VeriClouds CredVerify™

DATASHEET

VeriClouds CredVerify™ is a credential verification service that helps organizations detect compromised credentials before hackers do. VeriClouds uses the same data attackers do, proactively monitoring the dark web and systematically reducing user-centric risk. VeriClouds provides the best approach to eliminate the biggest cause of massive data breaches, the weak and/or stolen password.

VeriClouds Benefits

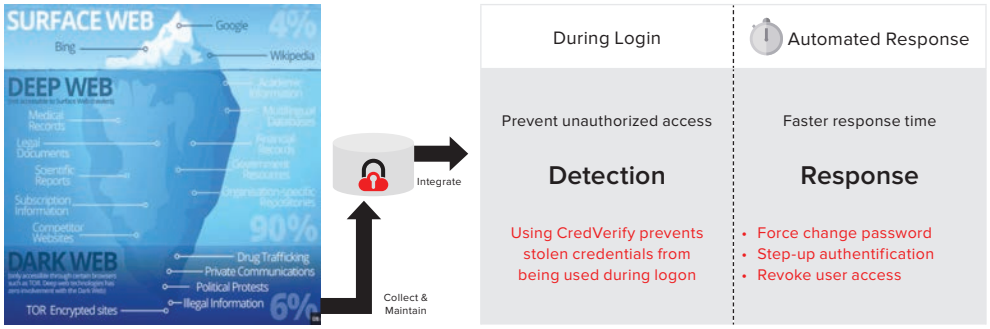
- Prevent stolen credentials from being used during logon
- Outsource legal liabilities of handling breach data
- Automate response and remediation to known data breaches
- Masking and encryption for maximum privacy and data protection
- Complement 2FA and MFA

VeriClouds Solutions

- The industry's largest commercially available data repository of compromised accounts with patent pending password matching technology
- Intelligent data graph provides visibility into risk of your organization's compromised credentials on 3rd party websites and the social web
- Support for NIST SP 800-63B password compliance

The Biggest Problem in Cyber Security

With 81% of confirmed data breaches involving weak or stolen credentials, having a solution that proactively detects and remediates this problem is no longer optional. To proactively detect threats before they can do damage, you need a solution to quickly identify when credentials have been compromised or reused, and act on that insight in real time. By automating the detection and response known leaked credentials, CredVerify™ can minimize risks and incurred costs from credential stuffing attacks and data breaches.



VeriClouds gives you visibility into over 90% of stolen credentials on the dark web, unleashing the full power of Risk Aware IAM.

A 360-degree View of Identity Centric Risk

Very few organizations can distinguish the genuine user from the sophisticated attacker. Even companies combining 2FA with contextual based authentication telemetry (device trust, IP reputation, geo-location, the protocol used to access an app, etc.) are doing so in response to an authentication attempt, and not proactively identifying and mitigating compromised accounts. To address this issue, organizations must have visibility into dark web activity to detect and respond to the risks associated with compromised credentials of its users. VeriClouds research team continuously monitors the dark web for stolen databases and identities, and maintains the encrypted data in our proprietary database. When integrated with an IAM solution, CredVerify™ provides superior visibility into user-centric risk and the ability to automate appropriate corrective actions, preventing the abuse of compromised credentials.

Between
15% and **40%**
of a typical
company's credentials
already exist
in our database

CredVerify™ REST API
CredVerify™ Appliance

CredMonitor for Enterprise

Privacy By Design

VeriClouds offers a differentiated solution that operates to promote security and safety for the true owners or persons entitled to the data. VeriClouds never sells sensitive data that can be used against one of its customers or partners. VeriClouds combines world class talent in monitoring the dark web with innovative product design to deliver the most secure offering in the industry, enabling risk informed IAM for our technology partners and enterprise customers.

- VeriClouds CredVerify™ uses only strong encryption to prevent tampering with potential PII and abuse by rogue admins or malicious users.
- Our products and services are designed with strict adherence to ethical hacking standards.
- Our privacy by design philosophy ensures compliance with data privacy governance frameworks and regulatory guidelines such as GDPR and NIST.

Support for NIST Special Publication 800-63B

Seeing the opportunity to improve the security of authentication, VeriClouds CredVerify™ goes beyond context and behavioral risk analysis by introducing credential verification into the authentication workflow, using real breach data and patent protected password comparison methods to detect and prevent password reuse and abuse from cyber adversaries. VeriClouds CredVerify™ helps enforce the NIST password requirement guidelines for IdPs by *screening of new passwords against lists of commonly used or compromised passwords*. The types of lists acceptable to the NIST guidelines include:

- Passwords obtained from previous breach corpuses
- Dictionary words
- Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
- Context-specific words, such as the name of the service, the username, and derivatives thereof

CredVerify™ NIST password compliance check capability supports and verifies all the above requirements.

Deep Integration Delivers Risk Aware IAM

VeriClouds CredVerify™ delivers actionable intelligence and integrates with existing IAM platforms to extend the ROI of your investment and unleashes the full power and potential of intelligence driven security. CredVerify™ provides visibility into over 90% of all compromised credentials that are being sold on the dark web and easily available to nation-state attackers and cyber criminals.

Integrating a credential verification service such as CredVerify™ with IAM systems complements existing contextual authentication and MFA solutions and provides enhanced visibility into risks of compromised credentials during authentication and self-service password resets.

CredVerify™ can be deployed and integrated in days and used to immediately protect hundreds of millions of your customers by checking them against VeriClouds's proprietary database of more than six billion known compromised credentials. Current integrations include Lieberman Software, Microsoft, SailPoint and Ping Identity.

About VeriClouds

VeriClouds is a credential verification services company helping organizations detect compromised credentials before hackers do, using the same data attackers do, proactively monitoring the dark web and systematically reducing user-centric risk. VeriClouds provides the best approach for eliminating the biggest cause of massive data breaches, the weak and/or stolen password. VeriClouds was founded in 2014 by Rui Wang, a former security researcher at Microsoft with a PhD in cyber security, and Stan Bounev, a successful entrepreneur with over 16 years of corporate and startup experience. VeriClouds has built one of the largest and most secure commercially available databases of known compromised credentials collected from the dark web and diverse data sources using privacy preserving principles and strong encryption.

Contact Info

For more information:

info@vericlouds.com

www.vericlouds.com

@vericlouds

AppBugs, Inc. DBA VeriClouds
1107 NE 45th ST., STE 423
Seattle, WA 98105 U.S.A.

Worldwide Inquiries: Phone: +1.844.532.5332