vericlouds

5 Key Insights for Credential Monitoring and Verification

The number of stolen passwords readily available to cyber criminals and nation-state attackers on the dark web now numbers in the billions and grows daily. A solution that can detect if a user's credentials are among these stolen records is essential for enterprise security and regulatory compliance. Credential monitoring and verification can minimize the likelihood that hackers will walk right through the front door undetected and keep your company out of the "data breach" headlines.

PRIVACY BY DESIGN MATTERS

Much of the data used by credential verification services are from public disclosures that have been released to the public and are available to bad actors on the dark web. Service providers that consolidate this data have a responsibility to follow data privacy and protection best practices.

Here are some important questions to ask when evaluating credential verification and monitoring services about privacy:

- How does the provider protect the privacy of user data in their compromised credentials store?
- How does the provider protect your company's information?
- How are APIs and web services secured by the provider?

A best in class credential verification service will not expose passwords by requiring them to be passed to a service provider via an API for comparison. Credential verification services should rely on encryption, data masking and client-side comparisons to prevent tampering. Such data protection controls can also help prevent your valuable data from being used as a cyber-weapon against your customers and your organization.

CREDENTIAL VERIFICATION MATTERS

It is no longer enough to simply answer, “Have I been pwned?” Core to any credential verification and monitoring services is an effective verification process for breached credentials.

Any credential monitoring and verification service must securely store usernames and passwords to provide effective detection and verification of breached credentials. The things you need to ask are:

- Is the service provider selling you a breach notification service, or something more?
- How does the provider verify credentials from data breaches and public disclosures?
- What is the provider’s accuracy and detection rate during verification?

Credential verification using commonly or previously hacked passwords, while valuable, will result in alerting users 2-6 times more often compared to when using a precision instrument based on data sciences and analytics.

ACTIONABLE INTELLIGENCE MATTERS

Another key area in evaluating credential verification providers is whether they provide actionable intelligence.

Visibility is a starting point for an effective credential verification and monitoring service, but the information regarding compromised credentials must be actionable to reduce your risk exposure and realize the full benefits of protection.

- Does your provider allow you to directly notify users with compromised credentials?
- Can you monitor identities of VIPs, privileged users and executives?
- Can you act based on identity risk indicators?
- Can you monitor linked personal identities related to corporate identities?

Finally, can you integrate with your in-house single-sign-on (SSO), identity management, or identity-as-a-service (IDaaS) provider?

CONTINUOUS INNOVATION AND AGILITY MATTERS

The risk that users and organizations face in a post breach world is dynamic and constantly changing. To be effective in the fast-moving world of data breaches and credential disclosures, continuous agility and innovation are key to offering differentiated solutions to your customers.

Highly automated solutions and teams with demonstrated agility to respond to changes in cyber-attacks and customer needs are essential for effectively mitigating the risk of compromised credentials. In evaluating a provider, consider these points:

- What is the service provider's release cycle?
- Have they demonstrated they can adapt quickly to new requirements?
- What does the service provider's roadmap look like?
- Are there relevant patents to help bring a differentiated and unique service to market?

BIG DATA MATTERS

The dark web offers vast troves of credential data that are easily available to nation-state attackers and cyber criminals. The risk that compromised credentials pose to users and business increases exponentially the longer they lay exposed online. Therefore, data is one of the most important areas to consider.

A world-class solution must focus on risk to the user, not just his or her credentials. The following questions will help you to identify the best in class solution:

- What is the breadth of coverage of leaked credentials and how is it measured?
- How often are updates made to the database?
- How does the service provider correlate identifiers to enhance risk scoring?
- What leaked data are stored in the service provider's database that may enhance risk scoring?

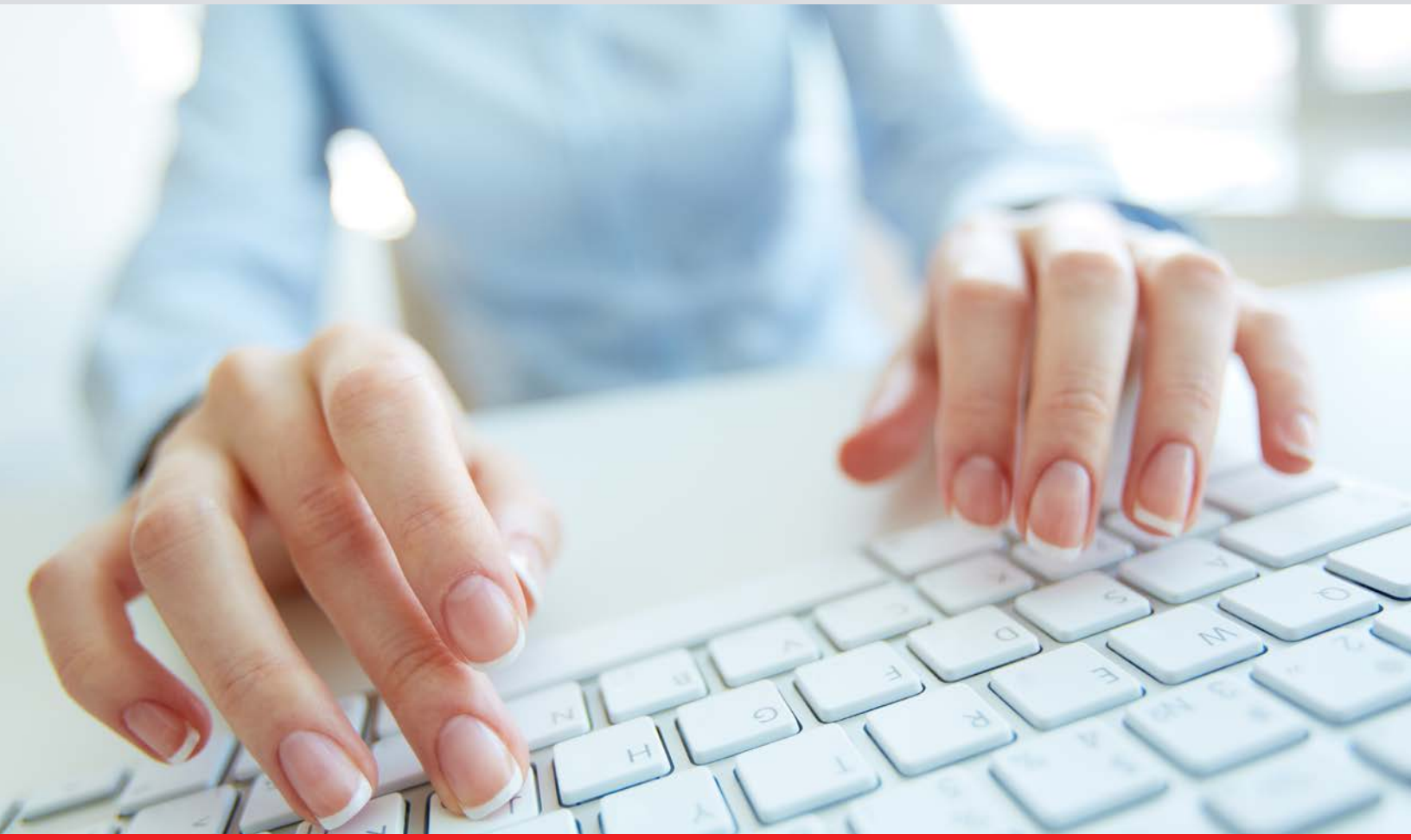
When it comes to data collection and management for identity threat intelligence, applying 80/20 thinking will endanger an organization. 20% of the leaked data from the dark web does not mitigate 80% of the risk. *Better data = better customer experience = better company performance.*

DELIVER SAFER ONLINE EXPERIENCES WITH CREDENTIAL MONITORING & VERIFICATION

Having the ability to prevent logins using breached credentials is a transformation for most organizations, and fills a huge gap left by low adoption rates of 2FA and MFA solutions. The right credential monitoring and verification solution will help you to Detect, Verify, and Prevent compromised credentials from impacting your organization, and that roughly translates into:

- Safer online experiences for your users
- More effective security and risk mitigation controls
- Protection against costly credential stuffing attacks
- Alignment with NIST SP 800-63B guidelines
- Reduced alert fatigue; the best balance between user experience and security

To learn more about how VeriClouds can help protect your business from the leading cause of data breaches, visit vericlouds.com



vericlouds

VeriClouds is a credential verification services company that helps organizations detect compromised credentials before hackers do – using the same data attackers do – by proactively monitoring the dark web and systematically reducing user-centric risk. We eliminate 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 cybersecurity, and Stan Bounev, a successful entrepreneur with over 15 years of corporate and startup experience in the financial services and technology industries. VeriClouds has built one of the largest commercially available databases of breached data from the dark web and diverse data sources using privacy preserving principles and strong encryption.