Security Whitepaper

aumni

Aggregated, Anonymized, Secured: Defining “AumniPresence” and the Importance of Client Data at Aumni

Aumni tracks and analyzes investment data from investors all over the world. We carefully extract thousands of data points and audit them for accuracy and completeness. We apply the same meticulous approach to protecting the data on our platform. At Aumni, we pride ourselves on trustworthiness, and we will continue to invest in information security to gain and maintain that trust. Since the importance of security is present in all that we do, we refer to our information security strategy as “AumniPresence.”

AumniPresence: Aumni’s security program

Aumni maintains a strong commitment to security foundations and certifications, such as SOC 2 Type II. We ensure that our systems meet industry standards for managing customer data in terms of data availability, processing integrity, confidentiality, and privacy. Compliance is an excellent foundation for any security program, but Aumni strives to be much more than compliant.

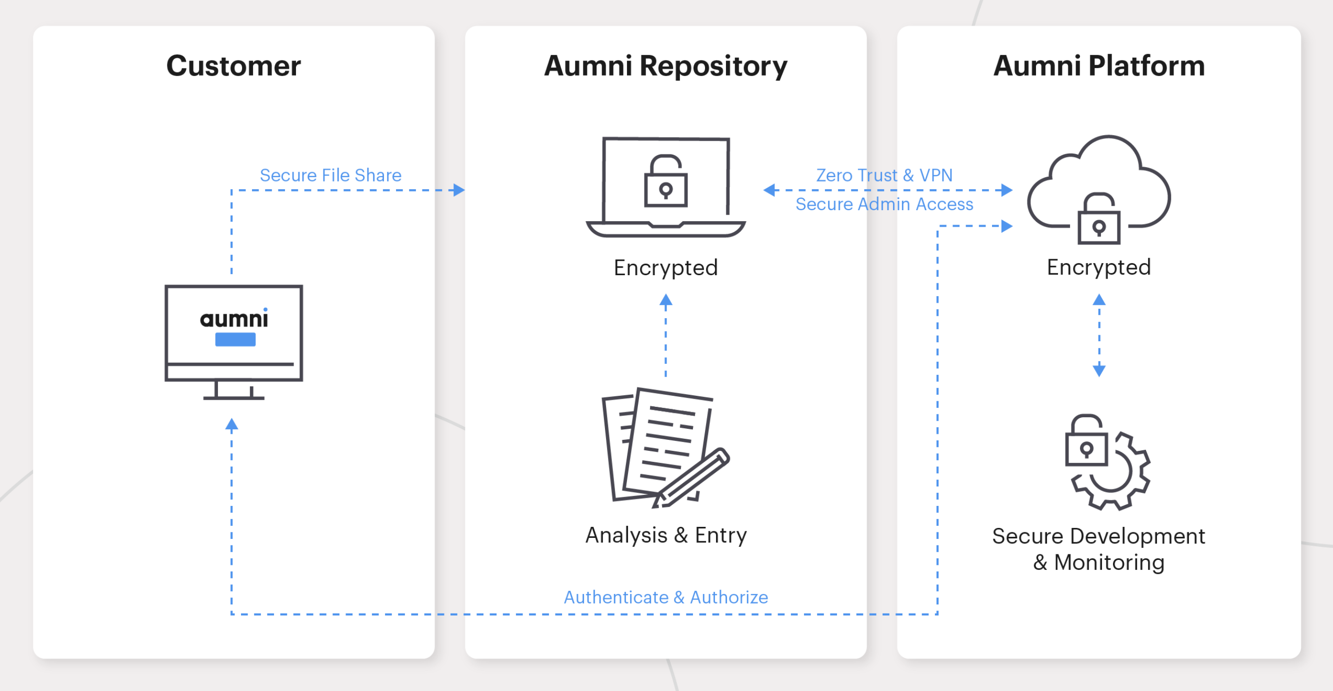
We firmly believe that security is a shared responsibility across the organization. Our best practices include but are not limited to:

- Access control
- Role-based security training for engineers
- General security awareness training for all employees
- Vulnerability management
- Asset management
- Incident response
- Business continuity and disaster recovery
- Logging and monitoring
- Vendor security
- Policy and security governance
- Data confidentiality and loss prevention
- Secure software life cycle management
- Risk assessment and mitigation

“Trust is of paramount importance to us, and data security is one of our top priorities.”

—Kelsey Chase, Co-Founder & President

How does Aumni manage data access?



All data that Aumni handles is considered valuable, whether structured or unstructured. Therefore, Aumni maintains a strict access control policy to verify the identity of a person before transmitting, collecting, accessing, or storing data.

All customers are required to log in using multi-factor authentication (MFA). Our internal operations require an even stricter level of access and authentication rigor across all tools and applications. Whenever possible, we automate or programmatically enforce our security practices, such as by leveraging zero-trust and single-sign-on to manage our internal access to systems and data based on least-privilege access. Access to Aumni's systems and data is restricted based on role and data classification of the data.

> **"At Aumni, we are very fortunate to have a healthy security culture mindset where security is always on the agenda. A security program that actually works is one supported by all leaders and employees, not just the security team."**
>
> **—Isaac Painter, VP Information Security**

How does Aumni store data securely?

All data at rest, including backups, is encrypted using AES-256 encryption and stored within the United States. Customer data is always stored securely for processing on the Aumni investment intelligence platform, and we use a mobile device management solution to ensure that each employee computer has full-disk encryption, anti-malware scanning, automatic software patching, and an always-on VPN.

To ensure that data cannot be leaked via system or product vulnerabilities and misconfigurations, even in encrypted form, Aumni maintains vulnerability and penetration tests conducted at an above industry-average frequency. When vulnerabilities are found, they are remediated in a timely manner. Additionally, we undertake continuous monitoring of systems, networks, and application events to identify trends, evolving threats, and anomalous conditions that pose a potential risk to Aumni or its customers.

How does Aumni transmit data securely?

When transmission between external entities is required, Aumni uses secure transfer methods. We apply TLS 1.2 or higher secure encryption for all data in transit. Data transfers are monitored and access from high-risk countries is prohibited.

All Aumni systems that collect, store, process, transmit, or dispose of data must record and retain audit-logging information. In the event of a vendor security breach that affects sensitive data, Aumni's response proceeds according to the terms of the written contract, including Aumni directing the vendor as to when it is appropriate to suspend data transmission.

A limited and approved set of employees handle sensitive customer data, and the data is fully encrypted in transit with access restricted via our zero-trust environment.

How does Aumni keep my data private?

No customer can see any other customers' data. If any Aumni data is made available to the public or other users (such as in developing market benchmarks or industry analysis), it is aggregated and anonymized so identifiable information is eliminated. All vendors that handle Aumni data are also vetted to ensure secure transmission and usage of the data.

> **"Providing our customer with the highest level of product quality and service is our top priority. Security plays a big role in that regard. Aumni's security team has been integrating security from the ground floor of our product and operations."**
>
> **—Rob Wise, Chief Technology Officer**

How does Aumni ensure that its web application product is secure?

Information Security, Engineering, and Product teams collaborate to ensure strict adherence to vulnerability detection and change management procedures. The large majority of our processes integrate automated security checks to identify vulnerabilities before they are ever introduced to production.

Aumni employs security and availability monitoring tools to detect suspicious or anomalous activity. For example, if an employee or customer logs in from two different locations where travel is impossible, our security team is immediately alerted. All alerts are acted upon in a timely manner. Additionally, we ensure that our assets in the cloud use hardened images (i.e., secure configurations) prior to deployment.

We deploy robust tooling to protect our perimeters: we use a zero-trust model for our endpoints (i.e., employee computers), and our web application is protected by a web application firewall that monitors for anomalous and suspicious activity. Our cloud infrastructure deploys firewall IDS/IPS capabilities.

How does Aumni ensure that its third-parties are maintaining good security practices?

A critical part of our security program is to perform security due diligence on any third-party that will be handling sensitive information on our behalf to support our services. This is important where if a vendor has a vulnerability, we have little control over how quickly it is remediated. Therefore, it is critical that we do business with third parties who have mature and well supported security programs.

We ensure that as a baseline the third-party has the appropriate security certifications proving that their security program has been independently assessed and deemed sufficient (e.g., SOC 2 Type II, ISO 27001). Also, we read through any additional security documentation provided by the third-party and follow up with questions with the vendor where there might be additional perceived risk. Aumni will not approve a third-party unless they have passed this rigor and agree to undergo such due diligence on at least an annual basis.

How does Aumni ensure their employees are practicing good security?

Security training is tailored by role, with all non-technical employees receiving general security awareness training both upon hiring and annually. We also seek to regularly update company employees at our company-wide all-hands on latest security developments and security's "tip of the week" presented by rotating information security personnel. Technical personnel undergo additional, role-based training.

For our overseas operations, the computer workstations do not have administrative rights and are managed remotely via a mobile device management solution. Additionally, we restrict access to personal email, social media, file share services, instant messaging, and any other medium by which sensitive customer or operational data could be leaked intentionally or unintentionally leaked.

Conclusion

While many service providers consider security to be the responsibility of engineering alone, at Aumni, we maintain a cultural recognition of security's centrality to our business. Aumni Information Security has full executive buy-in from the top-down. Divisional leaders meet regularly with our information security personnel to strategize and plan how their decisions can better facilitate security as well as foster a security-conscious culture.

At Aumni, we believe that protecting customer data is not a problem to be handled by the security team alone, and our approach springs from that belief. While rare in our industry, security's prominent role in the boardroom is in large part why Aumni can maintain a best-in-class security program.