Company: Cisco Systems, San Jose, CA, USA
Company Description: Shape the future of the Internet by creating unprecedented value and opportunity for our customers, employees, investors, and ecosystem partners.
Nomination Category: Product & Service Categories - Business Technology Solutions
Nomination Sub Category: Identity & Access Security Solution
Nomination Title: Secure Adaptive Password Reset (SAPR)
Service: Enhancing security and user experience

1. Which will you submit for your nomination in this category, a video of up to five (5) minutes in length about the the nominated new or new-version product or service, OR written answers to the questions for this category? (Choose one):

   Written answers to the questions

2. If you are submitting a video of up to five (5) minutes in length, provide the URL of the nominated video here, OR attach it to your entry via the "Add Attachments, Videos, or Links to This Entry" link above, through which you may also upload a copy of your video.

3. If you are providing written answers for your submission, you must provide an answer to this first question: If this is a brand-new product, state the date on which it was released. If this is a new version of an existing product, state the date on which the update was released:

   This is a brand-new service, released on December, 2024.

   The legacy password management solution was significantly outdated, relying on older security mechanisms such as security questions and SMS-based authentication. It lacked modern security features like multi-factor authentication (MFA), advanced encryption standards, and support for Single Sign-On (SSO). Additionally, the tool was built as an on-premises solution, requiring enterprise users to log in to VPN to change or reset their passwords. If a user forgot his password, he was unable to access the VPN and could not use the legacy password manager for self-service password resets. Instead, he had to create a support case to have his password reset by the support team.

   The new service adopts a passkey-first approach and is enabled with Zero Trust principles. It employs comprehensive end-to-end encryption to safeguard users' passwords. With enhanced security built into the solution, enterprise users no longer need to be on VPN to reset their passwords, providing a significantly improved user experience.

4. If you are providing written answers for your submission, you must provide an answer to this second question: Describe the features, functions, and benefits of the nominated product or service (up to 350 words):

   Total 337 words used.

   The new **Secure Adaptive Password Reset** -**SAPR**- service addresses the critical need for a secure, user-friendly, and adaptable password reset solution for enterprise environments.

   Functions:

   1. **Passkey-First Approach**: enforcement of passkey-based authentication as the primary method for password reset. This approach is resistant to phishing attacks and provides simpler user experience. 96% of the workforce is enabled by this approach.
   2. **Adaptive Multi-Factor Authentication –AMFA- Fallback:** for the users are not yet adopted to passkey authentication, this service dynamically assesses user risk profiles and device posture to determine the appropriate authentication factors required, such as, device trust, verified push, location, user behavior, email OTP etc.
   3. **Seamless User Experience with Contextual Flows:** intelligently presents the appropriate authentication flow based on the user's risk profile and device postures. For users with registered passkeys, the reset process requires minimal interaction. For those requiring AMFA, the system provides clear and concise instructions, minimizing confusion and frustration.
   4. **Enhanced Observability and Auditing:** integrates comprehensive logging and auditing functionalities, offering detailed insights into all password reset attempts.
   5. **Modular and Adaptable Architecture:** The system is designed to be adaptable to evolving enterprise needs and security landscapes. This includes the ability to easily integrate with emerging technologies as plug and play solution.
   6. **Proactive Fraud Detection:** Suspicious activity triggers automated alerts and can initiate further investigation or even temporarily block reset attempts.
   7. **End-to-End Encryption:** Passwords are encrypted with the user's public key; keys are provisioned at the time of user onboarding. This ensures that even if the system was compromised, the data remains protected.

   Benefits:

   Better Security: SSO enabled, Zero-Trust enabled, Passkey authentication enabled, comprehensive end-to-end encryption to safeguard user's password

   Improved User Experience: Enable quick password resets from trusted users and devices, while providing adaptive AMFA callback with clear instructions for the ones with lower trust score

   Future-Proof Architecture: A modular, plug-and-play design ensures the solution's longevity and adaptability to future security standards.

   Increased Efficiency and Reducing Support Cases: eliminating the need to contact the helpdesk when users forget their password and cannot access the password portal remotely.

5. If you are providing written answers for your submission, you must provide an answer to this third question: Outline the market performance, critical reception, and customer satisfaction with the product or service to date. State monetary or unit sales figures to date, if possible, and how they compare to expectations or past performance. Provide links to laudatory product or service reviews. Include some customer testimonials, if applicable (up to 350 words):

   Total 201 words used.

   - **96%** of the workforce is now able to reset their passwords using a Passkey-First approach, resulting in a **50%** reduction in password reset processing time.
   - **Improved User Experience:** according to a recent survey, the user satisfaction score is an impressive 9.8 out of 10, highlighting the highly positive reception of this new service among users.
   - **Reduced Support Cases:** Significant drop in password-related helpdesk cases.
   - **Enhanced Security Posture:** fewer password-related breaches
   - **Better Observability:** SAPR solution provides extensive logging for fast anomaly detections and risk remediation.
   - **User testimonials:** "The instructions were straightforward and easy to follow – no issues."; "The user experience felt nice and unique."; "Password reset has never been easier."; "Cisco's password management solution has not only strengthened our security posture but also enhanced productivity and user satisfaction. "; ""From a security perspective, the new password management solution represents a significant improvement in our overall posture. The shift to new hires setting their own passwords via a secure personalized link is a positive step in reducing the risk associated with temporary passwords. The self-service capabilities, particularly the remote password reset functionality, are valuable, but require ongoing monitoring to ensure proper usage and prevent potential abuse. " etc

6. You have the option to answer this final question: Reference any attachments of supporting materials throughout this nomination and how they provide evidence of the claims you have made in this nomination (up to 250 words):

   Total 43 words used.

   Please find the attached document for additional details:
   SAPR_Whitepaper_Stevie_submission.pdf

   The attached document covers:

   - Why the need for the new SAPR service and what are the advantages
   - The architecture
   - The user experience workflows
   - The impact of this new services and the user testimonials

Attachments/Videos/Links:

Secure Adaptive Password Reset (SAPR) Service: Enhancing security and user experience

[REDACTED FOR PUBLICATION]