UpGuard sales prep brief: Asana

Company at a glance

Website: asana.com
Industry: information technology & services
Employees: 1900
Revenue: 738.7M
HQ: San Francisco, United States
Founded: 2008

Qualification intel

- **Size & revenue:** Asana is a publicly traded company (ASAN) with 1900 employees, £738.7M annual revenue, and a £3.3B market cap, indicating a significant scale.
- **Likely compliance scope:** Given its US HQ, public status, and industry, compliance requirements likely include SOX, GDPR, and other data privacy regulations.
- **Vendor ecosystem complexity:** A large tech stack and global operations suggest a complex network of third-party vendors requiring robust management.

Pain indicators

- **Recent security incidents or peer breaches:** Unknown.
- **Regulatory or growth pressures that expand third-party risk:** Being a public company, Asana faces increased scrutiny over cybersecurity disclosures, driving demand for comprehensive third-party risk management.
- **Hiring or leadership changes in security:** Unknown.

Competitive landscape

- **Likely existing security/IT tools from tech_stack:** Heavily reliant on cloud services (Amazon AWS, Atlassian Cloud) and enterprise SaaS tools (Marketo, Greenhouse.io), indicating a distributed IT environment.

- **Gaps UpGuard can address:** UpGuard can centralise and automate third-party risk assessments, enhance continuous vendor monitoring, and provide clarity on their external attack surface.
- **Typical alternatives a company like this might consider:** Other GRC or TPRM platforms, or a continuation of manual vendor assessment processes.

Key talking points

- **Industry-specific risk examples and peer references:** Discuss supply chain risks pertinent to software companies and the importance of securing the customer data processed by their services.
- **Concise value props tailored to their stack and scale:** Highlight how UpGuard automates evidence collection for compliance and provides continuous visibility into their cloud-dependent vendor ecosystem.
- **1–2 proof points you can deliver quickly:** Offer to demonstrate risk ratings for their key AWS services or perform an external attack surface scan of asana.com.

Technical fit

- **Integrations suggested by tech_stack:** Potential integrations with AWS for cloud security posture, and other SaaS tools like Marketo or Greenhouse.io for vendor data.
- **Scale considerations:** The high employee count and Alexa rank indicate a large attack surface and a significant volume of vendors requiring continuous monitoring.
- **Data flows likely relevant to due diligence and continuous monitoring:** Focus on SaaS vendors handling customer data, cloud infrastructure providers, and HR/finance system vendors.

Additional research focus

Search for any recent security breaches