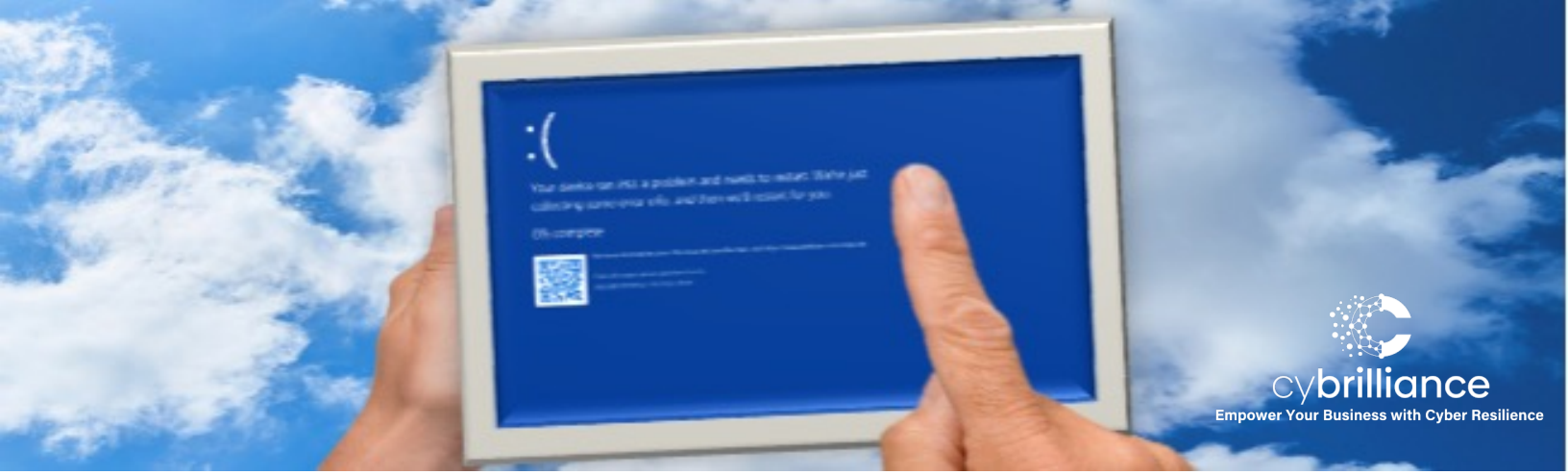

NeuShield
How much is your data worth?

Instant BSOD Recovery with NeuRestore

Microsoft would not normally allow software made by a third party company to have the kind of access that would be required to cause problems for the entire Windows operating system. This preventative measure is done to ensure any mistakes or malicious activity can be contained. In order to provide adequate protection to the entire system, certain security software is granted far greater system access than is normal.

What is BSOD?

Blue Screen errors (also sometimes called black screen errors or STOP code errors) can occur if a serious problem causes Windows to shut down or restart unexpectedly. You might see a message that says, "Windows has been shut down to prevent damage to your computer" or a similar message.

Kernel Driver Usage

Security products in the Windows ecosystem, commonly leverage kernel drivers as core components of a robust security offering.

Presence in the kernel offers rich visibility into system wide security-relevant activities, such as process and thread creation, or files being written, deleted and modified on disk.

CrowdStrike BSOD

The kernel allows software such as CrowdStrike drivers to enforce critical controls for its security product, such as inline prevention of malicious processes or blocking of malware files being written to disk.

CrowdStrike's kernel driver is loaded from an early phase of system boot to allow the sensor to observe and defend against malware that launches prior to user mode processes starting.

Incident

Unfortunately, an unexpected bad update of the CrowdStrike software caused an incident that blue screened the vast majority of CrowdStrike's 24,000 customers, affecting tens of thousands of devices.

Resolution

Microsoft developed three different device recovery processes for user and IT administrators to follow[1]. Each option anticipated that users may be confronted with differing device recovery needs, requiring them to either:

1. Identify and delete all occurrences of the bad file C-00000291*.sys, then restart the device.
2. Reboot the device into safe mode, then identify and delete all occurrences of the bad file C-00000291*.sys, then restart the device.
3. Perform a system restore to return the device to an operating levels prior to the date of the incident. Immaterial of option that was chosen the device always needed to be manually re-configured and rebooted by the user.

[1] - https://support.microsoft.com/en-gb/topic/kb5042421-crowdstrike-issue-impacting-windows-endpoints-causing-an-0x50-or-0x7e-error-message-on-a-blue-screen-b1c700e0-7317-4e95-aeee-5d67dd35b92f.

One Click Restore - NeuRestore

Organizations can simplify the recovery from any BSOD or faulty patching occurrence using NeuShield One-Click Restore (OCR). One-Click Restore (OCR) is included within NeuShield's core active data protection and instant recovery value propositions. In the event of a cyber or operational incident, the OCR feature provides instant recovery with a 'single click' to return the device operating system, applications and settings to a prior version.

When NeuShield Data Sentinel is implemented on a device, it installs a Driver in the same kernel area as that described with the CrowdStrike product. This ensures that the NeuShield patented technology protects all data under its control whether the data compromise is malicious (cyber attack) or unintended (user error or bad patching).

The ability of NeuShield to maintain multiple versions of all data types, OS, applications and data files, means that a clean version of data is always accessible on the device for recovery by the end user or IT administrator.

NeuRestore - Preparation

Check that NeuRestore is present in your current NeuShield bin subfolder.

NeuRestore has been available in the Business Edition since build 2275. A version is available in V3.0 preview build of NeuShield Datacenter Edition.

If your current version does not have NeuRestore, then copy the tool into: C:\Program Files\NeuShield\NeuShield Data Sentinel\bin\tools.

NeuShield Data Sentinel must be operational on all affected devices.

When an incident occurs, NeuShield Data Sentinel must have been operational on all affected devices to utilize the NeuRestore tool.

NeuRestore cannot be used on devices that did not have NeuShield Data Sentinel installed.

IT administrators should utilize the Microsoft tool to create a standard recovery disc/USB.

As a proactive policy, IT administrators should utilize the Microsoft tool to create a standard recovery disc/USB from the system files present on the device at that point.

If made readily available to the IT team (and updated after major patch updates), this proactive move would ensure an accelerated recovery and restoration of devices.

NeuRestore - Recovery

Step 1
Start Recovery

A: Boot up to the built-in recovery environment that already exists in the Windows install on the device. If the device is unbootable then it will probably boot into the recovery environment automatically.
Or
B: In exceptional circumstances where you need to rebuild the OS, insert the recovery disc/USB drive on the affected device and boot to a recovery disc.

Step 2
NeuRestore Tool

1: Go to the command prompt in the recovery environment (Troubleshoot\Advanced Options\Command Prompt).

2: Go to the NeuShield folder that contains the NeuRestore tool. (e.g. **cd /d c:\program files\neushield\neushield data sentinel\bin\tools**).

3: Type the command to run the tool –e.g. **start neurestore.exe**

4: At this point, the user selects their preferred NeuShield restore point and then One-Click Restore executes and restores the version of the operating system, applications and system settings that were running prior to the incident.

Step 3
Recovery Complete

1: When the recovery is completed the recovery tool will take the IT administrator back to the command line tool.

2: Clicking the '**x**' on the command prompt tool to exit and then select '**Continue**' to complete the reboot operation for your windows environment.