

Strengthening Your Cyber Defenses Against Invasive Attacks

- "123456" continues to be the most common password choice, indicating a lack of password complexity.
- Nearly two-thirds of Americans are found to reuse passwords across multiple accounts, creating a massive security vulnerability.
- A disturbing 13% of users go to the extent of using the exact same password for every online account they have.

Wallarm's advanced detection system is designed to combat the sophisticated nature of credential stuffing attacks. By focusing on authentication endpoints, a key area of vulnerability, Wallarm's system tracks and analyzes each login attempt. This meticulous approach allows for the accurate identification of compromised credentials being used, providing an essential layer of security.

Distinctive Benefits of Wallarm's Credential Stuffing Detection versus Conventional Tools



Exceptional Accuracy in Detection

Wallarm distinguishes itself through solutions that deliver high levels of accuracy in detection. These solutions target authentication endpoints, essential areas of vulnerability, ensuring superior accuracy in the identification and thorough analysis of every API-based login attempt. Contrasting with the broader approach of generic alternatives, Wallarm specifically concentrates on authentication endpoints, which are critical points of vulnerability.



Customization Powered by Intelligence

Wallarm's platform is distinguished by its intelligence-driven customization. It enables specific adjustments and configurations, ensuring a response tailored to your unique needs. This approach guarantees a more accurate alignment with security policies compared to standard, broad-spectrum solutions.



Automated Security and Privacy Measures

Wallarm's strategy in combating credential stuffing includes sophisticated automated systems. These systems not only secure your business operations, but also safeguard your reputation against such intricate threats. The automation efficiently counters attacks while preserving the confidentiality of sensitive data.

Wallarm Credential Stuffing Detection: Multifaceted Detection and Comprehensive Protection

Wallarm's approach to combating credential stuffing includes multiple detection methods. It combines the identification of brute force attempts with behavioral analysis through API Abuse Prevention. The newly added credential stuffing detection feature grants security analysts enhanced control, allowing for the identification of each instance where a known-compromised credential is used.

Supported by a vast database of compromised passwords, Wallarm enables organizations to quickly detect compromised user accounts. This feature provides more robust protection against credential stuffing threats.

The Credential Stuffing Detection capability is available as part of Wallarm's Advanced API Security platform and is integrated into the latest version of the Wallarm node. For more detailed information about this feature, users are encouraged to consult our documentation below.

Further Resources & Support

To gain further insight into protecting against credential stuffing, Wallarm provides a wealth of resources. Explore our comprehensive guide in the Learning Center. Alternatively, schedule a demo with Wallarm to discover how we safeguard against such attacks or find out more from our corporate blog or our information on Wallarm's Credential Stuffing Detection webpage.