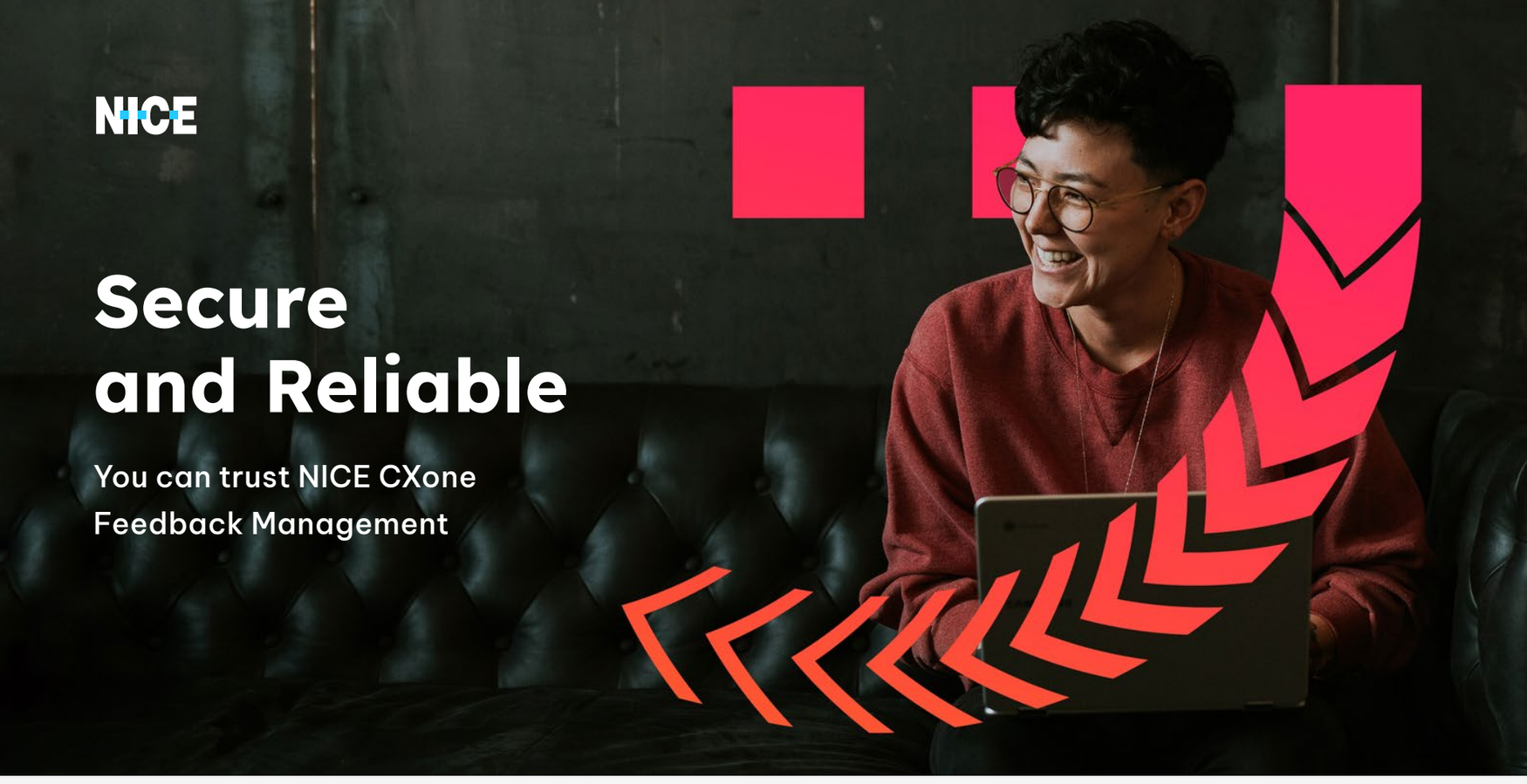


# Secure and Reliable

## You can trust NICE CXone Feedback Management

When you're on a mission to transform customer experiences, the last thing you need to worry about is the security of your customer data or downtime. With NICE CXone Feedback Management, you don't have to.

Every technical decision we make and action we take is with security and reliability in mind, so you can confidently focus on delivering your customers effortless, extraordinary experiences that make them smile.

### A MULTI-LAYERED APPROACH

It starts with a redundant, two-tiered network architecture infrastructure that we entrust to only the world's most secure data center provider.

It continues with multiple policies and processes that cover everything from account access and new development, to data retirement and disaster recovery.

It ends with dedicated staff, whose diligent monitoring safeguards each of our systems from security threats and network failures.

Together, they form a trusted system of controls and processes that can withstand just about anything that humans or nature can throw at it.

### VALIDATED PEACE OF MIND

To guarantee that we're adhering to industry best practices, as well as mandated standards for security, privacy, and availability, we regularly conduct and pass rigorous internal and external audits—including annual SSAE18 and ISO 27001 re-certification—so you can be confident that your CX data and programs will be secure and available to you at all times. You're welcome to request copies of the associated reports.

## SECURE CUSTOMER SURVEYS

Surveys are key to capturing feedback and understanding the voice of the customer (VOC), so NICE takes extraordinary measures to ensure that only authorized people with specific permission get access to your customer surveys, information, and reports.

Typically, those people include:

- Your customers who have been invited to complete a survey
- Your employees who have been approved to view survey results
- NICE employees who build and service the system

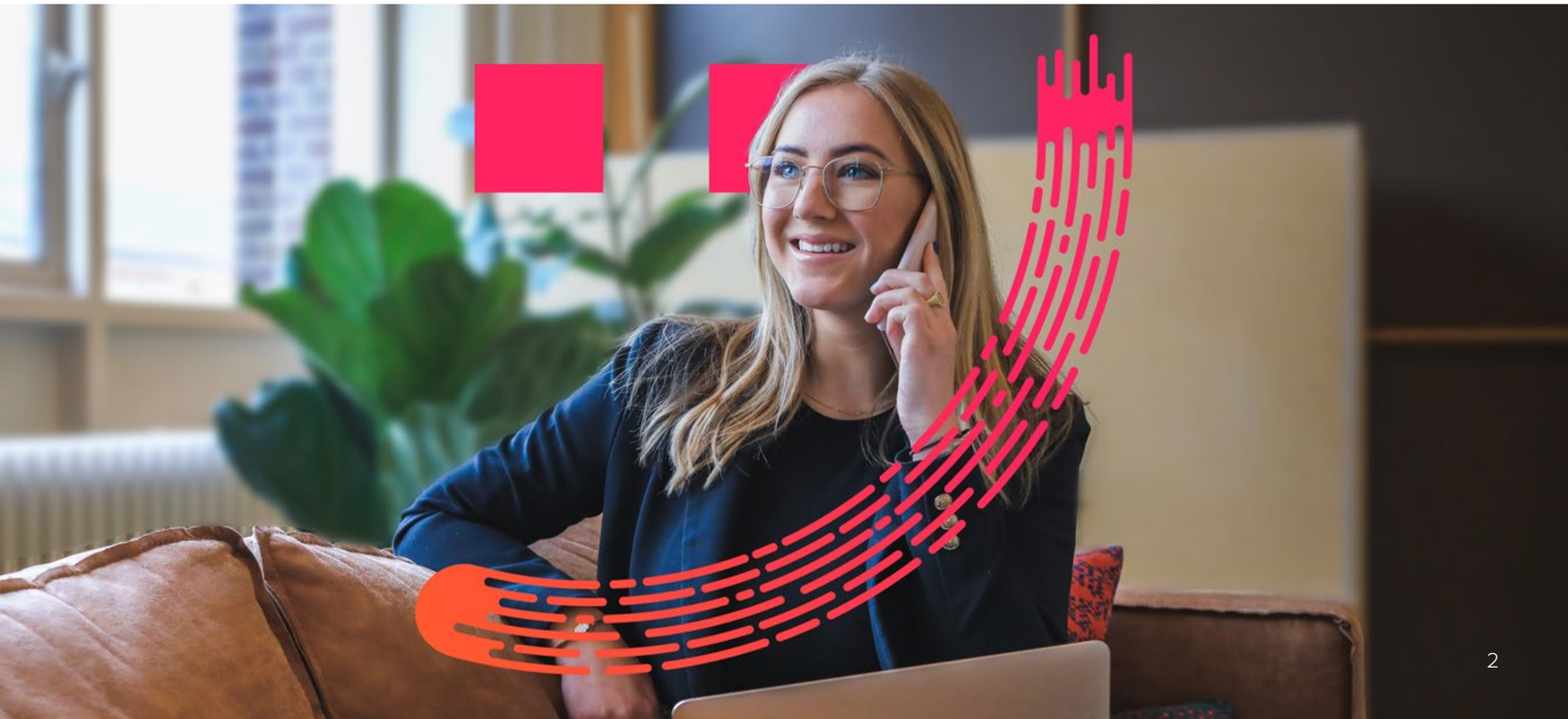
Authentication protocols guarantee the integrity and security of every survey and response. Potential respondents can only gain access to surveys via SMS conversational question or invitation with a URL link, an email invitation containing a URL link, or through an embedded link on a website. With a click, customers can securely submit their responses.

## SYSTEM ACCESS CONTROLS: THE POWER IS YOURS

Your customer information is, well, yours. So when you get started with NICE CXone Feedback Management, your organization will assign a designated account administrator who then has complete control to set, adjust, and revoke access permissions within your account.

Additionally, the NICE database stores all passwords in a hashed form and enforces strong password rules, such as minimum length, complexity, and expiration. If a user forgets their password, they're directed to a secure reset password page that requires a verification process. We will never email passwords to users.

For added security and control, all authorized development and monitoring are done via Virtual Private Network (VPN) connection that uses 128-bit encryption.



## MINIMIZING VIRTUAL AND PHYSICAL THREATS

We take the physical security of our infrastructure and global data centers seriously, so we only use Class A data centers managed by top-tier service providers. Overseen by NICE IT experts, all data centers must adhere to our rigorous standards for uptime, maintaining a precision environment, strict access control and physical security, and conditioned power—and they must earn SSAE18 re-certification annually.

To guard against virtual threats, we use a firewall that manages traffic, allowing connection only via certain required ports, as well as a threat minimization system specifically designed to protect from the latest malware or damage from component failure. We also periodically scan the network and perform security audits and penetration tests to identify and mitigate threats. We also deploy multiple controls—such as encryption and timed screen lockouts—to secure our office network and equipment from any unauthorized intrusions or access.

To make sure we have everything covered, a third-party security firm reviews our policies, procedures, and network architecture as part of our annual ISO 27001 re-certification process. They also conduct penetration tests on NICE CXone Feedback Management production systems to assess and mitigate any risks.

## ALWAYS-ON AVAILABILITY

You can't run an effective VOC program without ongoing access to accurate, up-to-date CX data and insights, so we've put multiple measures in place to make sure that your NICE CXone Feedback Management system and reports are always available.

Those measures include:

### Redundant infrastructure

The infrastructure on which NICE applications are hosted uses redundancy and failover to ensure that no single fault can cause a service interruption. All infrastructure, including network, storage, firewall, and load balancers are clustered, and we've set up redundant load balancers to distribute the workload of the web server cluster and keep everything running smoothly.

### Ongoing monitoring and backups

We use diagnostic tools to monitor network and system performance and proactively warn of possible failures and risk. Full weekly and daily incremental backups are stored in an encrypted and secure offsite data center and a globally-distributed workforce stands ready to mitigate any risks from business downtime.

## GOVERNANCE: MAKING EVERYONE ACCOUNTABLE

While the right technology choices are key, information security ultimately depends upon the people who manage it. That's why we've put in place a comprehensive combination of policies and procedures that makes every NICE employee responsible for the security of our clients' customer data and information. That includes HR processes that require all employees to acknowledge and understand our security policies, as well as audits and reviews that hold everyone accountable for upholding and adhering to them.

### Comprehensive security policy

As a condition of employment, all NICE employees must read and agree to a comprehensive security policy that strictly prohibits them from, among other things, divulging client-specific data to other clients or third-parties, and using anything but company-issued computers to work on company data and files.

### Corporate security practices

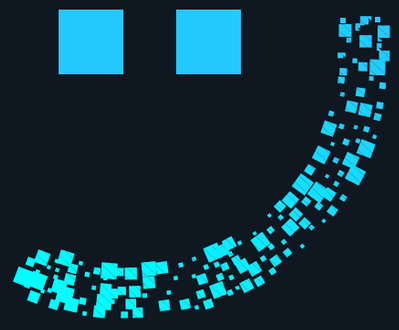
The NICE corporate network and technology is built and managed by internal IT staff. The IT staff is charged with staying up-to-date with new developments in security products, procedures, and practices and applying them to our technology. Because a portion of our staff frequently travels to visit clients, the network has been specifically designed to accommodate secure access for mobile professionals.

### Security audits

NICE performs periodic security audits that include reviews of security controls, network vulnerability, and penetration testing. We use these measures to evaluate and document possible vulnerabilities and implement mitigation strategies to eliminate potential threats to the system.

### Secure data transfers

Transferring data can leave it vulnerable to threats. To ensure your files are transferred safely, we support SFTP and provide a required public key so you can encrypt your files before sending them to us.



## About NICE

With NICE, it's never been easier for organizations of all sizes around the globe to create extraordinary customer experiences while meeting key business metrics. Featuring the world's #1 cloud native customer experience platform, CXone, NICE is a worldwide leader in AI-powered self-service and agent-assisted CX software for the contact center—and beyond. Over 25,000 organizations in more than 150 countries, including over 85 of the Fortune 100 companies, partner with NICE to transform—and elevate—every customer interaction.

www.nice.com



NICE
Make experiences flow