BUFFERZONE

www.bufferzonesecurity.com

BUFFERZONE® Endpoint Agent

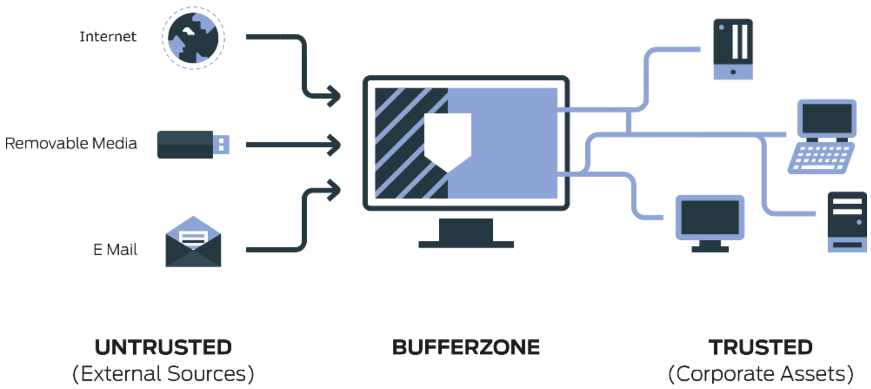
The Old Way: A Losing Battle

For years, cybercriminals have been playing a game of cops and robbers, with the criminals usually staying one step ahead. There's always another type of malware or evasion technique on the horizon. Much of the security industry now realizes that it's time to move away from security that's based purely upon discovery and detection.

Changing the Paradigm

BUFFERZONE endpoint isolation and containment keeps access to external, untrusted content such as unknown internet sites or removable media in a virtual container, along with processes started by those sessions and anything they save or download. Contained processes cannot reach the native endpoint or organizational resources such as an intranet; those are accessed only by uncontained browsing sessions and applications, which can't have accessed untrusted sites.

The advantage of this approach is clear: When malware strikes, no matter how new it is and what evasion techniques it implements – it cannot cause any damage to native endpoint or organizational resources. And, the container is periodically emptied, so even there malware can't last.



Key Features

BUFFERZONE features:

- **Virtual container**: Secure environment for accessing risky sources including websites, removable media and email.
- **BUFFERZONE viewer**: View a wide range of document and media types without removing them from the container.
- **Secure Bridge:** When needed, use CDR to disarm and extract data from the container.
- **Proxy passport**: BUFFERZONE can digitally sign contained and uncontained browser sessions, enabling your organizational proxy to allow only contained sessions to access the internet.
- **DLP**: To support Data Loss Prevention, hide valuable files from the container, and block uploading or copying from outside the container.
- **High-performance, small footprint**: The BUFFERZONE agent is lightweight and is supported on a wide range of endpoint hardware.

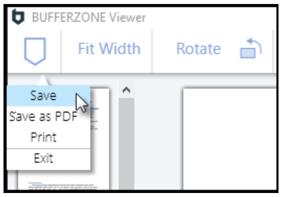
Business Continuity

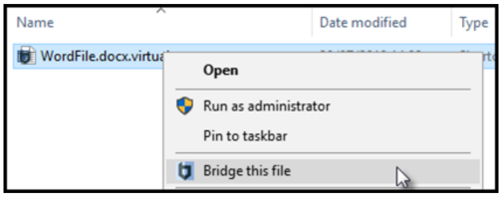
For when users do need to keep downloaded files or use them in trusted environments, you can deploy BUFFERZONE Secure Bridge (see separate data sheet) for Content Disarm & Reconstruction (CDR). With Secure Bridge, users can disarm downloaded files to securely extract them from the container. BUFFERZONE includes an integrated CDR solution, or you can integrate with your own deployed disarming service.

Seamless User Experience

The BUFFERZONE agent manages switching between contained and uncontained browser instances according to accessed sites. Several management paradigms are available (see *Zone Management* below).

The versatile BUFFERZONE Viewer displays contained files (downloads), supporting a wide range of document and media file types. For uncontained editing or long-term use and distribution, users can intuitively click 'Save' to bridge the original file or create a PDF. Additionally, on agent endpoints, users can Bridge contained files from the File Explorer:

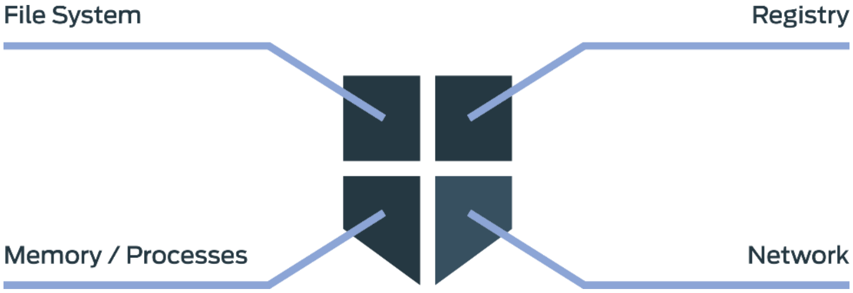




How it Works

The BUFFERZONE agent creates a virtual container on endpoints, isolated from the endpoint operating system's native resources. The agent keeps untrusted application processes in the container and trusted application processes outside the container. Only authorized processes are allowed in the container.

The container isolates the following system resources:



Network access isolation (optional) prevents uncontained applications from accessing untrusted destinations such as the internet, and prevents contained applications from accessing trusted IP ranges of organizational network destinations.

BUFFERZONE patented containment technology is transparent to contained applications, providing them with read-only access to native files and registry by using a kernel driver that resides in the operating system kernel. The driver transparently monitors application-level I/O requests, allowing read access to native resources but directing write actions (and subsequent read actions to the new content) to the container in a different disk area.

Zone Management

BUFFERZONE provides several ways to manage browser containment (IE, Chrome) in your organization:

- **Site list**: Configure a list of trusted URLs; browsing sessions to all other sites are contained. Zone switch is automatic, requiring no user intervention. Optionally also configure Neutral sites to be accessed in any current zone.
- **Proxy control**: Upon trying to traverse the organizational perimeter proxy to the internet, users are prompted to opt-in to browser containment. Browsing sessions are digitally signed by BUFFERZONE and the proxy allows only contained sessions.
- **Network separation**: Configure trusted IP ranges; users are prompted to opt-in to browser containment in order to access untrusted addresses.

System Requirements

- **OS**:
  Win 7 Enterprise 7601 SP1, 64-bit
  Win 10 Enterprise 64-bit, builds 1507, 1511, 1607, 1703, 1709
- **Processor**: As OS requirements
- **RAM**: As OS requirements
- **Disk**: 500 MB (agent) + 2 GB (recommended) for contained files

Supported Applications

The following applications are supported for containment:

- **Internet Explorer**, **Chrome**: Full containment and zone management
- **BUFFERZONE Viewer**: Displays a wide range of contained document and media file types
- **MS Office & other applications**: On request

Centralized Management

Centralized containment policy and agent deployment can be managed by:

- **BUFFERZONE Management Server** (BZMS; recommended)
- McAfee ePO (certified)
- Microsoft GPO

Centralized, Policy-Based Management

For centralized containment policy management and agent deployment, you can integrate BUFFERZONE with existing endpoint management systems (for example, McAfee ePO); or, for complete management capabilities, use the BUFFERZONE Management Server (BZMS – see separate data sheet) to manage BUFFERZONE agents across your organizational network, to gain visibility to relevant organizational endpoints, and to assign organizational policy by endpoint and/or user.