Today’s newest manufacturing technologies are quickly becoming varied and vast. Keeping up with the frameworks, ecosystem of tools, languages and data requirements is difficult. Safely implementing the technologies that have the greatest business impacts require considerable efforts from security and privacy teams.

Drishti is trusted by the world’s most advanced manufacturers. Ford, Hella, DENSO and Edwards Lifesciences, all use our AI-powered video analytics products to take the heavy lift out of deploying cutting edge technologies. It’s a vertically integrated cloud-based SaaS application that:

• Delivers video of the process on every manual assembly station providing complete traceability on production lines
• Creates data on top of video streams with specialized neural networks trained within hours for cycle time analytics
• Drives productivity-improving training content and decisions from insights on variability, line balance, bottlenecks & more

And, it does it all while meeting customers requirements for security and privacy.

Security & Privacy with Drishti
Safeguarding manufacturing data in the cloud

Drishti keeps your data secure

It’s important to ensure that the right people have appropriate access to the capabilities and data they need to stay productive with Drishti. And when they access the Drishti portal, assurances are needed for high availability, a safe transmission of data and appropriate use.

Drishti’s SaaS infrastructure is hosted on Google Cloud Platform (GCP) for its performance, availability, security and sustainability. Our shared security model delivers the best of the Google Cloud Platform (GCP) security infrastructure and Drishti capabilities for accessibility, integrity and availability.
### Permissions Management

The Drishti permissions model allows for streamlined, granular control. Controls are in place for access to all entities (projects, resources, tasks, requests, etc.). Permissions can be granted or revoked based on a user-type, group-type or at a profile level.

### Access for Customers

User access is managed by a customer designated administrator. Each Drishti user is uniquely identified by their email address. Strong passwords are required and user access is locked after five (5) unsuccessful password attempts.

Multi-factor authentication (MFA) is available for added security.

Portal access can be limited. A set of white-listed IP addresses can be designated and private networks (VPNs) can be enabled through white-listed corporate addresses.

### Access for Drishti Support

Drishti employees are only allowed access to customer data on a need to know basis. All access to a Drishti portal data requires two-factor authentication.

---

**Accessibility**

- Single Sign-On (SSO) is on our roadmap and will be available by June 30, 2021.

**Integrity**

### Physical and Environmental Security

The data Drishti collects is physically hosted in GCP data centers. Data for North American customers is stored and processed in us-west1 and us-central1 GCP regional centers. European customers are served out of GCP’s European regional centers. And, customers in Asia are served out of regional data centers per local regulations.

For more information, see [https://cloud.google.com/security/infrastructure](https://cloud.google.com/security/infrastructure).

### Audit Logging, Monitoring, and Traceability

Drishti takes advantage of GCP audit logging capabilities to track all access to data and other resources. GCP services provide audit logs to answer questions about who did what, where, and when while working within Drishti systems.
## Availability

### System Monitoring

Drishti employs a DevOps team and a comprehensive set of monitoring tools to ensure that our services are available to our customers at all times. Drishti portal uptime for the past year has been greater than 99.99%.

### Multi-layer Redundancy

Drishti’s cloud infrastructure is designed to leverage our cloud providers redundancy and maximum availability features. In the event of failure, all operation-critical components, including network, web, application and database servers are configured to maintain data integrity and availability.

### Data Recovery

Drishti leverages GCP RTO and RPO processes as the basis for disaster recovery. All video data is replicated three times (3x). All data is stored in high availability (HA) databases. In a hot disaster recovery, databases are brought back online by GCP automatically with minimal data loss. When video is recovered, Drishti can recreate all video analytics data.

Drishti takes daily snapshots of all databases as well as machine images. In case of a cold disaster recovery, the system will revert to the latest images with no more than twenty-four (24) hours of data loss.

If video streaming is interrupted before the video is stored, video may be lost permanently.

*In the past year, Drishti retained 99.7% of all video data collected. Video data loss was under 0.1% in the last quarter. This loss was due to network issues outside of Drishti’s cloud environment.*

### Drishti protects privacy rights

Data privacy protection is not just important for the business-to-consumer relationship, but also for business-to-business and business-to-employee relationships as well. At Drishti, we ensure that you stay compliant with current privacy regulations.

As processors of your data, our security operations team monitors the privacy regulation landscape to ensure we are in compliance with current guidance. Our policies are updated in accordance with rigorous standards that cover a broad set of privacy regulations worldwide, including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

### Data Ownership

All customer data and videos stored in Drishti’s web platform are owned solely by the customer. Customers can download their files at any time, either through the portal or by making a request to your Drishti representative. In case of termination of service, customer data will be made available for download for a limited period.

### Data Retention

Drishti retains customer data and videos for a period agreed upon in the Statement of Work. Data can be restored for a period of seven (7) days after deletion. Drishti may retain sample anonymized data for R&D and benchmarking purposes.

### Data Segregation

Data for training our neural networks is limited to only the data your company provides via the Drishti application. We do not use your data to train models for other customers.

Customer data is not commingled in storage.

*Drishti is currently working on new capabilities to protect employee privacy. Because Drishti technology relies solely on process footage, we can store video with blurring techniques – keeping identities protected and your processes in compliance with regional laws.*
ISO Certified Cloud Environment

GCP enables Drishti with a full set of independent 3rd-party certifications, including ISO 27001. As part of Drishti’s security roadmap, we plan to be ISO 27001 certified when appropriate for the company’s growth.

Compliant Cloud Provider

Drishti utilizes GCP ISO 27001 certified and SOC2/SSAE16 audited facilities. To learn more, details can be found at: https://cloud.google.com/security/compliance/iso-27001

Independent Audits

Drishti has not performed any security audits of its infrastructure and application so far. We performed third-party Security Audit and Penetration Testing in March of 2021. And, we will continue a cadence of PEN tests when appropriate.

About Drishti

Drishti’s mission is to extend human capabilities in an increasingly automated world. Its AI-powered video analytics technology provides visibility and insights that transform the pace and impact of manual assembly line improvement. Manufacturers use Drishti to anchor true digital transformation, driving sweeping improvements in quality costs, efficiency gains & time-to-proficiency for line associate training. And line associates rely on Drishti to be more consistent and efficient, becoming even more valuable on the factory floor. In 2019, Drishti was selected by the World Economic Forum as a Technology Pioneer; in 2020, Drishti was named to the Forbes AI 50 and a Top 5 AI Company in North America by NVIDIA. In 2021, Drishti was named a Manufacturing Leader by NAM and was named to the CB Insights AI 100. For more information, visit Drishti.com

Privacy Statement

Drishti does not collect any personal information from portal users other than their email address. Customer assigned administrators are able to view the email addresses of all users in the portal.

Drishti does not share portal user information with anyone, except as described in our privacy policy, nor does it sell or market this information to third parties. Drishti employees are allowed access to customer data on a need to know basis only. To access our privacy policy, please refer to our website: https://drishti.com/privacy-policy/

Drishti provides assurances now and for the future

Building on a solid foundation for infrastructure and policy, we continue to grow our security operations and privacy portfolio. We look forward to serving our customers better by adopting and continuing to follow proven standards.

Cookies

The Drishti Portal (app.drishti.com) uses cookies to optimize the user experience. Cookies help make Drishti work according to user expectations. They keep track of user session information and identify logged-in users. Customers may choose to turn off cookies using their browser preferences, but this may impact the performance of Drishti’s website and limit Drishti portal feature usability.

© 2021 Drishti | Patents Pending | Drishti.com