ChangePilot by Empowering.Cloud

Microsoft 365

Security Digest

A review of 4 Microsoft 365 Identity and Security changes published to the Message Center in September 2026, with deployment dates from 26 Sep 2026 through 31 Dec 2026.

Review admin and user impacts and act where required before each deployment date.

4	Total Changes Tracked
4	High Admin Impact
0	Medium Admin Impact

Identity

1 Identity change rated High admin or user impact this month — sorted by deployment date.

MC1458474

Retirement of custom CSS layout and positioning properties in company branding

Deploy: 26 Oct 2026

Admin: High

User: Low

DESCRIPTION

Microsoft Entra ID is retiring support for custom CSS layout and positioning properties in company branding to harden branded sign-in experiences against phishing. The change affects only organizations that currently use the retired custom CSS properties in Entra ID company branding or branding themes. Existing branded sign-in customizations that rely on those properties will stop honoring them, and affected branding elements will revert to default placement and presentation. Microsoft Entra External ID tenants are not affected. Admins should review branding configurations, remove or redesign use of the retired CSS properties, and test sign-in pages before the cutoff.

ADMIN & USER IMPACT

Admin: Review Entra ID company branding configurations for the retired CSS properties, remove or redesign any that are in use, and test branded sign-in pages before 26 October 2026.

User: Sign-in pages may look different if affected branding elements revert to their default layout, but the sign-in process itself is unaffected.

RISK OF NOT ACTING

Any branded sign-in page still leaning on the retired CSS layout properties will silently revert to default placement and presentation once enforcement lands on 26 October 2026, so branding that hasn't been reviewed and redesigned in advance can start looking broken or inconsistent to users with no warning.

Security

3 Security changes rated High admin or user impact this month — sorted by deployment date.

MC1462464

Microsoft Defender for Cloud Apps: App Governance support for the Cloud Application Administrator role is being retired

Deploy: 26 Sep 2026

Admin: High

User: Low

DESCRIPTION

Microsoft Defender for Cloud Apps is retiring App Governance access for administrators who rely only on the Cloud Application Administrator Entra role when URBAC is enabled. After the change, only supported Entra roles will retain access to App Governance. Organizations should review administrator role assignments and ensure anyone who needs App Governance has an approved role. Microsoft recommends using the least-privileged supported role that meets each admin's responsibilities.

ADMIN & USER IMPACT

Admin: Review administrator role assignments before 26 September 2026 and assign a supported role (Security Administrator, Compliance Administrator, Application Administrator, or similar) to anyone who needs App Governance access.

User: No end-user impact — this change affects administrator access to App Governance only.

RISK OF NOT ACTING

Administrators who currently rely solely on the Cloud Application Administrator role will lose the ability to access App Governance the moment enforcement begins on 26 September 2026, with no grace period to catch missed role assignments after the fact.

MC1457836

Tenant will be auto-enabled into Microsoft Defender Unified RBAC

Deploy: 30 Sep 2026 – 31 Dec 2026

Admin: High

User: Low

DESCRIPTION

Microsoft Defender Unified RBAC will become the single access model for Defender and Sentinel portal experiences, and this tenant will be auto-enabled. Existing legacy Defender RBAC roles will be automatically imported into Unified RBAC for in-scope workloads. Admins should review imported role assignments and scopes in the Defender portal, then adjust any access that does not match intended permissions. A self-service opt-out is available after activation, and API-based role management should move to the Unified RBAC API. Microsoft states that Entra directory roles, Exchange Online/Purview permissions, delegated access, and Azure RBAC for non-Sentinel resources remain unchanged.

ADMIN & USER IMPACT

Admin: Review the auto-imported Unified RBAC role assignments in the Defender portal (Permissions → Roles) as soon as the in-portal notification appears, and adjust any that don't match intended access before automatic activation roughly 30 days later.

User: No end-user impact — this change governs administrator access to the Defender and Sentinel portals only.

RISK OF NOT ACTING

Legacy Defender RBAC role assignments get auto-imported and then activated roughly 30 days after the in-portal notification with no admin action required to trigger it, so unreviewed or mismapped imports can leave the wrong people holding the wrong level of access once Unified RBAC becomes the sole authorization model for the Defender and Sentinel portals.

MC1392568

Microsoft Defender for Endpoint: Support for Amazon Linux 2 (ARM64) retiring October 31, 2026

Deploy: 31 Oct 2026

Admin: High

User: Low

DESCRIPTION

Microsoft is retiring support for Microsoft Defender for Endpoint on Amazon Linux 2 (ARM64); devices running AL2 on AMD64/x86_64 are not affected. The last supported MDE agent for AL2 (ARM64) is version 101.25122.0004; later Defender releases will not install on that architecture. Admins must identify devices running Amazon Linux 2 (ARM64), prevent upgrades beyond the last supported agent, and plan migration to a supported Linux distribution. Devices left on this platform after support ends will receive no security updates, bug fixes, or technical support and may face increased security and stability risk.

ADMIN & USER IMPACT

Admin: Identify any devices running Amazon Linux 2 (ARM64) with Defender for Endpoint, hold them on agent version 101.25122.0004, and migrate them to a supported Linux distribution before 31 October 2026.

User: No end-user impact — this retirement affects endpoint security agent support only.

RISK OF NOT ACTING

Any endpoint still running Amazon Linux 2 on ARM64 past 31 October 2026 gets frozen on the last supported Defender agent build with no further security updates, bug fixes, or technical support, leaving those specific devices increasingly exposed unless they're migrated to a supported distribution beforehand.

Full Feature Summary

MCID	Feature	Deploy	Admin	User
MC1462464 https://portal.changepilot.cloud/MC1462464	Microsoft Defender for Cloud Apps: App Governance support for the Cloud Application Administrator role is being retired	26 Sep 2026	High	Low
MC1457836 https://portal.changepilot.cloud/MC1457836	Tenant will be auto-enabled into Microsoft Defender Unified RBAC	30 Sep 2026 – 31 Dec 2026	High	Low
MC1458474 https://portal.changepilot.cloud/MC1458474	Retirement of custom CSS layout and positioning properties in company branding	26 Oct 2026	High	Low
MC1392568 https://portal.changepilot.cloud/MC1392568	Microsoft Defender for Endpoint: Support for Amazon Linux 2 (ARM64) retiring October 31, 2026	31 Oct 2026	High	Low