Addepar security overview

Security consciousness is fundamental to how Addepar operates. From employee security awareness education to formal processes and procedures to protect sensitive data, to defense in depth to secure network, application and endpoints — security is at the forefront of everything we do.

The Addepar approach to security

Addepar leverages leading industry standards to inform our security program, tailored to keep client data safe from all angles.

We regularly benchmark our program against security standards and best practices, select the most applicable elements of each, and implement enhancements to safeguard Addepar systems and data against evolving cyber threats. A few elements we've implemented are role-based access control, principle of least privilege and defense in depth.

To support the principle of least privilege, Addepar employees are provided access to only the systems they need to do their jobs. . For example, the systems and permissions available to our Engineering employees are different than those available to our Support employees.

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 potential security threat is detected, our 24×7×365 security monitoring teamwill receive an alert to investigate the event in line with defined policies and procedures.

Security organization and 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. Addepar's dedicated Security team reports to the Chief Information Security Officer. The Security team provides monthly updates on key security risks and initiatives to the Technology Risk Committee, a cross-functional group that consists of leadership from Engineering, Legal, Product and Security. Additionally, the CISO provides annual security and risk updates to the Board of Directors.

On an annual basis, Addepar undergoes an independent SOC 2 Type II security audit. We also hire an external, third-party company to conduct annual penetration tests of our core systems.

We have processes in place to ensure that all systems, especially those housing client data, are secure 24×7×365. We conduct a full security due diligence review of all key third-party vendors we consider hiring. Similarly, we conduct background checks on all Addepar employees and contractors prior to hiring them, ensuring only vetted personnel have access to our systems and client data. Addepar personnel are trained on security policies upon onboarding and receive regular information security awareness training on an annual basis.

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 document and communicate the incident, and the steps to contain and remediate the event. We use this 24×7×365 incident response system as a framework to investigate and resolve security and operational 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 access to client data is restricted to those with a legitimate business need for it and that their access is properly scoped in terms of breadth and time. 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, along with how that data must be securely handled. This policy is made available to all Addepar employees, and the key principles of this document are also re-enforced through regular security awareness training.

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.