BUFFERZONE®
Advanced Endpoint Security

Enterprise Endpoint Containment & Isolation with CDR Bridging

BUFFERZONE defends endpoints against a wide range of known and unknown threats with a patented containment & isolation solution, including CDR (Content Disarm & Reconstruction) for file bridging. Employees enjoy frictionless access to the internet, email and removable storage, without risk to the endpoint and enterprise.

The Challenge

For years, cybercriminals and the cyber security establishment have been playing a kind of game of cops and robbers, with the criminals usually staying one step ahead. Any time security software begins being able to identify new malware types and protecting against them, the hackers introduce a new evasion technique designed to circumvent the security products.

Once a malware package is identified, it can be caught by classical signature-based antivirus and antimalware detection-based tools. However, changes to malware packages easily and routinely circumvent these tools, creating significant delays between the introduction of new malware and the implementation of protection from it. During this gap, endpoints and organizations are vulnerable.

In an attempt to meet this challenge, organizations implement analysis tools that attempt to identify new, previously unknown malware before it causes damage.

One type of analysis that is used to identify malware is static analysis of a file's content. Static analysis inspects actual code lines found in files without actually running the code, and tries to understand what the file could potentially do.

However, for many suspicious files, only binaries are available, not readable code; even when code lines are available to scanners, malware writers employ various techniques to evade static analysis by automated inspection solutions. These include:

- Password protection (with the password supplied in an independent component of a socially-engineered communication)
- Code obfuscation
- Offloading actual malicious payloads to packages that are downloaded and/or called by initially activated files and documents, sometimes in a chain of several stages involving different files, some of which may be binaries, that are not easily analyzed

This makes it difficult for automated analysis tools to understand the code's full scope of activity. These limitations are the reason that static analysis results are often limited to technical details such as metadata, hashes, etc. and do not provide actual full understanding of files' potential effects.

To complement static analysis, or as an alternative, organizations make use of dynamic analysis tools. These tools actually run suspicious files, in secure, isolated environments – sandboxes – to test their effects. Various sandbox solutions provide cloud-based or on-premise automated analysis, enabling organizational systems to submit suspicious files for analysis. Dynamic analysis, while more difficult to implement, has a significant advantage over static analysis: it doesn't require error-prone analysis of complex and intentionally obfuscated code, since it's only interested in actual results of running the files under analysis.

However, cybercriminals have successfully introduced techniques that evade dynamic analysis as well, such as:

- Password-protection
- Various techniques for fingerprinting sandbox environments, avoiding running in those environments

- Stalling techniques, such as calling looped sleep functions or other looped benign commands to delay the malicious activity, fooling the analysis systems into thinking that the macro has already finished its activity
- Triggering malware execution on the malicious document being closed rather than on its being accessed

As these evasion techniques are developed by cybercriminals, various security products react by introducing appropriate countermeasures, eventually closing some of the gaps. Competing security vendors announce their evasion countermeasures as they implement them, hoping to convince security-conscious consumers to prefer their products.

If there's one thing that this constant cat-and-mouse game illustrates, it's that there's always another new type of malware or evasion technique on the horizon that security vendors haven't thought of yet. It is this situation that has brought about the realization that it's time to change our way of thinking and adopt a new security model, moving away from security that's based purely upon discovery and detection.

Even with the best perimeter and internal defenses, malware is getting through and is infecting user endpoints – the largest and most vulnerable attack surface in the organization. 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. It is now widely agreed that organizations must take a layered approach to protecting their networks and data.

Some organizations attempt to mitigate threats by restricting users' access to the internet and to risky applications. However, user restriction is, and will remain, an uphill battle. Internet, social media, email and removable storage are essential to business today, and organizations that try to limit access inevitably impact productivity as well as employee satisfaction. And since lists of dangerous sites and sources are constantly changing, it is impossible to maintain a foolproof access policy.

Changing the Paradigm

It's simply not possible to detect every threat. It is equally impossible to control human behavior - and the more restrictive and inconvenient the security control, the more likely users are to circumvent it. Given these realities, the key to keeping the organization safe without restricting employees is containment and isolation.

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.

From Theory to Reality

This sounds great in theory, but how to put it into practice? The following are some methods used by various solutions in the market; in the next section we'll introduce BUFFERZONE's solution.

Browser-only containment: Some solutions provide containment as a browser option. This can achieve a high level of protective isolation for risky sites. However, this solution is limited to a specific browser, while other browsers, not to mention other applications, or access to removable media, are

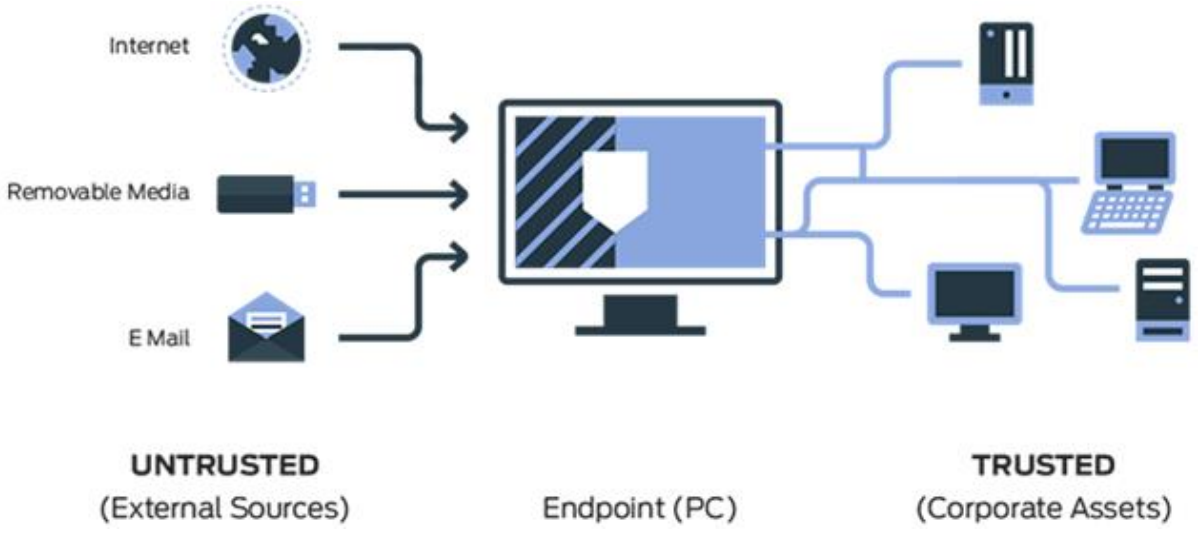
not protected. Securely downloading files and content for use in other applications are not supported; instead, the vendors recommend creating PDFs. In addition, for the solutions of this type that we're familiar with, system requirements are rather high.

Full VM: Another solution implements a full hypervisor to endpoints, with an independent, isolated guest VM complete with OS for each trust zone. A single user-level desktop environment unifies the environments. This type of solution may be expected to provide a high level of security, but performance impact is likely to be significant. Endpoints need to provide the necessary resources for a full hypervisor and multiple OS instances.

Per-task containment: Another available solution implements for each and every untrusted file task an ad-hoc, non-persistent guest virtual machine (VM). This effectively prevents potentially risky files from being able to cause damage to the host endpoint or to organizational resources. On the downside, because an independent VM is deployed per-file, including an independent copy of the host operating system, significant resources are consumed, resulting in some non-trivial performance impact and endpoint requirements. The need to provide the VMs with independent copies of the host OS may also create significant system management, configuration, and licensing challenges.

BUFFERZONE Solution Overview

Then there's **BUFFERZONE**. BUFFERZONE deploys a lightweight endpoint agent that creates a single virtualized container on top of the host OS. Processes that could access external, untrusted sources such as the internet or removable media are kept in the container, along with any data they download or save. At the same time, contained processes cannot reach native endpoint or organizational resources, and so can't inflict any lasting damage. Browsing sessions are directed into or out of the container according to whether the site is trusted or not; any files that are downloaded or saved from untrusted locations (including, for example, removable devices) are automatically contained, so that when they're eventually accessed, the opening process is contained as well. Periodically, the container is wiped clean along with any possible malware.



BUFFERZONE agents and the BUFFERZONE container have an extremely small performance impact, and are supported on Windows 7 and above (32/64 bit) on any PC, laptop or MS Surface tablet with any processor and hardware configuration supported for the OS.

With patented containment and bridging technologies, BUFFERZONE protects organizations from a wide range of threats. Instead of blocking access, BUFFERZONE keeps content that arrives from web browsers, email and removable storage in a secure, isolated virtual container.

For when users do need to move content out of the container, BUFFERZONE includes Secure Bridge: Content Disarm & Reconstruction (CDR) for securely transferring data from the isolated environment to trusted areas of the endpoint and the corporate network.

BUFFERZONE records logs for file and registry operation, and for process, system, network, and RPC events. These logs can be automatically sent to organizational SIEM / Syslog systems, providing critical intelligence for enterprise-wide security analytics to enable correlation of high-risk events.

BUFFERZONE maximizes user productivity with seamless, unrestricted access to information and media sources, while empowering IT with a simple, lightweight, centrally managed, and enforceable solution for thousands of endpoints within and beyond the corporate network.

BUFFERZONE is a cost-effective solution with a very small footprint and little impact on endpoint performance. Once policies are configured and agents are distributed to endpoints, BUFFERZONE requires little ongoing management, resulting in very low total cost of ownership for the organization.

BUFFERZONE's advanced endpoint security solution features:

- **Virtual container:** A secure, isolated environment for accessing content from any risky source 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:** Use CDR (content disarm & reconstruction) to securely extract data from the container, enabling collaboration between people and systems while ensuring security and compliance.
- **Proxy passport**: BUFFERZONE can digitally sign contained and uncontained browser sessions, enabling your organizational proxy to allow only contained sessions to access the internet.
- **Upload blocker**: As part of an organizational DLP strategy, restrict browser uploads to be only from an isolated location that can't have any data from uncontained, internal sources.
- **High-performance, small footprint**: The BUFFERZONE agent is lightweight and is supported on a wide range of endpoint hardware.
- **Centralized, policy-based management**: Centralized containment policy and agent deployment can be managed by the BUFFERZONE Management Server (BZMS; recommended), by McAfee ePO (certified), or by other endpoint distribution systems such as Microsoft GPO
- **Endpoint intelligence:** Detailed reporting and integration with SIEM and Big Data analytics to identify targeted attacks.

How it Works

The BUFFERZONE agent creates a virtual container (sandbox) 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.

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.

As a result, any harm inflicted by malware is completely sealed off in the virtual environment. Neither the endpoint nor organizational networks are infected. New threats with unpredictable behavior are contained just as effectively as known malware.

Separating Trust Zones

BUFFERZONE provides a secure, virtual environment for accessing risky content. For monitorable web browsers (IE and Chrome), centrally-managed policies define trusted and untrusted zones, to keep them separate. For example, a SharePoint server, organizational intranets and cloud-based organizational storage can be defined as trusted. When users visit the trusted zone, their browsers open outside the container, so any files that might be uploaded cannot be from trusted sources.

BUFFERZONE provides several ways to manage browser containment zones in your organization:

- **Site list**: Manually 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; the block message from the proxy triggers the BUFFERZONE prompt.

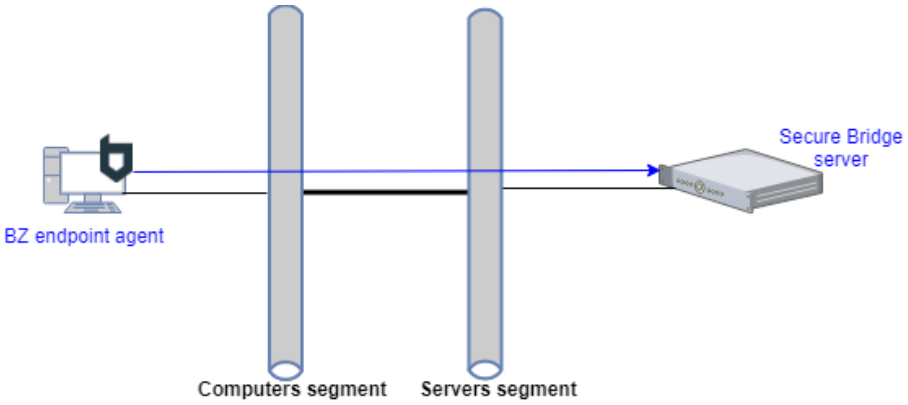
- **Network separation**: Configure trusted IP ranges; users are prompted to opt-in to browser containment in order to access untrusted addresses.

Secure Bridge CDR

Experience has shown that most of the time, it is not necessary to remove files or data from the container. Users can freely save and reopen files any time, within the container, without risk to the organization. However, sometimes it is necessary to transfer downloaded files to other parts of the organization; or, users may need to edit files in applications not supported in the container. For this purpose, BUFFERZONE includes Secure Bridge: Content Disarm & Reconstruction (CDR) for securely transferring data from the isolated environment to trusted areas of the endpoint and the corporate network.

BUFFERZONE includes an integrated CDR module, or you can use your own deployed disarming service for data reconstruction, multi virus scanning, and/or malware detection as needed.

With Secure Bridge, the BUFFERZONE agent transparently submits data to the Secure Bridge server, and, upon response indicating readiness, downloads the disarmed file. All communications are secured.

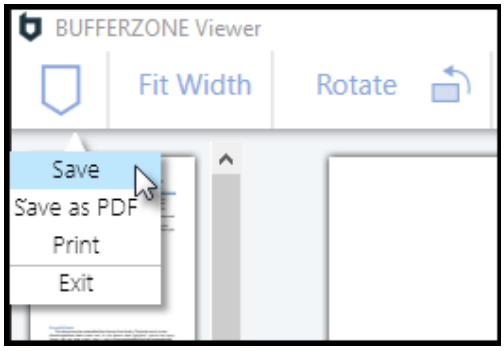


Intuitive User Experience

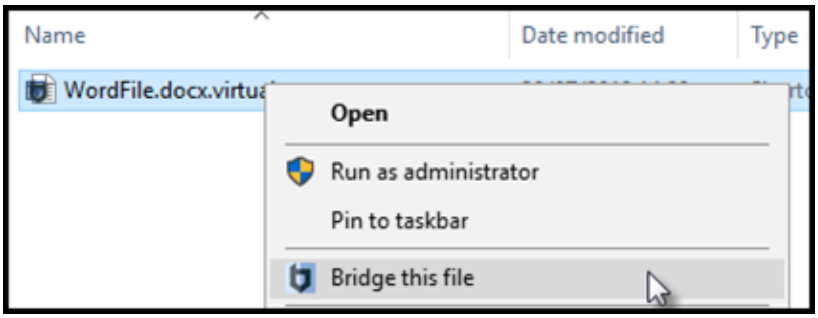
Contained browsers and other applications can be marked, for user awareness; or not, for even greater transparency. Available markings are a colored border of configurable thickness (as below), or an icon overlay.

BUFFERZONE has a small footprint and virtually no impact on performance, and does not require hardware or operating system upgrades.

While still in the BUFFERZONE container, downloaded files can be viewed in the contained browser or in the BUFFERZONE Viewer, which displays a wide range of contained 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:



On request, MS Office and other applications can be supported in the BUFFERZONE container.

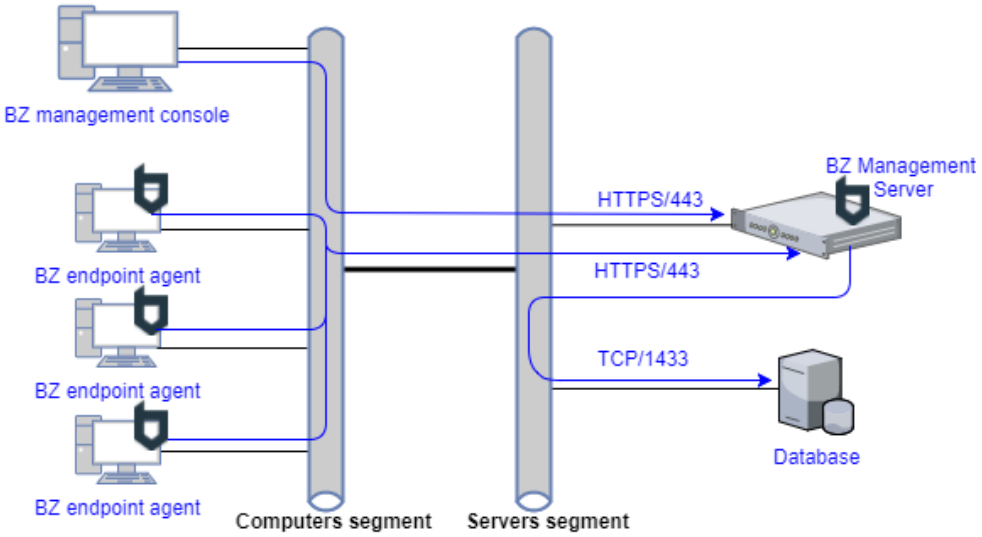
BZMS: Centralized, Policy-Based Management

For centralized containment policy management and agent deployment, you can integrate BUFFERZONE with existing endpoint management systems (for example, McAfee ePO). For complete management capabilities, use the BUFFERZONE Management Server (BZMS) 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.

BZMS uses an MS SQL Server database, which is usually recommended to be on a separate host from BZMS itself.

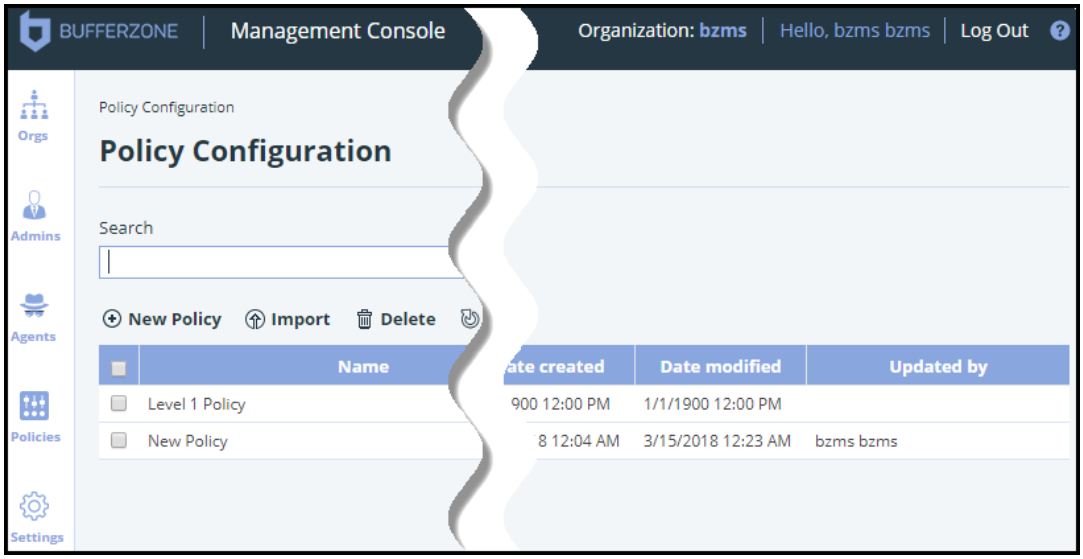
Communications between BUFFERZONE agents and BZMS are secured (HTTPS) and authenticated by certificate and endpoint UID. Console communication is configurable to be by HTTP or by HTTPS; the port number is also configurable.



For administering BZMS, you can authorize locally-configured user accounts and/or user groups from the organizational Active Directory. User and group authorization is role-based, with several levels of permission sets.

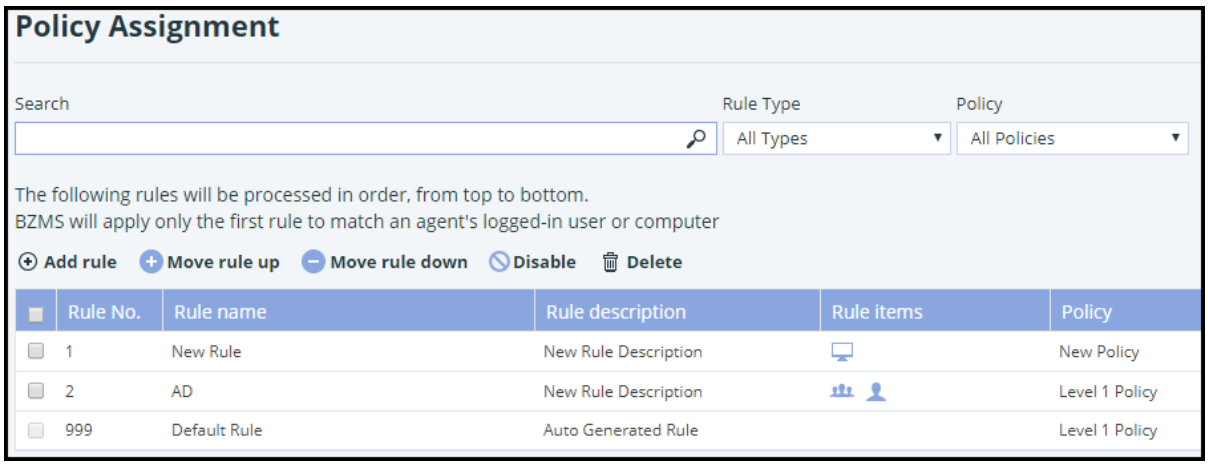
BZMS can be deployed in MSSP mode, enabling centralized management of multiple organizational deployments.

BZMS enables configuring multiple policies for assignment to different endpoint and user groups:



BZMS enables flexible and powerful policy assignment. In BZMS, you assign configured policies according to a set of configurable rules. Each rule assigns a specified policy to endpoint agents that match a set of specified conditions. Rules are processed in order, from top to bottom, and BZMS applies only the first rule to match an agent's logged-in user or computer. Available rule conditions are users and user groups (from organizational Active Directory), and known agent computers.

Agents periodically send updated user information to BZMS, upon which BZMS queries the organizational directory for current groups and recalculates policy assignment.



Upload Blocker for DLP

BUFFERZONE can restrict browser uploads to be only from a specified, contained location (for example, the contained Downloads folder). When configured along with BUFFERZONE's Hidden Files feature, which prevents contained applications from accessing locations that could contain sensitive data, BUFFERZONE contributes to a wider organizational DLP strategy, by ensuring that potentially sensitive information cannot be uploaded to the internet.

Correlating Information across the Enterprise

Advanced malware is highly distributed – it communicates with a network of hosts via a Command and Control server and often will infect a number of endpoints in your organization, especially if it is a targeted attack. Therefore it is essential to correlate threat information across the organization. BUFFERZONE collects information about suspicious software such as registry alterations, file system activity, network activity and more, and shares it directly with SIEM and other Big Data analytics platforms for effective organization-wide event correlation.

Summary

When it comes to protecting endpoints against modern and future threats, the most effective approach is 'containment first'. BUFFERZONE's patented isolation container technology enables employees to freely access information from anywhere without compromising the organization. It provides a safe place to run browsers and removable storage, and collects information that can be vital for attack detection and event correlation.

BUFFERZONE provides a complete solution for successfully integrating containment into the enterprise, including a secure bridge for transferring files according to industry best practices and advanced file disarming technologies. It has minimal hardware requirements, is easy to deploy and manage, and offers a very low total cost of ownership. With BUFFERZONE, organizations of all sizes can defend their endpoints against malware while giving employees seamless internet access to increase productivity and user satisfaction.