Lenovo

ThinkShield

BUFFERZONE

BUFFERZONE® Safe Workspace™ Enterprise

Introducing Source-Based Containment and Disarming

With source-based auto-containment and disarming, BUFFERZONE Safe Workspace™ intelligently manages endpoint agent containment and disarming decisions, according to configurable organizational policy. This creates a safe workspace for organizational users, inside and outside the organizational network.

The Safe Workspace™ agent is an advanced solution for endpoint protection. Content from untrusted sources is kept in a virtual container, protecting trusted resources from any potential threats. See separate *BUFFERZONE* Safe Workspace™ data sheet.

Depending on source type, Safe Workspace™ determines whether to consider it untrusted or internal. Untrusted sources, such as general internet sites, removable media, and email messages from non-organizational senders are contained; internal resources are isolated from contained processes and data.

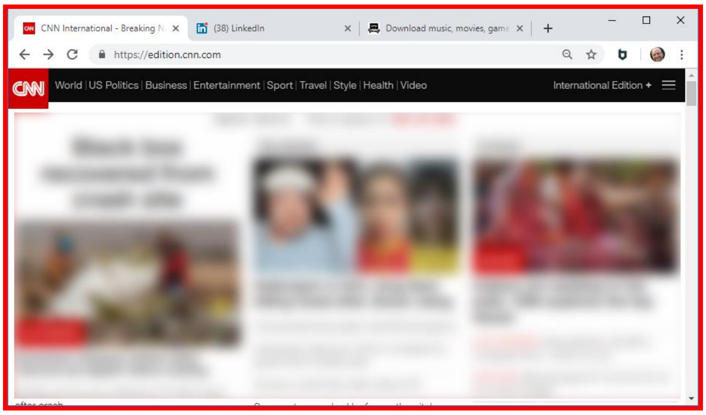
For ingesting data from container, Safe Workspace™ includes SafeBridge®. SafeBridge® performs Content Disarm & Reconstruction (CDR), disarming data of risky components (for example, Office file macros) and securely allowing the disarmed content out of the container. Organizational policy can have SafeBridge® activated automatically, or just allow manual bridging.

In Safe Workspace™ Enterprise edition, organizations can configure multiple policies of containment criteria to apply to different endpoint groups.

Safe Browsing

Safe Browsing can be user-controlled, or Safe Workspace™ can manage automatic zone switching between contained browsing sessions to untrusted sites and uncontained sessions to trusted sites. At untrusted sites, the browser instance process and any downloads are contained.

To make endpoint users aware of the environment they are working in, contained browser windows are marked. Marking is configurable; default behavior is a red border:


CNN International - Breaking N
(38) LinkedIn
Download music, movies, game
https://edition.cnn.com
CNN
World | US Politics | Business | Entertainment | Sport | Travel | Style | Health | Video
International Edition +

Downloaded, contained files appear in Windows File Explorer only in the secure BUFFERZONE folder (unless Auto Bridge is enabled). When opened, document and media files are securely displayed in the versatile BUFFERZONE Viewer / Editor, from where they can be securely bridged out of the container or saved as PDF. According to policy, Office applications may be contained instead.

Switching between zones can be automatic, or Safe Workspace™ can prompt users to switch.

You can centrally configure zone switching to be managed in any one of the following ways:

- **Site lists**: Configure a list of Trusted site URLs (for example, organizational intranet sites), and optionally of Neutral sites (for example, an IdP - Identity Provider). Unlisted sites are considered untrusted.
- **Passport**: Safe Workspace™ signs outbound connections as contained or uncontained, and your organizational proxy blocks uncontained connections to untrusted areas and contained connections to trusted areas. Upon block by the proxy, the agent triggers a zone switch.
- **Network separation**: Configure firewall-style access rules for outbound connections. Being blocked by network separation triggers a zone switch.

Key Features

Safe Workspace™Enterprise features:

- Containment of untrusted sites
- Automatic zone switch or user prompt
- Trust zone management by site list, proxy passport, or network separation
- Centralized organizational policy management and agent deployment
- Safe Mail
- Safe External sources

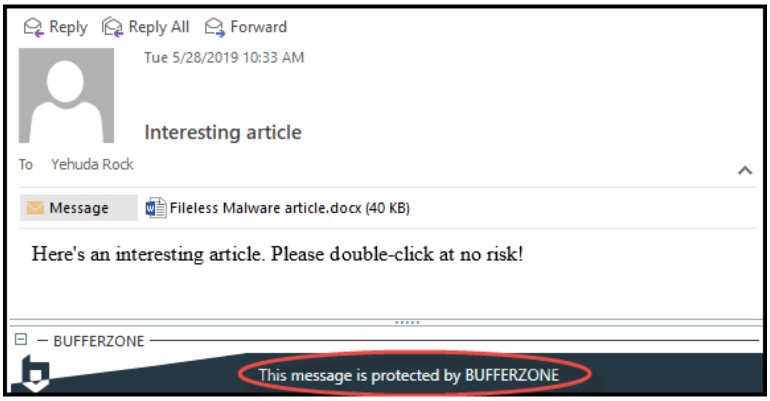
Safe Mail

Safe Workspace™ Safe Mail disarms Outlook email messages arriving from untrusted sources and contains their attachments, protecting the endpoint and trusted organizational resources from possible malware in messages and in attachments.

Disarming includes rendering inline images as HTML and blocking other inline attachments. Regular attachments are treated the same way as contained browser downloads.

For Safe Mail, configure your organizational mail server (Exchange or Exchange Online) to identify and mark (with a message header) untrusted email messages (for example, those arriving from outside the organization); on the endpoint, Safe Workspace™ will disarm only those and contain their attachments.

In Outlook, untrusted messages include an informative message:



Tue 5/28/2019 10:33 AM

Interesting article

To Yehuda Rock

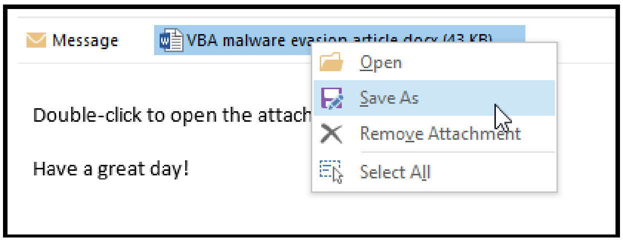
Message Fileless Malware article.docx (40 KB)

Here's an interesting article. Please double-click at no risk!

BUFFERZONE

This message is protected by BUFFERZONE

The message body is disarmed, and double-clicking an attachment opens it in the BUFFERZONE Viewer / Editor. Or, users can right-click > Save As to bridge an attachment:



Message VBA malware evasion article.docx (43 KB)

Double-click to open the attach

Have a great day!

To protect the organization, outgoing attachments can optionally be blocked or automatically disarmed, according to policy.

Safe Externals: Removable Devices and Network Shares

External file sources such as removable media (CDs and USB drives) should generally not be trusted. In addition, your organization may have a network location designated for untrusted content (for example, for sharing with external business partners).

You can contain endpoint access to these sources, preventing any malware that might be present from affecting native endpoint resources.