Solution Brief

BUFFERZONE Rounds Out Intel Security's Endpoint Protection

Prevent attacks through containment

One of the most daunting security challenges faced by enterprises today is how to empower business while defending against the daily onslaught of advanced targeted attacks (ATAs) and emerging threats that often lead to serious data breaches. Intel Security and BUFFERZONE have joined forces to help you meet that challenge by addressing the endpoint, the most vulnerable attack surface in your environment. According to Verizon, 93% of successfully executed advanced persistent threats (APTs) begin at the endpoint, through spear-phishing or other endpoint exploits.[1]

Intel Security addresses this issue with a comprehensive, layered approach to endpoint and data security that unifies top-rated protections through shared threat intelligence and an open and extensible security platform and enables them to work together across the entire environment to provide a stronger defense. BUFFERZONE, an Intel Security Innovation Alliance partner, adds an essential ingredient to this connected, collaborative ecosystem. Integrated with the McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform, BUFFERZONE's patented containment technology helps prevent both known threats and new threats from doing damage to your endpoints, data, and network—without restricting or slowing down user productivity. BUFFERZONE also relieves IT of the time-intensive burden of shifting through and responding to endless false alarms.

BUFFERZONE

McAfee COMPATIBLE

McAfee Compatible Solution

- BUFFERZONE 4.11 and above
- McAfee ePO software 4.6 and 5.1x

Supported OS

- Windows XP through Windows 10

Key Advantages

- Prevents known and new advanced malware from harming endpoints, data, and the network through patented containment technology.
- Enables secure sharing of data.
- Provides detailed threat intelligence about malware trapped in containers and shares this data through the McAfee Threat Intelligence Exchange and ESM solutions.
- Easy to deploy and manage via McAfee ePO software.

intel Security

Complete Threat Lifecycle Management Starts with Prevention

Intel Security's centralized, extensible framework empowers security components to detect and block attacks in progress and share threat intelligence to prevent future attacks. Effective prevention is also an important aspect of a defense-in-depth security strategy and needs to be integrated into complete threat lifecycle management. That's where BUFFERZONE comes into play.

BUFFERZONE's "Containment First" approach is a critical aspect of a comprehensive endpoint defense and adds another dimension to your prevention strategy. The sooner you stop an exploit in its tracks before it can cause harm, the lower the cost to your organization. Through BUFFERZONE's patented containment technology, potentially malicious files and code are isolated and securely removed. Best of all, BUFFERZONE's technology is transparent to users, so they can have unrestricted access to all the information and tools they need to be productive and creative while BUFFERZONE does its job behind the scenes. BUFFERZONE helps prevent emerging advanced attacks and significantly reduces the costs associated with loss of valuable corporate data, reputation repair, and complex operational tasks like detection, forensics, and remediation.

BUFFERZONE'S Advanced Technology

BUFFERZONE's advanced endpoint security solution consists of three key components:

- **Virtual container:** When an application (such as Internet browsers, removable media, and email) comes in contact with an environment BUFFERZONE deems untrusted, it runs in a secure, isolated environment that is separate from the rest of the endpoint. If malware is present, it is also trapped in the virtual container, so it cannot infect endpoints or the corporate network.
- **Secure bridge:** If the data in the virtual container needs to be shared, the secure bridge enables enterprises to configure automated processes and policies for extracting and disinfecting files and data before it is transferred, as a way of ensuring security and compliance across the network. This provides an extra measure of protection against under-the-radar, persistent malware that may not execute immediately.
- **Endpoint intelligence:** BUFFERZONE analyzes malware and distributes detailed information about suspicious files with security information and event management (SIEM) and Big Data analytics to help identify targeted attacks.

Containment: How It Works

Rather than blocking or detecting threats, BUFFERZONE isolates applications and files that originate from or come in contact with untrusted sources, such as the web or email. Suspicious code or files are placed in a secure virtual container that is sealed off from the rest of the endpoint. In effect, the container acts as a buffer that prevents both known and new malware from spreading to the endpoint and your corporate network. BUFFERZONE works much like protected memory in current operating systems, which is used to isolate applications from one another. BUFFERZONE isolates the entire application environment, including memory, files, the registry, and more, so any malware that tries to infect an endpoint is immediately confined in the container. When untrusted applications try to write or modify files or registry keys, they can go no further than the container. All of these operations are completely transparent to users and the applications they are accessing.

Browse safely

When employees go online, they don't think much about security—they just want to work safely and access online applications and information to get their jobs done. BUFFERZONE enables users to browse the web safely without restriction, unlike some endpoint defenses that may interfere with productivity, causing users to circumvent security controls.

In BUFFERZONE, administrators may define untrusted sources that need to be accessed within the isolated container and trusted sources that can be accessed outside of BUFFERZONE. When a user runs a file from an untrusted source (such as a browser or Skype) in a BUFFERZONE container, it is marked with a colored border but looks and acts no different in all other respects. If the user downloads a file intentionally or accidentally, the file, which might be in Microsoft Office, Acrobat, or another format, is sealed off inside the container—even when the user opens, edits, or saves it. Even if the user downloads a malicious file, your organization is not endangered. You can set policies to clean out the container at the end of the day or week. And in the meantime, users can work without interruption.

BUFFFERZONE defends users against a whole host of web-borne threats—malicious URLs in phishing emails, attacks that exploit zero-day vulnerabilities, drive-by downloads of malicious files, malvertising, Java exploits, and more.

Open email attachments securely

Email is an indispensable business tool—and a popular attack vector for socially engineered spear-phishing campaigns. According to the SANS Institute, 95% of network attacks result from spear phishing.[2] With BUFFERZONE, even if users open malicious email attachments, there's no cause for concern. All email attachments are opened in a special container, apart from the container used for web browsing or removable media. This dedicated virtual container for email attachments has no Internet exposure, so sensitive data contained in attachments is fully protected from web-borne threats. This separate environment exclusively for email attachments provides another layer of protection—users can securely open attachments that contain personally identifiable information (PII) or other sensitive data, without risk of data loss or leakage.

Use removable media without risk

External media, like smartphones, USB drives, and digital cameras can act as carriers of malware. It can be extremely risky to transfer files from external media to an endpoint and then share the files across the corporate network. BUFFERZONE opens files from any type of external media safely within a container. After the media is connected to the endpoint, BUFFERZONE automatically prevents viruses and other malware from executing. Your employees can view, edit, and save files back to the removable media without worry.

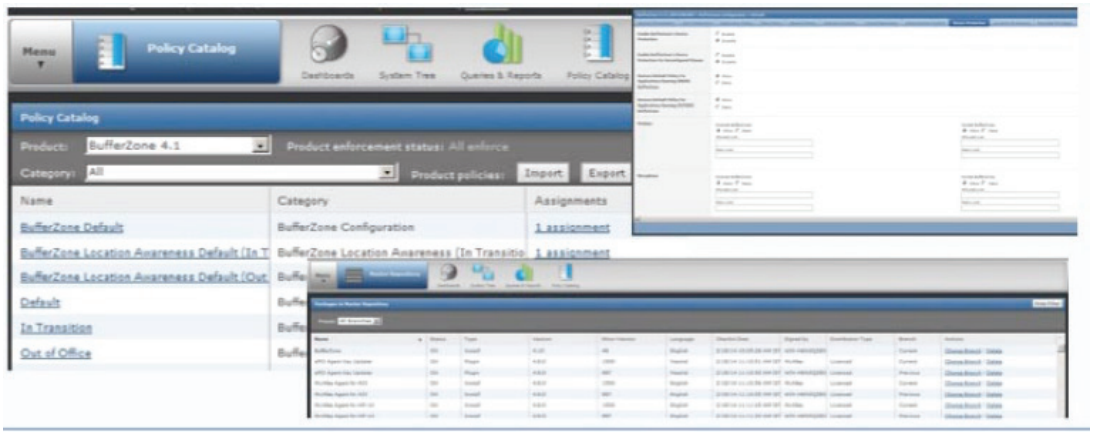

Figure 1. Complete integration with McAfee ePO software makes BUFFERZONE easy to manage and update.

Integration with the McAfee ePO Platform Optimizes Management

BUFFERZONE, which is McAfee Compatible with McAfee ePO software, is easy to deploy and manage and works seamlessly with other Intel Security endpoint security technologies in your integrated environment. Using McAfee ePO software, you can easily install and update BUFFERZONE using agent tasks. Through the McAfee ePO software policy catalog, you can define, distribute, and update BUFFERZONE policies. You can select default or basic organizational policies and create additional policies for groups or individuals. The Application Policy window allows you to determine which programs will run inside the BUFFERZONE container. For example, you can specify that web browsers should run in the BUFFERZONE container and then define "safe sites," like your corporate CRM system or Microsoft SharePoint, which can be viewed outside the BUFFERZONE container. You can also define policies and tasks for securely emptying files from containers via the McAfee ePO management platform.

Shared Threat Intelligence and Collaborative Protection

Endpoint security intelligence collected and analyzed by BUFFERZONE seamlessly integrates into Intel Security's unified platform. McAfee Data Exchange Layer, the Intel Security threat intelligence communication fabric, enables BUFFERZONE to participate in the collaborative ecosystem. In both targeted and untargeted attacks, bad actors can penetrate an organization through one or more endpoints, and often the associated malware spreads across the enterprise. The malware may communicate with a command and control (C&C) server or act independently. Either way, these attacks leave tracks. BUFFERZONE can gather data about suspicious software, including registry alterations, file system activity, or network activity, and can share that information about suspicious code found in BUFFERZONE's virtual containers to McAfee Threat Intelligence Exchange and McAfee Enterprise Security Manager (ESM). In turn, these systems analyze and correlate the data and immediately distribute protection as needed across your entire enterprise.

About BUFFERZONE

BUFFERZONE endpoint security solutions protect enterprises from advanced threats including zero-day, drive-by downloads, phishing scams, and APTs. With cutting-edge containment, bridging, and intelligence, BUFFERZONE gives employees seamless access to Internet applications, mail, and removable storage—while keeping the enterprise safe. Learn more at **www.bufferzonesecurity.com**.

About Intel Security Solutions and McAfee ePolicy Orchestrator

McAfee is now part of Intel Security. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in all architectures and every computing platform. With McAfee ePO software, Intel Security offers the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance. **www.intelsecurity.com**.

1. **http://www.networkworld.com/article/2889202/network-security/containment-security-solutions-for-endpoints-effectively-stop-attacks-before-harm-is-done.html**
2. **http://www.networkworld.com/article/2164139/network-security/how-to-blunt-spear-phishing-attacks.html**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com