



IAITAM ACE

May 7-9, 2024 The M Resort 🌴 Las Vegas, NV

Mitigating Data Breach Risks Through Remote Data Erasure

By: Sunil Chandna, CEO BitRaser



Finding your IAITAM Oasis



About Sunil Chandna

Sunil is the CEO of BitRaser, a leading data erasure software developed by Stellar, a company he co-founded in 1993, known for its expertise in data recovery. With a strong background in data management, Sunil has been a keynote speaker at various international trade events focusing on data destruction. He is also a distinguished member of the Data Sanitization experts group of SERI/R2 and the IEEE Security in Storage Working Group.



May 7–9, 2024 The M Resort  Las Vegas, NV

BitRaser

Increase in Remote Work Leads to Data Security Risks

Post-pandemic, **remote work culture** has increased phenomenally.

Forbes¹ predicts that **by 2025, 32.6 million Americans** will be engaged in remote work.

79% of organizations² have concern for **cybersecurity risks** associated with remote workers.

1

2

3

1

4

5

6



Malwarebyte³ states that **20% of organizations experienced a breach** because of a remote worker.

Prioritizing data security & data privacy is the need of the hour.

Managing Secure Data Disposal of Remote IT Assets at the end of Life-cycle is necessary to **Mitigate Data Breach Risks**

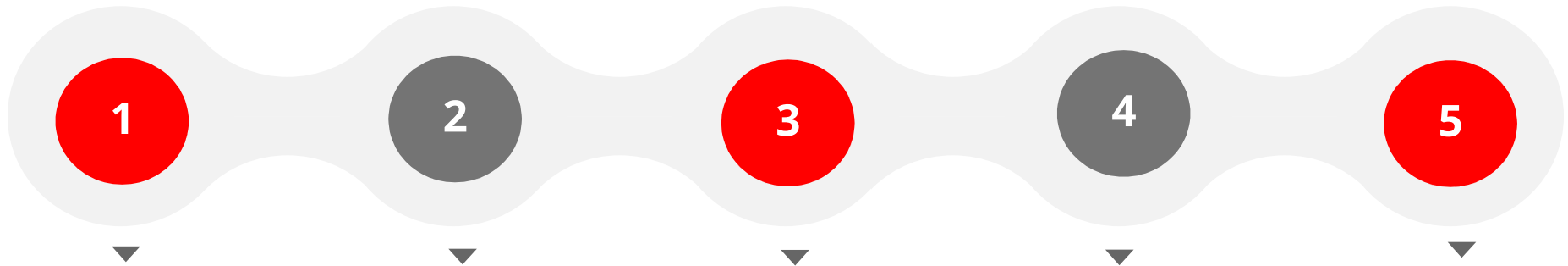
Source: Forbes¹ | Techrepublic² | Malwarebyte³



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

Data Security Challenges Faced In the Remote Work Environment



Ensuring the **Endpoint security** of remote devices like updating software patch, weak password, etc.

Enforcing **data access controls** like unsecure Wi-Fi network is complex for Remote Workers

Preventing Data from getting compromised – e.g. **phishing attacks, malware**

Educating employees **on data security best practices** to mitigate risks

Data Destruction is a concern when remote worker leaves, project completes or during mass layoff



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

Use Cases of Remote Data Destruction

1

Employee Separation or
End of term for Contractor

2

Employee is working under BYOD
policy & wants to sell device

3

Remote Device Recall at
IT Asset Refresh cycle

4

Contractual obligation at the
end of project mandates to
destroy data

5

Remote Device replacement
in event of hardware
malfunction

6

When Leased IT assets
are returned



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

Data Destruction Methods : Shredding, Degaussing & Data Erasure

Data Destruction Methods



Data Destruction

A process of getting rid of sensitive, confidential & obsolete data from storage devices permanently beyond scope of recovery.

Data Destruction can be done Onsite and Offsite.

Physical Method

Logical Method

- **Shredding** : Completely destroys data bearing storage devices
- **Degaussing** : Demagnetizing of media rendering drive unusable
- **Sanitization**: Aka 'Data Erasure', a software based technique that makes data recovery infeasible post data is erased & helps reuse the device.



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

Offsite Data Destruction Risks For Organizations

Chain of Custody Risks



- Data Leakage during Transit
- Loss of Shipment



Possibility of Data Breaches



Heavy Penalties for Organization



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

Onsite Data Destruction Challenges For Physical Method

1

Logistics Challenge

Physical destruction methods require 'Special Equipment' & Personnel on ground

2

Incomplete Destruction

Shredding may not completely destroy data and data remnants can be recovered

3

Environmental Challenge

Shredding & degaussing produce e-waste, generate SCOPE-3 emissions

4

Technical Challenge

SSDs cannot be degaussed because of their technology limitation

5

Economical Challenge

Modern devices have SSDs embedded on to motherboards making it financially infeasible to shred the device itself



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

Remote Data Erasure: The Wise Choice

Remote Data Erasure is a process of sanitizing endpoint devices containing sensitive information using a software with minimal intervention. By adopting 'Remote Data Erasure', organizations can effectively manage data destruction process across distributed environments minimizing data security risks in a cost-effective way.

Benefits of Remote Data Erasure

01

Remote Erasure Helps Mitigate Data Breach Risks

03

Certificate of Destruction – Automatic, Real Time Audit Trail

02

Simultaneous Erasure of Endpoint Devices

04

Reduce E-waste & Increase Reusable Devices Helping Organization Meet ESG Goals

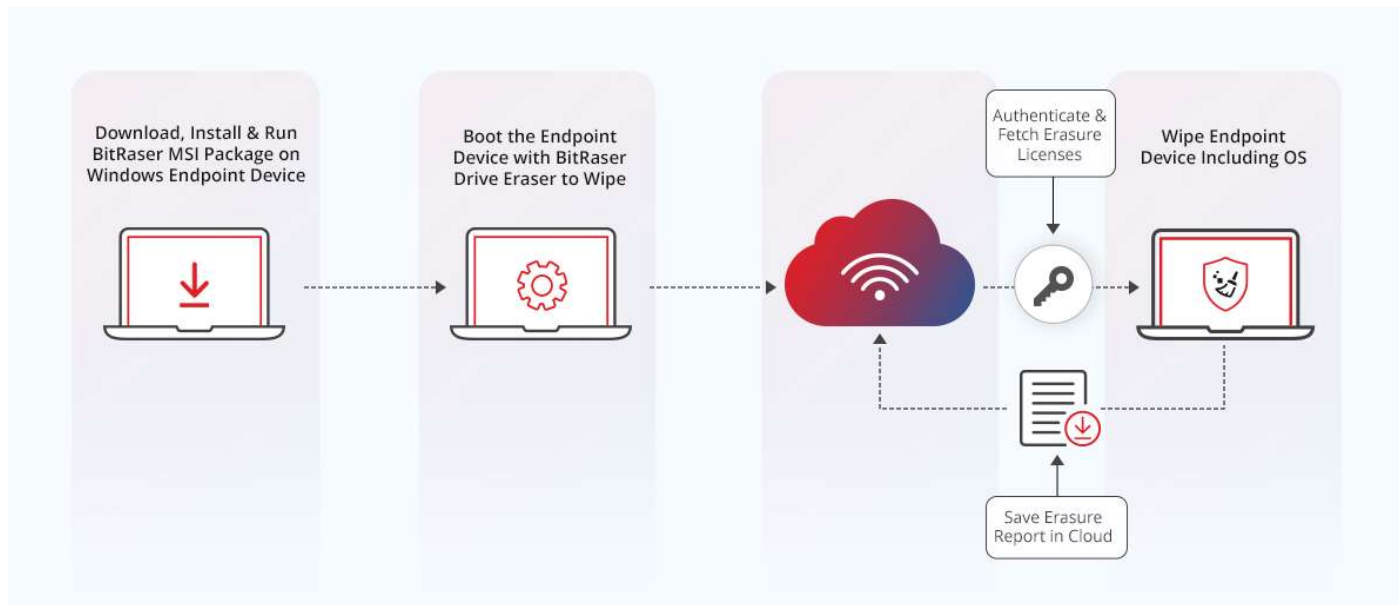


May 7–9, 2024 The M Resort  Las Vegas, NV

BitRaser

How to Implement Remote Data Erasure?

Method 1: Remotely Wipe Windows Endpoint Devices Using MSI Package

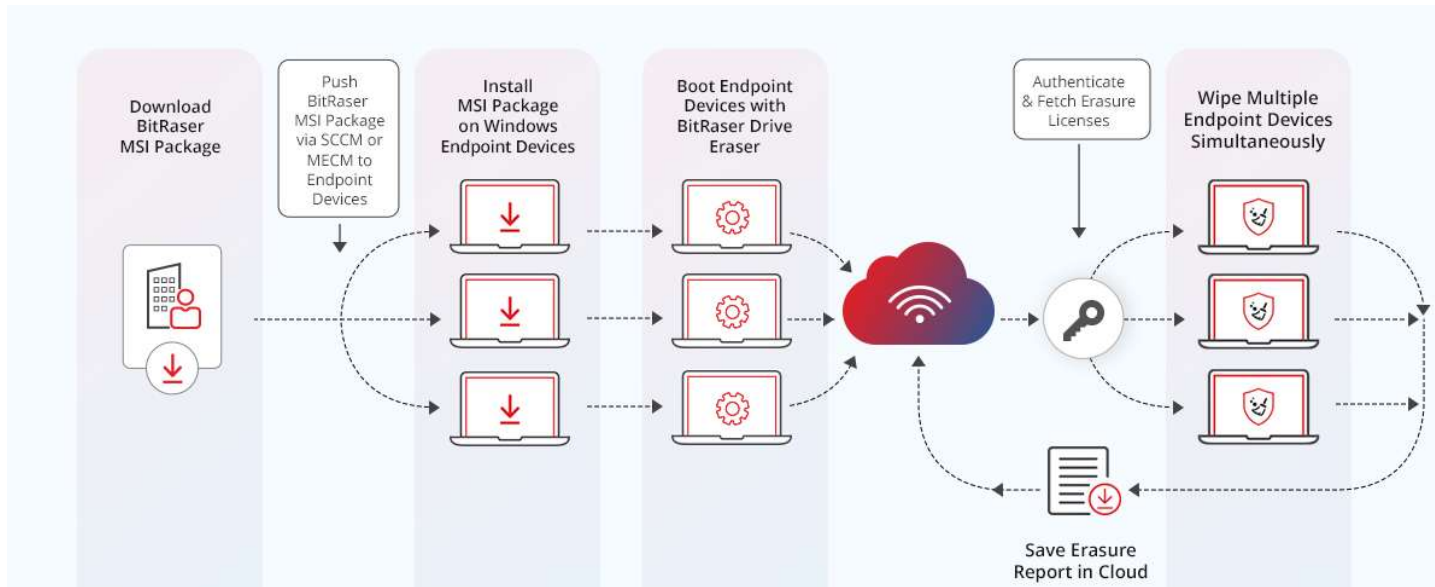


May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

How to Implement Remote Data Erasure?

Method 2: Remotely Wipe Windows Endpoint Devices Using SCCM



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser

Key Takeaways

- 1 Post-Pandemic Rise of Remote Work Amplifies Endpoint Data Security Challenges for Organizations
- 2 Importance of Onsite Data Destruction to Prevent Chain of Custody Risks
- 3 Traditional Data Destruction for Remote Workforce is Impractical due to Logistics, Security, Technology, Financial & Environmental Challenges
- 4 Remote Data Erasure helps Mitigate Data Breach Risks for Distributed Endpoint Devices. Helps organization meet ESG goals.



May 7-9, 2024 The M Resort  Las Vegas, NV

BitRaser