Deloitte.

Digital Identity

Deloitte Access Policy Assurance (DAPA)



THE CHALLENGE

Password attacks against identity and access management services such as Microsoft Entra ID happen at enormous scale every second, and many enterprises govern that perimeter with a large, sprawling set of Conditional Access (CA) policies. Those policies are usually sound on day one. The problem is drift: a helpdesk exception never rolled back, multi-factor authentication (MFA) added to a compliant-device policy without noticing the default is "require one of the selected controls," an exclusion that grew from one name to twelve. In real engagements, one change like this spreads quietly through a workforce because the easier path always wins, and once thousands are using it, so is anyone holding a stolen password.

WHAT IS DAPA?

DAPA was built in response to a real client engagement. In that tenant, a single CA policy was quietly changed, opening access for 27,000 employees, with no record of who made the change, when it occurred, or why. DAPA was created to catch this type of change. DAPA detects policy drift, explains each change in plain language, simulates policy decisions at scale, and reverts unintended changes once approved. This gives security leaders confidence that their CA policies continue to match the intended design, with an auditable record of each change.

THE DAPA ADVANTAGE

- **Continuous Assurance:** Every change captured, explained, and reconciled against the baseline within seconds. Drift becomes visible before it becomes risk.
- **A Visualization for Security Leadership:** CA policies are rendered automatically into a single diagram the CISO can read at a glance, and the engineers can defend in detail.
- **Simulation at Scale:** The estate evaluated against thousands of user, application, platform, location, and risk scenarios in a single run, well above the native what-if's one-at-a-time ceiling.
- **Investigation in Plain English:** Ask in plain language: DAPA writes KQL that correlates Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Entra, Purview, Defender, and any other log source the client connects, all in one workspace.

WHY SECURITY LEADERS TRUST DAPA

DAPA gives the engagement team one workspace to **baseline, simulate, investigate, visualize**, and **remediate** CA across the client's tenant. It runs through Microsoft Graph, reconciles changes against the baseline within seconds, and helps clients turn silent risk into a documented, auditable record the client owns at handoff.

Bulk What-If at Scale: Run thousands of access scenarios against the live policy set in a single pass and export the gaps as a working list.

Near Real-Time Drift Detection: Every save to a CA policy is captured, diffed against the baseline, explained in plain language, and remediated on approval.

Tokenized AI Across Every Path: Each identifier is rewritten to a token before any prompt reaches the model, so client data never leaves the tenant, and the AI never sees a real name, email, or ID.



Natural-Language Investigation: A question in plain English becomes a KQL query across AWS, GCP, Microsoft Entra, Purview, Defender, and any log source the client connects.

Policy Visualization: Put CA on a screen the CISO can read at a glance and the engineers can defend in detail, no slides to prepare and no translation needed.

AI-explained Policy History: Every version of every policy is preserved with plain-language commentary, well past the 30-day audit window most tenants run on.

**Note: Deloitte is Microsoft's independent auditor, and as such our actions and work are subject to the Securities and Exchange Commission and Public Company Accounting Oversight Board, as well as the standards and rules of the American Institute of Certified Public Accountants. Independence means that Deloitte is free from conflicting and mutual interests with Microsoft that may undermine the objectivity of Deloitte in fact or appearance.*

THE DELOITTE DIFFERENCE

Talent & Experience

- **Identity practitioners** with deep experience across Microsoft Entra ID, Conditional Access, and Zero Trust architectures
- **Persona-based design** drawing on community patterns from identity MVPs and CA-as-code practitioners
- **Hands-on engagement teams** that build, validate, and document every Conditional Access policy alongside the client

Technology & Innovation

- **DAPA integrates** directly with Microsoft Graph APIs, operating securely within the client's Microsoft Entra tenant within its existing identity and security boundaries
- **Tokenized AI on every path** every identifier is rewritten to a token before any LLM call, so the AI never sees PII
- **Near Real-time Graph reconciliation** that catches drift in minutes, well ahead of the daily cadence of native scoring and recommendation engines

Compliance & Outcomes

- **Documented policies at handoff** with full policy version history preserved beyond the 30-day audit log default
- **Zero Trust alignment** with Microsoft's Identity pillar and CISA's Zero Trust Maturity Model
- Audit-ready evidence **trail for every policy change**, simulation, and remediation performed during the engagement
- **Persona-aligned governance** mapping every policy to a clear persona model

DAPA MODULES

Baseliner: point-in-time snapshot of every CA policy, exclusion, and target at engagement start

Drift Watch: continuous reconciliation of the live tenant against the baseline, through Microsoft Graph audit events

Remediation Engine: approved one-click reversion of unintended changes, with full audit trail of every action

Policy History: versioned record of every CA policy change, narrated in plain language

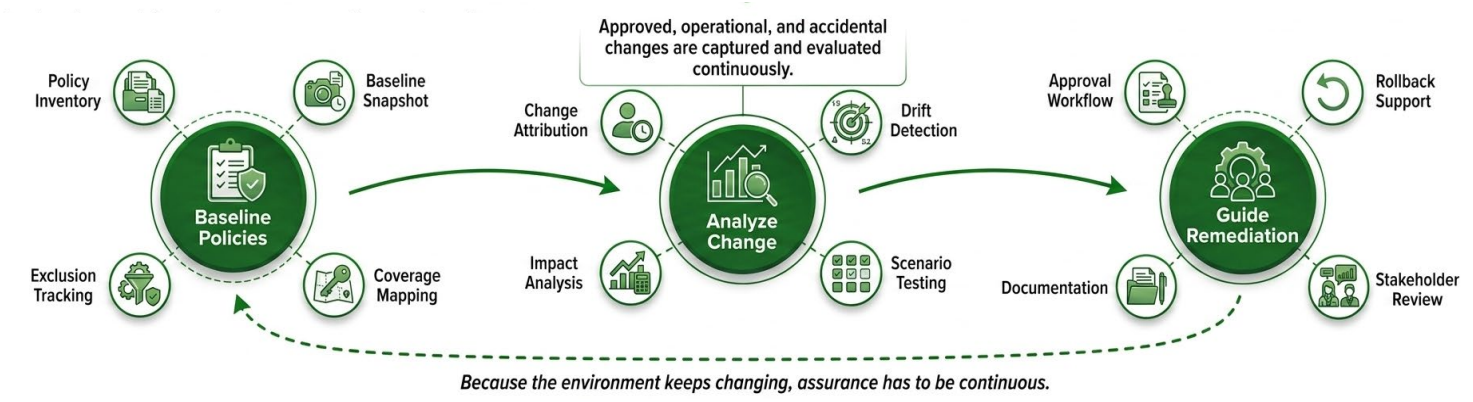
Evaluator: bulk what-if simulation across thousands of access scenarios in a single run

Investigator: natural-language to KQL across AWS, GCP, Microsoft Entra, Purview, Defender, and the client's other log sources

CA Policy Visualizer: single-canvas diagram of every CA policy, ready for a leadership review without preparation

Handoff: documented CA policies delivered to the client at engagement close

DAPA: The continuous CA Loop



GET STARTED WITH DAPA BY DELOITTE.

To learn more, contact our team today:



Andrew Rafla
Principal
Deloitte & Touche LLP
arafla@deloitte.com



Jean-Michel Heffron
Managing Director
Deloitte & Touche LLP
jeheffron@deloitte.com



Amit Chhikara
Principal
Deloitte & Touche LLP
achhikara@deloitte.com



Tom Colombo
Vice President
Deloitte & Touche LLP
tcolombo@deloitte.com

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

Product names mentioned in this document are the trademarks or registered trademarks of their respective owners and are mentioned for identification purposes only. Deloitte is not responsible for the functionality or technology related to the vendor or other systems or technologies as defined in this document. Inclusion does not constitute an endorsement of any company, product, or service.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.