ADDEPAR

SECURITY

Addepar Security Overview

Security consciousness is fundamental to how Addepar operates. From requiring security profiles on employees' mobile phones to the logic behind how our network is configured and maintained, security is at the forefront of everything we do.

The Addepar Approach to Security

Addepar uses a mixture of leading industry standards for security, tailored to keep client data safe from all angles.

We review the major security standards, select the most applicable elements of each, and implement them to the maximum benefit of our clients. A few elements we've implemented are role-based access control, principle of least privilege, and defense in depth.

In adherence to role-based access control, all Addepar employees are provided access to only the systems they need to do their jobs. Similarly, we follow the principle of least privilege to determine and grant employees the minimum amount of required access to each tool. For example, the systems available to our Engineering employees are different than those available to our Support employees. Within the Support team, a manager may be provided edit access in a particular system, whereas all individual contributors may be provided only view access.

Addepar also uses defense in depth to protect the systems containing client data from multiple angles and on multiple levels. For example, although we implement a Web Application Firewall to gate inbound network traffic to our application, we also employ intrusion detection, log monitoring, and other measures inside the network itself. If a security threat occurs at any level, our specialized security monitoring will detect it.

Security Organization & Processes

Addepar has a dedicated Security team and clearly-defined incident protocols in place to keep client data safe and secure.

Each member of the Security team was hired specifically to address Addepar security concerns. The team works closely with our Compliance team to ensure we meet annual audit commitments. Both teams work with our Legal team, and all three teams sit on a security council that regularly reviews the state of security at Addepar. The council also includes representatives from our Engineering, IT and DevOps teams.

All of these security-focused teams are involved with our regular security processes. On an annual basis, Addepar undergoes a SOC2 Type II security audit. We also hire an external, third-party company to conduct security reviews and penetration tests of all our systems.

We have processes in place to ensure that all systems, especially those housing client data, are secure 24/7/365. We participate in a bug bounty program to incentivize external, security-minded individuals to report potential security risks to us. We conduct a full security review of all third-party vendors we consider hiring. Similarly, we conduct background checks on all Addepar employees and contractors prior to hiring them, ensuring only trustworthy people have access to our systems and client data.

Addepar has a suite of formal security policies, and we review them on an annual basis to ensure they are relevant and up-to-date. This includes our incident response process. Our incident playbook outlines the steps we take if and when incidents arise, detailing the appropriate parties to contact, how to exhaustively document the incident, and the steps to take to fix the problem. We use this 24/7/365 incident response system as a framework for how to solve major security and product-specific incidents.

Data Stewardship

Addepar employees act as conscientious stewards of client data, and we ensure only the appropriate people can access that data.

We ensure that the only people with access to client data are those with a legitimate business need for it and that their access is properly scoped in terms of breadth and time. In this respect, we limit access to client data. For example, the Support team is given access to a client's production instance for only the amount of time it takes to investigate and address a client support request.

We have a data classification policy that outlines the levels of data confidentiality. Each level is associated with increasingly strict controls around who can access that level's data. All data in Addepar is covered by this policy, and it's made available to all Addepar employees for reference.

Security consciousness is a key aspect of the Addepar culture. We hire individuals with a security-conscious mindset, and we construct our policies and processes according to our stance on data stewardship. Keeping client data safe and secure is paramount in all that we do as a company.

About Addepar

Addepar is the financial operating system that brings common sense and data-driven investing to our financial world. Addepar gives asset owners and advisors a clearer financial picture at every level, all in one place. It handles all types of assets denominated in any currency. With customizable reporting, financial advisors can visualize and communicate relevant information to anyone who needs it. Secure, scalable, and fast, Addepar is purpose-built to power the global financial system. Hundreds of single and multi-family offices, wealth advisors, large financial institutions, endowments, and foundations manage over $1 trillion in assets on the Addepar platform. Addepar has offices in Silicon Valley, New York, Chicago, and Salt Lake City.

Learn more at addepar.com

Get in touch.

PHONE +1 (855) 464-6268
EMAIL inquiries@addepar.com