAMOUNT

But Is Not The Only Consideration

A secure & reliable SOFTWARE that simplifies erasure for organizations to stay secure & enables ITAD & MSP to deliver to the industry.

ENABLES
ITAD & MSP
TO DELIVER TO INDUSTRY

SIMPLIFIES
ENTERPRISE, GOVT. & SMB
TO STAY SECURE

CENTRAL MANAGEMENT

Central Console
Erasure License Distribution
Reports Repository

AUTOMATION & SCALABILITY

Cloud Management
Remote Network Erasure
Managed Bulk Erasure

SEAMLESS AUDIT TRAILS

Verifiable Reports
Reports For Audit
Tamper Proof Certificates

LOWER COST OF OPERATION

Reduces TCO With Device Reuse
No CAPEX Needed
Reduces E-waste Obligations

DID YOU KNOW

DATA ERASURE MYTH
Formatting or Deletion doesn't erase data. A Do-It-Yourself data recovery software can easily recover deleted & formatted data thus putting data privacy at risk.

PRESENTING

BitRaser®

Simple & Powerful - Data Erasure & Diagnostics Software

BitRaser is our cutting-edge technology that guarantees permanent wiping of sensitive data from all storage devices including laptop & desktop hard drives, removable storage media, servers, & mobile devices. It provides failsafe solution for IT asset disposition, reallocation or putting data-to-rest stages.

Delivering performance to ITAD, Enterprise, Managed Service Provider & Individual: BitRaser helps safeguard privacy and prevents data leakage. For organizations, BitRaser serves the need for a managed & certified data erasure solution that can support internal & external corporate audit requirements with traceable reporting. BitRaser can serve as a perfect risk mitigation tool!

DATA ERASURE SOLUTIONS FOR ALL

- » Enterprise, Govt. & SMB
- » ITAD & Refurbisher
- » MSP, SI & Retailer
- » Individual & Home User

SANITIZE DEVICES . MITIGATE RISKS . MEET COMPLIANCE

SECURE & CERTIFIED DATA ERASURE

A Software That Erases Sensitive Data & Meets Compliance

ACROSS DRIVES, DEVICES & PLATFORMS

BitRaser, a plug and play software, serves your need for certified & secured data erasure solution beyond data recovery for removable & portable drives, loose or rack mounted storage devices, mobile devices, drives in desktops & laptops or drives over LAN.

DEVICE SUPPORT	STORAGE TYPE	MEDIA SUPPORT	DATA TYPES
LAPTOP, DESKTOP	REMOVABLE	HDD, SSD	FILE & FOLDER
APPLE MAC®	PORTABLE	SATA, PATA	DRIVE PARTITION
TABLETS, iPAD®	LOOSE	SAS, SCSI	HIDDEN AREAS
SMARTPHONE	ON-BOARD	NVMe, PCI, M2.SATA	CHAT/ BROWSER HISTORY
MS SURFACE®	RACK-MOUNTED	FLASH DRIVE, USB	APPLICATION TRACES
SAN, NAS, DAS & FCAS	OVER NETWORK	IDE	LOG FILES

COMPLIANT WITH 24 GLOBAL STANDARDS

BitRaser complies with global standards of data erasure & offers 5 custom erasure algorithms		
NIST 800-88 Clear	US Army AR 380-19 (3 passes)	Pseudo-Random & Zeroes (2 passes)
NIST 800-88 Purge	NATO Standard (7 passes)	Random Random Zero (6 passes)
US - DoD 5220.22-M (3 passes)	US Air Force AFSSI 5020 (3 passes)	NAVSO P-5239-26 (3 passes)
US - DoD 5220.22-M (ECE) (7 passes)	Pfitzner Algorithm (33 passes)	NCSG-TG-025 (3 passes)
US - DoD 5200.28-STD (7 passes)	Canadian RCMP TSSIT OPS-II (4 passes)	BitRaser Secure & SSD Erasure
Russian - GOST-R-50739-95 (2 passes)	British HMG IS5 (3 passes)	Pseudo-Random
B.Schneier's Algorithm (7 passes)	British - HMG IS5 (Baseline Standard)	Peter Gutmann (35 passes)
German Standard VSITR (7 passes)	Zeroes	

TESTED, CERTIFIED & COMPLIANT

BitRaser is certified by globally renowned bodies & organizations.

U.S. DEPARTMENT OF HOMELAND SECURITY

NIST National Institute of Standards and Technology

PRODUCT ADISA CLAIMS TEST

STQC

HIPAA SEAL OF COMPLIANCE COMPLIANCY GROUP HIPAA VERIFIED

NYCE Safety and Trust

RELIABLE, MANAGEABLE & SCALABLE

Software With Excellent Capabilities

SECURE ERASURE

Securely erases sensitive data from HDDs & SSDs across desktop/laptop PCs and servers, and mobile devices beyond recovery, at end-of-lifecycle of devices.

CERTIFIED ERASURE

Generates 100% tamper proof erasure certificate that ensures compliance with EU-GDPR, SOX, GLBA, HIPAA & other international data protection regulations.

INTERNATIONAL STANDARDS COMPLIANCE

Supports extensive list of 24 International erasure standards including NIST, DoD 3 or 7 Passes, HMG, etc.

POWERFUL DIAGNOSTICS & TESTING

Accurate diagnosis of the health status of mobiles & hard drives to ascertain their functional status, maximizing resale value.

CLOUD INTEGRATION

Provides flexibility to create users, manage license distribution & maintain central repository of reports & certificates.

CENTRALLY MANAGED BULK ERASURE

Erases multiple devices or drives over a local area network with centralized console to manage & monitor erasure process & maintain reports.

REPORTS FOR AUDIT TRAILS

Generates erasure reports for audit trails with option to customize and save report in various formats like PDF, CSV & XML.

CONFIGURATION & AUTOMATION

Automates erasure process across IT assets with ability to customize erasure process as per international erasing standards.

AN INNOVATION FROM STELLAR®

The Global Data Care Experts

> “ We exist because we know that what matters most to you in this digital age is your data. We work to ensure that your data is safe while you take care of your business & live a worry free digital life. Our research & innovation enables us to create future-ready solutions for data recovery, data erasure & migration. ”

25+
YEARS OF EXPERTISE

400+
MOTIVATED TEAM

8000+
PARTNERS WORLDWIDE

3M+
HAPPY CUSTOMERS

190
COUNTRIES SERVED

SIMPLE SOLUTIONS FOR VARIED NEEDS

Data Erasure Software For All

Drive Erasure & Diagnostics Software

Erases HDD, SSD In Desktops, Laptops, Mac & Server

Ideal For
Enterprise, Government
& SMB

Bulk Drive Erasure Software

Erases Loose Drives Or Mounted, PC, Mac & Server Over Network

Ideal For
Large Enterprise,
ITAD, Refurbisher

Mobile Erasure & Diagnostics Software

Erases & Diagnoses iOS® & Android® Devices

Ideal For Enterprise,
ITAD, Mobile Retailer &
Repair Shop

File Erasure Software

Erases Files, Folders & Partitions From PC, Laptop, Server

stellar
BitRaser
File Eraser
Corporate
Erase Files, Folders & Volumes
SECURE · CERTIFIED · COMPLIANT

Ideal For Enterprise,
Government, SMB &
Individual

BITRASER® DRIVE ERASER

Certified. Compliant.

ERASES DATA ACROSS DRIVES, DEVICES & PLATFORMS

BitRaser serves your need for a certified solution that can assure permanent data erasure when disposing or returning leased IT assets. It can securely wipe data beyond data recovery from all kinds of storage devices & generates tamper proof audit trails. BitRaser's trusted automated reporting helps you to meet internal & external data security audit requirements and comply with global data privacy laws or regulations like – EU GDPR, GLB, SOX, HIPAA, ISO27001, PCI-DSS etc.

SECURE & CERTIFIED DATA ERASURE

» Securely erases data from PCs, Servers, laptops & rack mounted drives
» Simultaneously erase multiple drives at high speed
» Supports erasure of all major drive types - SATA, PATA, SSD, NVMe, M.2, PCI, SAS, SCSI, IDE, USB, Fibre Channel & FireWire
» Supports 24 global (+5 custom) erasure standards like DoD 5220.22, NIST 800-88, British HMG Infosec, etc.
» Identifies and erases hidden areas like HPA, DCO & remapped sectors
» Supports multiple block size drives & RAID dismantling
» Secure client server communication with AES encryption

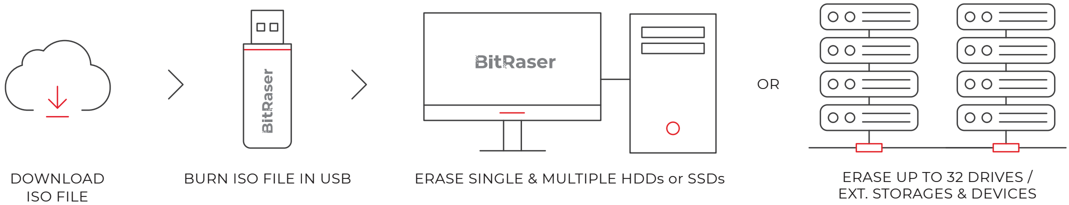
CONFIGURATION & AUTOMATION

» Create bootable USB using downloadable ISO image from Cloud
» Supports One Click Wiping with ISO customization (standards, verification, certificate type, etc.)
» Cloud based console for user, license management & maintaining repository of reports
» Supports transfer of licenses from cloud console to BitRaseroffline dongle
» Allows two methods to verify erasure process
» Ability to add asset tag & pre-report information before erasure
» Identifies dead drives through LED notification

ERASURE REPORT & CERTIFICATE

» Generates secure & 100% tamper proof erasure certificates for audit trails in PDF, CSV & XML
» Export reports from client to cloud in digital & physical versions
» Option to customize report

BITRASER DEPLOYMENT


BitRaser
BitRaser
OR
DOWNLOAD ISO FILE
BURN ISO FILE IN USB
ERASE SINGLE & MULTIPLE HDDs or SSDs
ERASE UP TO 32 DRIVES / EXT. STORAGES & DEVICES

+ FOR ERASING DEVICES WITHOUT INTERNET CONNECTIVITY, BITRASER IS ALSO AVAILABLE VIA SECURE USB SOLUTION

BITRASER® DRIVE ERASER WITH ADMIN CONSOLE

Scalable. Manageable.

AUTOMATES ERASURE WITH CENTRALIZED REPORTING

A managed & certified data erasure solution, BitRaser meets the data wiping needs of large corporations, R2, ITADs & government organizations. It offers easy-to-use, centrally managed data sanitization across storage devices there by mitigating risks, increasing scalability & reducing the total cost of ownership when it comes to reallocating, reselling or recycling IT assets. Equipped with an 'Admin Console' application it helps you to perform erasure remotely over LAN with central control & provides a repository of reports & certificates that helps meet statutory & regulatory compliance.

SECURE & CERTIFIED DATA ERASURE

- Securely erases data from PCs, Servers, laptops & rack mounted drives
- Supports erasure of all major drive types - SATA, PATA, SSD, NVMe, M.2, PCI, SAS, SCSI, IDE, USB, Fibre Channel & FireWire
- Simultaneously erase up to 65000 drives through BitRaser Admin Console
- Compliant with 24 international erasure standards
- Option to add 5 customized erasure standards

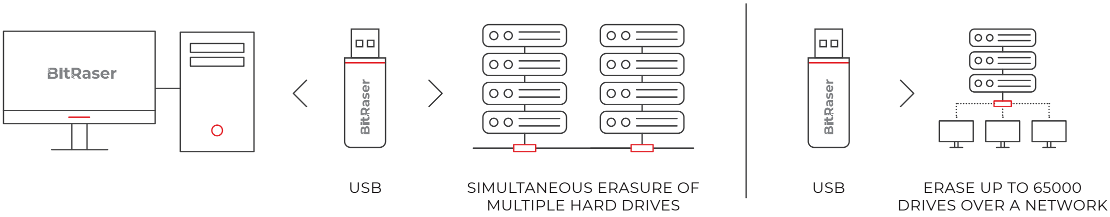
CONFIGURATION & AUTOMATION

- Erase using bootable USB or through PXE over network
- Customize erasure process as per international erasure standards (DoD 5220.22, NIST 800-88, British HMG Infosec, etc.)
- Allows two methods to verify erasure process
- Option to provide asset tag and customer information
- Internet connectivity through Ethernet or Wi-Fi

ERASURE REPORT & CERTIFICATE

- Central repository for all your erasure reports & certificates on MySQL database
- Generates secure, 100% tamper proof reports & erasure certificates for audit trails
- Easy search of reports in seconds

BITRASER DEPLOYMENT


BitRaser
BitRaser
USB
SIMULTANEOUS ERASURE OF MULTIPLE HARD DRIVES
BitRaser
USB
ERASE UP TO 65000 DRIVES OVER A NETWORK

BITRASER®
MOBILE ERASER & DIAGNOSTICS

Effortless. Reliable.

SECURELY ERASES & DIAGNOSES iOS® & ANDROID® DEVICES

BitRaser Mobile Eraser & Diagnostics software helps you erase & test iOS® & Android® based devices to increase efficiency, improve security & guarantee compliance. This privacy safeguarding software permanently wipes data & performs series of assisted & automated tests to diagnose health & functioning of mobile devices. This guarantees that sensitive data does not fall in wrong hands when, mobile devices are disposed, recycled or sold.

CERTIFIED DATA ERASURE & DIAGNOSTICS

- » Single, unified interface for erasure or diagnostics
- » Permanently erases data from iOS® & Android® devices
- » Supports erasure & diagnosis of iOS® devices on iOS® v7 & above
- » Supports erasure & diagnosis of Android® devices on OS v5 & above
- » Simultaneous high-speed erasure & diagnostics of up to 40 devices
- » Erase locked iOS® devices

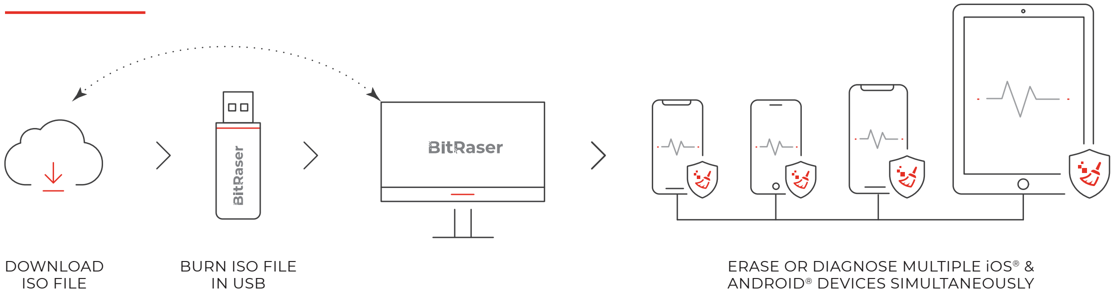
CONFIGURATION & AUTOMATION

- » Easy installation with no requirement of pre-installed OS on workstation
- » Cloud integration for user creation, license distribution & reports
- » Allows customization to preconfigure erasure & diagnostics process
- » Supports 10 international erasure standards like DoD, NIST 800-88, etc.
- » Analyzes mobile device health through 40+ automatic & manual tests
- » Allows to print labels for erased or diagnosed mobile devices
- » Options to provide asset tag and custom information
- » Supports Internet connectivity through Ethernet or Wi-Fi

ERASURE REPORT & CERTIFICATE

- » Generates verifiable erasure & diagnostics reports for audit trails
- » Maintains repository of reports on workstation or on cloud for anytime access
- » Allows to grade mobile devices
- » Allows saving of erasure report in PDF, CSV, & XML

BITRASER DEPLOYMENT


BitRaser
BitRaser
DOWNLOAD ISO FILE
BURN ISO FILE IN USB
ERASE OR DIAGNOSE MULTIPLE iOS® & ANDROID® DEVICES SIMULTANEOUSLY

stellar
BitRaser
File Eraser
Corporate
Erase Files, Folders & Volumes
SECURE · CERTIFIED · COMPLIANT

BITRASER® FILE ERASER

Simple. Secure.

ERASE SENSITIVE & CONFIDENTIAL DATA BEYOND RECOVERY

BitRaser File Eraser is a privacy safeguarding software that permanently erases files, folders, partitions, Internet history etc. stored on laptop,desktop, server beyond the scope of data recovery. The software meets daily data sanitization requirements of organizations and individuals by erasing data securely. The software allows you to schedule erasure process & maintain detailed log reports of all files deleted for meeting statutory & regulatory compliance needs for data security & privacy – SOX, GLB, HIPAA, ISO27001,EU-GDPR, PCI-DSS.

CERTIFIED DATA ERASURE

- » Permanent erasure of files, folders & volumes beyond recovery
- » Performs high-speed & simultaneous erasure of multiple files
- » Erases application traces, unused space, system traces & internet history
- » Erases data from mapped drives in your system
- » Remote erasure of files & folders on servers & storage areas across the network
- » Supports 17 global erasure standards

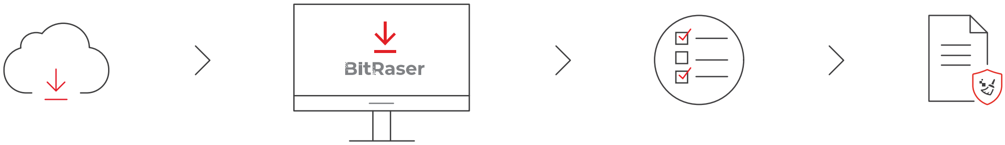
CONFIGURATION & AUTOMATION

- » Schedule erasure tasks at regular intervals
- » Schedule erasure of selected files on workstations and servers on local area network
- » Option to search for a specific file using its name
- » Ability to create erasure list containing the names of files & folders that can be erased in a single step

ERASURE REPORT & CERTIFICATE

- » Generates reports to ensure compliance with PCI DSS, requiring erasure of file-level data
- » Generates digitally-signed certified reports of erasure in PDF & XML for audit trail purposes

BITRASER DEPLOYMENT



DOWNLOAD
EXE FILE

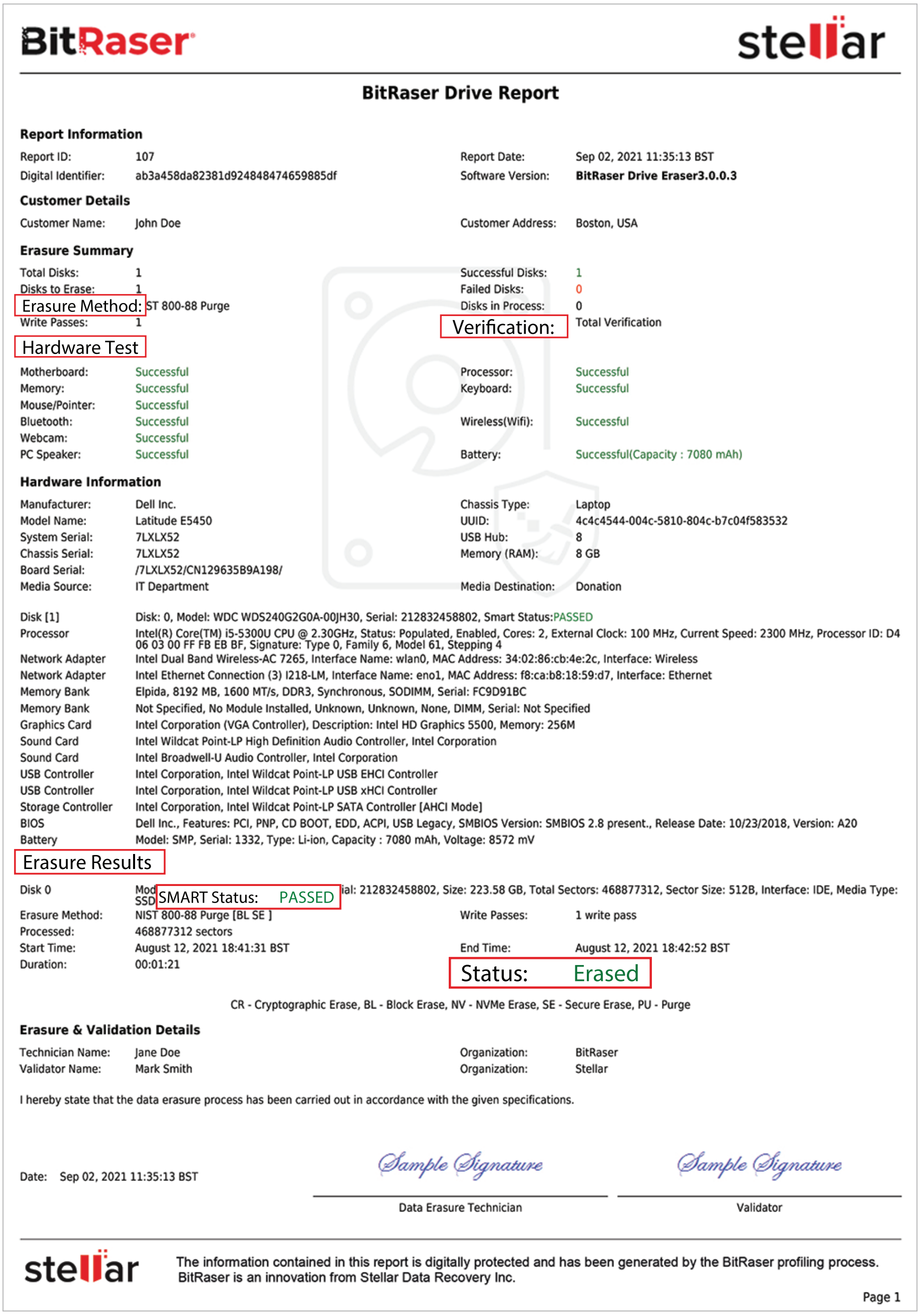
INSTALL BITRASER FILE ERASER

SELECT FILES/FOLDERS/
VOLUMES TO ERASE

ERASE

SAMPLE REPORT

100% Customizable & Tamper-Proof Report



BitRaser

stellar

BitRaser Drive Report

Report Information

Report ID:	107	Report Date:	Sep 02, 2021 11:35:13 BST
Digital Identifier:	ab3a458da82381d924848474659885df	Software Version:	**BitRaser Drive Eraser3.0.0.3**

Customer Details

Customer Name:	John Doe	Customer Address:	Boston, USA

Erasure Summary

Total Disks:	1	Successful Disks:	1
Disks to Erase:	1	Failed Disks:	0
Erasure Method:	ST 800-88 Purge	Disks in Process:	0
Write Passes:	1	Verification:	Total Verification

Hardware Test

Motherboard:	Successful	Processor:	Successful
Memory:	Successful	Keyboard:	Successful
Mouse/Pointer:	Successful		
Bluetooth:	Successful	Wireless(Wifi):	Successful
Webcam:	Successful		
PC Speaker:	Successful	Battery:	Successful(Capacity : 7080 mAh)

Hardware Information

Manufacturer:	Dell Inc.	Chassis Type:	Laptop
Model Name:	Latitude E5450	UUID:	4c4c4544-004c-5810-804c-b7c04f583532
System Serial:	7LXLX52	USB Hub:	8
Chassis Serial:	7LXLX52	Memory (RAM):	8 GB
Board Serial:	/7LXLX52/CN129635B9A198/		
Media Source:	IT Department	Media Destination:	Donation

Disk [1]	Disk: 0, Model: WDC WDS240G2G0A-00JH30, Serial: 212832458802, Smart Status:PASSED
Processor	Intel(R) Core(TM) i5-5300U CPU @ 2.30GHz, Status: Populated, Enabled, Cores: 2, External Clock: 100 MHz, Current Speed: 2300 MHz, Processor ID: D4 06 03 00 FF FB EB BF, Signature: Type 0, Family 6, Model 61, Stepping 4
Network Adapter	Intel Dual Band Wireless-AC 7265, Interface Name: wlan0, MAC Address: 34:02:86:cb:4e:2c, Interface: Wireless
Network Adapter	Intel Ethernet Connection (3) I218-LM, Interface Name: eno1, MAC Address: f8:ca:b8:18:59:d7, Interface: Ethernet
Memory Bank	Elpida, 8192 MB, 1600 MT/s, DDR3, Synchronous, SODIMM, Serial: FC9D91BC
Memory Bank	Not Specified, No Module Installed, Unknown, Unknown, None, DIMM, Serial: Not Specified
Graphics Card	Intel Corporation (VGA Controller), Description: Intel HD Graphics 5500, Memory: 256M
Sound Card	Intel Wildcat Point-LP High Definition Audio Controller, Intel Corporation
Sound Card	Intel Broadwell-U Audio Controller, Intel Corporation
USB Controller	Intel Corporation, Intel Wildcat Point-LP USB EHCI Controller
USB Controller	Intel Corporation, Intel Wildcat Point-LP USB xHCI Controller
Storage Controller	Intel Corporation, Intel Wildcat Point-LP SATA Controller [AHCI Mode]
BIOS	Dell Inc., Features: PCI, PNP, CD BOOT, EDD, ACPI, USB Legacy, SMBIOS Version: SMBIOS 2.8 present., Release Date: 10/23/2018, Version: A20
Battery	Model: SMP, Serial: 1332, Type: Li-ion, Capacity : 7080 mAh, Voltage: 8572 mV

Erasure Results

Disk 0	Mod SMART Status: PASSED ial: 212832458802, Size: 223.58 GB, Total Sectors: 468877312, Sector Size: 512B, Interface: IDE, Media Type: SSD		
Erasure Method:	NIST 800-88 Purge [BL SE]	Write Passes:	1 write pass
Processed:	468877312 sectors		
Start Time:	August 12, 2021 18:41:31 BST	End Time:	August 12, 2021 18:42:52 BST
Duration:	00:01:21	Status:	Erased

CR - Cryptographic Erase, BL - Block Erase, NV - NVMe Erase, SE - Secure Erase, PU - Purge

Erasure & Validation Details

Technician Name:	Jane Doe	Organization:	BitRaser
Validator Name:	Mark Smith	Organization:	Stellar

I hereby state that the data erasure process has been carried out in accordance with the given specifications.

Date: Sep 02, 2021 11:35:13 BST

Sample Signature — Data Erasure Technician

Sample Signature — Validator

stellar

The information contained in this report is digitally protected and has been generated by the BitRaser profiling process. BitRaser is an innovation from Stellar Data Recovery Inc.

Page 1

CLIENT SPEAK

What Our Clients Say About Us

WE MEASURE OUR SUCCESS WITH OUR CLIENTS SATISFACTION

CompuCycle

“ CompuCycle is extremely satisfied with the BitRaser software we are using to sanitize hard drives. From the software customization, implementation of software, customer support & overall experience, BitRaser’s service is exceptional. It is wonderful to have a software company who meets & often exceeds our expectations. Thank you BitRaser. ”

JOHONNOT TECHNOLOGIES

“BitRaser allows us to bring value back to our customers while maintaining the highest standards of security. It has allowed us to increase our throughput drastically. BitRaser has the best customer service and we're happy to be associated with BitRaser. ”

Panasonic

“ BitRaser helps us meet our compliance requirements by generating automated erasure reports immediately after erasure is completed. We also appreciate that It helps us monitor as well as erase several devices simultaneously, helping us save time as well as manpower. ”

AVAYA

“Our selection of BitRaser over competition was based on the promising features the software offers. Our choice to select BitRaser for performing data erasure has been a fruitful one as BitRaser software exactly delivered to it promises. We are glad to have used their services & are really thankful. ”

Nikon

“ We have used the Stellar BitRaser and we are completely satisfied by the same. Also it's easy to use and manage in the corporate sector. In future also we will consider the same for Data removal whenever required. ”

OUR CLIENTS

Few Of Our Esteemed Clients

hp

Deloitte.

CISCO

Coca-Cola

McDonald's

KNORR BREMSE

accenture

DELL

Google

FUJITSU

भारतीय रिज़र्व बैंक RESERVE BANK OF INDIA

MITSUBISHI HEAVY INDUSTRIES AIR CONDITIONING

SAMSUNG

INGRAM MICRO

amazon.com

IBM

TransRe We value risk.

DUCATI

Adobe

PHILIPS

Gulf

NBA

CITRIX

GE

pwc

LAMBORGHINI

Nestlé

Microsoft

RENAULT Passion for life

Unilever

BitRaser®

For more information, contact our
BitRaser representatives

☎ +1-844-775-0101

✉ sales@bitraser.com

🌐 www.bitraser.com