

Mitigating OWASP Automated Threats

COMBAT CREDENTIAL STUFFING WITH WAF AND THREAT INTELLIGENCE

Account takeovers are a financial burden and reputation risk!

63%

of data breaches involve stolen or weak credentials¹

\$8^B

annual loss from account takeover by 2018²

95%

of breaches are financially motivated³

CREDENTIAL STUFFING Attack Kill Chain



Capabilities
Required to
Combat
Credential
Stuffing



Threat Intelligence: Bad Bots, CAPTCHA, Bad IPs, Anonymous Proxies, TOR networks



Web App Firewall: Application Profiles, Correlated Attack Validation, Velocity Checks

With millions of stolen credentials circulating on the dark net, a 1% success rate can mean tens of thousands of compromised accounts. Fight back.

[Learn More](#)

Mitigating OWASP Top-20 Automated Threats

IMPERVA®

1. 2016 Verizon DBIR

2. Javelin Data Breach Fraud Impact Report

3. 2016 Verizon DBIR

4. World's Largest Data Breaches

©2016, Imperva, Inc. All rights reserved. Imperva, the Imperva logo, SecureSphere, Incapsula, ThreatRadar, Skyfence and CounterBreach are trademarks of Imperva, Inc. and its subsidiaries. All other brand or product names are trademarks or registered trademarks of their respective holders.