Executive summary: using BufferZone™ to prevent the next *Target Credit Card Breach*

The Point-Of-Sale vulnerability

Point-Of-Sale (POS) application is typically a standard process, running on a dedicated or a shared PC (with other non-related applications). It may be connected to the Internet directly or to a local server in the same location (typically a store).

Possible POS vectors of attack

- Through an infected PC in the same network
- Through an infected removable media inserted to the POS be it Intentional or Unintentional
- Through an infection occurring while browsing the Internet from the POS itself

BufferZone™ solution

BufferZone™ Isolates programs originating from untrusted sources (Removable Media/internal or external network) and prevents it from accessing / modifying trusted local PC resources (e.g. POS process, disk, registry)

The POS Process is considered Trusted, and runs isolated from external sources. Once BufferZone™ isolates the untrusted program from the Trusted POS process, it secures the POS by the following:

- BufferZone™ Memory Isolation prevents access to the POS user mode process, and prevents access to its memory by Untrusted processes (Memory Scrapping)
- BufferZone™ Removable Device Protection prevents infections through removable devices; Only POS Vendor Digitally signed files could be copied from Removable Media to the POS PC:
    - Unintentional execution of malware or installing a tampered package will not be possible, and will only be allowed to run in BufferZone™'s virtual container.
    - Intentional copying of (any) code, (NOT signed by POS vendor digital signature) will only be allowed to run in BufferZone™'s virtual container .
- BufferZone™ protects against unauthorized network and TCP connections to and from the POS to the Malware Command and Control (C&C) by Activating BufferZone™ Network Isolation.
    - Isolates the POS from unnecessary/unauthorized connections
    - Prevents data upload to malware C&C – in some cases, as unauthorized processes will not have access to the Internet, while the POS will.

*"What happens in **BufferZone™**, stays in **BufferZone™**"*