Data Spill Cleanup & Optimizing Resources

Evolving from a Reactive to a Proactive Approach

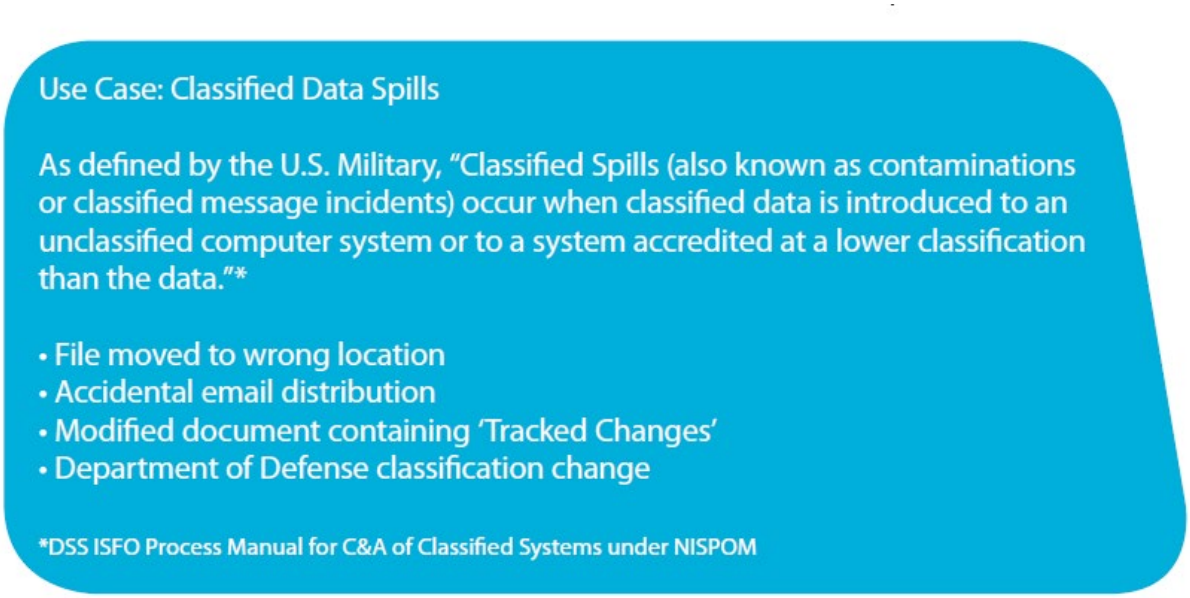
WHITEPAPER

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'.



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

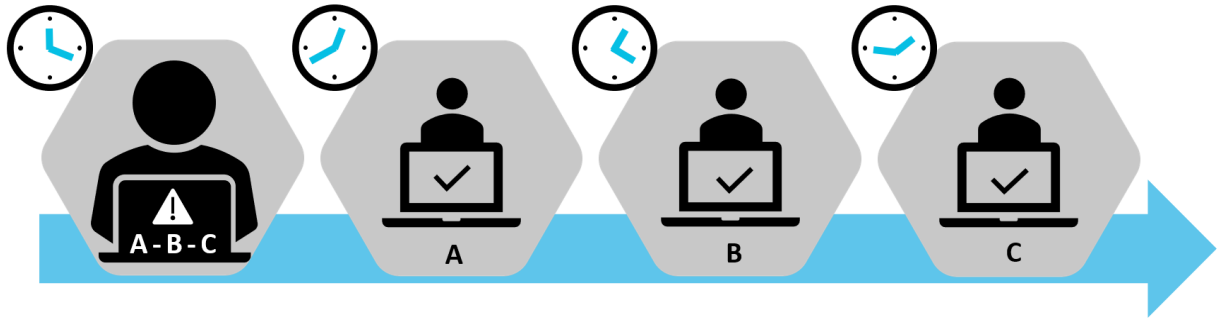
Responding to a data spill often involves five phases:

1. **Identify** affected computers
2. **Contain** the spill by taking computers offline or isolating endpoints
3. **Assess** the scope of the incident and find temporary hardware replacements for personnel
4. **Remediate** by securely erasing files on each affected computer; for SSDs, ensure free space is wiped to eliminate residual data
5. **Prevent** by analyzing the root cause and re-running data discovery scans to verify that all spilled data has been addressed

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

Main concerns impacting productivity:

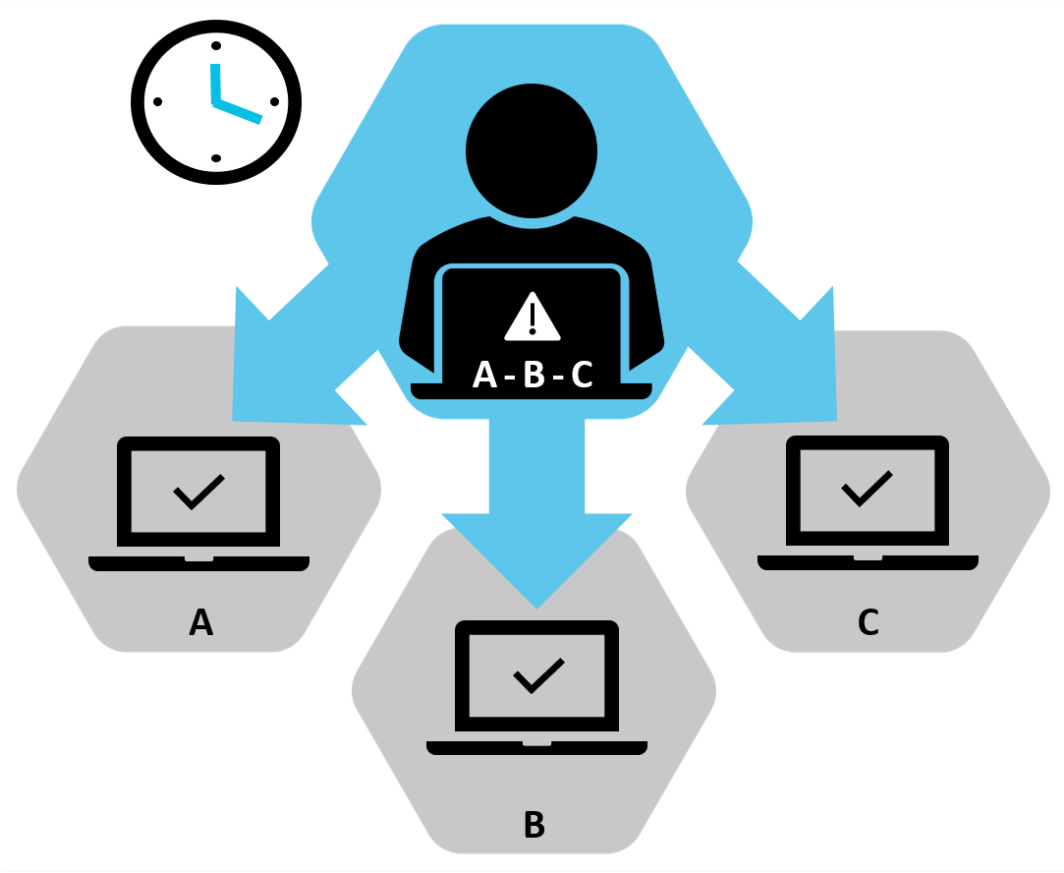
- **Identifying all spilled files** across the entire network, including similar or duplicate copies across local drives, shared folders and cloud storage
- **Logistical time** required to physically reach every affected computer
- Limitation of cleaning up **only a single endpoint** at a time – data 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. Block all local wiping options to avoid interference with the wiping task and prevent policy violations.

2. **Define Scope of Data Spill with a Data Discovery Tool**
   Use a data discovery tool to identify all files related to the spill across the organization. Analyze the search output to confirm the list of affected files. Select all relevant files on impacted computers to prepare them for wiping.
   Best practice: Rely on an integrated solution to avoid exporting or importing data, which may introduce errors or leave behind additional traces that must also be erased.

3. **Create & Assign Wiping Task**
   With the affected files selected, create an ad-hoc wiping task, including an option to wipe free space where applicable, and assign it to the affected computers.

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.
   Best practice: It is recommended 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.

7. **Re-Run Data Discovery to Verify Clean-Up**
   Re-run the latest scan to confirm all traces are removed and no new copies have surfaced. Generate a report to verify that no files matching the same filters were found.

Jetico

Complete Endpoint Data Protection

BCWipe – Enterprise Edition

Trusted for over 20 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.

Now enhanced with an integrated Search feature, BCWipe – Enterprise Edition becomes the first and only solution to combine advanced data discovery with military-grade wiping. This streamlines the entire response process and eliminates the need for external tools that increase complexity and risk.

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

Contact Us

Phone (EU) +358 50 339 6388

Phone (US) 202 742 2901

sales@jetico.com