vericlouds | SailPoint

HIGHLIGHTS

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

No organization is immune to the risk of compromised credentials.

Compromised credentials pose an enormous and growing risk to businesses users alike. Billions of credentials are available to cyber criminals online which provide easy access into organizations; even worse, attacks by cyber criminals are difficult to detect and mitigate. The threat of compromised credentials means organizations must change to protect themselves very quickly; each new breach immediately raises the risk profile and footprint for both new and existing credentials.

An organization might have little to no risk one day and the next day be at very high risk. Even one major breach can spell trouble because the risk profile around credentials may change radically overnight. Both active and passive intelligence is necessary to continuously address and mitigate these risks.

VeriClouds CredVerify™ offers an easily integrated identity threat intelligence solution for organizations running SailPoint IdentityIQ; these services significantly reduce risk and can provide a full block against the hazard of compromised credentials.

VeriClouds CredVerify™ proactively collects, organizes and secures leaked credentials from the data breaches of the world. CredVerify™ actively monitors for the possible breached credentials of executives and privileged users, integrates into IdentityIQ to automate its responses, and enforces adaptive policies in real-time.

BETTER DATA = BETTER CUSTOMER EXPERIENCE = BETTER COMPANY PERFORMANCE

With VeriClouds CredVerify, SailPoint customers can check for stolen credentials and privately compare passwords of their accounts against billions of leaked records. CredVerify™ automatically transforms risk insight into actionable intelligence and stops preventable data breaches at the front door.

Use of industry standard REST APIs, which is fully supported by SailPoint IdentityIQ, adds identity threat intelligence to any rule, form, workflow, or task that uses credentials and passwords within IdentityIQ.

Because the VeriClouds database is constantly updated with new password threat intelligence, actions taken one day may be entirely different the next. This brings unprecedented agility to enterprises while keeping them protected from the internet's fastest growing threat.

PARTNER PRODUCT

- SailPoint IdentityIQ

VERICLOUDS PRODUCTS

- CredVerify™

VERICLOUDS

VeriClouds is an identity threat management company helping 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 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 compromised credentials; our database is collected from the dark web and diverse data sources using privacy-preserving principles and strong encryption.

SAILPOINT

As the leader in identity and access management (IAM), SailPoint helps hundreds of global organizations securely and effectively deliver and manage user access from any device. SailPoint connects this data to applications residing in their datacenter, on mobile devices, and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services, including identity governance, provisioning, and access management, which can be delivered on-premises or from the cloud (IAM-as-a-service).

ACTIVE SCANNING & COMPROMISED CREDENTIALS INTELLIGENCE

Organizations leveraging SailPoint IdentityIQ often implement and rely on password intercept technology, which is provided by IdentityIQ, to intercept and reset user passwords within Windows, Linux and Unix environments. VeriClouds CredVerify™ has a proven and tested integration with the IdentityIQ password intercept workflow; this intercept enables organizations to react to and easily address compromised or weak credentials.

Employees often need to unlock accounts or reset expired passwords. An organization can educate its users through automated emails to explain why actions have been taken to mitigate compromised credentials. This education can be accomplished within password intercept workflow. CredVerify™ provides your employees with "compromised" or "uncompromised" intelligence during password changes to help SailPoint customers align with the latest NIST SP 800-63B guidelines.

The same approach works for self-service registration and password reset integration within IdentityIQ. Your organization can contact CredVerify™ to access the intelligence you need for registration or password reset requests. IdentityIQ may then respond in real-time to disallow risky actions, send alerts or notifications, educate the end-user or any other action your organization desires to address your specific requirements for self-service registration or password reset use.

PASSIVE SCANNING & IDENTITY THREAT MANAGEMENT

A company's infrastructure does not have to suffer a direct breach for its employee or customer passwords to be vulnerable. Outside of user-initiated password resets, any new data breach on the internet may result in compromised credentials affecting your organization and therefore put sensitive data and systems at risk.

SailPoint's IdentityIQ out-of-the-box capabilities connect to more than one hundred types of systems; VeriClouds CredVerify™ can therefore help your organization with multiple approaches to scan its systems, proactively identifying compromised credentials and automatically remediating exposures and risks.

SailPoint IdentityIQ can perform scans by connecting to important organizational systems, probe credentials on those systems and check access to those systems for at-risk accounts. IdentityIQ can then take immediate action, expiring or locking those accounts with compromised credentials, as well as sending notifications or easily performing any other actions your organization may choose.

SUMMARY

Darran Rolls, CTO of SailPoint, adds that "Appropriately managed passwords remain an effective and user-friendly way to secure an account or a service. It is however critical that everyone (and I mean everyone) minimizes the risk of dealing with passwords, by employing a closed loop system of governance that enables good password hygiene throughout the lifecycle of every account."

Integrating VeriClouds CredVerify™ with SailPoint IdentityIQ provides organizations with unprecedented visibility and an automated response to the risk of compromised credentials of privileged users and executives within the organization. With an easy-to-use, intuitive integration over industry standard REST, VeriClouds CredVerify™ effectives bridges the gap left by missing 2FA and brings the power of big data analytics into a purpose built next generation identity threat management platform.