

## Compliance & Security Support for Mid-Market Contact Centers

### Complete, COMPLIANT CAPTURE of useful customer data

Industry compliance is a necessary but challenging aspect of every contact center operation, regardless of your industry focus. In a high-pressure and dynamic operation, where sensitive customer information is shared every day, NICE can help you minimize the risk of costly regulatory breaches.

That's why NICE Uptivity Workforce Optimization (WFO) solutions are ideally suited for mid-sized contact centers—with the flexibility to ensure secure storage and transmission of audio and video recordings in accordance with far-reaching industry regulations like these:

- **Payment Card Industry (PCI) Data Security Standard (DSS) compliance:**

A critical checkbox when agents interact with customer orders and payment information

- **HIPAA compliance:**

Required adherence when working with healthcare and patient records

- **MiFID compliance:**

A key consideration when handling financial transactions

NICE Uptivity offers PCI-compliant recording solutions to help you capture valuable customer interaction data to fuel your performance and quality management efforts, while maintaining complete adherence to PCI and other industry-specific regulations.

Put measures in place that ensure sensitive authentication data (SAD) is not recorded via voice or desktop recording features. Using programmable triggers, your system can “blackout” portions of your calls containing SAD by engaging specific starts and stops. NICE Uptivity gives you the power to advance your workforce optimization plans without compromising the integrity of your compliance efforts.

# NICE Uptivity WFO solutions protect data from every angle



Sensitive Data



Permission Settings



Security Settings



Encryption Keys



Monitoring Data

## BLACKOUTS PREVENT CAPTURE OF SENSITIVE DATA

Use NICE Uptivity's API to control recording from your application code, to pause and resume recording when agents enter or view sensitive data. Available desktop analytics functionality monitors application activity and triggers blackouts when needed without requiring changes to your applications.

## 256-BIT AES FILE-LEVEL ENCRYPTION

Stored files cannot be read (decrypted) without the associated password-protected encryption key, so your data remains protected and secure. Encryption keys can be cycled (changed) on as-needed basis, allowing you to adhere to your security policies.

## NETWORK ENCRYPTION

NICE Uptivity supports use of encrypted Transport Layer Security (TLS) for all client-to-server and server-to-server communications while recording, and for browser-to-server communications during playback.

## ROLE-BASED PERMISSIONS

Set granular security controls, allowing only qualified users to access, listen to or export audio and video recordings. Permissions can be customized based on a user's job responsibilities.

## PASSWORD SECURITY

Built-in password protections can enforce a character length and complexity requirement, mandatory 90-day password change and re-authentication after 15 minutes of idle time. NICE Uptivity also works with your corporate identity systems via LDAP, Active Directory and SAML 2.0.

## MONITOR ACCESS TO DATA

Allow administrators to conduct full trace audits to determine who has accessed any recording in the system for playback, export or any other critical functions.

## DATA ARCHIVING AND PURGING

Create custom archival rules that enable records to be auto-archived and/or purged in compliance with both business rules and PCI regulations.