KEEPER FORCEFIELD

Endpoint Protection for Windows

Challenges

Protect Windows endpoints from memory-based attacks with industry-first kernel-level technology – the only solution independently verified to block infostealers, credential scrapers and session hijackers.

01

Windows allows processes running under the same user account to read each other's memory – a fundamental OS design gap that malware actively exploits to steal passwords, session tokens and credentials.

02

Infostealers such as RedLine, Lumma, Raccoon and Vidar use standard Windows API calls to scrape sensitive data directly from application memory, bypassing encryption-based defenses entirely.

03

Independent testing by Venak Security confirmed that every major competing password manager – including 1Password, LastPass, Bitwarden, Dashlane, NordPass and Proton Pass – failed all memory attack tests.

04

Session hijacking via stolen browser cookies enables attackers to bypass multi-factor authentication, granting persistent, authenticated access to critical accounts and applications.

Solution

Keeper Forcefield is an industry-first endpoint security product for Windows that closes the critical memory security gap. Forcefield installs a lightweight kernel-level driver that monitors and restricts which processes can access the memory of protected applications – blocking infostealers and credential-stealing malware even when running under the same user account.

Forcefield protects all major web browsers (Chrome, Firefox, Edge, Brave, Opera and Vivaldi) and all Keeper applications, including browser extensions, and runs silently in the background without impacting system performance. It is the only solution independently verified to block both user-mode and kernel-mode memory attacks and the only platform to protect browser extensions from in-memory data theft.

Learn more
keepersecurity.com

Request a demo
keeper.io/demo

Partner inquiries
partners@keepersecurity.com

About Keeper Security

Keeper Security is the global leader in zero-trust and zero-knowledge cybersecurity, protecting passwords, passkeys, secrets, endpoints and privileged access for thousands of organizations and millions of users worldwide.

How Forcefield Works

Kernel-Level Driver

Installs a lightweight driver that actively monitors and blocks memory access attempts targeting protected applications.

Selective Memory Restriction

Blocks only unauthorized processes from reading protected app memory. Trusted system processes and protected apps continue to function normally.

Smart Process Validation

Validates each process by name, file name and code signature before granting or blocking memory access, ensuring zero false positives.

Zero Performance Impact

Runs silently in the background with no measurable impact on system or application performance.

Business Value

Proven Protection

- Only password manager independently verified to block user-mode and kernel-mode memory attacks and browser extension memory theft (Venak Security, 2025)
- Protects against infostealers that bypass encryption by targeting in-memory credentials, session tokens and browser cookies
- Stops session hijacking by preventing cookie theft from browser memory, protecting MFA-secured accounts
- Zero performance impact – Forcefield runs silently without affecting system or application speed

Flexible Deployment

- User-controlled activation via a single toggle in Keeper Desktop
- Enterprise deployment via MSI installer, Microsoft Intune, Group Policy or any RMM tool
- Silent install and uninstall supported for automated rollouts
- Admin-controlled updates via software distribution tools with daily auto-check

Key Capabilities

- **Kernel-level memory protection:** Lightweight kernel driver blocks unauthorized memory reads at the OS level
- **Browser protection:** Protects Chrome, Firefox, Edge, Brave, Opera and Vivaldi including browser extensions
- **Keeper application protection:** Covers Keeper Desktop, Web Vault, Browser Extensions, Gateway, Bridge, Commander, KSM and KeeperChat
- **Code signature validation:** MSI packages are EV code-signed; the updater verifies signatures before installation
- **Platform support:** Windows 10 and above, including Windows 11 for ARM (x86/64-bit and ARM/64-bit)
- **Standalone MSI installer:** Available independently of the Keeper Desktop application for flexible deployment
- **Minimal network footprint:** Requires only outbound HTTPS to download keepersecurity.com for updates

Keeper Outperforms Every Other Platform

Keeper is the only platform that blocked all attacks. All other password managers failed in at least three critical areas, often exposing sensitive information, such as credit card data, during live attack simulations.

Security Mechanism	Keeper	1Password	Bitwarden	Dashlane	LastPass	NordPass	Proton Pass
Zero-Knowledge Encryption	✓	✓	✓	✓	✓	✓	✓
Client-Side Encryption	✓	✓	✓	⊗	✓	✓	✓
Online Authentication	✓	⊗	⊗	✓	⊗	⊗	⊗
Memory Protection (User-land)	✓	✓	⊗	⊗	⊗	⊗	⊗
Memory Protection (Kernal-land)	✓	⊗	⊗	⊗	⊗	⊗	⊗
Web Browser Extension Protection	✓	⊗	⊗	⊗	⊗	⊗	⊗