Solution Brief

Safeguard your workforce with AI-based anti-phishing

Analyst firm IDC calls generative artificial intelligence (genAI) "trigger technology" that will usher in a new era of computing, which it dubs the Era of AI Everywhere.[1] "Everywhere" includes the PC, which is evolving with built-in AI functionality that improves security, performance, and functionality. IDC forecasts the market for PC systems with built-in AI capabilities will increase 60% over the next three years, from 50 million in 2024 to more than 167 million in 2027.[2]

IDC forecasts the market for PC systems with built-in AI capabilities will increase 60% over the next three years, from 50 million in 2024 to more than 167 million in 2027.

The advanced capabilities of AI PCs play a critical role in helping organizations protect their people and systems from a variety of cyber threats, including phishing.

As phishing attacks become more sophisticated, security and IT teams are deploying AI-based anti-phishing as part of a defense-in-depth security strategy that extends to all endpoint devices. The goal is to help safeguard the workforce without compromising performance or productivity.

To address these challenges, BUFFERZONE® and Intel® have pioneered the first endpoint-based anti-phishing solution that harnesses the computational power of Intel's AI PC technologies. The BUFFERZONE® NoCloud™ solution is part of Lenovo ThinkShield, a comprehensive portfolio of hardware, software, and services to help protect critical business information.

The PC's expanding attack surface

The PC attack surface is growing, driven by a rise in hybrid/remote workers and growing IT complexity. Both trends make it harder to regularly update applications and endpoint devices to reduce vulnerabilities that bad actors can exploit.

Phishing attacks are the main entry point. Phishing was cited as the most prevalent attack vector in IBM's 2023 Cost of a Data Breach report, with the average cost of a phishing-related data breach at a whopping $4.76 million.[3]

The threat is getting worse, not better. Cybercriminals are now using AI, including genAI, to turbocharge their phishing attacks. One study found malicious phishing emails increased 1,265% over the 12-month period following the launch of ChatGPT in late 2022.[4]

It's impossible to eliminate all phishing attacks, which makes it critical to quickly identify and mitigate infected systems before criminals can begin moving laterally. The lateral movement is used to infect an entire fleet of devices or reach the systems that hold the sensitive corporate or customer data they're seeking.

How AI helps with anti-phishing

AI helps safeguard against phishing with advanced analysis and detection capabilities such as brand detection, image context understanding, and natural language processing. AI algorithms use these capabilities to identify social engineering scams or content such as fake virus alerts.

Despite the benefits of AI-based anti-phishing, security teams are learning that traditional cloud-based solutions can have limitations, including latency, privacy, cost, and power/performance concerns.

The best solution brings together Intel®, BUFFERZONE®, and Lenovo technologies to deploy AI locally on the PC to strengthen anti-phishing protections without compromising on performance or privacy. The BUFFERZONE® NoCloud™ AI anti-phishing detection solution provides a 91% reduction in anti-phishing operational costs and 100% privacy.[5] Its deep learning engines specialize in uncovering malicious behavior from different threat perspectives and work collectively to stop evasive phishing attacks while utilizing Intel® Core™ Ultra processor technology and NPU acceleration.

A Multi-layered, holistic approach to security

The solutions and capabilities from BUFFERZONE®, Lenovo, and Intel do more than provide advanced protections from phishing — they enable organizations to deploy a multilayered cybersecurity approach to reduce the attack surface and protect workers. Together, these technologies span hardware, BIOS/firmware, hypervisors, virtual machines (VM), operating systems (OS), and applications. This holistic approach helps ensure every aspect of the PC's operation is safeguarded against a wide range of threats, from sophisticated cyberattacks to common phishing schemes.

Intel vPro® and Intel® Core™ Ultra: Hardware-based security for business

The Intel vPro® platform has helped set the gold standard for business PC security and has been deployed on over 300 million endpoints in corporate fleets. Secure foundations are established at every layer: hardware, BIOS/firmware, hypervisor, VM, OS, and applications.

Key benefits

- The BUFFERZONE® NoCloud™ AI anti-phishing detection solution, part of the Lenovo ThinkShield portfolio, uses deep-learning engines that utilize Intel technology to accelerate the time to detect phishing attacks while ensuring user privacy.
- Lenovo ThinkShield AI-powered endpoint protection provides coverage from OS to the cloud, providing extended detection and response against cyber threats.
- The Intel® Core™ Ultra processor integrates CPU, graphics processing unit (GPU), and neural processing unit (NPU) capabilities into a single package that accelerates AI on endpoint devices.

Intel vPro® capabilities, including Intel® Hardware Shield and Intel® Threat Detection Technology, establish a secure foundation directly below the operating system. This integration provides enhanced security from the hardware level up, ensuring strong protection against external threats.

The Intel® Core™ Ultra processor, which lies at the heart of the Intel vPro® Platform, includes an integrated NPU that can handle sustained, heavily used AI workloads, including anti-phishing engines, at low power for greater efficiency.

Lenovo ThinkShield: Total protection, wherever work happens

Lenovo ThinkShield is a comprehensive cybersecurity portfolio that encompasses hardware, software, and supply chain components. Combined with Intel's hardware security, Lenovo ThinkShield offers an extra layer of defense with its own set of hardware-based security features like the Trusted Platform Module and self-healing BIOS.

Lenovo ThinkShield leverages a combination of advanced hardware, software, and AI technologies to enhance the security features of its portfolio. It utilizes AI to monitor and analyze system behaviors and network traffic, identifying unusual activities or potential threats for quicker response to security incidents. This proactive approach enhances overall system security.

Lenovo ThinkShield brings world-class security providers, including BUFFERZONE®, together to defend against phishing and other cyber threats.

BUFFERZONE® Safe Workspace®: Intelligent detection and prevention

The BUFFERZONE® Safe Workspace® suite integrates seamlessly with Lenovo and Intel security frameworks to provide users with a secure computing environment, safeguarding critical data and systems from the entry point all the way to the core.

Safe Workspace® is a comprehensive suite of cybersecurity solutions, each designed to address a major attack vector:

- Safe Browser: Secure web browsing and file downloads
- Safe Removables: Secure USB/CD/DVD and auto-execution prevention
- Safe Mail: Secure email content and attachments
- SafeBridge®: Content disarming and reconstruction solution that prevents file-based attacks
- BUFFERZONE® NoCloud™: The anti-phishing solution, powered by the NPU in the Intel® Core™ Ultra processor, uses advanced AI to detect and prevent phishing attempts more efficiently. This AI-driven approach not only enhances privacy protection but also reduces reliance on cloud-based services, lowering operational costs.

Better together

Phishing is a significant threat to organizations of all sizes, in any industry. And it's not going away — in fact, it's getting worse as bad actors deploy AI to increase the scale and sophistication of phishing attacks.

Staying ahead of the threat requires a defense-in-depth strategy that protects data and systems across multiple layers, from the cloud to the core. This holistic approach to security also requires the right partners that can provide cutting-edge technologies, including AI, to help organizations reduce the attack surface and protect their workforce.

The BUFFERZONE® NoCloud™ AI anti-phishing detection solution, part of Lenovo's ThinkShield portfolio and powered by Intel vPro® and Intel® Core™ Ultra processor technology, is a critical part of a defense-in-depth strategy, allowing organizations to take their safeguards to the next level.

To learn more about Intel AI PC, visit: www.intel.com/aipc

1 IDC, "No Turning Back: AI Everywhere Causes a Seminal Shift in the Tech Market," https://blogs.idc.com/2023/06/28/no-turning-back-ai-everywhere/

2 IDC, "Worldwide Artificial Intelligence PC Forecast, 2023-2027," https://www.idc.com/getdoc.jsp?containerId=US51747324

3 IBM Security, "Cost of a Data Breach Report 2023," https://www.ibm.com/downloads/cas/E3G5JMBP

4 SlashNext Security, "The State of Phishing 2023," https://slashnext.com/state-of-phishing-2023/

5 PR Newswire, "BUFFERZONE® and Intel® AI Anti-Phishing Solution presented at Mobile World Congress," https://www.prnewswire.com/il/news-releases/bufferzone-and-intel-ai-anti-phishing-solution-presented-at-mobile-world-congress-302072202.html

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

All versions of the Intel vPro® platform require an eligible Intel processor, a supported operating system, Intel LAN and/or WLAN silicon, firmware enhancements, and other hardware and software necessary to deliver the manageability use cases, security features, system performance and stability that define the platform. See intel.com/performance-vpro for details.

Intel vPro® - 1 | Performance Index

Lenovo does not validate the content, security standards, or regulatory compliance of any products mentioned of referenced. Any information provided regarding products, including but not limited to their specifications, features, or compliance, is solely based on information provided by our partners.

Products and offers are subject to availability. Lenovo reserves the right to alter product offerings and specifications, at any time, without notice. Lenovo makes every effort to ensure accuracy of information but is not liable or responsible for any editorial, photographic, or typographic errors. Images are for illustration purposes only. For Lenovo products, services, and warranty specifications, visit www.lenovo.com