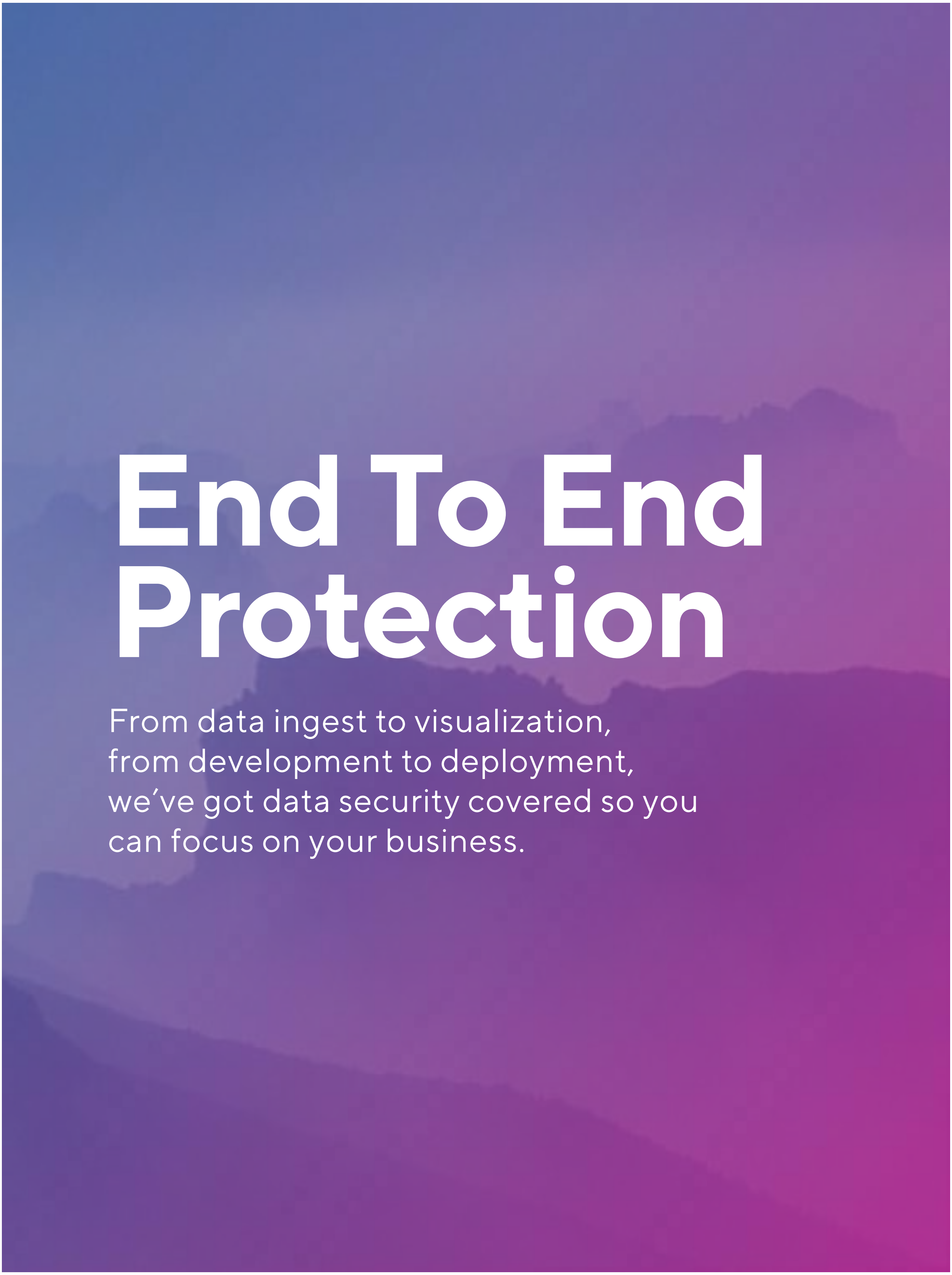


End To End Protection

From data ingest to visualization,
from development to deployment,
we've got data security covered so you
can focus on your business.

platformone

Control Access

Our platform allows for granular role controls throughout the application suite so whether it's your enterprise network accessing voc dashboards to monitor kpi's and manage action plans, or, allowing your customers to seamlessly access a community portal, we fully support integration with most industry standard identity and access management systems (aims).

SSO

Single Sign-on is implemented based on the SAML 2.0 standard and whilst supporting all major (AIMS) vendors, we can also support multiple AIMS within a single instance of our platform. This allows different divisions or companies within a group to be able to utilize the same application suite.

Multi Factor Authentication

For further security you can incorporate MultiFactor Authentication where a challenge is made during login for the user to either answer a phone call and validate, enter a code from an SMS, or authenticate via an app based push notification.

Application And Data Access Privileges

At logon we execute role-based access controls using the 'least privileges' principle. The privileges granted to a user determine which applications a user can access within the platform, what features of those applications are available and what data the user can see.

For example you can define a user as only having access to "Vision" and then specific views within "Vision", or you can give edit permission to your choice of "Vision" pages allowing them to interact and build their own reports. You can allow users to moderate group conversations, to build and publish their own surveys and distribute to the desired audience using our inbuilt advanced sampling toolkit.

Additional Visibility Control

Data visibility can be controlled automatically in line with your organizations hierarchy with override capabilities via attribute based access control at dashboard tile level.

Administrators can configure which application is the home application at user level allowing survey authors to head straight to the control center, "Connect", whilst report users land on a "Vision" dashboard page.

With Employee based Experience programs we understand that it is critical to not allow data to be filtered to the point of making a response attributable to an individual – Our base limiting feature allows you to customize the minimum base size before result masking occurs.

Column Level Secondary Encryption

When there's a requirement to hold data but not expose it to many users of the platform (for compliance purposes under GDPR/HIPAA etc.) we offer our UI based data column control mechanism allowing you to determine which fields should have a secondary encryption applied and what roles have privileges to view the data be it PII or general sensitive data.

Data Security And Compliance Controls

Hosting

We utilize Microsoft Azure regions for hosting with our own virtual environments giving the security, stability and scalability enterprises demand from their platform providers. All application and network access is monitored and logged centrally within region

Data remains in Region without exception. Data regions we currently support include...

- US
- Canada
- Australia
- Europe
- UK

Data Encryption

Storage
All databases are encrypted using TDE with secondary column level encryption for PII /Sensitive data. Physical storage is encrypted as standard.

Transit
Transport level encryption is via TLS 1.2.

Transfer
As a base we provide SSL access to your data via sFTP and REST-based API's. For additional security we offer IP Whitelisting and SSH on sFTP along with email + seed hashing for data pass back removing the need to pass back any PII.

Attack Surface

We internally pen test and run vulnerability scans on a continuous basis. Alongside this we utilize industry leading external partners to continuously assess our application and network vulnerability, we have bug bounty programs in place, and, overall, have a high level of confidence in our ecosystems security.

Unsubscribe / Opt-Out And General Suppression

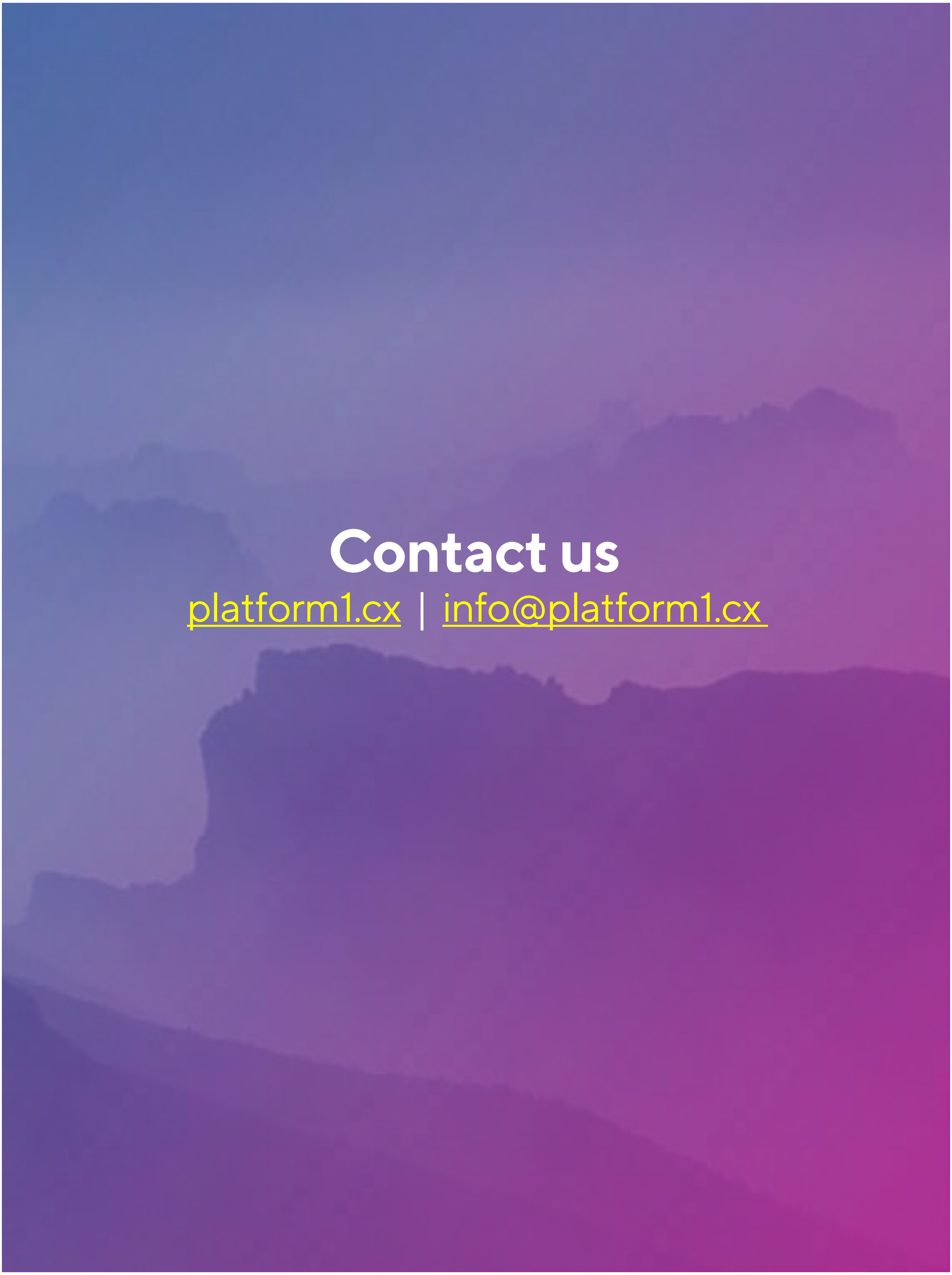
We provide link based opt out embedded within email content as well as site based opt out for our community clients. SMS requests to STOP are automatically processed extending to already queued messages. Complex contact rules can be applied to EXM programs catering for contact frequencies limitations / ratio's of segments etc.

GDPR/CCPA

Baked into the core of the platform are the principles and controls of the European Union's (GDPR) and subsequently the California Consumer Privacy Act (CCPA), allowing you to be fully compliant as a DIY user or as a serviced partner.

Certification

Our processes and controls from development to delivery are regularly audited by internal and external parties. We are ISO27001 Certified (in Australia and Sri Lanka) and are compliant with HIPAA.



Contact us

platform1.cx | info@platform1.cx

platformone