Executive summary: using BufferZone™ for VDI (Protecting *Virtual Desktop Infrastructure)*

VDI

VDI empowers you to deploy remote desktop services architectures that provide employees the flexibility to work anywhere, while allowing them to seamlessly access their corporate windows desktop or application environment running in the datacenter from a range of devices. The features and unified management infrastructure for centralized desktops, combined with application and user state virtualization technologies, increases flexibility of access for remote desktops and applications, delivering personalized, consistent, and secure experiences for users, while also improving compliance through centralized control and access to confidential data.

VDI facilitates optimal use of hardware by enabling access to multiple Windows environments (Dev—Test, Business—Personal) from the same client device. They also enable organizations to pursue “Bring Your Own Device Programs” for employees, where they use their personally owned hardware for both personal and work. This helps IT to keep the corporate environment secure even when it is accessed from unmanaged devices.

BufferZone™ for VDI solution

- VDI client sessions are prone for infection in a similar way to standard desktop environment: Each client session may be protected by conventional security measures (e.g. local Anti- Virus/End point Security Suite) it is still exposed to common modern attack.
- Once a client session is infected, a potential breach to the entire organization occur, and the infection may spread across other VDI sessions, eventually infiltrating the organization back end system.
- BufferZone for VDI provides an additional level of security for each client session in the same way it protects standard desktop activities:
    - BufferZone wraps around all defined internet activities, creating an isolated environment within the VDI session for potentially hazardous activities.
    - Any infection remains inside the BufferZone and will not infect the VDI session, thus preventing the spread of the malicious code.

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

VDI20140115.2