INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-25 06:50 UTC

Microsoft Entra Device-Bound FIDO2 Passkeys Expand Passwordless Coverage to Unmanaged Windows Devices

SECURITY ANALYSIS | MEDIUM | CVSS 5.0

SCC Item ID	SCC-STY-2026-0083
Type	Security Analysis
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Microsoft Entra ID, Windows (managed and unmanaged/personal devices), Windows Hello, Microsoft Entra-protected SaaS resources
Published	2026-04-24T14:13:55
Discovery Source	Rss

Executive Summary

Microsoft is expanding credential-phishing-resistant FIDO2 passkey authentication in Entra ID to cover unmanaged and shared Windows devices, closing an authentication gap that adversaries have actively exploited through password spray, MFA fatigue, and token theft against Entra-protected SaaS environments. This rollout, targeting general availability by mid-June 2026, represents a structural shift in how organizations can extend strong authentication beyond managed device fleets without requiring full device enrollment. Security and IAM leaders should treat this as a policy review trigger, not a passive upgrade, as Conditional Access configurations will determine whether the new credential class is trusted appropriately relative to hardware-backed and managed device credentials.

Technical Analysis

The authentication gap Microsoft is closing reflects a documented pattern in Entra ID-connected SaaS environments, where credential-based attacks have exploited inconsistencies between managed device posture and unmanaged device access. See MITRE ATT&CK T1078 (Valid Accounts), T1078.004 (Cloud Accounts), and T1110 (Brute Force) for attack framework context. Adversaries exploiting these techniques have relied on the inconsistency between managed device posture and unmanaged device access, where weaker factors remained the only available options for users on personal or shared Windows hardware.

Device-bound FIDO2 passkeys address this structurally. The credential is scoped to the relying party domain at creation time, which eliminates the replay and interception risk that makes password spray (T1110) and

adversary-in-the-middle phishing (T1566, T1111) effective. The passkey cannot be extracted and reused across domains, which directly counters token theft patterns observed in T1550.001 (Web Session Cookie) and T1539 (Steal Web Session Cookie) attacks, where stolen artifacts from weaker authentication sessions have been used to maintain persistence in Entra SSO chains.

The CWE alignment in the item data is accurate: CWE-287 (Improper Authentication) and CWE-308 (Insufficient Authentication Steps) describe the conditions passkeys remediate; CWE-522 (Insufficiently Protected Credentials) describes what password-based fallbacks exposed; CWE-295 (Improper Certificate Validation) is relevant where certificate-based authentication intersects with passkey trust chain configuration.

The operational complexity lies in the policy layer. Device-bound passkeys on unmanaged hardware carry different attestation characteristics than TPM-bound credentials on Intune-enrolled endpoints. A trust flattening problem occurs when Conditional Access policies treat all passkey authentication as equivalent: a hardware-backed credential on a managed corporate device becomes trusted at the same level as a software-backed credential on a personal machine with unknown security posture, which partially negates the security benefit of the rollout. IAM teams need to evaluate this distinction before general availability, not after.

Microsoft Entra ID Protection's detection capabilities for protected resource risks are the relevant monitoring surface here, as the rollout changes the authentication signal landscape that risk-based policies rely on. Microsoft's documentation on ID Protection detection (learn.microsoft.com/en-us/entra/architecture/id-protection-guide-detect) is the authoritative reference for understanding how new credential types affect risk scoring and sign-in risk policies.

Source note: Primary reporting on the rollout timeline and scope comes from BleepingComputer (T3 tier). The Microsoft Learn documentation on Entra ID Protection is a T1 primary source for policy and detection behavior. No Microsoft Security Blog or official Entra product announcement was included in the provided source set; teams should verify rollout specifics against official Microsoft Entra release notes before finalizing timelines.

Action Checklist

1. Step 1: Assess exposure, inventory all Entra ID-connected applications and identify which access paths currently allow or require authentication from unmanaged or personal Windows devices; these are the paths this rollout directly affects
2. Step 2: Review Conditional Access policies, audit existing CA policies to determine how device compliance and authentication strength are currently enforced; identify whether passkey authentication from unmanaged devices will be trusted at the same level as TPM-backed credentials from managed endpoints, and adjust trust tiers before GA
3. Step 3: Evaluate attestation requirements, determine whether your organization's risk posture requires hardware attestation (TPM-bound) for passkey trust, or whether software-backed passkeys on unmanaged devices are acceptable for specific access tiers; document the decision and its rationale
4. Step 4: Update threat model, incorporate the post-rollout authentication signal changes into your threat register; adversaries who have relied on weaker authentication paths will shift focus to registration and enrollment flows (T1556, Modify Authentication Process), which become the new primary attack surface once password-based access is blocked. Monitor for anomalous passkey registration events and unusual enrollment patterns
5. Step 5: Brief IAM and SOC teams, communicate the Conditional Access policy changes to both IAM (who manages the policy) and SOC (who interprets sign-in risk signals); ensure both teams understand

how the new credential class affects risk-based Conditional Access behavior in Entra ID Protection

6. Step 6: Monitor developments, track the official Microsoft Entra release notes and Message Center for GA confirmation, staged rollout details, and any changes to attestation behavior; the BleepingComputer reporting cites late April staging and mid-June GA as the current timeline, but verify against official channels before setting internal deadlines

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if Entra ID Audit Logs or Identity Protection detections show evidence of T1556-aligned activity — specifically 'Register security info' events for FIDO2 passkeys from unfamiliar IPs or high-risk users, or if Conditional Access policy misconfiguration during the rollout staging period results in unmanaged devices gaining access to Entra ID-protected resources at a trust tier exceeding the organization's documented risk acceptance decision.
Recovery Notes	Following the GA rollout, verify that Conditional Access policies correctly enforce the intended authentication strength tier for each access path by reviewing Entra ID Sign-in Logs filtered on authenticationRequirement and deviceDetail.isManaged for at least 30 days post-GA, confirming no unmanaged device passkey authentications are reaching resources designated for managed-device-only access. Monitor Entra ID Protection for any spike in FIDO2-related risk detections during and after the staged rollout window (late April through mid-June 2026), as adversary targeting of registration flows is the most likely post-rollout tactic shift. Update the threat register and CA policy documentation once Microsoft confirms final attestation behavior at GA, and schedule a formal policy review 60 days post-GA to capture any behavioral drift from the rollout.
Forensic Artifacts	Entra ID Audit Logs — activity 'Register security info' with authentication method 'FIDO2 SecurityKey': captures every passkey registration event including UPN, IP address, device ID, and timestamp; critical for detecting adversary-controlled passkey registration (T1556) during and after the rollout window | Entra ID Sign-in Logs — fields authenticationDetail (method: FIDO2), deviceDetail.isManaged (false), deviceDetail.isCompliant (false), conditionalAccessStatus, and ipAddress: the primary forensic record for confirming whether unmanaged device passkey authentications are reaching intended vs. unintended resource tiers post-rollout | Entra ID Protection Risk Detections export — risk detection types 'unfamiliarFeatures', 'anonymizedIPAddress', and 'mcasSuspiciousInboxManipulationRules' co-occurring with FIDO2 sign-in or registration events: identifies sessions where adversaries may be attempting passkey registration from anonymizing infrastructure or unfamiliar device contexts | Conditional Access policy JSON export (pre- and post-rollout snapshots): provides the configuration baseline for forensic comparison if a policy misconfiguration during rollout staging results in improper trust elevation for unmanaged device passkey authentication — diff the pre- and post-change exports to identify unintended policy modifications | Microsoft Entra Authentication Methods Policy export (GET /policies/authenticationMethodsPolicy via Graph API) — specifically the FIDO2 section including 'isAttestationEnforced' boolean and configured AAGUID allowlist: forensic evidence of whether attestation enforcement was active or disabled at the time of any suspicious passkey registration event, and whether the authenticator model used was on the organization's approved allowlist

Per-Action IR Details

Step 1: Assess exposure — inventory all Entra ID-connected applications and identify which access paths currently allow or require authentication from unmanaged or personal Windows devices; these are the paths this rollout directly affects

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing asset visibility and authentication surface awareness before a structural authentication change reaches GA

Controls: NIST IR-4 (Incident Handling) — baseline preparation requires knowing which systems and access paths are in scope before a control change is deployed, NIST SI-5 (Security Alerts, Advisories, and Directives) — consuming the Microsoft Entra advisory and Message Center notification triggers this inventory action, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — extend asset inventory scope to include unmanaged and BYOD Windows devices that authenticate to Entra ID, CIS 2.1 (Establish and Maintain a Software Inventory) — catalog Entra ID-connected SaaS applications and their current authentication method requirements to scope rollout impact

Compensating: Run Microsoft Graph API query (GET /applications and GET /servicePrincipals) using the free Microsoft Graph Explorer (https://developer.microsoft.com/graph/graph-explorer) to enumerate all Entra ID-registered applications and their sign-in audience settings. Cross-reference with Entra ID Sign-in Logs filtered on 'deviceDetail.isCompliant eq false' and 'deviceDetail.isManaged eq false' using the free Entra ID portal log export (CSV) — a 2-person team can complete this in a single shift using Excel pivot tables on the exported data.

Evidence: Before scoping this inventory, export and preserve the current Entra ID Sign-in Logs (Microsoft Entra admin center → Monitoring → Sign-in logs, retention up to 30 days on free tier) filtered for authentication events from non-compliant and non-managed devices. Capture the Conditional Access policy export (JSON) from Entra ID → Protection → Conditional Access → Policies → Export, dated prior to any rollout changes, as a configuration baseline artifact. These records establish pre-rollout authentication path visibility and will be the forensic baseline if post-rollout anomalies arise.

Step 2: Review Conditional Access policies — audit existing CA policies to determine how device compliance and authentication strength are currently enforced; identify whether passkey authentication from unmanaged devices will be trusted at the same level as TPM-backed credentials from managed endpoints, and adjust trust tiers before GA

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: pre-incident hardening of authentication controls to prevent exploitation of the trust gap that exists between device-bound and software-backed passkey classes before GA closes it

Controls: NIST AC-17 (Remote Access) — CA policy enforcement governing authentication strength for remote and unmanaged device access paths is a direct remote access control mechanism, NIST IA-3 (Device Identification and Authentication) — adjusting trust tiers between TPM-backed managed device credentials and software-backed passkeys on unmanaged devices maps to device authentication assurance requirements, NIST SI-2 (Flaw Remediation) — the authentication gap between managed and unmanaged device trust in Entra CA policies is the structural weakness this step closes before adversaries exploit the transitional state, CIS 6.3 (Require MFA for Externally-Exposed Applications) — CA policy audit must confirm phishing-resistant authentication strength is enforced for all externally-exposed Entra ID applications, not just managed-device access paths, CIS 6.5 (Require MFA for Administrative Access) — verify that CA policies requiring phishing-resistant MFA for privileged Entra roles are not inadvertently relaxed by new passkey trust policies scoped to unmanaged devices

Compensating: Use the free Entra ID Conditional Access policy workbook (available in Azure Monitor Workbooks at no additional cost for tenants with Entra ID P1) to visualize policy gaps. If workbooks are unavailable, export all CA policies via Microsoft Graph: GET /identity/conditionalAccess/policies using Graph Explorer, save as JSON, and use the free 'jq' CLI tool to filter for policies where 'grantControls.authenticationStrength' is null or not set to 'phishingResistant' — this identifies every policy that does not yet enforce the correct authentication strength tier for the new passkey class.

Evidence: Capture a full JSON export of all Conditional Access policies before making any changes (Entra admin center → Conditional Access → Policies → each policy → Export). Additionally, export the Entra ID Authentication Methods Policy (GET /policies/authenticationMethodsPolicy via Graph API) to record which users and groups are currently enabled for FIDO2 security keys and passkeys prior to the rollout. These exports serve as the pre-change

configuration baseline for any post-incident policy drift investigation.

Step 3: Evaluate attestation requirements — determine whether your organization's risk posture requires hardware attestation (TPM-bound) for passkey trust, or whether software-backed passkeys on unmanaged devices are acceptable for specific access tiers; document the decision and its rationale

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing documented authentication assurance decisions and risk acceptance criteria before the new credential class is available to users, preventing ad-hoc trust expansion under adversarial conditions

Controls: NIST IA-8 (Identification and Authentication — Non-Organizational Users) — software-backed passkeys on personal unmanaged Windows devices introduce a non-organizational user authentication scenario that requires explicit trust decision documentation, NIST RA-3 (Risk Assessment) — the decision between TPM-bound hardware attestation and software-backed passkeys is a formal risk acceptance decision that must be documented with rationale, owner, and review date, NIST CA-7 (Continuous Monitoring) — attestation decisions must include monitoring criteria to detect if the accepted credential class is later found to be misconfigured or abused in the Entra ID environment, CIS 4.6 (Securely Manage Enterprise Assets and Software) — attestation policy documentation is part of the configuration management process that governs how authentication credentials are trusted on both managed and unmanaged assets

Compensating: Document the attestation decision in a one-page risk acceptance record (template: decision, scope, risk owner, compensating controls, review date). For organizations using the free Microsoft Entra ID tier, verify FIDO2 attestation configuration via the Authentication Methods Policy in the Entra admin center (Security → Authentication methods → FIDO2 security key → Configure) and confirm whether 'Enforce attestation' is toggled on — this setting controls whether Entra ID requires verified hardware attestation metadata from the FIDO Alliance Metadata Service (MDS3) before accepting a passkey registration.

Evidence: Before finalizing the attestation decision, pull the Entra ID Audit Logs filtered on activity 'Update Authentication methods policy' and 'Add FIDO2 security key' (Entra admin center → Monitoring → Audit logs) to establish the historical baseline of passkey registration activity in the tenant. Also capture the current FIDO2 attestation enforcement setting (on/off) and the configured AAGUIDs (Authenticator Attestation Global Unique Identifiers) that are currently allowlisted in the FIDO2 policy — these define exactly which authenticator models are trusted, and this baseline is critical if an unauthorized authenticator model is later used in a credential theft scenario.

Step 4: Update threat model — incorporate the post-rollout authentication signal changes into your threat register; adversaries who have relied on weaker authentication paths to unmanaged Windows devices will shift tactics; monitor for increased targeting of the enrollment and registration flows themselves (T1556 — Modify Authentication Process)

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: integrating updated threat intelligence about adversary tactic shifts into detection logic and threat registers before those tactics manifest in Entra ID registration and enrollment telemetry

Controls: NIST IR-4 (Incident Handling) — threat model updates are a preparation and detection activity within the incident handling lifecycle that ensures detection capability keeps pace with adversary adaptation, NIST SI-4 (System Monitoring) — monitoring for MITRE ATT&CK T1556 (Modify Authentication Process) targeting Entra ID FIDO2 registration flows requires specific detection logic, not generic authentication anomaly alerts, NIST RA-3 (Risk Assessment) — updating the threat register with post-rollout adversary tactic shifts (from password spray and MFA fatigue toward registration flow abuse) is a risk assessment update triggered by a known environmental change, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — the threat model update should feed directly into detection rule prioritization for Entra ID passkey registration abuse scenarios

Compensating: Create a free Microsoft Sentinel analytic rule (or, if Sentinel is unavailable, an Entra ID alert rule) targeting Entra Audit Logs for the activity 'Register security info' combined with a risk signal from Entra ID Protection showing 'unfamiliarFeatures' or 'anonymizedIPAddress' risk detections on the same user within the same session. For teams without Sentinel, configure an Entra ID alert via Microsoft Graph: POST /identityProtection/riskDetections and

review the free Identity Protection Risk Detections report weekly. Additionally, reference the public Sigma rule repository (github.com/SigmaHQ/sigma) for rules targeting Azure AD authentication method changes as a starting detection baseline for T1556 in Entra environments.

Evidence: To detect T1556-aligned activity against Entra ID FIDO2 registration flows, monitor Entra Audit Logs for: (1) activity type 'Register security info' with auth method 'FIDO2 SecurityKey' from IP addresses not previously associated with the user (cross-reference with Entra ID Sign-in Logs 'ipAddress' field); (2) activity 'Delete security info' followed immediately by 'Register security info' within a short window, which may indicate an adversary replacing a legitimate passkey with an attacker-controlled one; (3) Entra ID Protection risk detections of category 'userRisk' or 'signInRisk' co-occurring with FIDO2 registration events. Preserve these log records before any policy changes, as they establish the pre-rollout registration behavior baseline.

Step 5: Brief IAM and SOC teams — communicate the Conditional Access policy changes to both IAM (who manages the policy) and SOC (who interprets sign-in risk signals); ensure both teams understand how the new credential class affects risk-based Conditional Access behavior in Entra ID Protection

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring communications, role clarity, and shared understanding of how new authentication signals affect detection and response workflows before the GA rollout introduces those signals into production telemetry

Controls: NIST IR-2 (Incident Response Training) — IAM and SOC teams require specific training on how device-bound FIDO2 passkey authentication signals differ from legacy MFA signals in Entra ID Protection risk scoring before the rollout creates live confusion, NIST IR-8 (Incident Response Plan) — the IR plan must be updated to reflect how SOC analysts should interpret Entra ID Protection risk detections that involve the new passkey credential class, including what constitutes a true positive versus a false positive during the rollout staging period, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — SOC analysts must understand which new Entra ID audit and sign-in log event types are generated by FIDO2 passkey authentication on unmanaged devices so they can correctly analyze and report on those records, CIS 8.2 (Collect Audit Logs) — the briefing must confirm that the correct Entra ID log categories covering FIDO2 passkey registration and authentication events are enabled and flowing to the SOC's analysis environment before GA

Compensating: For a 2-person team without a formal training program, produce a one-page SOC runcard specific to Entra ID FIDO2 passkey authentication events: map the Entra Audit Log activity names ('Register security info' with method 'FIDO2 SecurityKey', 'Sign-in' with authenticationDetail 'FIDO2'), the expected Entra ID Protection risk detection types that may co-occur, and the CA policy names that govern this credential class. Distribute via email with a read-receipt for documentation. Use the free Microsoft Entra admin center 'Diagnose & Solve' tool to simulate sign-in scenarios for the new credential class and capture screenshots as training reference material.

Evidence: Before the briefing, export the current Entra ID Protection risk detection definitions relevant to authentication method changes (Entra admin center → Protection → Identity Protection → Risk detections) and the current named locations and trusted IP configurations from Conditional Access — these are the context SOC analysts need to correctly interpret whether a FIDO2 passkey sign-in from an unmanaged device is triggering a risk detection legitimately or as a false positive due to misconfigured policy. Document the current baseline false-positive rate for sign-in risk detections prior to rollout so post-rollout delta is measurable.

Step 6: Monitor developments — track the official Microsoft Entra release notes and Message Center for GA confirmation, staged rollout details, and any changes to attestation behavior; the BleepingComputer reporting cites late April staging and mid-June GA as the current timeline, but verify against official channels before setting internal deadlines

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: maintaining continuous awareness of vendor-driven authentication control changes and incorporating confirmed GA details into updated policies, detection logic, and threat model documentation as the rollout progresses

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — the Microsoft Entra Message Center and official release notes are the authoritative advisory channels that must be monitored on an ongoing basis for attestation

behavior changes, staged rollout scope updates, and GA confirmation, NIST IR-8 (Incident Response Plan) — the IR plan and associated CA policy documentation must be updated each time Microsoft confirms a material change to the FIDO2 passkey rollout scope, attestation requirements, or trust model behavior, CIS 7.2 (Establish and Maintain a Remediation Process) — the internal deadline for CA policy and attestation configuration changes must be set against the confirmed Microsoft GA date from official channels, not third-party reporting, to ensure the remediation timeline is accurate

Compensating: Configure a free Microsoft 365 Message Center email digest (Microsoft 365 admin center → Health → Message Center → Preferences → Email) to receive Entra ID feature update notifications directly. Additionally, subscribe to the official Microsoft Entra blog RSS feed (techcommunity.microsoft.com/t5/microsoft-entra-blog) using a free RSS reader (e.g., Feedly free tier) as a secondary authoritative channel. Create a shared tracking document with columns for: announcement date, source (Message Center ID vs. blog vs. third-party), confirmed action required, internal deadline, and owner — this gives a 2-person team an auditable change-tracking record without a ticketing system.

Evidence: Preserve copies of each Microsoft Message Center notification (downloadable as PDF from the Message Center detail view) and each official Microsoft Entra blog post that confirms rollout milestones, attestation behavior, or policy changes. These records serve as the authoritative evidence base for any post-rollout audit inquiry into why specific CA policy or attestation configuration decisions were made at particular points in time, and they document the delta between third-party reporting timelines (BleepingComputer) and the official Microsoft confirmation dates.

Detection Guidance

The primary detection surface for this story is not the passkey rollout itself, but the adversarial behaviors it is designed to displace and the new attack surface it introduces.

For existing threat patterns the rollout addresses:

- Monitor Entra sign-in logs for password spray indicators against Entra ID accounts: high-volume failed authentications across multiple accounts from single or rotating IPs (T1110)

- Hunt for MFA fatigue patterns: repeated MFA push requests to the same account within short windows (T1621, MFA Request Generation)

- Review Entra ID Protection risk detections for token theft indicators: unfamiliar sign-in properties, impossible travel, and anomalous token claims (T1550.001, T1539)

- Alert on legacy authentication protocol usage for Entra-connected applications; device-bound passkeys do not help if legacy auth fallbacks remain enabled

For new attack surface introduced by the rollout:

- Monitor passkey registration events in Entra audit logs; adversaries who have obtained temporary account access may attempt to register a passkey to establish persistent phishing-resistant access (T1556)

- Watch for registration events from unexpected locations, device types, or outside of expected enrollment windows

- Review Conditional Access sign-in logs for passkey authentication events from devices with low or unknown compliance posture; these will be identifiable by the absence of device compliance claims in the sign-in token

Policy audit items:

- Verify that named locations and device filter conditions in Conditional Access policies are not inadvertently granting elevated trust to passkey authentication from unmanaged devices

- Confirm that authentication strength policies explicitly define the trust tier for device-bound passkeys versus hardware-backed passkeys

Reference: Microsoft Entra ID Protection detection documentation (learn.microsoft.com/en-us/entra/architecture/id-protection-guide-detect) covers the risk detection signals relevant to sign-in and user risk policies.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1556** — Modify Authentication Process
- **T1550.001** — Application Access Token
- **T1078.004** — Cloud Accounts
- **T1539** — Steal Web Session Cookie
- **T1621** — Multi-Factor Authentication Request Generation
- **T1111** — Multi-Factor Authentication Interception
- **T1566** — Phishing

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A02:2021** — Cryptographic Failures
- **A04:2021** — Insecure Design

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **3.10** — Encrypt Sensitive Data in Transit
- **5.2** — Use Unique Passwords
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access
T1550.001	Application Access Token	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1111	Multi-Factor Authentication Interception	Credential-Access
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/microsoft/microsoft-to-roll-o...	T3
	https://www.bleepingcomputer.com/news/microsoft/microsoft-to-roll-o...	T3

Source	URL	Tier
	https://www.bleepingcomputer.com/news/microsoft/microsoft-entra-bri...	T3
	https://www.bleepingcomputer.com/news/microsoft/microsoft-is-killin...	T3
Microsoft Entra ID Protection to Detect Protected Resource Risks	https://learn.microsoft.com/en-us/entra/architecture/id-protection-...	T1

Generated 2026-04-25 06:50 UTC by TJS Security Command Center