How We Can Work Together to **Keep Your Data Secure**

Raven is committed to working with its customers to keep their data secure. We take a global approach when it comes to protecting your data which includes protecting our infrastructure, Raven Cloud applications; providing ongoing training to our employees in security and privacy practices and building a culture where transparency and trust are our highest priorities. Additionally, we have partnered with strategic vendors who share our values and commitment to security.

Security By Design

We understand that you count on us to protect your data. That's why we work hard at Raven to build smart products and services that our customers can use for their personal and business needs. Here is a snapshot of some of the things we do to keep your data safe.

Ultra Secure Data Centers

At Raven we only use data centers with state of the art layered security. This means you can rest easy knowing your data is securely stored in facilities that are protected 24/7 with guard staff, secure perimeter defense systems, comprehensive camera coverage, biometric authentication and extensive security training for all data center employees.

Limit Employee Access

Another way we protect your data is by limiting who has access to it. Only authorized employees have access to our backend systems. Moreover, we will never access your Raven Cloud files without your permission. When access is authorized, it is limited only to necessary employees and only to the extent required to do their job. Access to our systems and your Raven Cloud Account is controlled and monitored.

Ongoing Security and Compliance Training for Employees

We understand that knowledge is power and that's why we provide initial security and compliance training when people join our team, in addition to required ongoing security and compliance training for our employees.

End-to-End Data Encryption

You have options when it comes to accessing your data. You may use our web app, our desktop app, mobile app or all of the above. Regardless of which app is being used, you can rest assured knowing your data is being encrypted in transit and at rest. Here is a breakdown of what we mean.

- ### Data in Transit

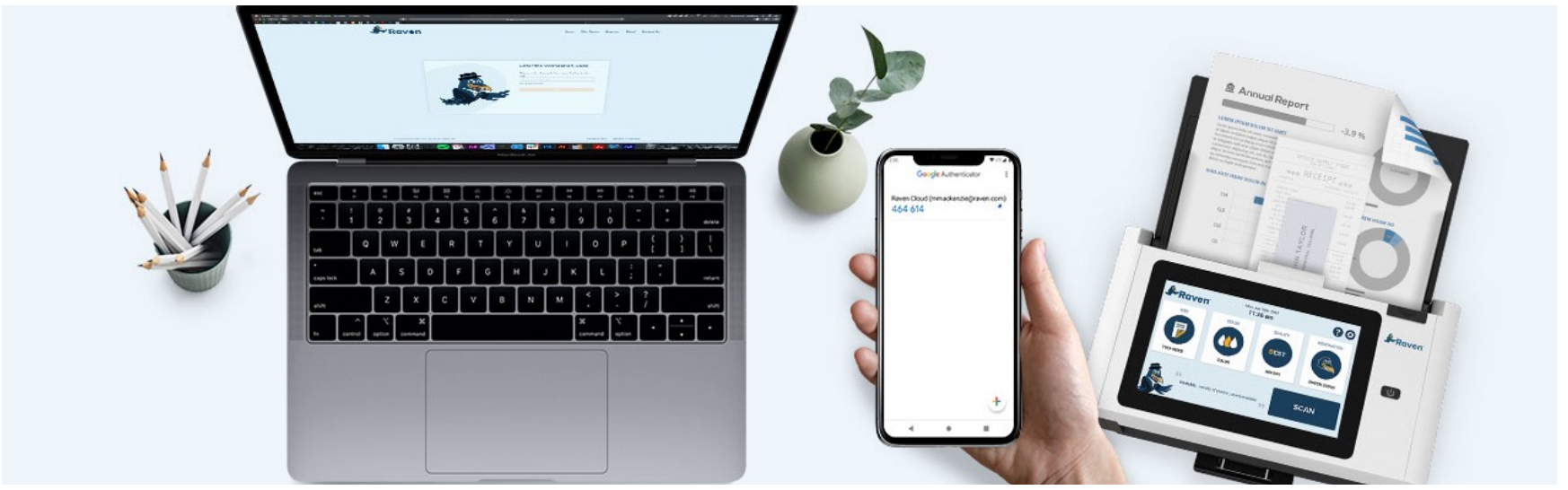
  Data in transit is simply data that is being sent from one location to another. In the case of our company, it is when data is being sent from a Raven app to our Raven API or a third party cloud platform. We use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfers. This creates a tunnel that is protected by a 128-bit or higher Advanced Encryption Standard (AES) encryption. Regardless of which app you're using to access your Raven account, you can rest assured knowing your data is being sent securely.

- ### Data at Rest

  Data at rest is defined as data that is stored either physically, like on a computer or other piece of hardware, or electronically like in the cloud or other platform. It can be temporarily or permanently stored, and can be structured, meaning it is easy to categorize, identify and analyze, or unstructured, meaning it is hard to categorize, identify and analyze, like a large unsearchable database.

  Your files at rest are encrypted using 256-bit Advanced Encryption Standard (AES). Additionally the files are broken down into multiple segments and then encrypted using encryption keys and stored in multiple data centers across the country. By breaking down the files into multiple segments creates an additional layer of security.

What you Can Do to Help Protect Your Data: **Account Holder's Responsibilities**



Account Holder's Responsibilities

You play an important role in ensuring that your data is secure. As the administrator of your Raven account, you have the ability to configure, use, and monitor your account in ways that meet your security, privacy, and compliance needs. We've put together this guide to help you understand what Raven does to keep your account safe, and what you can and should do to maintain visibility and control over your or your organization's data.

Multi-Factor Authentication

We offer two-factor authentication for all Raven Cloud accounts. Two-factor authentication or (2FA) is an additional security feature that requires the person signing in to the account to verify their account access by requiring an additional verification by either: SMS or Authenticator App during login. This is in addition to just knowing someone's username and password. This optional security feature is something we highly recommend for all of our customers.

Monitor Your Raven Account and Email for Unusual Activity

We will always send emails to the email address that was used to set up the Raven Cloud account whenever an account change like a password change is requested, or a new user is added. If you see an email like this come through and you did not request this activity immediately contact us at 1-800-713-9009.

Conduct Regular Raven Account Access Reviews

Make sure you know who has access to your Raven Cloud account. Never share your Raven Cloud Account password with anyone and make sure your friends, family, employees and any other user do the same. If you see a user listed on your Raven Cloud account, immediately contact us at 1-800-713-9009. Remember to keep your access fresh and current and to have people removed when you no longer want them to have access to your Raven Cloud Account.

Smart File Naming

We don't recommend you put any confidential information in the name/title of any of your files. Invest in a system of smart naming based on your personal or business needs. If you must put some confidential information, such as a credit card number or social security number, use only a small portion of it. Remember to protect your file library with the same degree and care you use to protect your files in your Raven account.

Ongoing Compliance and Security Education and Training

Make sure that both you and anyone else accessing your Raven account stay informed on the latest in cybersecurity awareness and training. Phishing attempts have never been greater and hackers continue to evolve and improve their methods.