Keeper Security's Industry-First Forcefield™ Protects Against Memory-Based Attacks on Windows Endpoints

Kernel-level protection defends against infostealers targeting sensitive data

LONDON, UNITED KINGDOM, November 6, 2025 /EINPresswire.com/ -- Keeper Security, the leading cybersecurity provider of zero-trust and zero-knowledge Privileged Access Management (PAM) software protecting passwords, passkeys, privileged accounts, secrets and remote connections, today announces Keeper Forcefield™, the first-of-its kind protection against memory-based attacks on Windows devices. Forcefield is a groundbreaking kernel-level endpoint security product that proactively defends against memory-based attacks, including credential theft from infostealers and runtime memory-scraping malware. Keeper® is the first cybersecurity software company to deliver real-time memory protection at both the user and kernel levels, raising the standard for endpoint security in enterprise environments.

Attackers are increasingly bypassing traditional cybersecurity defences by targeting unprotected memory rather than exploiting vulnerabilities. Malicious software delivered through phishing attacks or other methods can access application memory to extract passwords, session tokens and other sensitive data – circumventing traditional encryption methods. Keeper Forcefield closes this dangerous gap by locking down memory access at the kernel level. Unlike conventional antivirus or Endpoint Detection and Response (EDR) tools, it enforces real-time memory protection capable of blocking non-privileged, fileless and zero-day attacks without degrading system performance.

"Forcefield closes one of the most dangerous blind spots in endpoint security," said Craig Lurey, CTO and Co-founder of Keeper Security. "Malware can extract sensitive information directly from a device's memory, even at the user level where administrative privilege isn't required. Forcefield prevents this type of exploit entirely without disrupting trusted applications or everyday workflows."

In the UK, where 43% of businesses experienced a cyber-attack in the past year, organisations are preparing for new obligations under the forthcoming Cyber Security and Resilience Bill. The Bill reinforces the National Cyber Security Centre's Cyber Assessment Framework (CAF) and the government's 'Secure by Design' principles. These measures aim to mitigate vulnerabilities that enable advanced threats such as memory exploits and credential theft. Keeper Forcefield directly supports these objectives.

Forcefield provides peace of mind by actively safeguarding sensitive data from unauthorised access while operating silently in the background. It installs a lightweight, kernel-level driver that shields protected application memory from unauthorised access. Users can easily toggle Forcefield on or off within the Keeper Desktop application or deploy it via Group Policy. The solution continuously differentiates between trusted and untrusted processes in real-time, ensuring legitimate activity continues uninterrupted while malicious or unknown processes are blocked from scraping sensitive data.

How Keeper Forcefield works:

- Kernel-level protection - Actively monitors and restricts memory access to protected applications.
- Selective memory restriction - Blocks unauthorised processes from reading protected application memory.
- Smart process validation - Differentiates between trusted and untrusted processes in real time.
- Uninterrupted system performance - Runs quietly without impacting system or application performance.

Windows applications protected by Forcefield include:

- Web browsers - Chrome, Firefox, Edge, Brave, Opera and Vivaldi
- Keeper software - Desktop App, Web Vault, Browser Extensions, Gateway, Bridge, Commander and KeeperChat
- Operating systems - Windows 11 x64 and ARM64

Forcefield is available for both individual users and enterprise environments. Organisations can deploy protection across fleets of Windows devices in minutes using existing management tools, ensuring scalable and consistent endpoint defence without added friction.

For more information or to download Keeper Forcefield, visit www.keepersecurity.com/forcefield-endpoint-protection.

###

About Keeper Security

Keeper Security is one of the fastest-growing cybersecurity software companies that protects thousands of organisations and millions of people in over 150 countries. Keeper is a pioneer of zero-knowledge and zero-trust security built for any IT environment. Its core offering, KeeperPAM®, is an AI-enabled, cloud-native platform that protects all users, devices and infrastructure from cyber attacks. Recognised for its innovation in the Gartner Magic Quadrant

for Privileged Access Management (PAM), Keeper secures passwords and passkeys, infrastructure secrets, remote connections and endpoints with role-based enforcement policies, least privilege and just-in-time access. Learn why Keeper is trusted by leading organisations to defend against modern adversaries at KeeperSecurity.com.(https://www.keepersecurity.com/en_GB/)

Learn more: KeeperSecurity.com(https://www.keepersecurity.com/en_GB/)

Bethany Smith
Eskenzi PR and Marketing
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
TikTok
X
