concentrix™

1KOSMOS

The Secure Choice for Contact Centers

Concentrix secures the facility, 1Kosmos delivers passwordless identity at the workstation: together, every access point is protected.

Your contact centers handle thousands of operations benefiting your customers every day, but sometimes this requires confidential data. Agents access bank accounts, sensitive information, medical records, and insurance claims through shared workstations. But here's the problem: most contact centers still rely on passwords and basic authentication that creates serious security gaps.

Banks, fintechs, insurance companies, and other regulated actors face increasingly stringent regulatory requirements, which also apply to your contact centers. Together, 1Kosmos biometric authentication and Concentrix secure contact center facilities provide a complete solution to close both physical and digital security gaps. Every agent gets verified through identity checks certified to NIST 800-63-3 before touching your customer data. No shared passwords, no authentication workarounds, no gaps in your audit trail.

Bottom line

Complete visibility into who accessed what customer data, when they did it, and proof that they were authorized to be there.

Contact Center Security Challenges

Client contractual security requirements: Highly regulated industries like banking, financial services, healthcare, and insurance increasingly require dedicated secure facilities with multi-floor access controls and advanced authentication measures. These contractual specifications are becoming standard requirements rather than optional security enhancements.

Shared workstation vulnerabilities: Traditional authentication methods don't adequately secure shared workstations containing sensitive customer data. Agents log into workstations with generic credentials, making it impossible to definitively prove who actually accessed which customer account when issues arise.

Uncontrolled operational costs from security incidents: Weak authentication leads to account takeover attempts and fraudulent activity surges that require emergency staffing increases. These operational cost spikes - often 20-30% above normal volume - get passed directly to your organization, creating unpredictable budget impacts during coordinated attacks.

Regulatory compliance gaps: Traditional contact center security creates compliance vulnerabilities for your organization. Without biometric identity verification tied to specific data access events, you cannot prove adequate controls during regulatory examinations, potentially exposing your organization to penalties and enforcement actions.

Operational complexity and inefficiencies: Multiple security layers including badging, metal detectors, and guards create bottlenecks and operational overhead. These traditional measures reduce agent productivity and create operational inefficiencies while still leaving authentication gaps.

End-to-End Contact Center Security Solution

Secure facilities with multi-floor access controls designed for regulated industries: Concentrix operates dedicated floors with metal detectors, badge controls, surveillance, and multi-floor access controls built specifically for handling sensitive financial and healthcare data. This infrastructure integrates with existing physical security systems while meeting your specific security and contractual requirements.

Biometric identity verification integrates with existing infrastructure: 1Kosmos uses NIST-certified biometric recognition that seamlessly integrates with your current contact center applications and Concentrix's physical security infrastructure. This eliminates shared passwords and ensures only verified individuals can access customer information, significantly reducing breach risk even if someone gains physical access to a workstation.

Predictable operational costs despite coordinated attacks: Strong biometric authentication prevents account takeover attempts from succeeding, eliminating surges in fraudulent activity that typically require emergency staffing. This maintains stable operational costs even during coordinated security attacks, protecting your budget from unexpected volume spikes.

Complete audit trails simplify regulatory compliance: Every login, customer record access, and system action is logged with verified biometric identity. Regulatory examinations become straightforward with detailed reports showing exactly who accessed specific data and when, eliminating the challenge of reconstructing incomplete audit trails during compliance reviews.

Improved productivity through passwordless authentication: Agents authenticate through biometric recognition for immediate access, eliminating complex passwords and two-factor authentication delays. This results in faster system access, fewer password-related support requests, and reduced IT overhead while also improving security.

Industry-specific compliance gets easier

Banking.

Clear audit trails for SOX and PCI compliance, protection for account and card data

Healthcare.

HIPAA-compliant access to patient records and insurance information

Insurance.

State regulator requirements met with detailed access logging for claims data

Next Steps

Delivery center security gaps pose serious risks to your organization. Shared passwords expose customer data, incomplete audit trails create compliance vulnerabilities, and weak authentication methods lead to costly operational surges when fraudulent activity spikes during coordinated attacks.

The 1Kosmos + Concentrix solution eliminates the guesswork while protecting your operational budget. Every agent gets verified without passwords, every data access gets logged, and you get complete visibility into who's touching your customer information - without the cost spikes that come from security incidents.

Ready to strengthen your contact center security? Contact our team to learn more about this integrated approach to protecting customer data and ensuring compliance.

1KOSMOS