Solution Brief

AI PCs and Cybersecurity
Intel® Core™ Ultra Processors

BUFFERZONE® SafeBridge® AI Disarms Files Vulnerable to Cyber Threats with Intel-Powered AI PCs[1]

BUFFERZONE® SafeBridge® AI enables secure file transfers on endpoints and explains file risks to end users by running AI locally on Intel® Core™ Ultra processor-based AI PCs.

"BUFFERZONE® has collaborated with Intel to pioneer the first endpoint-based content disarm and reconstruction solution that harnesses the computational power of Intel® technologies in AI PCs."

–Mor Miller, VP of Business Development, BUFFERZONE®

Challenge: Strengthen human resilience in the cybersecurity chain

Today's organizations face a critical cybersecurity challenge, where human behavior represents both the greatest vulnerability and the most promising opportunity for defense. Despite general security awareness, businesses continue to experience data breaches and malware attacks through everyday digital touchpoints like email and web browsing.

The solution lies in transforming employee behavior from a security liability into a powerful defensive asset. By implementing sophisticated technical security safeguards and educating employees on file risk potential, organizations can create a proactive security posture, where employees become empowered in identifying and preventing potential cyber threats before they can impact critical business operations.

Solution: BUFFERZONE® SafeBridge® AI on AI PCs with Intel® Core™ Ultra processors

BUFFERZONE® SafeBridge® AI is one of several technologies included in the BUFFERZONE® Safe Workspace® suite of security solutions.

BUFFERZONE® Safe Workspace®, based on two novel technologies—Protection By Containment™ and NoCloud™—intelligently combines virtual containment and disarming technologies in various ways.

- Protection By Containment™ uses application isolation technology to help prevent external attacks from web browsing, file downloads, removable media, email links, and attachments.
- NoCloud™ handles threats beyond containment using advanced deep learning technologies running on the endpoint, eliminating the need to upload any sensitive or private information to the cloud.

While BUFFERZONE® Protection By Containment™ technology creates an isolated virtual environment for users to safely access potentially risky content from the web, emails, or external storage, BUFFERZONE® SafeBridge® AI disarms downloads and attachments on the endpoint so they can be securely allowed out of the isolated container.

Leveraging content disarm and reconstruction (CDR) technology, BUFFERZONE® SafeBridge® AI acts as an advanced file handler, skillfully disarming content of risky file components that malware can exploit. It preserves data content integrity while nullifying threats and returns a secure file.

Further, now integrated with the BUFFERZONE® NoCloud™ anti-phishing detection solution on Intel-powered AI PCs, BUFFERZONE® SafeBridge® AI can run advanced large language models directly on the endpoint—leveraging Intel Core Ultra processor compute engines—to assess and explain file risks directly to the user. As a result, end users gain insight into the risks associated with untrusted content, can choose to remove files that may pose threats, and receive AI-driven explanations of file risk factors—all in parallel to a secure file version.

Key benefits of BUFFERZONE® AI SafeBridge® on Intel-powered AI PCs

BUFFERZONE® SafeBridge® on AI PCs with Intel® Core™ Ultra processors enables employees to perform everyday tasks securely without exposing the organization to cyber threats. Further, it uses GenAI to help employees recognize and mitigate potential risks in real time.

Disarm content of risky file components while preserving data content integrity.

Nullify threats on the endpoint, and return a secure file to the user.

Maintain privacy on user content by processing AI on local endpoint devices.

How it works

SafeBridge® AI is an advanced, zero trust file security solution that runs entirely on the endpoint device. It creates a secure bridge between the BUFFERZONE® virtual container and the trusted user environment, providing comprehensive protection against malicious files and cyber threats. At its core, the solution employs a CDR engine that processes files from various sources, including email attachments, downloads, and removable media, effectively removing potential attack vectors while preserving functionality. Further, integration with BUFFERZONE® NoCloud™ technology provides file risk explainability and visibility. This combination delivers a robust zero trust security framework that significantly enhances organizational cybersecurity posture.

By leveraging AI that runs locally on Intel Core Ultra processor-based AI PCs, BUFFERZONE® delivers high performance, efficiency, and low latency while keeping user privacy intact. Sensitive data stays on the device, and endpoints can run AI without impacting productivity or increasing cloud costs.

The BUFFERZONE® SafeBridge® AI solution is user friendly and flexible. There are two BUFFERZONE® Safe Workspace® editions for BUFFERZONE® SafeBridge® AI: the Pro version delivers automatic disarming capabilities, while the Enterprise edition offers customizable organizational policies.

Maximizing AI security performance on endpoints
In the AI era, automation and intelligence can be anywhere, including endpoint devices. Intel-powered AI PCs with Intel Core Ultra processors leverage a CPU, integrated GPU, and NPU on the processor die to efficiently handle AI workloads locally.

Intel Core Ultra processors are the first Intel® processors to feature an NPU on the processor die, providing a new compute engine that helps sustain heavily used AI workloads at low power directly on the endpoint. Additionally, workloads running on the NPU don't touch the CPU or integrated GPU, allowing these compute engines to operate normally or potentially more efficiently in the presence of AI.

When it comes to cybersecurity on the endpoint, it's critical to protect company data and user privacy, reduce analysis latency, and minimize impact on the quality of the user experience. BUFFERZONE® SafeBridge® AI zero trust file security achieves this on the endpoint by leveraging the Intel Core Ultra processor compute engines.

"I'm excited about the Intel Core Ultra processor because it means more compute efficiency for complex workloads," says Miller. "When leveraging the GPU and NPU in Intel-powered AI PCs, users can access all the features of AI for enhanced performance and experience while still maintaining overall system power."[2]

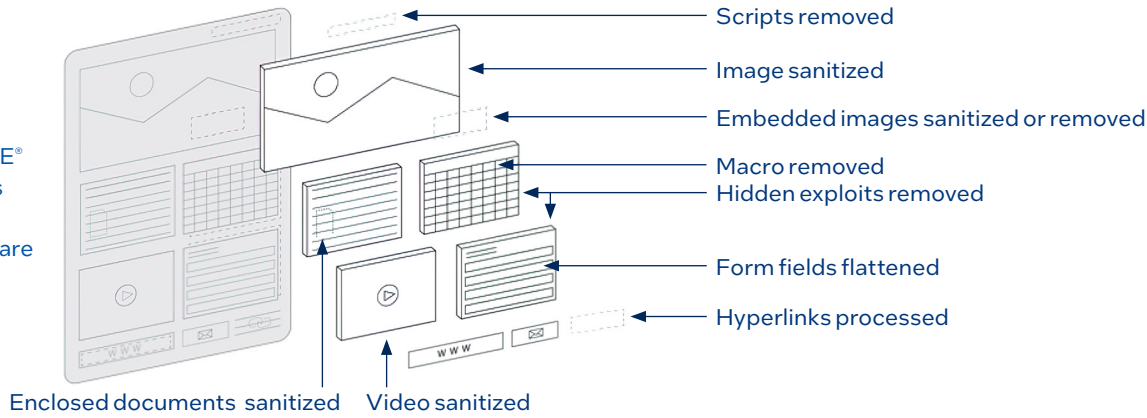

Figure 1: BUFFERZONE® SafeBridge® AI disarms content of risky file components that malware can exploit.

BUFFERZONE® reimagines protection against external threats

Through integration with BUFFERZONE® NoCloud™ technology, BUFFERZONE® SafeBridge® provides AI-based insights to end users about suspicious and potentially dangerous file activities. When identified, BUFFERZONE® SafeBridge® AI uses CDR on the host system to disarm potentially harmful file components before returning a clean file to users, enabling confidence in downloading and opening attachments and websites.

BUFFERZONE® NoCloud™ offloads complex AI tasks from the cloud to endpoint devices. This allows for real-time prevention of phishing or malware locally without the need for cloud processing. Processing on the Intel Core Ultra processor NPU or GPU helps to reduce latency associated with file vulnerability detection and increase inferencing speed and data privacy.[2]

AI PCs help deliver more-efficient cybersecurity

The powerful combination of BUFFERZONE® innovative security software and Intel Core Ultra processors delivers next-generation cyber protection through advanced AI capabilities.

By processing AI workloads directly on the local device, this integrated solution enables rapid threat detection and analysis while preserving user privacy and provides users with clear AI-generated risk assessments and explanations.

Through intelligent computing that unites proactive security with adaptive learning, organizations gain a more resilient and contextually aware protective technology ecosystem that can identify and respond to threats with unprecedented speed and sophistication.

Conclusion: An intelligent approach to cybersecurity protection

"Together with AI PCs powered by Intel, BUFFERZONE® has the ability to enhance BUFFERZONE® SafeBridge® with AI insight and explain the hidden risks in untrusted files, educating and enabling users about the risks of untrusted online data in a simple way," Miller says.

The integration of BUFFERZONE® SafeBridge® AI with AI PCs powered by Intel Core Ultra processors represents a significant leap forward in endpoint security. Businesses gain robust technological safeguards as well as innovative, AI-driven, user-centric interventions that help employees recognize and mitigate potential risks in real time.

About BUFFERZONE®

BUFFERZONE® Security redefines endpoint protection with cutting-edge solutions to safeguard users against advanced threats like phishing, file download, web browsing, removable media, and email links and attachments. By combining real-time NoCloud™ AI-powered capabilities on the endpoint with robust Protection By Containment™ isolation technologies and SafeBridge® zero trust file security, BUFFERZONE ensures the endpoint stays safe while preventing sophisticated attacks.

bufferzonesecurity.com

Get started with AI PCs from Intel

Explore Intel-powered AI PC use cases ›

Learn more about Intel Core Ultra processors ›

Learn more about BUFFERZONE® technologies ›

Notices and disclaimers

1. AI features may require software purchase, subscription, or enablement by a software or platform provider or may have specific configuration or compatibility requirements. Data latency, cost, and privacy advantages refer to non-cloud-based AI apps. Learn more at intel.com/AIPC.
2. BUFFERZONE® has released software to support running on the Intel® Core™ Ultra processor GPU and NPU. Final NPU support is pending. Check with BUFFERZONE® for the latest information on GPU and NPU deployment.

1224/JL/CMD/PDF