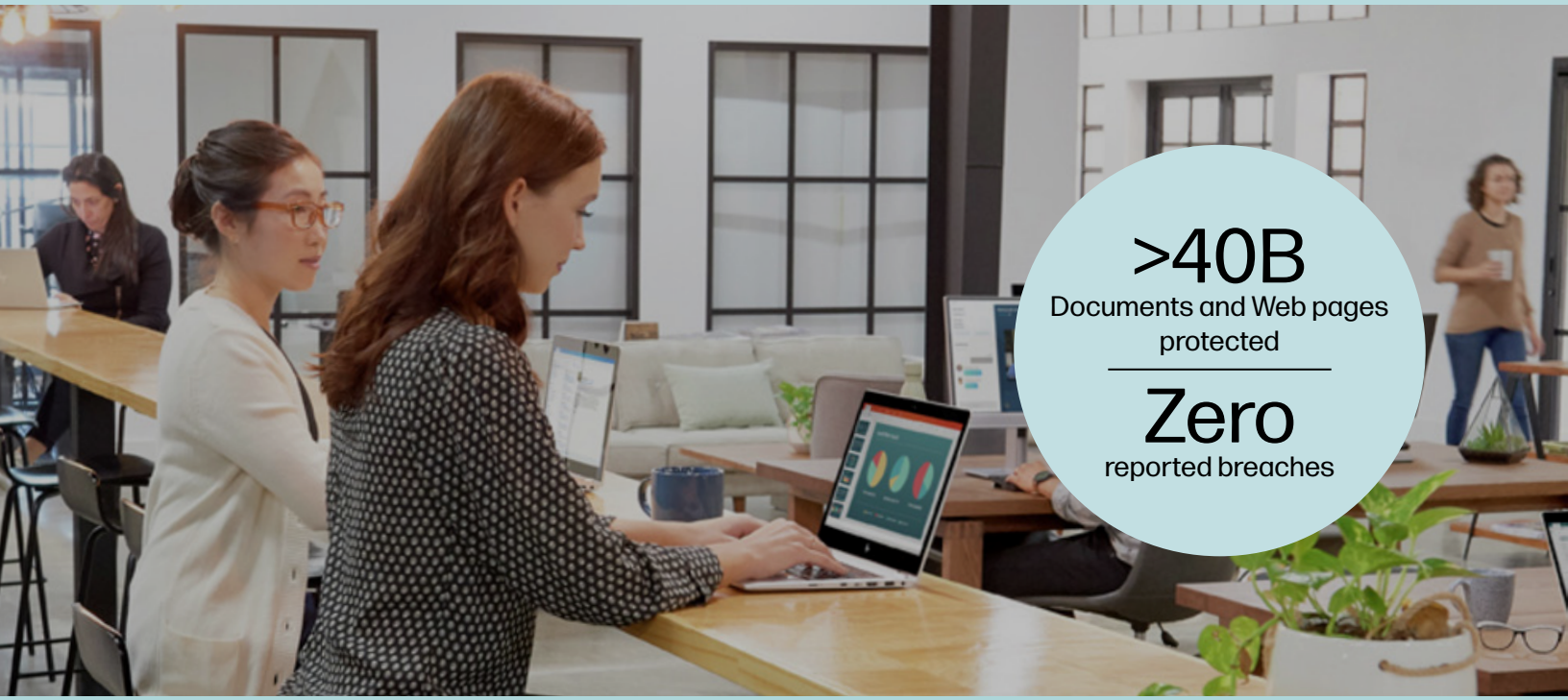
Sure Click Enterprise and Wolf Pro Security

HP Threat Containment for AI-based Attacks



CHALLENGE

The Rise of AI-Enhanced Cyberattacks

Artificial Intelligence (AI) is transforming an endless number of industries and business processes, a fact not lost on cyber security threat actors.

AI is already being used by cyber adversaries of all kinds, from amateurs to nation states. A popular technique is to use AI to craft more believable phishing and spear-phishing content. By gathering information easily available in sources such as social media posts, AI can craft malicious emails, documents and websites that are both targeted to individuals, and highly credible.

The goal is to make it even harder for employees to reliably spot these fakes, so that the attacker can penetrate the network faster and easier.

It is axiomatic that end users struggle to consistently identify phishing emails and fake websites, even with periodic security awareness training. The attacker only needs to be successful once to get in, and many staff roles (accounts payable, public-facing government employees) require that emails from unknown sources be opened.

Given that successful phishing attacks were common without AI, the conclusion must be that new approaches are required to cope with the avalanche of AI-enhanced attacks.

HP THREAT CONTAINMENT

Zero Trust Protection Against AI-Enhanced Attacks

The rise of AI-enhanced social engineering attacks necessitates a Zero Trust approach. All incoming email, or clicks on untrusted websites, must be considered risky.

This is exactly the assumption used by HP's Threat Containment technology. This approach assumes all such content can't be trusted, and therefore only opens them in isolated "micro virtual machines" (micro-VMs) created in software on the endpoint PC. A micro-VM, enforced by the CPU's hardware, is opened for each webpage tab or email attachment. The micro-VM's tightly controlled attack surface makes it next to impossible for an attacker to compromise the endpoint PC, or any other device on the network. When the task completes, the micro-VM is destroyed, taking the malware instance with it.

Five Crucial Benefits

Unlike other cybersecurity technologies, Threat Containment delivers five benefits that span risk management, user experience, and operational efficiency:

INHERENT PROTECTION	Protects by default, without attempting to detect attacks. By assuming all content is malicious, Zero Trust security is achieved, including against AI-based attacks.
VISIBILITY	Monitors activity within the micro-VMs and transmits threat intelligence information to the centralized Wolf Controller. This facilities analysis and integration with threat intelligence analysis platforms using industry standards such as STIX and TAXII.
POSITIVE USER EXPERIENCE	Users are relieved of the burden and anxiety associated with trying to spot phishing attacks or fake websites designed to steal credentials. They can "work without worry" knowing that HP Threat Containment will prevent attackers from using social engineering to trick them.
SECURITY OPERATIONS EFFICIENCY	Lowers the volume of urgent tickets due to false positives caused by detection technology failures. It also lowers the amount of remediation required for compromised endpoints. Lastly, there is less reliance on security awareness training to spot phishing, so training time can be re-purposed to higher-value objectives.
EFFICIENT COMPLIANCE CONTROL	Compliance and audit directives require proof that security controls are continuously active. Threat Containment works without a complex process, making it trivial to operationalize, and therefore to demonstrate compliance when requested by auditors.

CONCLUSION

A Superior Defense Against AI-Enhanced Attacks

AI is empowering threat actors with more credible content at increased volume and velocity.

HP's Threat Containment used in Sure Click Enterprise and Wolf Pro Security is well-suited to defeating such attacks. Its Zero Trust, hardware-enforced isolation of content assumes everything is suspect, eliminating the impossible task of accurately "detecting" each and every attack. It also provides comprehensive benefits across visibility, user experience, security operations, and compliance. Organizations of all sizes seeking to improve their defenses against AI-based attacks should consider HP's Threat Containment for the best combination of protection and operational efficiency.

4AA8-4070ENW, May 2024