GoldFynch.com Security Overview

Secure eDiscovery for your case data with GoldFynch.com

Hundreds of lawyers, paralegals, and law firms manage their case eDiscovery with GoldFynch.com, and we value their trust. We follow the top professional security standards to ensure their data stays confidential and secure. This involves focusing on the reliability of our service, technology, infrastructure, and procedures. We use comprehensive security at all levels to help provide a safe, but simple, affordable, and scalable service. There are three elements to our security model: physical, network, and content. Here is a breakdown of how each element contributes:

Physical Security

We host GoldFynch.com across many layers of the Google Cloud environment on their world-class data centers. We use their cloud application servers and cloud file storage servers. Google Compute handles our web servers, and we use Google Cloud for file storage.

The physical security of the Google Cloud data centers includes strict physical access control to the buildings that house them. They also feature start-of-the-art seismic bracing, and smoke and fire early-detection systems. Digital surveillance systems are used to watch the sites 24x7x365.25.

The Google Cloud Firewall, Spam and DDOS protections secure our systems and your data. They are only visible to specifically-monitored IP addresses. And since your connection is through the Google Cloud secure network, any issue related to the location of the servers is negated. But for reference, GoldFynch.com is spread across many 'zones' in the Google Iowa Data Center. (Some international customers may be hosted on other Google sites, but this is only done on customer request)

At the Google data centers, all the databases are backed up once a day by one of the file servers. Data can be restored from these if needed - just contact our customer service team for help.

The servers are safe from physical harm, while software firewalls and spam protection keep your data safe, and data is always backed up.

GoldFynch eDiscovery was launched in 2016 (beta version in February 2016). Since then, we've had a consistent 99% uptime. Traditional ISP hosting or dedicated self-hosting carries a risk of physical hardware failures. But we host GoldFynch.com in the Google environment, (and Linode and Rackspace before that,) so all our services are in effect virtual. They are not vulnerable to such physical failures.

Network Security

There are two elements of Network Security: Infrastructure security and hosted data security.

GoldFynch's network infrastructure is built on industry standard protection procedures. Our team has years of experience with each aspect of network security. An understanding of the entire scope helps equip us for specific protection mechanisms.

All your data on GoldFynch is encrypted with 256-bit Secure Socket Layer (SSL) with the AES algorithm and 2048-bit key length. This is analogous to the data security used in banking and leading e-commerce sites. And regardless of your case size, we use the same high level of security.

Content Security

Content security relates to the access of your data. Primarily two groups have access: GoldFynch staff, and your team members who you give access rights to via case sharing.

GoldFynch's staff have years of experience in developing and running data centers. They are also proficient in improving processes for efficiency and effectiveness. Drawing from this, GoldFynch has world-class practices for data protection, and risk management.

Managing data center infrastructure needs more than just technology though. It needs a methodological approach to the processes involved. Knowledge sharing, risk assessment, escalation, management and day-to-day operations must all be rigorous.

We tightly control access to customer data by team members and log all such access. This access is only provided when a need for troubleshooting or support arises. Data is never accessed without your permission (for example a support request.)

GoldFynch has an authentication system that ensures only valid users can access data. Your case, the files in it, and review elements like tags and redactions, by default, are only visible to you. Other users need you to explicitly share the case with them. Each GoldFynch user has a unique password-protected account linked to a verified email address that is needed for login.

Once in GoldFynch, each user is limited to those actions that are allowed by the case owner. Not all users who have access to a case can perform actions like adding or deleting files to it. These depend on permissions granted to the user by the case owner. Only the case owner and Administrator can determine who can do what in that case.

In case you or a user you give access deletes files by mistake, they are still recoverable. Just contact GoldFynch support within a month.

Want to Know More?

For more information on how GoldFynch.com collects and processes your data, refer to our Privacy Policy. To learn more about how GoldFynch.com's service is delivered, please read our Terms of Service. If you have any questions about GoldFynch.com's security, contact us anytime at support@goldfynch.com and we'll get back to you quickly.