



Data Spill Cleanup & Optimizing Resources

Evolving from a Reactive to a Proactive Approach

WHITEPAPER

Overview

Cleaning up data spills is a critical and time-sensitive task for organizations handling data for national security. While preventing all data spills is nearly impossible, optimizing resources can still be an option to mitigate risk and reduce downtime. This whitepaper shows how embracing a proactive approach can significantly improve response time while minimizing the impact on productivity.

What Is a Data Spill?

Data has a frequent and troublesome habit of residing somewhere it shouldn't. In national security spaces, sensitive or classified data can end up in unauthorized locations. This is known as a Classified Message Incident (CMI) or 'data spill'.

Use Case: Classified Data Spills

As defined by the U.S. Military, "Classified Spills (also known as contaminations or classified message incidents) occur when classified data is introduced to an unclassified computer system or to a system accredited at a lower classification than the data."*

- File moved to wrong location
- Accidental email distribution
- Modified document containing 'Tracked Changes'
- Department of Defense classification change

*DSS ISFO Process Manual for C&A of Classified Systems under NISPOM

In the event of a data spill, clearing all endpoints affected by the incident is an urgent priority. The wiping process can target...

- Entire drives
Disk erasure tools get rid of all endpoint data by overwriting every sector. This cleans everything off the drive, including user files and operating system data.
- Selected files
Selective wiping can overwrite only specific files without needing to erase the entire hard drive. Selective wiping is a more efficient alternative to full disk wiping.

PROBLEM

Physical Distance from Affected Computers & Just One Endpoint at a Time

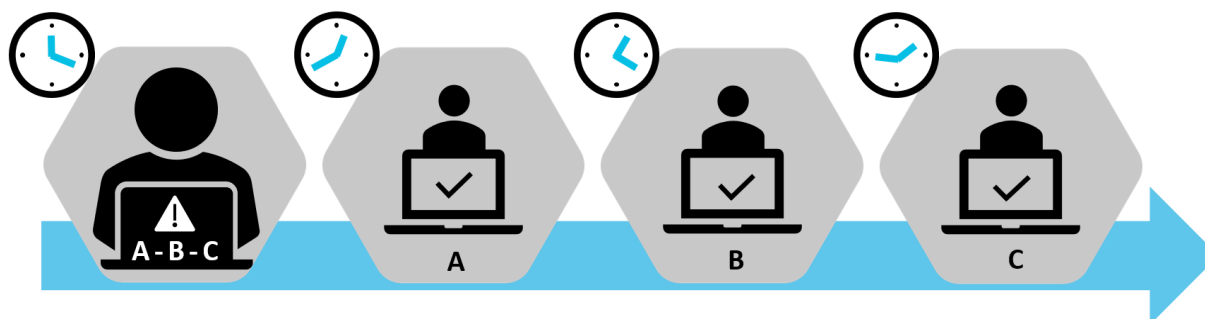
Responding to a data spill often involves five phases:

1. Identify affected computers
2. Take computers offline or isolate endpoints
3. Find temporary hardware replacements for personnel
4. Clean up files on each computer individually
5. Wipe free space (necessary on SSD)

Each phase of the reaction plan requires a considerable amount of resources – including, but not limited to, time and personnel.

Main concerns impacting productivity:

- **Logistical time** required to physically reach every affected computer
- Limitation of cleaning up **only a single endpoint** at a time – data spills typically affect multiple computers; common process includes running software, selecting files, monitoring wiping progress and collecting logs for reporting
- **Downtime** of end-users and inaccessible computers during clean up
- Time required to **wipe free space** (organizations may have terabytes of free space)

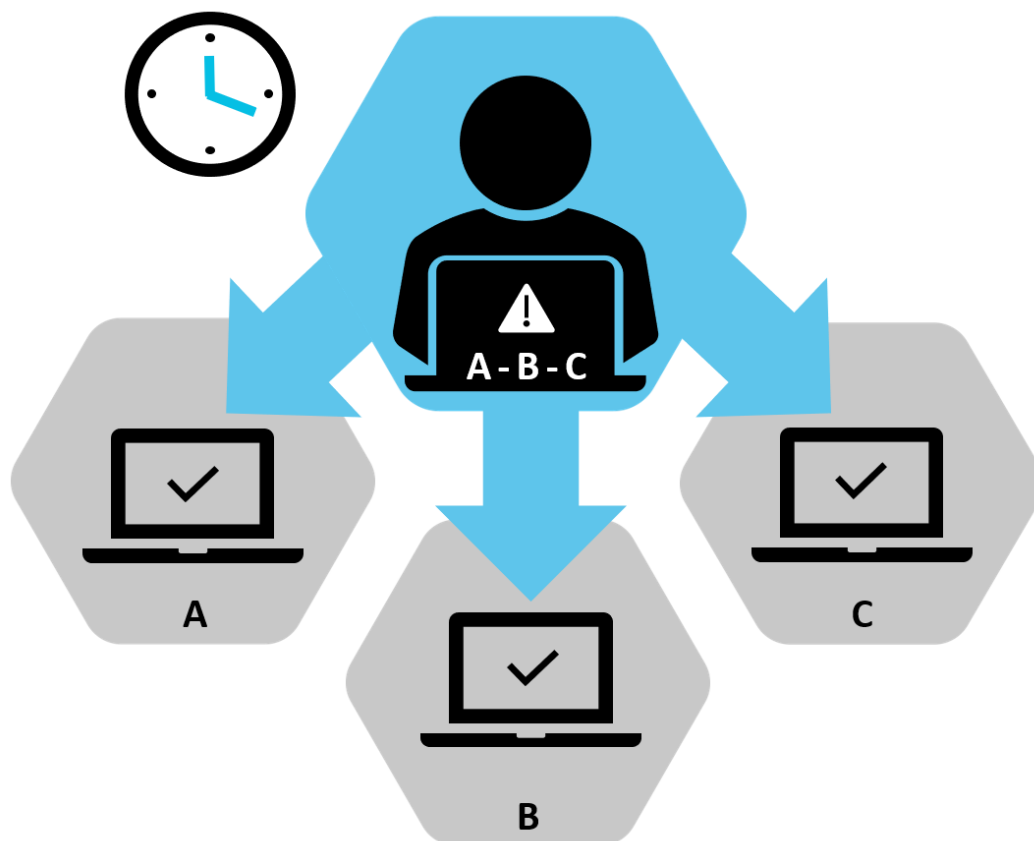


SOLUTION

Central Management of Wiping Tasks

The following solution evolves the approach to cleaning up data spills from reactive to proactive, based on implementing a wiping solution with central management capabilities.

This proactive approach significantly improves response time by removing the need to physically visit and clean up data spills on a single machine at a time.



Preparing for a Data Spill

To achieve the benefits of optimizing resources, a proactive approach requires preparation.

- Deploy wiping solution on all computers
Use a solution with central management to remotely deploy a selective wiping tool on all computers within your environment.
Benefit: Wiping software is ready to run immediately on all affected computers without requiring installation after contamination or demanding a physical visit from personnel in charge of handling the data spill.
- Create company-wide policy for managing free space
Wiping free space can be a time-consuming task – large sizes of free space take more time to overwrite. To minimize the time required for this operation, Admins can create a wiping policy that will clean and preserve a chosen portion of free space, reducing the size of available free space that would need cleaning in the future.
Benefit: Wipe free space in a controlled way in significantly less time – affected computers are available sooner and personnel get back to work faster.

Responding to a Data Spill

When a data spill occurs, the central management console – already used to deploy the wiping tool – enables Admins to clean up all affected computers simultaneously without needing to physically visit each one of them.

Steps for clean-up:

1. Block wiping options from local endpoints
End-users can cause problems intentionally or unintentionally. Data spills, for example, are often attributable to end-user error. Best practice is to block all local wiping options to avoid interference with the wiping task and prevent policy violations.
2. Create wiping task
The ad-hoc wiping task needs to target all files associated with the data spill followed by a free space wipe.
3. Select affected computers
Identify and select the computers affected by the data spill and assign the created wiping task.
4. Start wiping process
The wiping task can take effect immediately or be scheduled for a later time – including at logout or outside business hours to avoid impacting on productivity. It is recommended, however, to run the wiping task instantly to reduce exposure and prevent further spread of the data spill.
5. Monitor wiping task
Follow progress of the wiping task on all affected computers from the central management console. Wiping tasks and policies can be pushed from the central management console without end-user intervention.
6. Collect logs for reporting
Documenting proof of successful completion of the data spill clean-up is essential. The central management console generates reliable reporting.

BCWipe – Enterprise Edition

Trusted for over 15 years by the U.S. Defense and National Security community, Jetico's BCWipe is the de-facto standard for classified data spill clean-up, wiping selected files beyond forensic recovery.

BCWipe – Enterprise Edition comes with Jetico Central Manager to remotely deploy, control and monitor client software across all workstations using a simple web browser. 'Enforcer Mode' allows Admins to remotely wipe selected data, wipe free space and more – all without end-user intervention.



Contact Us

Phone (EU) +358 50 339 6388

Phone (US) 202 742 2901

sales@jetico.com