PRESENCE AUTHORITY / SECUREAUTH

The In-Session Security Audit

Authentication verifies the credential. Presence Authority verifies the operator.

The Post-Login Gap

$17.4M[1] Average annual cost of insider risk (up from $16.2M in 2023)

91%[2] Of visual hacking attempts succeed in capturing sensitive screen data

27%[3] Of visually captured data is sensitive, in under 15 minutes per attempt

[1] Ponemon Institute, 2025 Cost of Insider Risks Global Report (sponsored by DTEX Systems). [2, 3] Ponemon Institute & 3M, Global Visual Hacking Experimental Study.

Most identity programs invest heavily in login and stop watching the moment authentication succeeds. This assessment helps security and compliance leaders identify post-login exposure across operator presence, screen-level data capture, mid-session enforcement, audit evidence, and third-party workforce coverage. Mark each item Yes, No, or Partial, then review the score guide below.

15 QUESTIONS
5 CONTROL LAYERS

I. Operator Presence

1. Can your security team confirm, in real time, that the person sitting at an authenticated workstation is the credentialed user and not someone else operating an open session? ☐ ☐ ☐
2. When an authorized user steps away from the workstation, does the session lock within a few seconds without depending on the user remembering to lock it? ☐ ☐ ☐
3. When the authorized user returns, does the session resume without prompting for a fresh password or full re-authentication? ☐ ☐ ☐
4. If an unauthorized person appears in the camera view alongside the authorized user, does your environment generate an alert or lock the screen? ☐ ☐ ☐
5. Can you produce evidence of continuous operator presence for any session in the last 30 days? ☐ ☐ ☐

II. In-Session Screen Capture

6. If a remote employee or contractor pointed a phone camera at their screen, would any current control in your stack detect that action? ☐ ☐ ☐
7. Can your environment block screenshot and screen recording attempts at the session level, regardless of operating system or local user permissions? ☐ ☐ ☐
8. Are screen sharing applications detected and restricted during sessions handling regulated or confidential data? ☐ ☐ ☐
9. Do screens displaying sensitive data carry dynamic watermarks that tie any captured image back to the specific user, session, and timestamp? ☐ ☐ ☐

III. Mid-Session Enforcement

10. Once a session is authenticated, do your access policies continue to evaluate risk signals throughout the session? ☐ ☐ ☐
11. If a session is hijacked or transferred to another person after legitimate login, what control in your stack would surface that event before data is exfiltrated? ☐ ☐ ☐
12. Are application-level restrictions enforced continuously throughout a session, not only at session start? ☐ ☐ ☐

IV. Audit Evidence

13. When an auditor asks who was actually at the screen during a specific transaction, do your current logs answer that question? ☐ ☐ ☐
14. For investigations involving suspected insider activity, can your team retrieve continuous presence records, or only login and logout timestamps? ☐ ☐ ☐

V. Third-Party Coverage

15. Do the same session security controls apply to your contractors, BPO workforce, outsourced staff, and offshore teams as to your direct employees? ☐ ☐ ☐

Your Score

_____ **Yes** _____ **No** _____ **Partial**

Score Guide

13–15 Yes
Strong post-login posture
Validate specific control coverage and benchmark against phone-camera capture and operator handoff scenarios.

8–12 Yes
Moderate gaps
Your stack covers some post-login signals but leaves identifiable exposure. The lowest-scoring area is your priority.

7 or fewer Yes
Significant exposure
Operator presence, visual exfiltration, and session evidence layers are not in place. Common in environments scaled rapidly to remote work.

Map your gaps to specific control coverage.

LEARN MORE secureauth.com/products/screen