SOLUTION BRIEF

Information Technology
Security

VeriClouds CredVerify* Uses Intel® Software Guard Extensions (Intel® SGX): Credential Verification with Privacy By Design

Intel® SGX protects credential verification to prevent reusing leaked credentials

VeriClouds CredVerify* is a credential verification service that helps organizations detect compromised credentials before hackers do. VeriClouds proactively monitors the dark web and systematically reducing user-centric risk.

VeriClouds CredVerify uses Intel® Software Guard Extensions (Intel® SGX) to protect the sensitive credential verification process with hardware-based crypto built inside the CPU. The solution significantly advances the security of VeriClouds service.

> "VeriClouds CredVerify* with Intel® SGX enables enterprises to detect compromised credentials with privacy protected by design. This service provides enhanced protection against the biggest cause of data breaches - weak or stolen user credentials."
>
> – Steve Tout
> CEO, VeriClouds

Leaked Credentials are Inevitable

It's no longer surprising to wake up on any given day to news of yet another mega data breach compromising hundreds of millions of user accounts. In total, billions of credentials are breached every year and this trend shows no signs of abating. Leaked credentials are continuously used by hackers to breach additional services because of one simple fact - people reuse passwords. Over 80%[1] of people reuse passwords across services, and 81%[2] confirmed breaches in 2017 involve weak or stolen passwords.

Very few organizations can distinguish a genuine user from a sophisticated attacker with valid user credentials. Even companies combining two factor authentication (2FA) with contextual based authentication telemetry (device trust, IP reputation, geo-location, the protocol used to access an app, etc.) do so as part of an authentication attempt, and do not proactively identify compromised credentials without integrating a credential verification service into their authentication workflow.

VeriClouds CredVerify: Credential Verification with Dark Web Data

To address this issue, organizations must have visibility into dark web activities to detect and respond to the risks associated with compromised user credentials. VeriClouds' research team continuously monitors the dark web for stolen databases and identities, and maintains collected data in an encrypted database. Powered by this database, VeriClouds CredVerify provides users with visibility into account-centric risk and the ability to automate appropriate corrective actions, thereby reducing the abuse of compromised credentials.

VeriClouds maintains the industry's largest commercially available database of compromised credentials with over 6 billion records. VeriClouds research team continuously monitors and collects breached databases from the dark web daily.

VeriClouds' offers a unique solution that operates to promote security and safety for the true owners of or persons entitled to the data. VeriClouds uses patent pending encryption and masking techniques to protect the credentials data and the verification process.

Solution Benefits:

- Helps prevent stolen credentials from being used during logon
- Automate response and remediation to known data breaches
- Intel® SGX encryption technology – providing maximum privacy and data protection
- Complement 2FA and MFA for increased security.

Users may choose between a cloud API, hybrid or on-premise appliance solution to best fit architectural requirements and satisfy privacy and security regulations.

VeriClouds CredVerify* supports the latest NIST (National Institute of Standards and Technology) password requirement guidelines for identity providers by screening new passwords against lists of commonly used or compromised passwords.

VeriClouds service complements 2FA and multifactor authentication (MFA) with additional threat intelligence information to help customers proactively identify accounts using credentials already compromised by previous data breaches. This additional information can be combined with 2FA and MFA to further enhance account security for customers.

Privacy By Design with Intel SGX

Intel® Software Guard Extensions (Intel® SGX) is the latest Intel® technology for application developers who seek to protect selected sensitive code and data from disclosure to or modification, by attackers, even those with OS-level privileges. Intel SGX enables such protection through the use of enclaves, which are hardware-protected areas of execution.

Figure 1 shows the structure of CredVerify API service with Intel SGX. The CredVerify API service runs its credential verification process inside an SGX enclave. Compromised credentials stored in VeriClouds database are encrypted with military grade (i.e., AES 256-bit) encryption and can only be decrypted for comparison against the credentials from the clients within the enclave. This solution can be deployed to the data center of an enterprise customer or enabled through a cloud provider.

This architecture enhances privacy of the sensitive credential data at the design level. With the protection by Intel SGX of the credential verification process, the solution helps defend against internal and external attackers, including malware running on the host machine and malicious cloud providers.

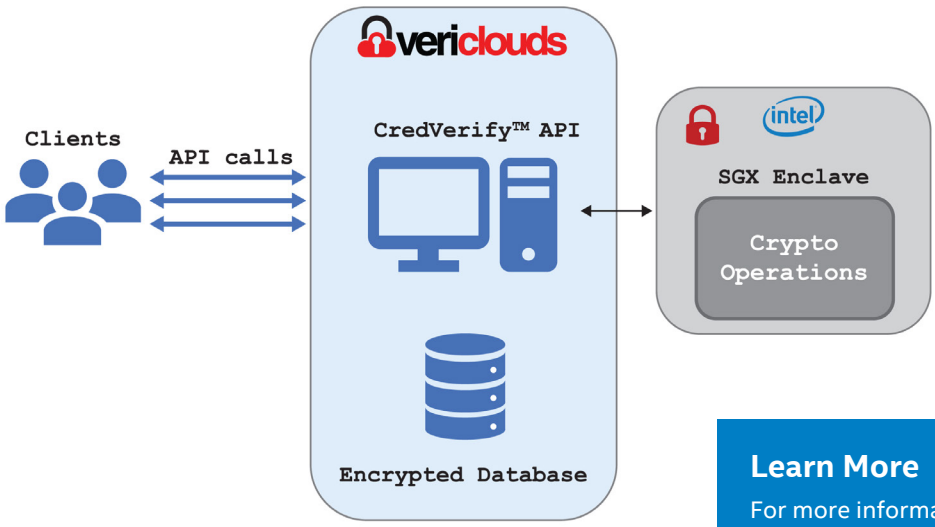

Figure 1: VeriClouds CredVerify* with Intel® SGX

Learn More

For more information about Intel SGX visit:
software.intel.com/en-us/sgx

For Support go to: **intel.com/content/www/us/en/support/contact-support.html#@11**

For more information about VeriClouds visit:
support@vericlouds.com | +1 844 532 5332

[1] http://www.crn.com/news/security/300080151/telecom-partners-say-cloud-security-is-top-of-mind-in-wake-of-verizon-breach.htm [2] Forrester "Forrester Wave™: Privileged Identity Management, Q3 2016" by Andras Cser [1762] with Stephanie Balaouras [1123], Laura Koetzle [607], Merritt Maxim [9125], Salvatore Schiano, and Peggy Dostie, July 2016

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration.

Printed in USA 1017/IA_VERICLOUDS/PSD/DCC/PDF ♻ Please Recycle 1017/PSD/ 00000-001US