BUFFERZONE

SAFE WORKSPACE®

In an age where perfect detection is a myth and ransomware and data-stealing malware attacks are rampant, it is time to rethink endpoint cybersecurity.

Endpoint security should be easy, private, intuitive, and affordable.

Meet the BUFFERZONE® Safe Workspace® security suite.

PROTECTIONS

Safe Browser: Anti-malware

Robust, proactive zero-trust protection from malicious browser-based attacks, including drive-by malware and downloads, including zero-days, trojans and ransomware.

Proactive containment and disarming avoids the pitfalls of relying on error-prone detection.

Safe Browser: Anti-phishing

Intelligently combines multiple information sources and detection criteria with AI-based learning to determine if visited sites might be masquerading as reputable sites to steal submitted information, preventing phishing attacks.

Unlike similar products, entails minimal network latency and ensures user data privacy.

Safe Removables

Eliminates security weak points by providing secure, zero-trust seamless access to files on external devices (USB / CD/DVD).

Also available for designated network locations or drives (Enterprise edition)

Safe Mail (MS Outlook)

Transforms email security with proactive zero-trust defense against malicious messages and attachments.

Web-based email such as Gmail and Office 365 are covered by Safe Browser.

BUFFERZONE

SAFE WORKSPACE®

TECHNOLOGIES

To provide its unique set of protections (see previous page), BUFFERZONE Safe Workspace® incorporates and utilizes the following technologies.

The exact configuration and combination of the technologies depends on the protection, and in the Safe Workspace® Enterprise edition is organizationally configurable.

BUFFERZONE® SafeBridge® skillfully disarms content of risky components, preserving data content integrity while nullifying threats.

SafeBridge® can work locally, to avoid reliance on cloud submissions and network; or, with the Enterprise edition can integrate with third-party providers for analysis and disarming.

The **BUFFERZONE® container** provides application and data isolation, proactively preventing risky sources from harming the endpoint, until content is disarmed and securely removed from the container.

BUFFERZONE® NoCloud™ phishing detection shifts the paradigm in data security by combining multiple information sources and detection criteria with AI-based machine learning to reliably identify phishing attacks.

NoCloud™ phishing detection leverages next-generation CPU/NPU (Neural Processing Unit) acceleration to perform local processing, thus minimizing network latency and maximizing user privacy.

www.buffer.zone

BUFFERZONE

SAFE WORKSPACE®

EDITIONS

Safe Workspace® is available in these editions:

Pro: For home and professional users, individually or in organizations. Users have control of protections as licensed. Available from our partner Lenovo .

Enterprise: Enables organizations to deploy, enforce and configure, as licensed centrally.

The following Safe Workspace® features are available per edition. Pro included protections depend on licensing and on user enablement; Enterprise included features depend on licensing and organizational policy configuration.

Feature	*Pro*	*Enterprise*
Safe Browser Anti-malware: Browser process and downloads containment	✓	✓
Safe Browser Anti-phishing: Identify and prevent web-based phishing attacks, including NoCloud™ acceleration	✓	✗
Safe Mail: Outlook secured messages and download containment	✓	✓
Safe Removables: Containment of files from USB / CD / DVD	✓	✓
SafeBridge®: Disarm contained data files (documents and media) of risky components, and securely uncontain the file	✓	✓
Autobridge: Automatic disarming and uncontaining of contained files (downloads, attachments etc.)	✓	✓
Full user control: Users can suspend any protections	✓	✗
Safe Network Shares: Containment of files from designated network share	✗	✓
Zone switching: Automatic browser containment decision by site list, organizational proxy, or IP ranges	✗	✓
Central deployment	✗	✓
Central policy configuration, assignment, and enforcement	✗	✓
MSSP environment and user separation	✗	✓
Network separation: Separate endpoint firewall for contained / uncontained applications	✗	✓
BUFFERZONE® Viewer/Editor: Contained (unbridged) document and media access	✗	✓
MFA: Endpoint multi-factor authentication	✗	✓
Clipboard isolation	✗	✓
Central log collection	✗	✓

www.buffer.zone