How certain are you about who is accessing your sensitive data right now?

Introducing Continuous Identity Assurance for the remote workforce.

The New Perimeter is Everywhere, and It’s Full of Blind Spots.

Traditional Office Perimeter

Decentralized Remote Work Environment

Remote work has dissolved the traditional office perimeter. Your critical data is now accessed from countless unmanaged environments. This introduces new, persistent vulnerabilities that traditional security models were not designed to handle.

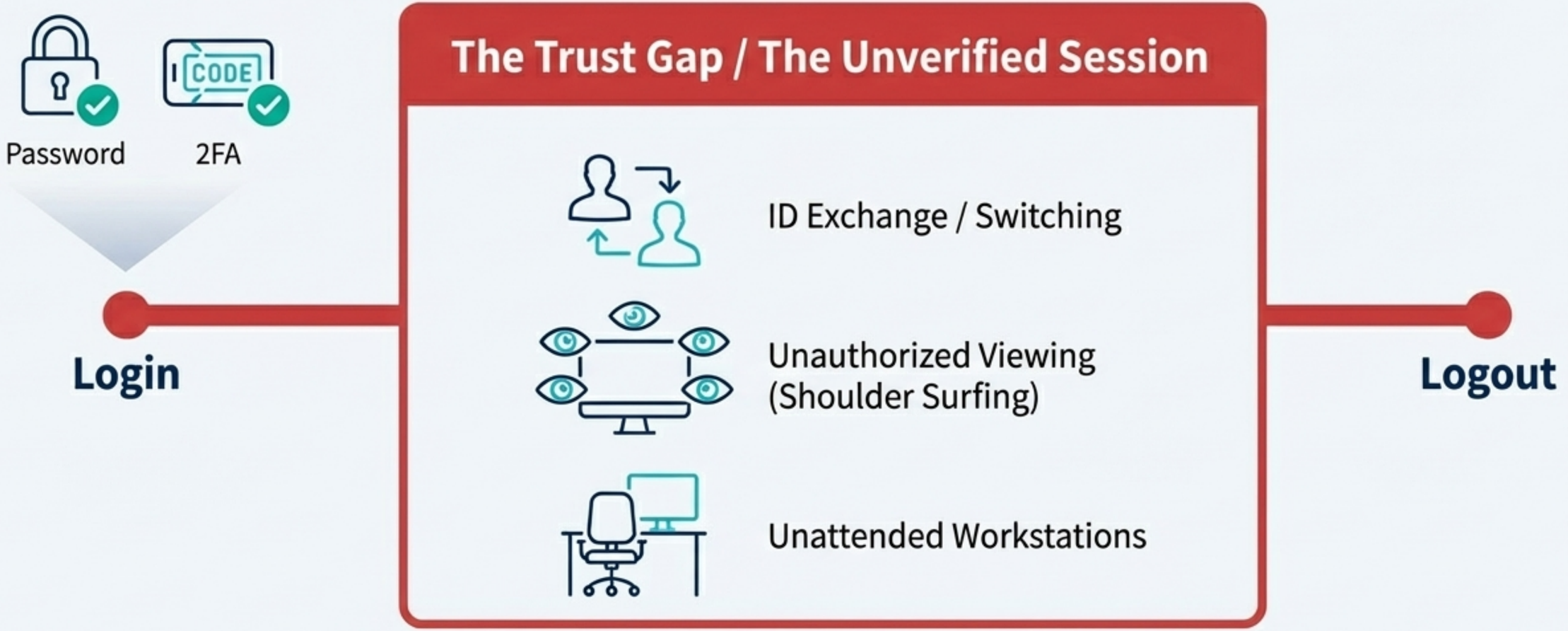
Unsecured Home Networks

Shared Physical Spaces

Personal Devices

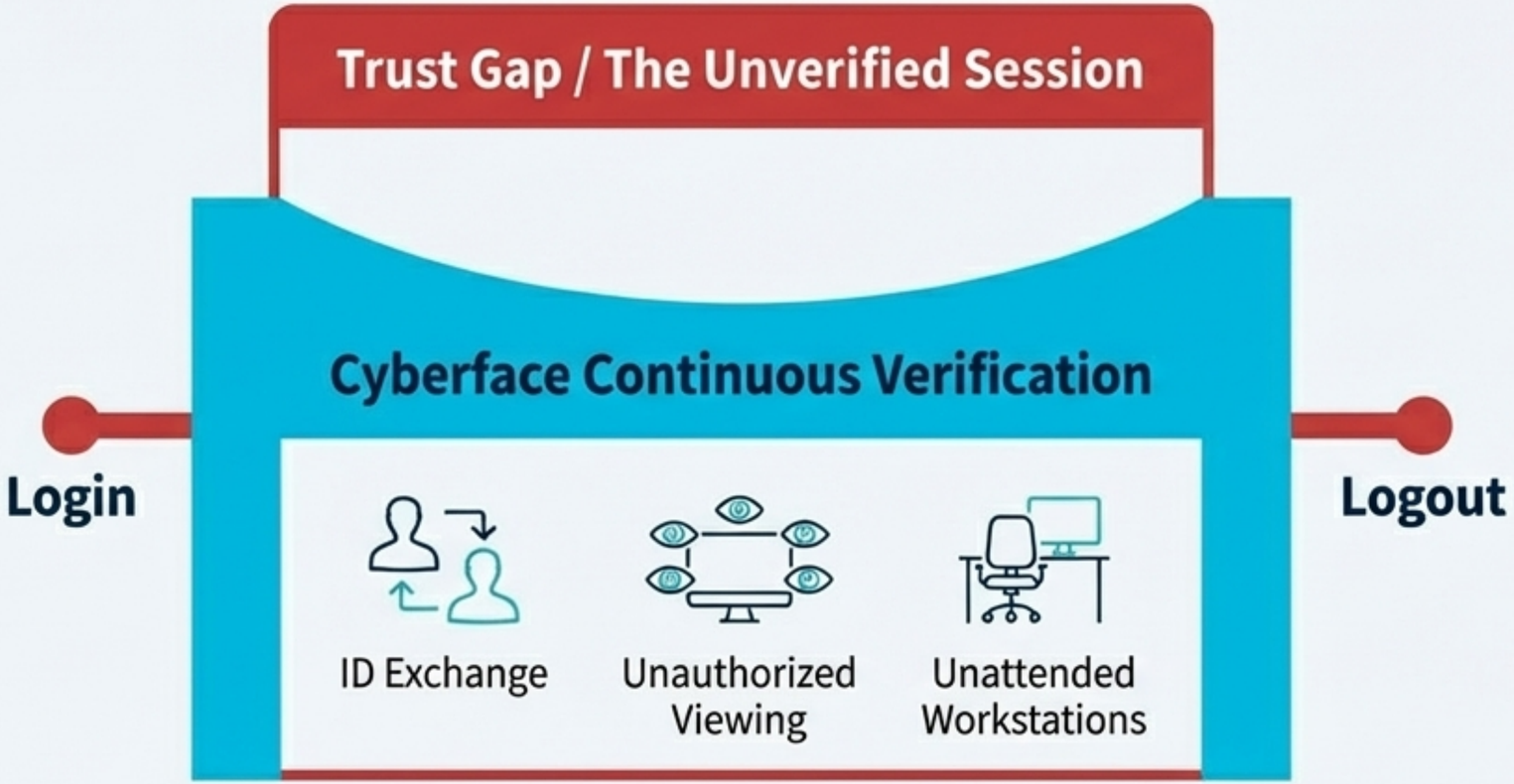
The Critical Security Gap: Between Login and Logout.

Standard authentication—even with 2FA—verifies a user's identity only at the moment of login. But what happens during the hours-long session that follows? This "Trust Gap" is where your organization is most vulnerable.



Introducing Cyberface: Closing the Trust Gap with Continuous Identity Assurance.

Product: Cyber Secure Environment



Cyberface provides fully protected access for remote work. We go beyond one-time authentication to deliver perpetual, biometric verification for the entire work session. This ensures that the authorized user—and only the authorized user—has access at all times.

- Dual biometric authentication upon access.
- Perpetual verification throughout the work session.
- Secure access for VPN & RDP connections.

Our Solution is Built on Three Pillars of Certainty.

Pillar 1: Secure Entry

A robust, multi-factor login process establishes initial identity with certainty, combining passwords, OTP, and an initial biometric scan.

Pillar 2: Continuous Verification

Our core innovation. The system uses the workstation's camera to perpetually ensure the authenticated user remains present and alone throughout the entire session.

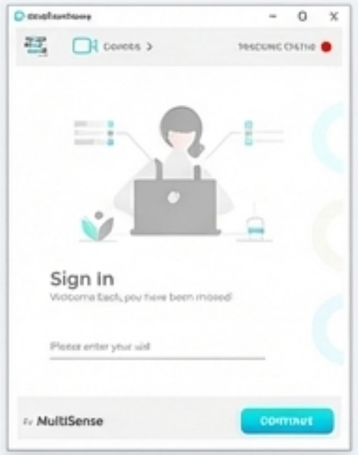
Pillar 3: Intelligent Response

Automated, real-time actions are triggered by security events, instantly locking the screen and logging the incident to prevent breaches before they happen.

The User Journey: A Seamless Path to a Secured Session.

1 Step 1: Standard Login

User enters their username and password on the desktop application.



2 Step 2: 2-Factor Authentication

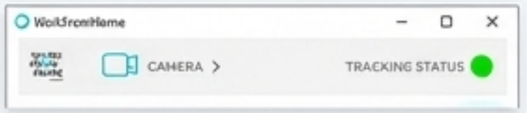
User receives a One-Time Password (OTP) via their registered smartphone app, SMS, or by scanning a dynamic QR code.

3 Step 3: Biometric Verification

User performs a facial recognition scan via the desktop app to provide the final, definitive identity confirmation.

4 Step 4: Continuous Monitoring Activated

Access is granted. The system's continuous verification is now active, monitoring the entire session.

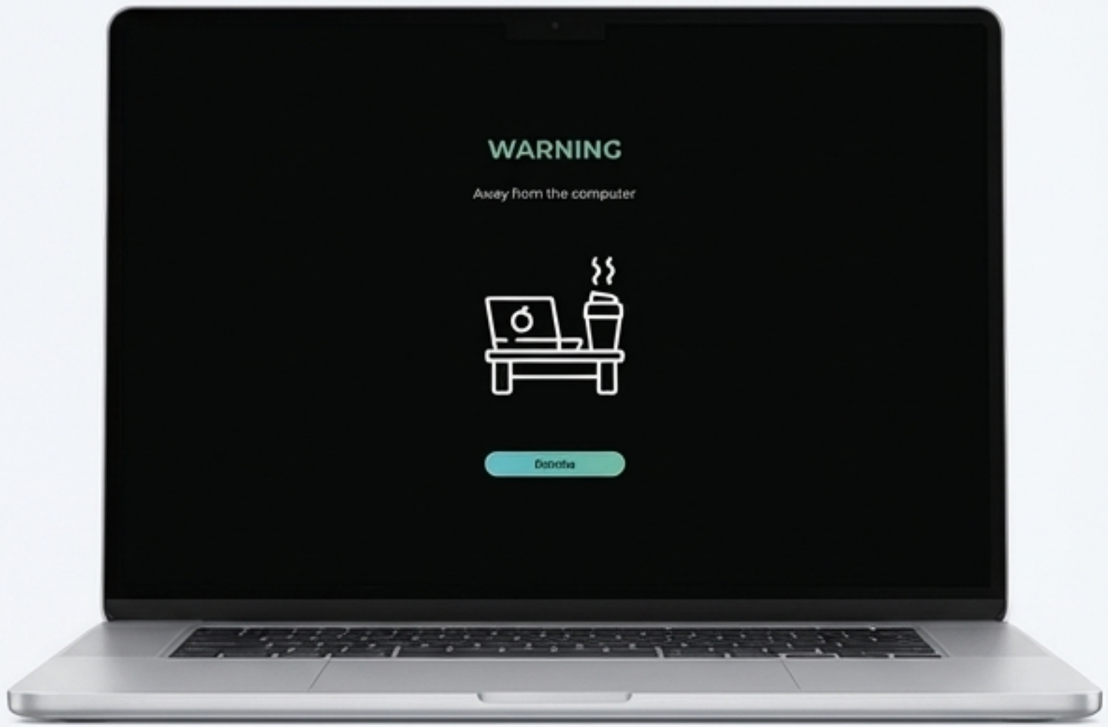


Intelligent Response: The Unattended Workstation.

Scenario: An employee walks away from their computer for a coffee, leaving a sensitive session active.

System Action: Cyberface detects that no authorized face is present (“Away from the computer”).

Result: The system instantly locks the screen to prevent unauthorized access and logs the “time away” event for auditing purposes.

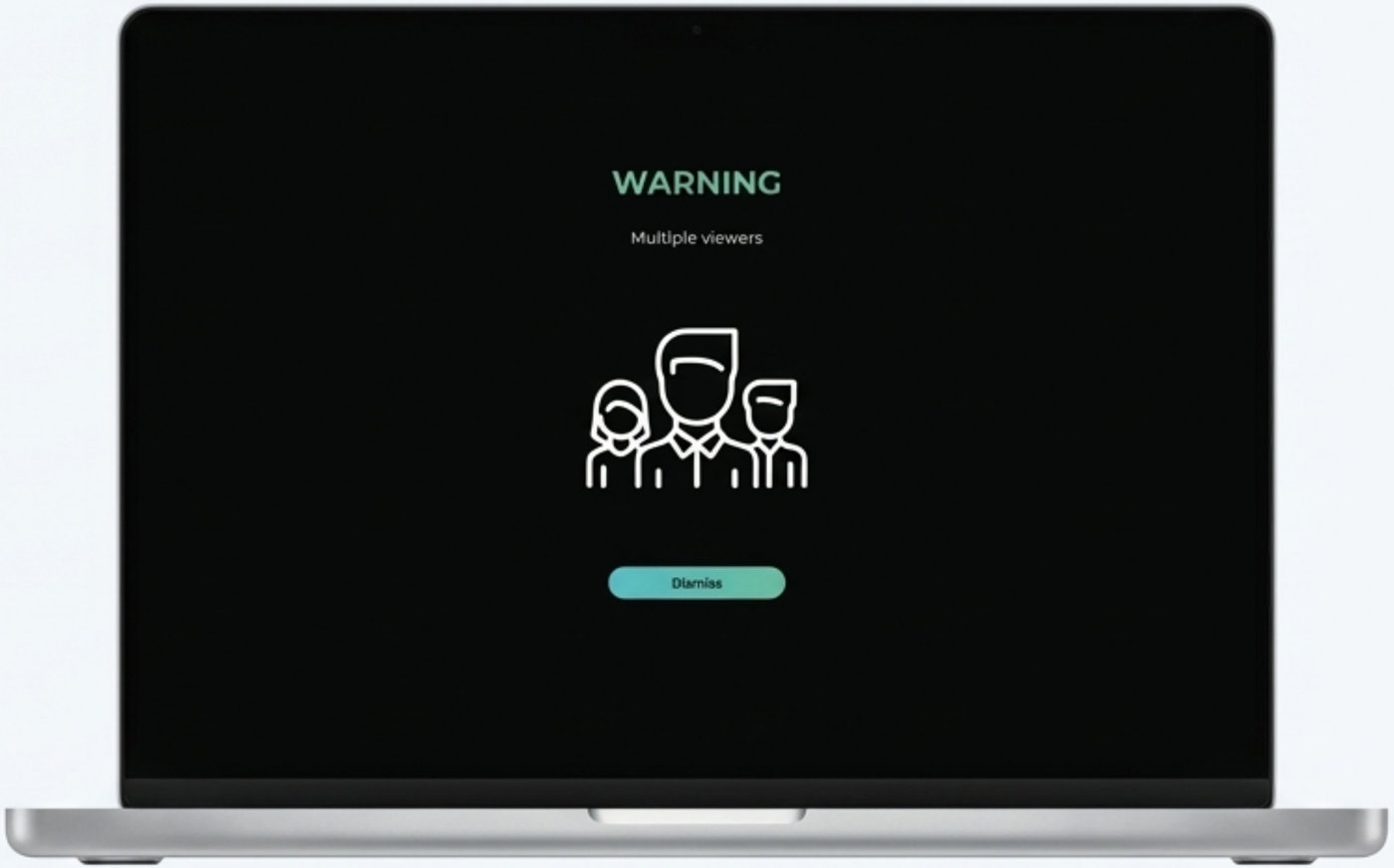


Intelligent Response: The Unauthorized Viewer.

Scenario: While the authorized employee is working, a family member or roommate looks over their shoulder at the screen.

System Action: Cyberface detects multiple faces in the camera's view.

Result: A ‘Multiple viewers' warning is triggered. *The session can be configured to lock or simply alert the user and log the event, enforcing a “one-to-one” designated employee identification policy.*

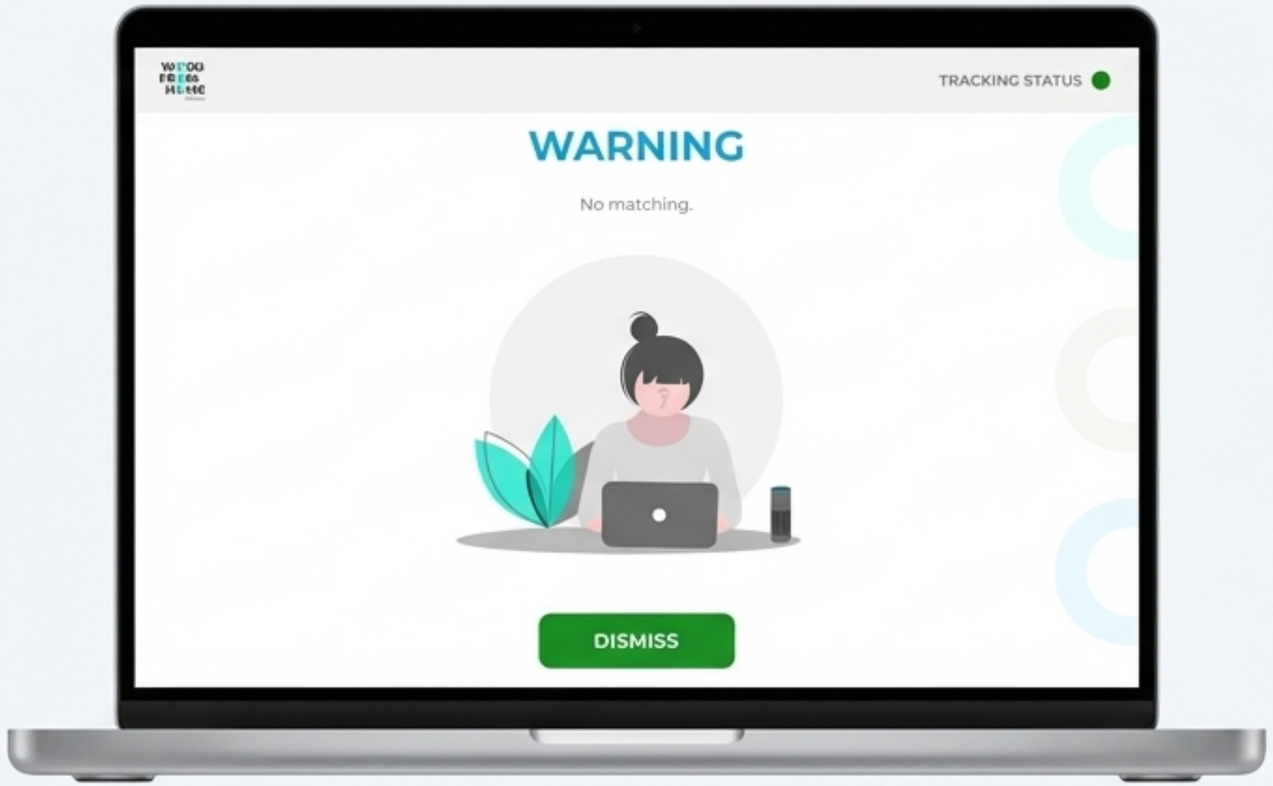


Intelligent Response: The Impersonator.

Scenario: The authorized user logs in, but another person attempts to take over the session.

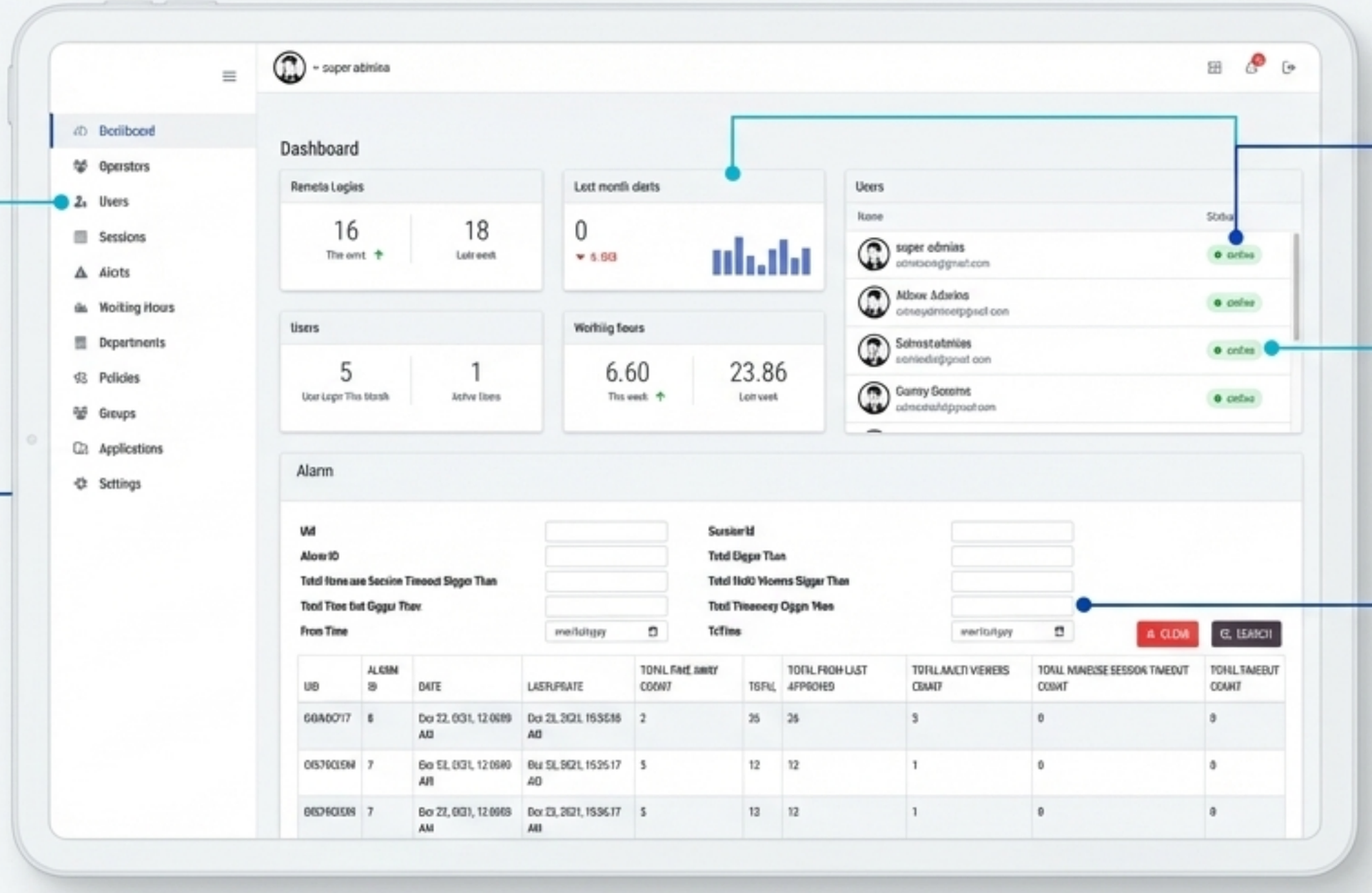
System Action: Cyberface detects a face, but it does not match the biometric profile of the authorized user.

Result: A 'No matching' alert is generated, and the screen is immediately locked, preventing any further action. The security incident is logged in the central dashboard.



The Command Center: Complete Visibility and Control Over Your Remote Workforce.

The Cyber Secure Environment dashboard is your central hub to manage users, monitor activity, set policies, and get detailed information on all security events.



Comprehensive Management

At-a-glance metrics

Live Status

Detailed Alarm Logs

Benefits That Go Beyond Security to Strengthen Your Entire Operation

Ironclad Security

- Eliminate unauthorized screen viewing and illicit login breaches.
- Prevent ID exchange and switching with definitive biometric proof.
- Go beyond simple 2-factor authentication to achieve true session security.

Operational Integrity

- Maintain a precise time-log of employee activity in front of the authorized screen.
- Enforce one-to-one designated employee identification for compliance and accountability.

Effortless Oversight & Implementation

- Centralized Command & Control system for simple management.
- Easy installation that supports both workgroup and Active Directory environments.
- Robust process with no modification to existing VPN or RDP connections.

Achieve Absolute Certainty in Your Remote Security Posture.

With Cyberface, you no longer have to guess who is accessing your data. You can be certain. Our Cyber Secure Environment provides the continuous, real-time identity assurance needed to protect your organization in the era of remote work.

Schedule a Personalized Demo

demo@cyberface-security.com
www.cyberface-security.com
+1 (800) 555-0199

CYBERFACE
Biometric Digital Identity