[Joint Solution Brief]

Zero Trust Password Reset: Closing the Loop on Scattered Spider Tactics

WHY THIS MATTERS NOW

High-profile attacks from groups like Scattered Spider have exposed a critical weak point in many enterprises: password reset requests. These actors bypass MFA and helpdesk defenses by convincingly impersonating employees and contractors especially in large, distributed environments with complex identity ecosystems.

A compromised password reset = full compromise of an identity.

The Threat Pattern

- Attackers impersonate users via helpdesk or self-service channels
- Exploit weak reset flows: insufficient identity verification, over-reliance on call scripts
- Bypass MFA enrollment by owning the reset pathway
- Laterally move via SSO-integrated systems

Impacted Roles	Risk Domains
Helpdesk, IAM Teams, Security Ops, Remote Userbase	Unauthorized access, account takeover, data breach, compliance violation

THE SOLUTION

Zero Trust Password Reset: Verified Identity Reset Loop

SDG and ID Dataweb have partnered to embed real-time, zero trust based identity proofing directly into the password reset process ensuring only legitimate users can request and complete resets.

ID Dataweb Verification Layer

Leverages trusted data sources (credit bureau, telecom, device ID, real-time images) to verify users in real-time before reset flow continues.

SDG Managed ID Proofing Services

SDG implements, monitors, and escalates across the reset lifecycle:

- Tiered reset flows: self-service, verified, escalated
- Helpdesk integration with ID proofing checkpoints
- Reporting and threat detection for anomalous reset behavior

HOW IT WORKS

Once ID Dataweb is deployed, SDG can support your long-term success, offering tailored support, and managed services:

1. Reset Request Initiated	Trigger ID Dataweb challenge (KBA, device match, document upload, etc.)
2. Verified or Escalated	Verified users continue; uncertain cases routed to SDG's support with enriched context
3. Reset Finalized + Logged	Risk-scored, tracked, and auditable

WHY ENTERPRISES TRUST THIS MODEL

- Designed for global, hybrid enterprises
- Reduces risk of helpdesk social engineering
- Aligns with Zero Trust & NIST 800-63 standards
- Integrates with existing IAM platforms (Okta, Entra ID, etc.)
- Modular rollout: Start with high-risk user groups or VIPs

NEXT STEP

Assess Your Helpdesk / Password Reset Process

SDG offers a **no-cost discovery workshop** to map your current reset flows, identify exposure, and show how ID proofing cemented in zero trust principles can reduce risk by over 90%.

Contact us to secure the weakest link in your identity lifecycle. **Solutions@sdgc.com**

ABOUT SDG

With more than 30 years of experience partnering with global enterprises on complex business and IT initiatives, SDG is a trusted provider of advisory, transformation, and managed services. The firm empowers organizations to strengthen cyber resilience by integrating AI into identity, threat, and risk management solutions that protect digital assets and deliver measurable business value. Learn more at www.sdgc.com.

ABOUT ID DATAWEB

ID Dataweb provides cross-channel digital trust to prevent account takeover and account opening fraud. As organizations move towards 100% digital interactions with their users, they need to ensure that the digital person on the other end of the line is the physical person they expect, whether a customer, partner or employee. ID Dataweb provides a frictionless yet highly-secure process to provide that digital trust with the user by verifying their identity to the highest level of assurance. For more information, visit iddataweb.com.

SDG
75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com

Contact Us: solutions@sdgc.com

© Copyright 2025. SDG Corporation. All rights reserved.