THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Identity Is the New Perimeter

Traditional network borders have dissolved; identity now defines trusted access for users, devices, and services.

CONTROL FRAMEWORK

Centralized Identity Governance Eliminates Orphan Accounts

A unified governance layer provides real-time visibility and automated remediation of stale or excessive privileges.

→ Single source of truth for entitlements

→ Automated certification cycles

→ Policy-driven deprovisioning

CONTROL FRAMEWORK

Adaptive Multi-Factor Authentication Applies Risk-Based Controls

MFA challenges are issued only when contextual risk signals—such as location, device health, or behavior—exceed defined thresholds.

→ Dynamic policy engine

→ Reduced friction for low-risk sessions

→ Higher assurance for high-value assets

CONTROL FRAMEWORK

Passwordless Authentication Eliminates Credential Theft

Biometric, hardware token, or cryptographic key methods replace passwords, removing the most common attack vector.

→ Phishing-resistant login

→ Zero password management overhead

→ Improved user experience

THE ARCHON

TECHNOLOGY INTELLIGENCE

CONTROL FRAMEWORK

Automated Provisioning Aligns Access With Role Changes

Integrations with HR and ITSM systems trigger instant creation, modification, or removal of accounts as employees move through the organization.

→ Real-time onboarding/offboarding

→ Consistent role-to-access mapping

→ Audit-ready entitlement logs

THE ARCHON
TECHNOLOGY INTELLIGENCE

CONTROL FRAMEWORK

Continuous Entitlement Analytics Detect Anomalous Privilege Use

Machine-learning models monitor entitlement changes and usage patterns, flagging deviations that may indicate insider threat or compromised accounts.

- → Baseline behavior profiling
- → Alerting on privilege escalation
- → Integration with SOAR for automated response

CONTROL FRAMEWORK

Federation and Zero Trust Extend Secure Access to Cloud Apps

Combining identity federation with zero-trust network access creates seamless, policy-driven connectivity to software and infrastructure services in the cloud.

→ Single sign-on across cloud environments

→ Identity-driven micro-segmentation

→ Less reliance on traditional VPNs

CONTROL FRAMEWORK

IAM Integrated With Security Orchestration Automates Incident Response

When a compromised identity is detected, IAM APIs trigger session termination, credential reset, and containment playbooks without manual intervention.

→ Instant revocation of tokens

→ Automated user notification

→ Feedback loop to risk engine

EXECUTIVE TAKEAWAY

Executive Takeaway

Modern IAM is no longer a peripheral control; it is the architectural backbone that enables zero-trust, rapid provisioning, and automated defense across the enterprise.