Soliton®

OneGate

USE CASES

Soliton

Why Soliton OneGate?

Soliton OneGate provides a centralised approach to strong authentication, enhancing security and efficiency through a single authentication method.

Imagine a world where security seamlessly intertwines with user convenience. Soliton OneGate brings this vision to life, providing a centralised gateway for access to networks and applications. With Soliton OneGate, users have a streamlined access point and an intuitive, effortless logon experience. Behind the scenes, we've integrated the latest and most reliable safety measures, so you don't have to compromise on security. Dive into the future of secure, user-friendly digital interactions with Soliton OneGate.

How Soliton OneGate Makes the Difference

One Identity, One Point of Management

With one identity, one point of management, one set of policies and one secure and strong authentication mechanism, all the identity management projects - single sign-on, provisioning, password management, directory consolidation, strong authentication, role management and audit/compliance - will be simplified.

Logins made easy for the user

Soliton OneGate offers a unified identity solution that simplifies user management across various systems. It streamlines single sign-on, provisioning, and password management through centralised management and consistent policies.

Strong authentication mechanisms enhance security, ensuring reliable access control. Users enjoy password-free entry to networks and cloud services, improving usability.

USE CASE

Use Case 1:

Secure access to networks and Wi-Fi with client certificates

Challenge

Without robust protection, especially in the case of Wi-Fi networks, vulnerabilities arise. Absence of strong authentication can lead to unauthorized access, and Wi-Fi signals are susceptible to interception, potentially granting unauthorized entry without detection.

Opportunity

Implementing strong authentication protocols and security measures for company networks, including Wi-Fi, effectively blocks unauthorized access, safeguarding seamless business operations.

Solution

Soliton OneGate, combined with on-premises NetAttest EPS, delivers robust network authentication minus the typical complexity. Soliton KeyManager aids in client certificate deployment.

USE CASE

Use Case 2:

Divide a network into smaller segments to reduce risks

Challenge

The greater the number of devices on a network, the higher the potential risk of compromise. The initial device could serve as a stepping stone for lateral movement across networks. Moreover, malware spreads more readily, intensifying the extent of damage.

Opportunity

By implementing thorough network segmentation, the risk of device compromise and lateral movement is minimized. This strengthens network resilience and preserves integrity.

Solution

Soliton OneGate and NetAttest EPS simplify network segmentation through dynamic VLAN assignment for devices. If certificates aren't feasible, the integrated MAC-address support offers an alternative solution.

USE CASE

Use Case 3:

Enable federated access to cloud applications using a client certificate

Challenge

Setting up accounts individually for every cloud service poses challenges, including heightened complexity in credential management, increased security vulnerabilities from multiple passwords, and inefficiencies in access control across diverse platforms.

Opportunity

Employing federation and a single identity provider simplifies access management, strengthens security via centralized authentication, and increases user experience with seamless single sign-on capabilities.

Solution

Soliton OneGate can provision chosen cloud services and establish federation with nearly all of them. A valid client certificate is a required authentication factor in this process.

USE CASE

Use Case 4:

Eliminate passwords from the login process

Challenge

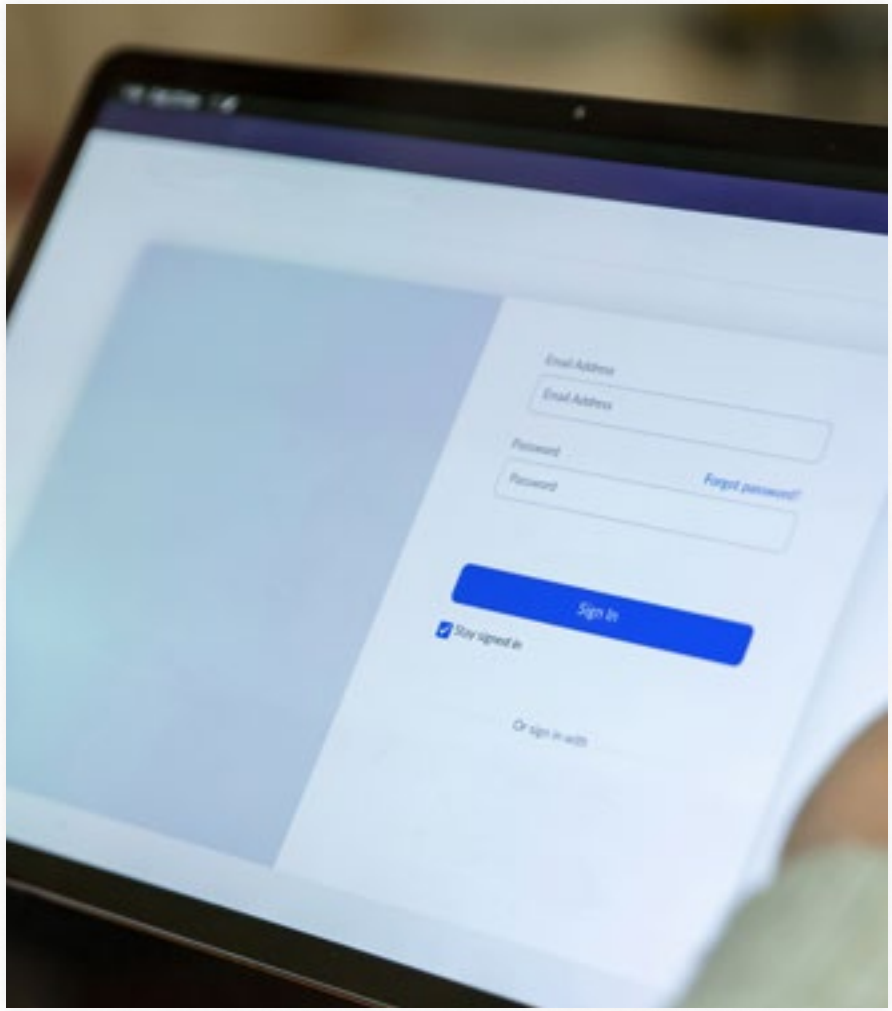
Passwords pose challenges as they demand users to recall numerous intricate strings for various services. This can result in security risks if passwords are forgotten, reused, or managed incorrectly.

Opportunity

Implementing a solution that supports multiple passwordless login methods would not only enhance security but also significantly elevate the user experience.

Solution

Soliton OneGate supports the FIDO2 standard and an authenticator app, both of which enable the elimination of passwords from the login process. This can be achieved through alternatives like Windows Hello or a YubiKey.



USE CASE

Use Case 5:

Use password management when federated logins are not feasible

Challenge

When applications lack support for federated logins or their implementation is cost-prohibitive, the situation shifts to managing various standalone authentication processes. This amplifies access control complexity, heightens security vulnerabilities, and culminates in a fragmented and inefficient user experience.

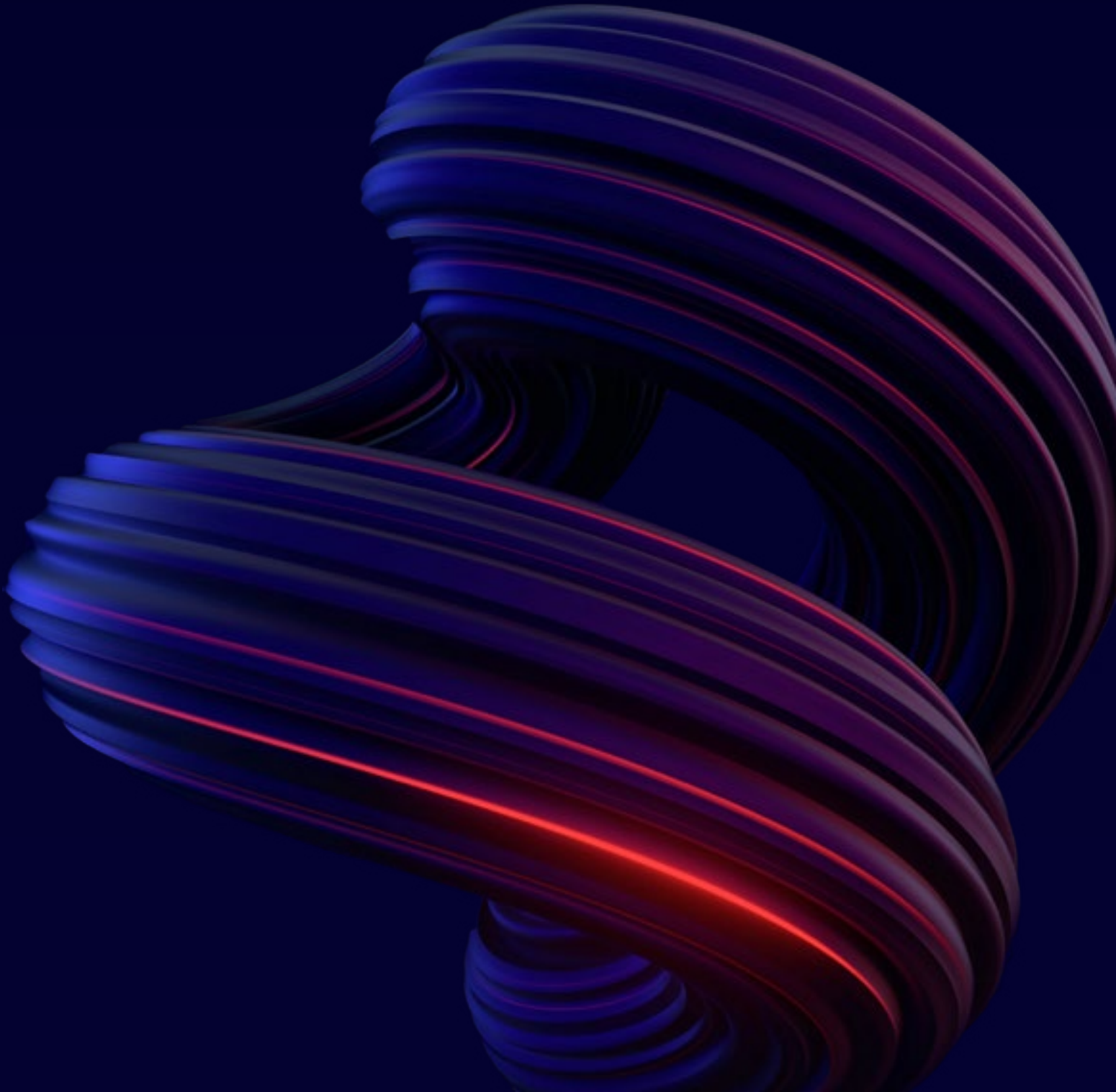
Opportunity

Utilizing a password manager that automatically inserts intricate passwords on behalf of the user eliminates the requirement to memorize or manually handle individual passwords. This approach effectively boosts security.

Solution

If federated access isn't an option, the integrated password manager can furnish applications, both internal and cloud-based, with usernames and intricate passwords.

Soliton®



Thinking about Soliton OneGate?

Contact us via one of the channels below to find out more about how Soliton OneGate can help

solitonsystems.com

emea@solitonsystems.com

+31 20 896 5841