

ZeroPassword™ for Defense & Aerospace

Account Takeover Protection Brief



The Challenge: Identity is the New Attack Surface

Attackers targeting the Defense Industrial Base don't need to break in when they can log in.

- Credential theft and phishing are primary attack vectors
- Remote access (VPN, RDP, SSH) systems remain exposed
- Compromised identities often have elevated privileges
- Production systems rely on passwords and lack MFA coverage

The gap - most organizations:



Have MFA for cloud apps



Lack coverage across desktops, legacy apps, and privileged workflows



Rely on passwords + weak MFA (OTP, push, SMS)

At the same time, regulators are raising the bar:

- CMMC Level 2 requires MFA for all privileged accounts, and all network access to non-privileged users
- Contractors must prove enforcement and produce evidence during assessments
- Failure to comply can result in loss of DoD contracts

Why traditional approaches fall short

SSO	Password managers	Standard MFA
<ul style="list-style-type: none"> ✓ Strong for SaaS 	<ul style="list-style-type: none"> ✓ Improve hygiene 	<ul style="list-style-type: none"> ✓ Improves security when implemented right
<ul style="list-style-type: none"> ✗ Do not cover legacy apps, endpoints, RDP, SSH, or air-gapped systems 	<ul style="list-style-type: none"> ✗ Still rely on user managed credentials that can be stolen 	<ul style="list-style-type: none"> ✗ Still phishable, lack of coverage for legacy apps

The bottom line: As long as passwords exist, compliance remains a challenge, and identity remains an attractive attack surface.

The Solution: ZeroPassword™

Eliminate passwords. Close the gaps. Prove compliance.

ZeroPassword™ by Secret Double Octopus replaces passwords with phishing-resistant, device-based authentication and extends it across all workforce access points - including legacy systems.



Eliminates passwords (not just hides them)

- Removes user-managed credentials entirely
- Prevents credential theft, replay, and phishing
- Uses cryptographic, device-bound MFA

→ No passwords = nothing to steal



Extends phishing-resistant MFA everywhere

Covers systems traditional IAM cannot: on-prem, mission-critical, old and legacy infrastructure, non-modernized systems, operationally sensitive environments

→ Full workforce coverage, not just SaaS



Helps closing CMMC & NIST compliance gaps

- Enforces MFA across privileged and non-privileged access
- Aligns with CMMC Level 2 expectations
- Enables consistent enforcement across all systems

→ From partial compliance → defensible posture



Provides audit-ready evidence

- Centralized control & visibility of workforce authentication
- Proof of enforcement across systems and users

→ Simplifies audits and CMMC assessments



Modernizes without disrupting mission systems

- No need to rewrite or replace legacy applications
- Works alongside existing identity infrastructure (AD, IdPs, biometric / authentication hardware)
- Preserves operational continuity

→ Secure legacy without breaking it



The ZeroPassword™ Advantage

	ZeroPassword™	Password-based MFA
Secrets set by	✦ Algorithm	👤 Users
Reused across apps	🛡️ Never	🛡️ Often
Phishing-resistant by design	✅ Yes	❌ No
Resistant to guessing/brute-force	✅ Yes	❌ No
Automatically rotates	✅ Yes	❌ No
Works across legacy + modern systems	✅ Yes	❌ No

Key benefits for defense & aerospace

Reduce mission risk

- Eliminate credential-based attacks
- Protect engineering environments and CUI

Secure legacy environments

- Extend modern authentication to systems others cannot reach

Improve compliance readiness

- Meet CMMC / NIST MFA requirements
- Reduce audit findings and remediation cycles

Lower operational burden

- Eliminate password resets and credential management

About Us

At Secret Double Octopus, we believe authentication should be stronger, simpler, and completely password-free. Our patented ZeroPassword™ technology eliminates passwords even from legacy and on-prem systems, delivering unmatched security and user experience. Our platform integrates seamlessly into any infrastructure, supporting any system, use-case, or authentication method.

Trusted by Fortune 500 defense manufacturers and financial organizations alike, we secure billions of authentications annually, enabling organizations to achieve modern, phishing-resistant security at scale.

See how ZeroPassword™ eliminates passwords and secures your entire workforce environment-without disrupting operations.

[Get a Demo](#)

Trusted by the world's most heavily regulated organizations.

