Case Study

AI PCs and Cybersecurity
Intel® Core™ Ultra Processors

intel ai

Improving data security with AI PCs

BUFFERZONE® uses AI to deliver advanced phishing detection and to identify confidential files for protected storage. The AI capabilities of Intel® Core™ Ultra processors make it all possible on the user's device.

> **"Once we understood that Intel allowed us to run AI on the endpoint, we grabbed it and threw away our cloud. Today, we don't have any cloud inference, not even for testing. I don't need to pay for expensive cloud GPUs anymore."**
>
> *—Ran Dubin, CTO of BUFFERZONE®*

Using the cloud for security scanning introduces latency and increases the risk of data exposure if the cloud service provider is hacked. That's why BUFFERZONE® runs its security software on the user's device, powered by BUFFERZONE® NoCloud® AI technology. Its Anti-phishing solution uses AI to analyze unfamiliar web pages, while Safe Data uses AI to scan for sensitive files and images. The company is enhancing its SafeBridge® solution with AI to explain the risks in downloaded files. AI PCs enable rapid AI processing, giving users a seamless experience.

Challenge

- Security threats are increasingly sophisticated, including using AI to create phishing websites quickly and at scale.
- Although the cloud can provide processing power for AI-based threat detection, it can be costly and raises concerns about sensitive data exposure.
- Users accumulate files on their hard drive (data at rest) that may contain confidential business information, personally identifiable information (PII), and medical data, all of which are targets for data thieves and ransomware.
- Users may struggle to understand the risks associated with downloading files, and also need to understand how to identify and protect their sensitive information before it leaves their PC.

Solution

- AI PCs with Intel Core Ultra processors offer enhanced AI performance to enable new security applications.
- BUFFERZONE® Anti-phishing uses an AI model running on the Intel® Core™ Ultra processor's neural processing unit (NPU) to analyze webpages and identify phishing sites.
- BUFFERZONE® Safe Data protects data at rest from advanced ransomware and data-stealing attacks using an AI-driven data classification engine. It uses AI running on the GPU inside the Intel® Core™ Ultra processor to scan the

BUFFERZONE

device for newly stored or modified files containing confidential information. Those files can then be stored in a virtual vault on the device.

- BUFFERZONE® SafeBridge® isolates incoming files and strips active content from them using content disarm and reconstruction (CDR) before the files can be moved out of the isolated container. Generative AI on the GPU will explain the risks to users if they want to use the original file.

Results

- 70% decrease in latency detection for Anti-phishing, compared to cloud inference.[1]
- More than 40% improvement in phishing detection speeds by optimizing for the NPU, compared to CPU inference.[1]
- BUFFERZONE® cut its operational AI costs by 91% by migrating from the cloud to the device.[1]

Cyberattacks are smart and relentless

With the sophistication and scale of cyberattacks, modern security solutions need a lot of processing power to detect and neutralize threats.

Many organizations have traditionally relied on cloud AI or on-site servers, but these approaches often cost significantly. Analysis in the cloud also introduces latency because of the time taken to transmit data. Beyond technical considerations, companies may have concerns about data security in the cloud: Who has access to it? How vulnerable is it to exposure in the event of a data breach?

Moreover, security has always had a human dimension that has been complex to address. Users frequently struggle to recognize the threat that might be present in a downloaded file or to identify sensitive information among their stored files. The key challenge lies in empowering users to handle files safely and in a way that protects the organization's confidential data without compromising ease of use.

At the same time, AI is intensifying phishing threats by making it possible for attackers to create vast numbers of fake websites quickly. "Attackers can build millions of websites, and when one of them is detected, they can just throw it away and create a new one," says Ran Dubin, CTO of BUFFERZONE®.

Solution: Running AI on the device

Thanks to AI PCs based on Intel® Core™ Ultra processors, BUFFERZONE® has moved its anti-phishing technology to the user's device. As a result, users can be confident that their web browsing behavior is not being analyzed or stored outside their device, enhancing their privacy and manageability. There's no risk of their online activities being tracked or their web history being exposed as a result of them using the anti-phishing tool. This is beneficial not only to individuals researching sensitive topics such as medical concerns or financial planning, but also to businesses where online behavior might disclose their research and development interests.

Running security solutions on the user's device has several benefits:

- **Enhanced privacy:** Users can be confident that their data remains on their device and is not sent to the cloud for processing.
- **Faster threat detection:** Files and user activities can be analyzed in real time, and there is no delay resulting from network communications.
- **Greater mobility:** The solution continues to work effectively even if no network connection is available, and there is no dependence on an external cloud solution.

"Once we understood that Intel allowed us to run AI on the endpoint, we grabbed it and threw away our cloud," says Dr. Dubin. "Today, we don't have any cloud inference, not even for testing. I don't need to pay for expensive cloud GPUs anymore."

Many anti-phishing solutions are based on the reputation of the website visited, which makes it hard to keep up with the pace of AI attacks. BUFFERZONE® Anti-phishing uses AI on the device to conduct a real-time site analysis instead. "Our anti-phishing solution was designed to be aware of AI attacks," says Dr. Dubin. "When our software sees a webpage you haven't browsed before, it scans the page. Using our own object detection AI model, we understand the context in the page, the login information, the objects detected, and the brands, and we warn users if there is a mismatch between the page and the website address."

Bringing anti-phishing scanning to the device

Intel-powered AI PCs have a CPU, integrated GPU, and NPU (neural processing unit) on the processor die to efficiently handle AI workloads locally. BUFFERZONE® Anti-phishing has been optimized for NPU but also works on the GPU or CPU if the NPU is unavailable. Although BUFFERZONE® sees similar performance on the NPU and GPU, the NPU is more available because fewer workloads

use it, Dr. Dubin says. "Our consumption of the processing units is optimized and low, so it will be easy to coexist with other solutions that run on the NPU in the future," he adds.

Identifying confidential information

The power to run large language models and vision language models on the end device has also enabled BUFFERZONE® to launch additional products that help users manage files more securely. BUFFERZONE® Safe Data scans the device for newly stored or modified files that contain confidential information. Those files can then be stored in a virtual vault on the device. The vault is designed only to be accessed by authenticated users. This way, files are protected from ransomware encryption attacks and other security breaches.

"Protecting your data at rest is one of the biggest challenges," says Dr. Dubin. "Safe Data replaces high-end data leakage prevention (DLP) solutions, which are cloud-based or run on servers in the organization. Those solutions are expensive and hard to maintain. Our software is simple and runs on the user's device. Adding data classification so users can understand the sensitive information on the device and automatically offering to protect it in our vault gives our customers a significant edge."

Safe Data runs its AI workloads on the GPU and CPU, with NPU support in development.

Advising users on security risks

BUFFERZONE® SafeBridge® AI isolates applications such as web browsers and email clients so that downloads cannot harm the system. When the file is removed from the isolated container, the software uses content disarm and reconstruction (CDR) technology to strip out all active elements that might pose a threat. BUFFERZONE® is enhancing the solution with generative AI running on the NPU to explain the risks to users if they want to use the original file. This solution runs faster on the GPU today, but is expected to move to the NPU after software optimizations enable it to deliver the same performance.

Intel enables transformation from cloud to device

AI PCs have freed BUFFERZONE® from the cloud's complexity and cost. The company has created its NoCloud® brand to communicate the benefits of running AI on devices and differentiate its solutions from competitors.

"Everyone loves the cloud," says Dr. Dubin. "I love the cloud, too. But it's expensive, and your costs increase as you grow. When you move from deep learning to more complex, large language models, the hardware requirements are more costly, too. Creating applications in the cloud is easy, but scaling them to millions of users is complex, and you need to develop a lot of infrastructure to do that."

"As an endpoint solution provider, our goal was always to do everything on the device and to use the cloud as little as possible," he adds.

While customers appreciate the increased privacy from not uploading to the cloud, Dr. Dubin also values the simplicity. "If I have to upload customer content that might be sensitive or private, I need to harden my infrastructure and create more controls to ensure we comply with data protection legislation like GDPR," he says. "Once we cut all those cloud ties, I don't have all those problems. I simply don't have any customer data."

BUFFERZONE® has also seen cost savings. "I don't need to pay for expensive cloud GPUs anymore," says Dr. Dubin.

He adds: "Customers worry about sensitive and confidential information in their files. They love it when we tell them we don't take their data and we do everything on their device."

The ability to run AI on the endpoint has enabled BUFFERZONE® to launch SafeBridge and Safe Data, and is opening the opportunity to enter new markets in education

Technical Components of Solution

- **Intel® Core™ Ultra processor.** Intel Core Ultra processors are high-efficiency processors built to deliver next-gen AI experiences in sleek and slim mobile form factors. These processors are the foundation of the AI PC, with a high-throughput GPU, low-power NPU, and fast-response CPU.
- **BUFFERZONE® Anti-Phishing.** This solution combines multiple information sources and detection criteria with AI-based learning to determine if visited sites might be masquerading as other sites to steal submitted information.
- **BUFFERZONE® Safe Data.** Using large language models (LLMs), Safe Data automatically scans stored and newly modified files and images for sensitive information. Safe Data recommends storing the information in a protected vault on the user's PC if found.
- **BUFFERZONE® SafeBridge® AI.** This software disarms downloads and attachments so they can be safely used. SafeBridge supports common document and media content types.

and the consumer market. Using the power of the AI PC, BUFFERZONE® has been able to migrate away from the cloud and deliver high-performing AI applications on user devices.

Faster AI output, reduced costs

The speed of AI inference is important to ensure a smooth user experience. BUFFERZONE® has measured a 70% decrease in detection latency for Anti-phishing compared to cloud inference1 and a more than 40% improvement in inference speeds by optimizing its software for the NPU, compared to CPU inference.[1]

By migrating from the cloud to the device, BUFFERZONE® has also reduced its AI operational costs by 91%[1]. The company continues to use the cloud for license verification and software downloads.

Find the solution that is right for your organization. Contact your Intel representative or visit www-ssl.intel.com/content/www/us/en/enterprise-security/a-better-way-to-work.html.

Lessons Learned

- AI PCs, based on Intel® Core™ Ultra processors, enable AI applications that would previously have run in the cloud to run on devices.
- This reduces network communications latency and helps eliminate any security risks associated with uploading sensitive data to the cloud.
- As cyberattacks increasingly use AI to rapidly scale up attacks, old methods based on the reputation of website addresses may struggle to keep up. Having powerful AI capabilities on the device enables more dynamic defenses based on deep learning.
- Running AI on the user device, using technologies like NoCloud® AI, enhances user privacy because the user's data does not need to leave their computer for analysis.

Learn more

Intel® Core™ Ultra processors

AI PCs

Webinar: Re-architecting Endpoint Security with AI on Clients

Solution Brief: BUFFERZONE® Delivers AI-Driven Cybersecurity Against Ransomware and Data Theft

Video: BUFFERZONE® NoCloud™ Anti-Phishing Solution Powered by Intel Core Ultra

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

BUFFERZONE® Safe Data Protects Sensitive Data on Endpoint Devices with Intel-Powered AI PCs

intel ai

[1] See https://bufferzonesecurity.com/news-events/bufferzone-and-intel-ai-anti-phishing-solution-presented-at-mobile-world-congress/

0625/AC/CAT/PDF 365770-001EN