**Sandboxes and Application Isolation**

**An isolated environment for running apps or code**

A virtual container to keep the contents confined to the sandbox

Used for high-risk applications such as those that interact with untrusted sources like browsers or email clients

Although, all sandboxes have exploits or holes too

* So, it is necessary to add additional sandboxes on top of already implemented security services to plug those holes
* Exploits are prepared for the sandbox it expects i.e., chromium sandboxes, however they will struggle o bypass unexpected sandboxes that are manually added

**BufferZone**

* A sandbox that allows for easy security
* Any ransomware picked-up by something like a phishing attack via email will be handled by BufferZone
* A word document containing a macro virus will be opened in the BufferZone container (Sandbox) and the malware will only have access to the copy files
* BufferZone is also separate from the network, so the malware can’t escape to other devices
* To remove the malware, just empty the container

**Shadow Defender**

* Can run system in virtual environment   
  (shadow mode)
* Redirects each system change to a virtual environment instead of the real physical environment

**Depp Freeze**

* Kernel level driver that protects hard drive integrity by redirecting information written to the hard drive or partition, leaving the original data intact
* The redirected info is no longer referenced pone the computer is restarted
* Thus restoring the computer to the original state
* Every time you restart your computer, itll return to the exact same state
  + No level of protection until the reboot is done though, malware will remain active until reboot

**Returnil**

* Uses virtual environment and will return to machine original state when rebooted

**BitDefender**

* Limited functionality browser that provides sandboxing

Sandboxie