THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

The Front-Door is a Maze

Employees encounter dozens of login screens, inconsistent branding, and repeated MFA prompts across the enterprise, turning identity into a productivity drain.

CONTROL FRAMEWORK

Current Landscape: Fragmented Experiences

SaaS apps, legacy on-prem systems, and cloud services each enforce their own authentication flow, often built on separate IdPs and protocols.

CONTROL FRAMEWORK

Key UX Pain Points

Users report password fatigue, MFA fatigue, inconsistent UI language, and lack of contextual help when accessing critical resources.

CONTROL FRAMEWORK

Business Impact of Friction

Support tickets rise, onboarding slows, and users adopt insecure workarounds such as password reuse or credential sharing.

CONTROL FRAMEWORK

Architectural Root Causes

Siloed Identity Providers, legacy protocols (SAML, LDAP), and missing policy orchestration force each application to reinvent its login UI.

CONTROL FRAMEWORK

Emerging Pattern: Identity Experience Framework

Modern platforms (e.g., Azure AD B2C, Okta Identity Engine) separate authentication logic from presentation, delivering reusable UI components and adaptive policies.

CONTROL FRAMEWORK

Recommended Architecture Blueprint

A centralized policy layer feeds a library of brand-consistent UI widgets to all applications via API-first integration. Adaptive MFA is invoked only when risk signals exceed thresholds.

CONTROL FRAMEWORK

Implementation Roadmap

→ Inventory all authentication flows and protocols

→ Define enterprise UI/branding standards

→ Pilot the framework with a low-risk internal app

→ Iterate based on user feedback and risk metrics

→ Scale to all SaaS and on-prem workloads

CONTROL FRAMEWORK

Governance Checklist

→ Accessibility compliance (WCAG 2.1)

→ Consistent branding and language

→ Privacy-by-design data handling

→ Audit-ready logging of authentication events

→ Periodic risk-based MFA policy review

EXECUTIVE TAKEAWAY

Executive Takeaway

A unified Identity Experience Platform eliminates friction, strengthens security posture, and reduces operational cost—making identity a strategic advantage rather than a bottleneck.