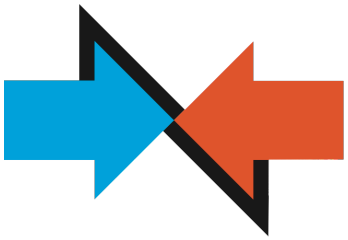


NITRIO

OVERVIEW FOR IT TEAMS

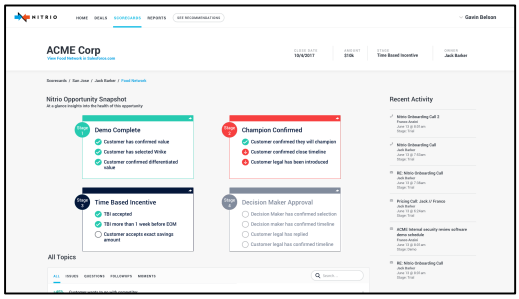
NITRIO, INC. | 425 Sherman Ave. Palo Alto, CA

What is Nitrio SalesAware?

Nitrio SalesAware is an artificial intelligence platform that helps sales teams win more business through better conversations with customers. Powered by the latest advancements in AI technology from Stanford, Nitrio is a breakthrough for sales teams looking to take advantage of modern technology to boost sales productivity.

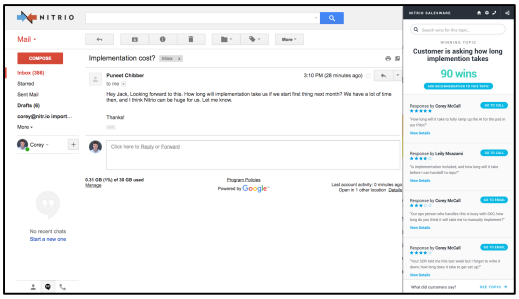
Opportunity Scorecards

Opportunity scorecards in salesforce show sales reps and leaders, at a glance, which milestones have actually been successfully completed based on Nitrio's AI analysis of the conversation between the rep and the customer. Sales leaders no longer need to rely on the accuracy and timeliness of CRM updates since Nitrio knows exactly how far the conversation has progressed.



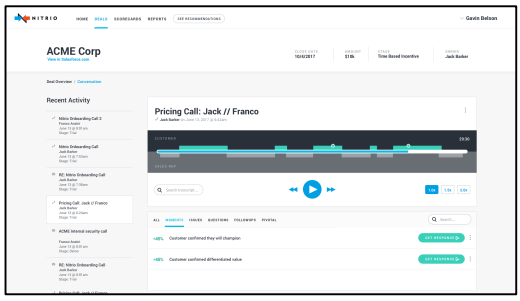
Real time Coaching in Email

Nitrio notifies reps when an important topic comes up in email, and shares examples of successful responses from other reps on the team in real time. In this way, every rep on the team can sell as well as the best rep in the company, and new reps can ramp up much more quickly.



Call recording and Transcription

Nitrio records every discovery call, pitch demo, and conversation between sales reps and their prospects. SalesAware processes these conversations and provides detailed insights into the sales topics that were discussed. Managers can dissect a sales call at a glance and know what was discussed, and what wasn't.



What Data Nitrio Accesses

Nitrio's AI works with sales conversations, and requires accesses to related data from Salesforce, Google Apps, and conference calls.

CRM data is accessed from Salesforce

- Account
- Activities
- Contact
- Forecast Category
- Lead
- LeadHistory
- Opportunity
- OpportunityContactRole
- OpportunityFieldHistory
- OpportunityHistory
- Profile
- RoleHierarchy
- User
- UserRole

Salesforce data is accessed through the official Salesforce API and can be revoked by you at any time. All data that is accessed is read-only, we do not update your CRM data.

Conversation data is accessed from Google Apps

- The headers and text of all sales-related emails
- The calendar invitation information for all sales-related meetings scheduled in Google Calendar

Google Apps data is accessed from authorized users through the Nitrio Chrome Extension on an individual rep basis. Nitrio does not centrally access Google Apps data outside of the extension, and data access is therefore restricted to the users who individually authorize it. With the exception of usage logging, the Nitrio Chrome extension does not collect any other data from users.

Phone call data is accessed from all web meetings and the Nitrio Dialer

- Call recordings from any sales calls scheduled in Google Calendar
- Call recordings from any call made using Nitrio's in-app dialer

Web meetings are recorded by Nitrio servers via a "silent listener" that will virtually join all conference calls scheduled by Nitrio users. Automated notice will be sent to the sales reps and their prospect before the call takes place in the form of a friendly meeting reminder. If a sales rep or their prospect wishes to erase a call recording, this can be done easily by the rep before, during, or after the call. Recorded calls can also be made through the in-app dialer.

How Nitrio Securely Stores and Processes your Data

Your data security is extremely important at us. We have modeled our security practices and policies after industry standards such as the official Salesforce ISV partnership requirements, the official Amazon Web Services (AWS) security best practices, and the SANS information security institute policies. The specific requirements for these are linked at the end of this document.

How Nitrio stores your data

We encrypt your data, including CRM data, emails, calendar events, and calls, using 256-bit AES encryption in storage and 256-bit SSL/TLS encryption in transit. Our database is hosted in a Virtual Private Cloud with AWS. AWS follows top IT security standards, including SOC 3, PCI DSS Level 1, and MTCS Level 3. Furthermore, we also encrypt all of your data in our database using 256-bit AES encryption.

How Nitrio accesses your data

Nitrio exclusively uses officially supported APIs from Google and Salesforce to interact with your data, and we ensure user information and identity protection by adhering to OAuth 2.0. OAuth is the industry standard for authorizing secure access to external applications without providing them with your password. When connecting Nitrio to Google and Salesforce via OAuth, we never receive or store your password, and you can revoke access to Nitrio at any time by revoking Nitrio's security token in your Google or Salesforce settings.

Who will have access to your data

Access to your data within Nitrio is given on an as-needed basis, and is available strictly to limited Nitrio employees and vetted full time contractors that have been security certified and require access in order to build our technology. All Nitrio employees and contractors who have this limited access are also subject to background checks conducted during the employment process. Any data accessed directly is subject to commercially reasonable efforts to de-identify it so that it does not contain company or person names, or other individually identifying information.

End users may have access to sales-related conversations from other sales reps, aggregate statistics related to the company's sales conversations (e.g. number of times a particular topic comes up in their communications with customers), and firmographics from Salesforce related to historical deals that are similar to the deal the rep is currently working on. All conversations without a corresponding record in Salesforce are considered non-sales-related and are not accessible by other users.

Security related training at Nitrio

All Nitrio employees are briefed on Nitrio's extensively documented security policies, which are adapted from standard SANS information security institute policies and linked at the end of this document. All employees who have access to customer data are subject to periodic recertification, where key security policies are reiterated.

In addition, no live or anonymized data lives on employees' computers. Nevertheless, we still enforce that all employee computers have full disk encryption enabled and use strong passwords.

How Nitrio monitors and protects its system

Encrypted backups are saved each day to ensure your data is safe and secure. We use high availability backups that are stored redundantly across geographically-separated availability zones to minimize the chance of data loss. We also use third-party monitoring services to track Nitrio's availability, with engineers on call to address any outages.

How to Deploy Nitrio

Deploying Nitrio involves three steps: (1) Connecting Nitrio to Salesforce, (2) Connecting individual reps to the Nitrio Chrome Extension and Google Apps, and (3) the Nitrio onboarding training.

1. Connecting Nitrio to Salesforce

Once you formally engaged with Nitrio, you will receive an email with an invitation to connect to Salesforce through the API. You need to click this link and login with a Salesforce account that has access to data of the team you are deploying Nitrio to.

2. Connecting individual reps to the Nitrio Chrome Extension and Google Apps.

The easiest way to connect individual reaps to Nitrio is to have them self-onboard. This requires reps to have authorization to install Chrome extensions. To self-onboard, each rep should:

1. Download & Install the Nitrio Chrome Extension by clicking here: https://chrome.google.com/webstore/detail/nitrio-salesaware/dniinonmliiclhbbkamokcmabdhfjioh
2. Once installed, click the Nitrio logo in the list of extensions in the top right of Chrome.
3. Click login and login with your Google Apps for Business credentials.

If reps are not authorized to install Chrome extensions, or if you would like to centrally deploy the extension to a group of reps, a Google Apps administrator should do the following:

1. Login at http://admin.google.com/
2. Click *Device Management*
3. Click *Chrome Management*
4. Click *User Settings*
5. Select the user group you will be deploying Nitrio to on the left side of the screen
6. Go to the section titled *Force-installed Apps and Extensions* and click *Manage force-installed apps*
7. Click *Specify a Custom App* and enter the following information:
   ID: dniinonmliiclhbbkamokcmabdhfjioh
   URL: https://chrome.google.com/webstore/detail/nitrio-salesaware/dniinonmliiclhbbkamokcmabdhfjioh
8. Click *Save*

The Nitrio Chrome Extension will now be installed on your team's Chrome browsers. **Each Individual rep is still required to click the Nitrio logo in the list of extensions in the top right of Chrome and click Login before Nitrio will be activated.**

3. Nitrio onboarding training

Once installed, Nitrio will schedule a face to face onboarding and training meeting with all users

How to Revoke Nitrio's Access to Your Data

Individual reps can uninstall the Nitrio Chrome Extension from Chrome, then revoke Nitrio's access to their data at the following URL:
https://accounts.google.com/b/0/IssuedAuthSubTokens

If the Nitrio Chrome Extension was deployed centrally, you may follow the same steps above and instead of adding the extension in Step 7, remove the extension.

To revoke Nitrio's access to Salesforce, you should do the following:

1. From your personal settings, enter *Advanced User Details* in the Quick Find box, then select *Advanced User Details*. If there are no results, enter *Personal Information* in the Quick Find box, then select *Personal Information.*
2. Go to the *OAuth Connected Apps* section and click *Revoke* to remove Nitrio's access to your data.

About Nitrio

Nitrio was founded with the vision of better sales conversations through artificial intelligence. The founding team are AI experts from Stanford and CRM experts from salesforce.com. Nitrio is backed by Silicon Valley venture capitalists such as Pear, Amino, and Illuminate Ventures

Resources

- Nitrio Security Policies adopted from SANS: *http://www.nitr.io/s/Nitrio_Security_Policy.pdf*
- Nitrio Cloud Services Agreement: http://nitr.io/csa
- Nitrio Privacy Policy: http://nitr.io/csa#privacy
- Salesforce ISV Security Requirements: *https://developer.salesforce.com/page/Security_Review*
- Amazon Web Services Security best Practices: https://aws.amazon.com/whitepapers/aws-security-best-practices/