# MultiFactor Authentication: From Zero to Implementation

**Phillip Reynolds**
Datacenter Engineer
preynolds@datanetworksolutions.com

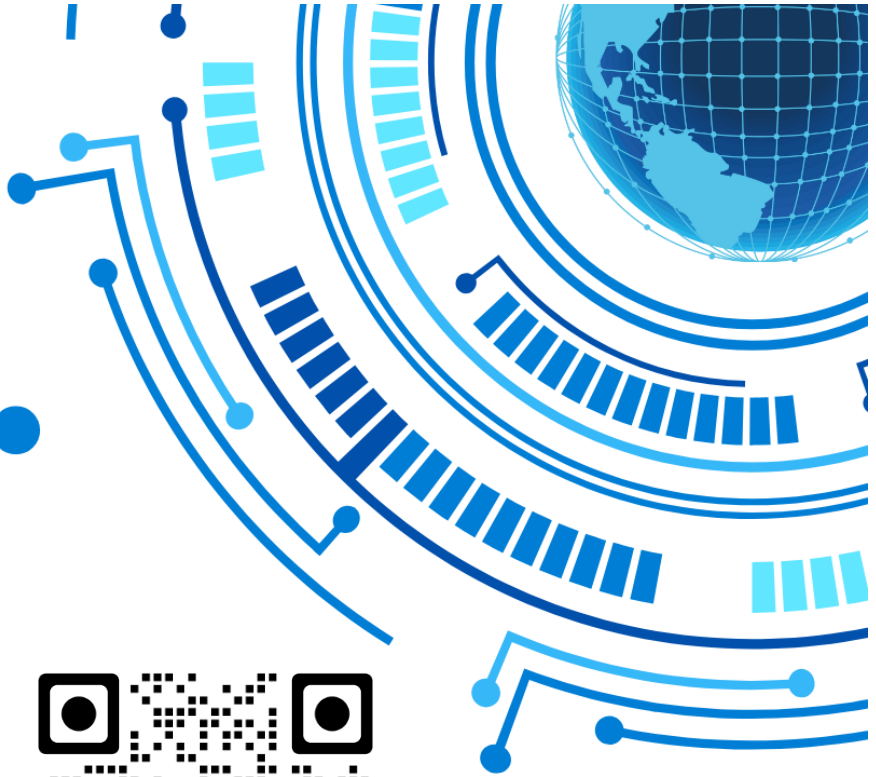

Data Network Solutions

# About Me

**Datacenter Pre-sales Engineer**

- **Datacenter (SAN, VM, etc.)**
- **Nutanix**
- **VDI**
- **Security**

**Former VP of IT and Compliance for a student loan collection agency**



# About DNS

**Value added, services oriented organization specializing in:**

- **Security-Firewall**
- **Network**
- **Datacenter**
- **Wireless**
- **Backup and Disaster Recovery**

**www.datanetworksolutions.com**

# Our Core Partners

# Additional Technology Partners

# Current Threat Landscape

**80%+**

**Credential Breaches**

Data breaches involving compromised credentials according to Verizon DBIR 2024

**4.5B**

**Exposed Records**

Credentials exposed annually through various attack vectors

**99.9%**

**Attack Prevention**

Reduction in automated attacks when MFA is properly implemented

Credential stuffing attacks exploit password reuse across platforms, while ransomware campaigns frequently begin with stolen login credentials. MFA deployment significantly reduces unauthorized access risk.


***“If we ain’t killin’ chickens, we ain’t making money.”***

-Anonymous Chicken

Farmer IT Director

# Learning from High-Profile Incidents

### Colonial Pipeline (2021)

**Attack Vector:** Compromised VPN credentials without MFA protection

**Impact:** National fuel supply disruption, $4.4M ransom payment

### Uber (2022)

**Attack Vector:** MFA fatigue exploitation through persistent push notifications

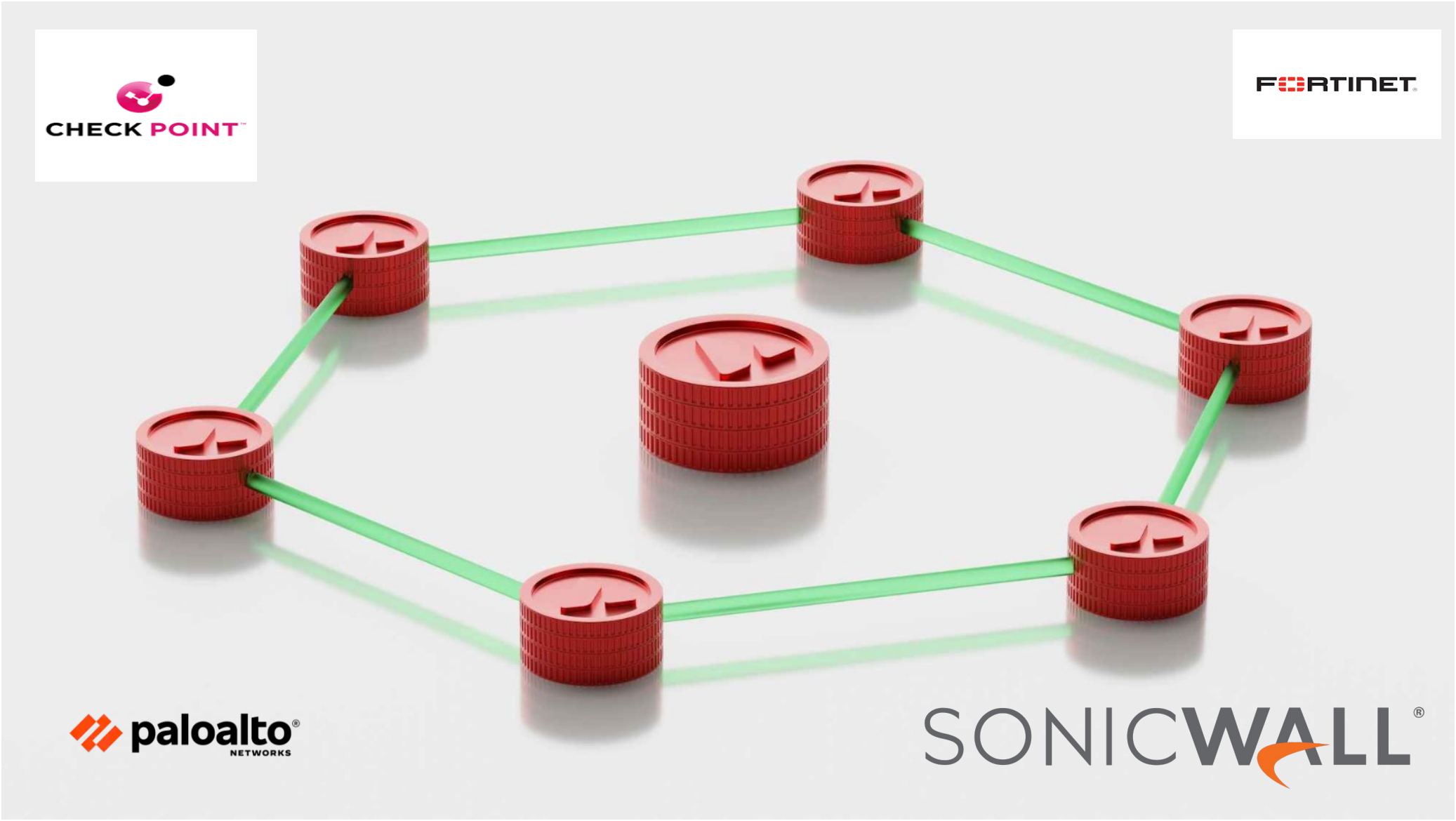
**Impact:** Complete corporate network compromise

### Microsoft (2023)

**Attack Vector:** State actors bypassed weak authentication flows

**Impact:** Access to sensitive government communications

⊗ **Critical Lesson:** Absence of MFA or poorly implemented MFA creates systemic organizational risk that can lead to catastrophic business disruption.


CHECK POINT
FORTINET
paloalto NETWORKS
SONICWALL

**Identity is the new perimeter.**

# Understanding Multifactor Authentication

MFA requires authentication using two or more independent factors from different categories, creating multiple security barriers against unauthorized access.

## Something You Know

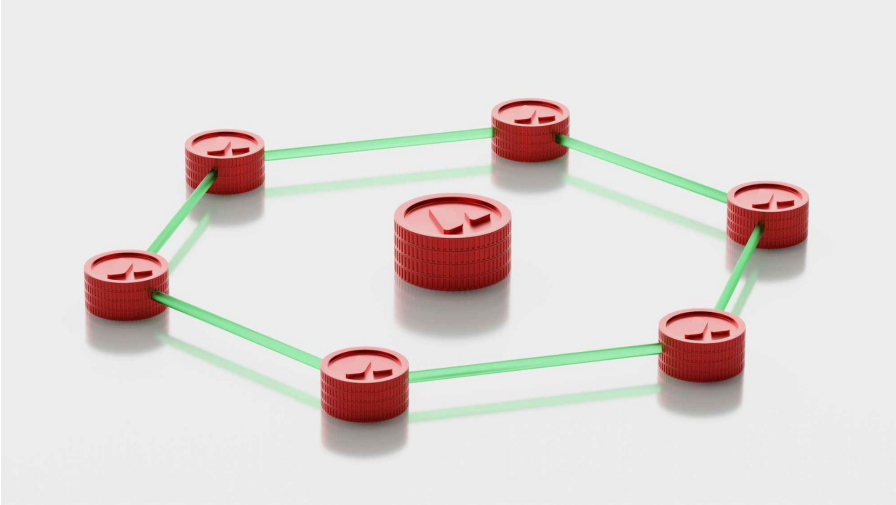
Passwords, PINs, security questions, or other knowledge-based credentials

## Something You Have

Hardware tokens, smartphones, smartcards, or physical authentication devices

## Something You Are

Biometric identifiers including fingerprints, facial recognition, or iris scanning



**Technical Distinction:** 2FA specifically uses exactly two factors, while MFA encompasses two or more authentication factors for enhanced security.


# Strategic Benefits of MFA Implementation

**Phishing Mitigation**

Significantly reduces effectiveness of credential harvesting and social engineering attacks

**Breach Containment**

Prevents lateral movement within networks following initial credential compromise

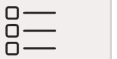
**Remote Access Security**

Secures VPN connections, SaaS applications, and cloud management consoles

**Compliance Requirements and Cyber Insurance**

Meets requirements for PCI-DSS, HIPAA, NIST frameworks, and ISO 27001 standards

# Phase 1: Comprehensive Assessment



**Asset Inventory**

Catalog all user accounts, systems, and applications requiring authentication across the entire infrastructure

**Risk Classification**

**Critical:** Domain administrators, financial systems
**Medium:** Departmental applications
**Low:** Non-sensitive services

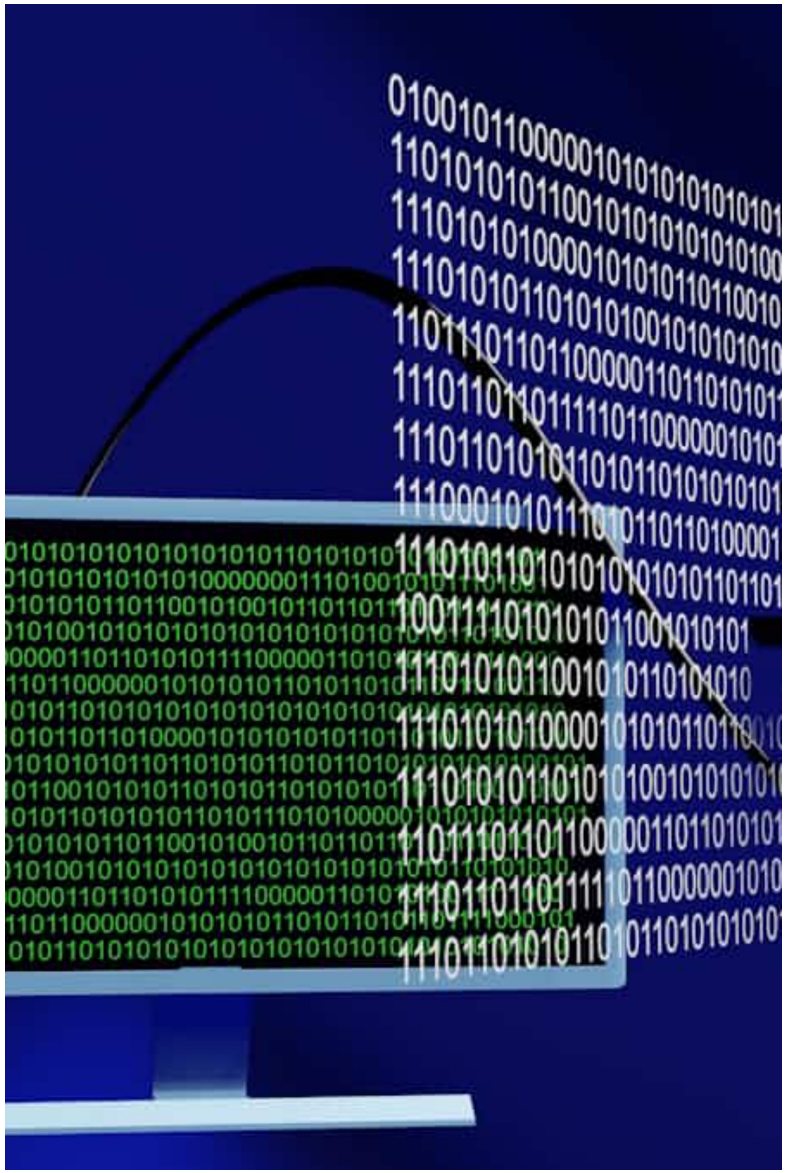
**Compliance Mapping**

Align MFA requirements with industry regulations and internal security policies

# Phase 2: MFA Method Selection Matrix

| Method | Security Level | User Experience | Cost |
|---|---|---|---|
| SMS/Voice | Low | High | Low |
| Authenticator Apps (TOTP) | Medium | Medium | Low |
| Push Notifications | Medium | High | Medium |
| Hardware Tokens (FIDO2) | High | Medium | High |
| Biometrics | High | High | High |

Strategic selection requires balancing security requirements, user adoption, and operational costs. SMS remains vulnerable to SIM swapping attacks, while hardware tokens provide strongest protection.
Expect new methods in the future.



# Phase 3: Infrastructure Readiness

01

## Directory Integration

Ensure compatibility with Active Directory, Azure AD, LDAP, and other identity providers

02

## Protocol Validation

Verify support for SAML, OIDC, OAuth 2.0, and RADIUS federation protocols

03

## Device Compatibility

Test endpoint devices, mobile platforms, and legacy system integration capabilities

04

## Network Segmentation

Implement proper network isolation for authentication servers and certificate authorities

# Step 1: Policy Framework Development

| Scope Definition | Method Authorization | Fallback Mechanisms |
| --- | --- | --- |
| • Universal MFA vs. role-based requirements<br>• Administrator account prioritization<br>• Service account exceptions | • Approved authentication factors<br>• Mandatory vs. optional methods<br>• Device registration limits | • Temporary bypass procedures<br>• Recovery code generation<br>• Emergency access protocols |

Comprehensive policies should address edge cases including device loss, network connectivity issues, and emergency access scenarios while maintaining security standards.


# Step 2: Application Integration Validation

**Native Integration Testing**

- Azure AD and Office 365 integration
- Okta, Duo, and Ping Identity platforms
- Native mobile and web application support

**Standards-Based Integration**

- SAML and OIDC federation protocols
- RADIUS authentication for network devices
- API authentication and service accounts

- **Critical Workflow Testing**

  Validate SSO portals, VPN clients, SSH connections, and cloud management consoles

- **Performance Monitoring**

  Track authentication success rates, response times, and user experience metrics

- **Failure Analysis**

  Monitor failed attempts, timeout issues, and integration compatibility problems

# Step 3: Controlled Pilot Deployment

01

**Pilot Group Selection**

Deploy to IT staff, security team, and selected power users who can provide technical feedback

02

**Enrollment Testing**

Validate user registration workflows, device pairing, and backup authentication methods

03

**Experience Validation**

Monitor login patterns, failure rates, and gather comprehensive usability feedback

04

**Configuration Refinement**

Optimize settings based on pilot results before enterprise-wide deployment

Pilot phase typically involves 5-10% of total user base and runs for 2-4 weeks to identify potential issues.

# Step 4: Strategic Rollout Approach

1. **Phase 1: Critical Assets**

   Deploy to high-privilege accounts, domain administrators, and financial system users first

2. **Phase 2: Remote Access**

   Implement for VPN users, remote workers, and cloud service administrators

3. **Phase 3: Department Rollout**

   Deploy department by department, starting with IT-savvy groups

4. **Phase 4: Complete Coverage**

   Extend to all remaining users including contractors and third-party access

Phased implementation reduces support burden while ensuring critical systems receive protection first. Include comprehensive training and communication campaigns to minimize user resistance.

# Step 5: Monitoring and Incident Response

### Centralized Logging

Integrate MFA events with SIEM platforms for comprehensive security monitoring and correlation

### Alert Configuration

Set triggers for repeated failures, MFA fatigue attacks, and unusual OTP request patterns

### Incident Playbooks

Develop response procedures for compromised accounts, device theft, and authentication bypasses

# Step 6: Optimization and Continuous Improvement

### Metrics Analysis

Track adoption rates, user satisfaction scores, and authentication performance indicators

### Future Readiness

Prepare for emerging standards including WebAuthn and complete passwordless frameworks

### Method Upgrades

Migrate from weak factors like SMS to stronger FIDO2 tokens and passwordless authentication

### Security Reviews

Conduct regular policy assessments and penetration testing of authentication systems

# MFA Implementation: Critical Success Factors

### Proven Attack Mitigation

MFA prevents 99.9% of automated attacks when implemented correctly, making it essential for modern security

### Implementation Excellence

Success requires thorough assessment, careful method selection, and robust infrastructure preparation

### Operational Discipline

Phased deployment with comprehensive policies and continuous monitoring ensures long-term effectiveness

# Entra ID MFA and Conditional Access Tips

# Entra ID Tips

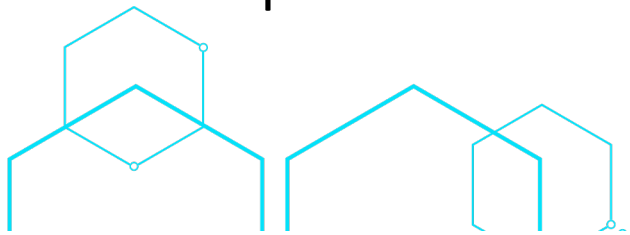
- **Protect Registration from Sign-in Risk Events**
  - –Users:  All Users
  - –Target Resources:  User Actions > Register security info
  - –Conditions:  Sign-in Risk > High, Medium, Low
  - –Grant:  Block
- **Protect Registration from User Risk Events**
  - –Users:  All Users
  - –Target Resources:  User Actions > Register security info
  - –Conditions:  User Risk > High, Medium, Low
  - –Grant:  Block

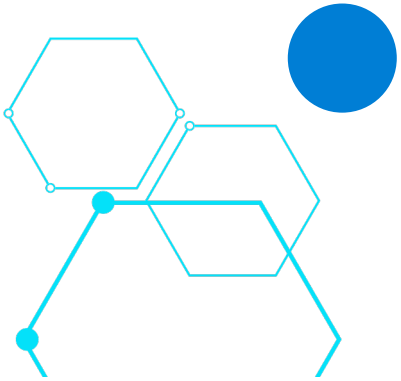
*****Always put in monitor mode first*****

# Service Accounts

- **Where possible, use PKI**
- **Block interactive logons** (RDP and log in locally) via Group Policy
- Create Conditional Access policies exempting the service account application's IP address from MFA
- Use privilege escalation management tools
- 25+ character passwords hidden in a password vault…

*In other words…* a human should never know a service account's password



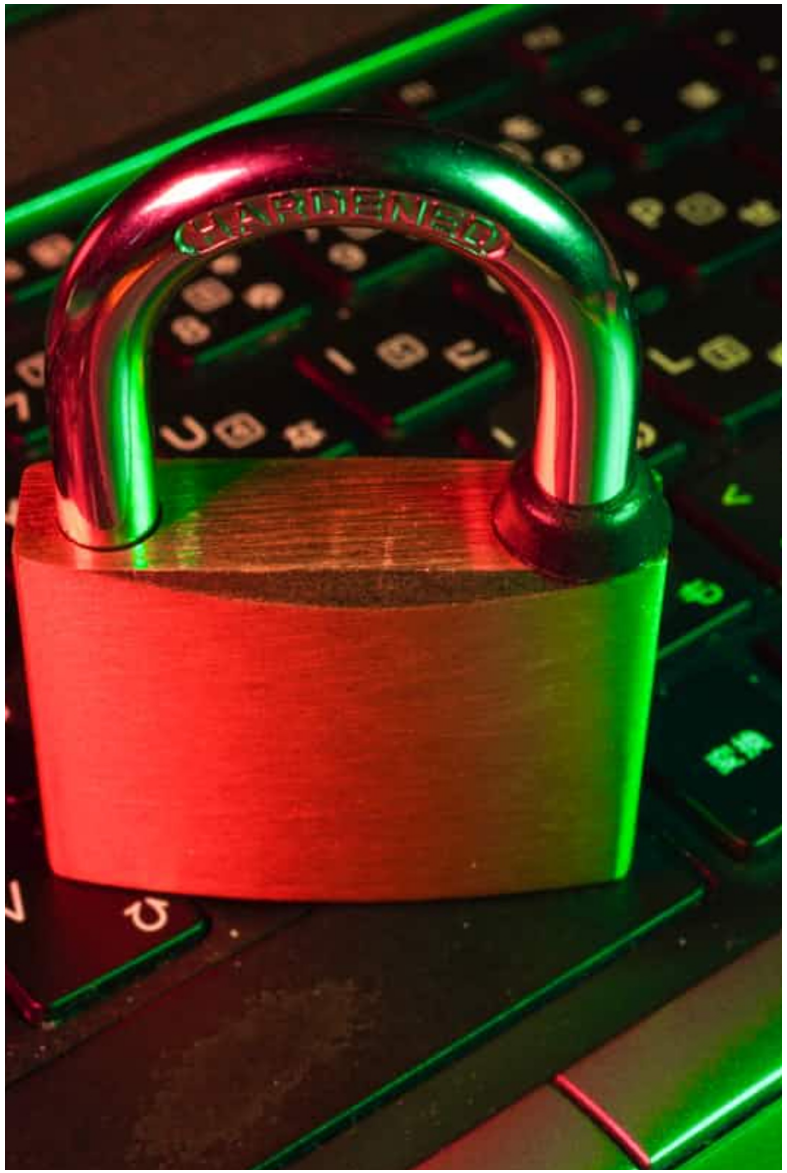


# MFA is not perfect

- Token/session-based MFA bypass is **one of the most prevalent post-authentication attack vectors** in Microsoft 365.
- MFA **is not the end of the road** — continuous monitoring and token hygiene are essential.

# MFA is not optional—it's a critical security baseline

*Organizations without comprehensive MFA deployment face unacceptable risk in today's threat landscape*




# Multifactor Authentication (MFA): From Zero to Implementation

**Phillip Reynolds**
**Engineer, Data Network Solutions**
**803-722-0574**
**preynolds@datanetworksolutions.com**