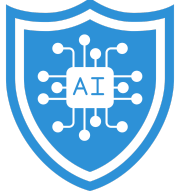


Augment's Security and Privacy

August, 2024



Building Trust from the Ground Up

On day zero, we adopted organizational commitments to protect the confidentiality, integrity, and availability of our customers' and corporate data. From there, we built our systems from the ground up, with five Security Principles guiding every design decision: Data Minimization, Layers of Security, Principle of Least Privilege, Reduce Human Involvement, and Fail-Safe.

No Training on Customer's Proprietary Data

We guarantee that our customers' proprietary data will never be used for training by us or a third party. We built our tech from the ground up, using foundational models and adding our secret sauce. We back up our commitments with an indemnification clause in our terms and conditions.

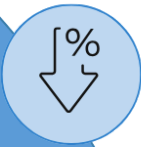


This approach safeguards your data against unauthorized use and reinforces our promise to maintain a clear boundary between customer data and our model development. This is the only way we can ensure that the insights and outputs you receive are generated without compromising the privacy of your sensitive information, providing you with peace of mind and security in our services.



Secure by Design, Private by Default

To adhere to our commitment outlined in our Data Classification and Secure Handling Policy, we invest in comprehensive resources in R&D to build security and privacy controls from the ground up. We train our teams to deepen everyone's understanding of privacy and security principles and their critical importance to our customers. We maintain transparency about our data practices, including how data is used, stored, and protected - never storing it for longer than is absolutely necessary. For accountability, we maintain meticulous data logs and diligently respond to privacy requests. Customers have the final say over their personal information, ensuring we comply with privacy regulations such as GDPR and CCPA.



Data Minimization

Augment adheres to the principle of data minimization, ensuring that only the necessary data is collected and processed to provide our services, thereby enhancing user privacy and security.



Layers of Security

Augment employs a layered security approach, integrating multiple defensive mechanisms across our infrastructure to provide comprehensive protection against a wide range of cyber threats.



Principle of Least Privilege

Augment rigorously applies the Principle of Least Privilege, granting system access only to the extent necessary for users and services to perform their specific functions, minimizing potential vulnerabilities.



Reduced Human Involvement

Augment minimizes human involvement in critical processes through automation, enhancing both the efficiency and security of our AI-driven services.



Fail-Safe

Augment incorporates fail-safe mechanisms across our systems, ensuring that in the event of a malfunction or threat, operations default to a secure state to protect data and functionality.

Proof-of-Possession API Authorization

Further, our Proof-of-Possession API architecture eliminates the need for manual authorization configurations in Augment. Our advanced Proof-of-Possession ensures there's no risk of data leakage between different developers, even within your organization. Every request for a code completion includes a cryptographic Proof-of-Possession within the API request, which authorizes the server to use the requested context.



This Proof-of-Possession API architecture guarantees that each code completion operates only on code developers possess locally. As such, no information leakage is possible, mitigating risks of data breaches and unauthorized access from internal and external sources through our APIs.

Augment's security-focused architecture combines the robustness of on-premise security with the flexibility of a SaaS. Your data benefits from a non-extractable API setup with advanced, multi-layered security measures, offering protection that rivals many on-premise solutions.



3rd Party Attestation and Continuous Pentesting

At Augment, we recognize the importance of third-party attestation in validating and improving our security, privacy, and operational commitments. We employ independent third-party experts to conduct penetration testing across our entire production services and underlying infrastructure to validate our threat model. Additionally, we undergo annual SOC 2 Type II audits.

Surpassing On-Prem in Every Way

Move from expensive on-prem systems to our secure, cloud-based API infrastructure. Enjoy advanced security, compliance, and performance with access to the latest AI hardware and instant security upgrades. Join us to enhance your AI strategy with greater efficiency, security, and innovation.

