THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

The Blind Spot: Browser Sessions

Zero Trust verifies who you are, what device you use, and which network you connect from. Once a user reaches the browser, continuous verification often ends, leaving the session exposed to credential theft, malicious scripts, and data leakage.

CONTROL FRAMEWORK

Step 1 – Identity & Access Verification

Enforce risk-based MFA, adaptive SSO, and continuous authentication checks before granting any web access.

→ MFA on every login

→ Contextual risk scoring (location, behavior)

→ Session re-authentication for high-value apps

CONTROL FRAMEWORK

Step 2 – Device Posture & Endpoint Assurance

Validate OS version, patch level, and security agent health before allowing the browser to connect to corporate resources.

- → Endpoint detection and response (EDR) status check
- → Compliance policies enforced via MDM
- → Quarantine non-compliant devices

CONTROL FRAMEWORK

Step 3 – Application & API Authorization

Apply least-privilege policies to SaaS apps and APIs, using token-scoping and runtime verification.

→ OAuth 2.0 with fine-grained scopes

→ API gateway policy enforcement

→ Zero-trust service mesh for internal services

CONTROL FRAMEWORK

Step 4 – Browser Session: The Trust Gap

In 2023, browser-based attacks represented the majority of web-traffic threats, exploiting the lack of continuous verification after login.

→ Malicious extensions

→ Credential-stealing scripts

→ Cross-site request forgery

CONTROL FRAMEWORK

Step 5 – Continuous Browser Trust Enforcement

Deploy real-time browser isolation, strict Content-Security-Policy (CSP) headers, and Secure Access Service Edge (SASE) controls to verify every page load.

→ Remote rendering isolates malicious code

→ CSP blocks inline scripts and unsafe sources

→ SASE enforces policy per request, not per network

CONTROL FRAMEWORK

Step 6 – Post-Session Monitoring & Data Loss Prevention

After the browser closes, log all data transfers, apply DLP rules, and trigger alerts on anomalous outbound traffic.

→ Encrypted session logs stored for 90 days

→ DLP scans for PII in uploads/downloads

→ Automated quarantine of compromised accounts

EXECUTIVE TAKEAWAY

Executive Takeaway – Extend Zero Trust Into the Browser

Treat the web session as a dynamic trust boundary. Combine identity, device, and application checks with real-time browser isolation, CSP enforcement, and continuous post-session analytics to eliminate the blind spot that attackers exploit.

→ Add browser isolation to your SASE stack

→ Enforce CSP and strict same-origin policies

→ Integrate session logs with SIEM for ongoing risk scoring