

# ID Verification for Microsoft Entra



## The Human Firewall

**Protect Critical Access Points from  
Onboarding to Account Recovery**



# State-sponsored attackers are infiltrating organizations through digital impersonation.



Recent investigations have revealed North Korean IT workers successfully infiltrating Fortune 500 companies by using stolen identities and sophisticated deception techniques. These foreign operatives are dispatched to deceive businesses worldwide into hiring them as remote workers, with security experts reporting that numerous major companies have unknowingly hired these threat actors.

These sophisticated attackers bypass traditional security measures by exploiting the weakest link in security chains: **human verification**.

## Protect Critical Access Points: New Hires and Existing Staff

### Building a human firewall starts at organizational entry points

The onboarding process represents a significant security vulnerability for organizations. Investigations have documented how sophisticated threat actors establish "laptop farms" in the U.S. to mask their true location and use advanced tactics to appear legitimate during traditional hiring processes.

Without robust identity verification during onboarding:

- Imposters gain legitimate credentials in systems
- Threat actors obtain authorized access to sensitive data
- Security breaches occur with valid authentication
- Foreign agents can exfiltrate proprietary data and conduct extortion
- Organizations face compliance violations and reputational damage

### Extending verification to existing staff and privileged access

While onboarding presents the primary entry point for imposters, robust identity verification is equally critical for existing staff, particularly when accessing sensitive systems or performing high-risk actions. Adding identity verification for privileged access helps mitigate insider threats and prevent account takeovers of established identities.

# Beyond Devices: Verify the Person

## Device verification alone leaves security gaps

While Multi-Factor Authentication and device verification provide essential security layers, they cannot answer the most critical question: Is this actually the person they claim to be?

ID Verification with biometrics creates an essential human firewall by:

- Authenticating government-issued IDs through advanced document proofing
- Confirming physical presence with sophisticated liveness detection
- Matching biometric identifiers to prevent impersonation attempts
- Creating a verified digital identity within Microsoft Entra ID environments

## Enhance Existing Security Measures

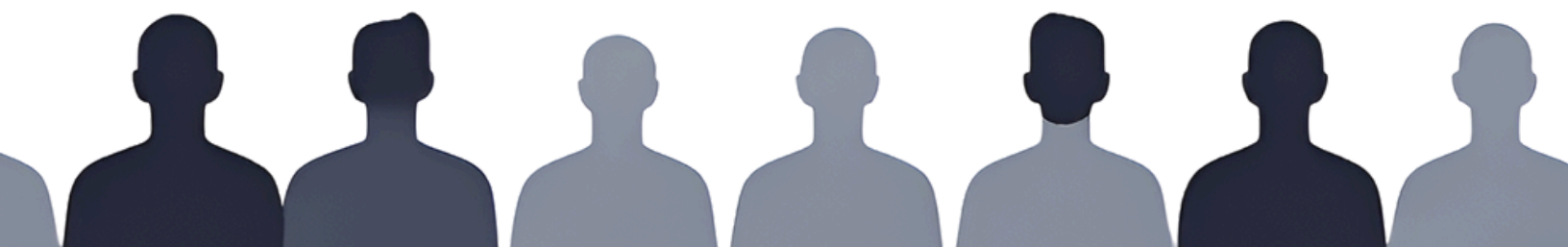
**ID Verification doesn't replace current security investments—it strengthens them:**

- Reinforce MFA processes by adding biometric verification to traditional factors
- Secure account recovery workflows to prevent credential reset exploits
- Add human verification to high-risk transactions and access requests
- Create a continuous trust model that extends beyond initial authentication

## Protect Account Recovery - A Common Security Vulnerability

Account recovery processes are frequently exploited by attackers who bypass strong authentication by targeting weaker recovery methods. ID Verification adds critical protection to password resets and account recovery workflows by:

- Requiring identity verification before recovery processes begin
- Validating the requestor's identity against their established enrollment record
- Preventing unauthorized access through compromised email accounts or social engineering
- Creating an auditable verification trail for all recovery attempts



# The Power of ID Verification Orchestration

## A comprehensive security approach transforming enterprise identity assurance

ID Verification Orchestration serves as the foundation for building effective human firewalls. This strategic platform connects verification touchpoints across organizations—from onboarding to account recovery to high-risk transactions—creating a consistent, enterprise-wide identity verification fabric. By orchestrating biometric verification, document proofing, and liveness detection at each critical access point, organizations establish continuous identity assurance that adapts to evolving threats.

ID Verification Orchestration integrates document verification, biometrics, and liveness detection into unified security workflows that can be implemented across multiple use cases and systems—creating a comprehensive identity verification strategy rather than isolated point solutions.

## Enterprise-Grade Identity Assurance

**Built for large organizations with complex security requirements.**

Our ID Verification solution integrates seamlessly with Microsoft Entra, providing:

- **Enterprise-scale deployment** across global operations
- **Zero-code implementation** - no custom development required
- **Harmony with the entire MS Entra suite** including integration with Microsoft's robust range of security and governance tools
- **Enhances Verifiable Credentials** - adds powerful identity proofing to Microsoft Entra's Verified ID decentralized identity solution
- **Continuous authentication** beyond initial verification
- **Detailed audit trails** for security and compliance reporting
- **Seamless user experience** balancing security and accessibility

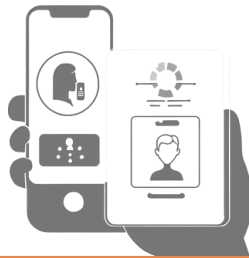


# Implementation Without Disruption

**Rapid deployment with minimal effort—go live in days, not months:**

- **Zero-code deployment** - implement without any custom development
- **Phased deployment** tailored to organizational needs
- **Seamless integration** with existing Microsoft environment
- **Customized workflows** for specific verification requirements
- **Vendor flexibility** - works with any ID Verification provider of choice




This solution is designed to integrate with preferred ID Verification providers, allowing organizations to leverage existing partnerships or select the vendor that best meets specific requirements and compliance needs. The provider-agnostic approach enables organizations to switch vendors without disruption or even combine multiple providers for enhanced verification options and redundancy.



**Take Action Now**

Don't wait for a security breach to expose vulnerabilities. Protect your organization beyond devices—verify the person. Contact IdRamp today.

## FOR MORE INFORMATION

-  +1 (515) 808-2822
-  <https://idramp.com/contact>
-  [info@idramp.com](mailto:info@idramp.com)

