Anduin

SECURITY WHITE PAPER

2024

security@anduintransact.com

Anduin

Security at Anduin

Security is our top priority.

In today's digital landscape, safeguarding sensitive information - including personally identifiable information (PII), proprietary transaction terms, and more - is imperative. At Anduin, our mission transcends the enhancement of productivity and efficiency; we prioritize your security and privacy.

Our products are engineered with advanced security features at their foundation. Beyond product delivery, we actively engage with you and your partners to integrate best security practices into your operations.

The following guide highlights Anduin's industry-standard security features.

SECTION 1

Compliance and Data Protection

This section offers an overview of Anduin's comprehensive security approach to safeguard both our systems and customer data, as well as our compliance with various international security standards.

Physical Security

Anduin platform and services are hosted in AWS, which operates state-of-the-art SOC 1 Type II, SOC 2 Type II, and ISO 27001 certified facilities.

Anduin utilizes strict security measures that are enforced in our offices. This includes strict perimeter and border security, access controls, surveillance to prevent unauthorized access, and ensure the security of facilities and information systems.

The policy details requirements for equipment protection, visitor management, restricted area access, and regular reviews and updates to security equipment and practices.

Customer Data Privacy

Anduin's privacy policy can be found here. At Anduin, our customer's privacy is our first concern. We strive to use information to provide the best possible service while respecting the confidentiality of the information we are entrusted with. Currently, we are compliant with the U.S. ESIGN Act of 2000, EU General Data Protection Regulation (GDPR), California privacy regulations (CCPA & CPRA), and have SOC 2 Type II Certification.

Security Certifications and Tests

Anduin systems undergo rigorous scrutiny by internal and third-party auditors to assess and validate security measures that we have in place.

- Continually and consistently meet international security standards
- Compliance with applicable laws and regulations
- Regularly hire external experts to conduct penetration testing
- Regularly hire certified auditors to validate our security commitments
- Share latest test results and external assessments with our partners and customers

Anduin Compliance and Data Protection

Compliance

Anduin is compliant with the following:

- SOC 2 Type II
- The Uniform Electronic Transactions Act
- The U.S. ESIGN Act of 2000
- eIDAS 2.0 Advanced Electronic Signature
  (option to use a qualified 3rd party e-signature)
- Write Once Read Many Archiving (WORM)
- EU General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Cloud Security Alliance (CSA) - Security, Trust, Assurance and Risk program (STAR)

SECTION 2

Security Architecture and Framework

This section presents the structured approach of our security framework to ensure that each component is clearly defined, providing stakeholders with a thorough understanding of how Anduin maintains the integrity and confidentiality of its data assets.

Zero Trust Approach

At Anduin, we implement a zero-trust security model, designed under the premise that all devices, networks, and users could potentially be compromised. This approach mandates that access to sensitive data is strictly controlled and only granted on a verified, need-to-know basis. Utilizing Cloudflare's SASE solutions, our architecture includes:

- **Advanced Firewalls and Security Service Edge:** These ensure that only authenticated users can access designated resources, enhancing protection against threats like malware, phishing, and data exfiltration.
- **Zero Trust Network Access:** Continuously validates every access request by any user, device, or application, thereby minimizing unnecessary access and reducing the potential impact of security breaches.
- **Zero Trust Secure Web Gateway:** Acts as a centralized control point that enforces strict web traffic verification and access controls, ensuring compliance with zero trust principles by granting least privilege access at all times.

Multi-tenant Security

Our multi-tenant SaaS architecture is supported by Amazon Web Services (AWS), which provides robust scalability, security, and reliability across all layers of our infrastructure:

- **Logical Data Separation:** Despite the shared nature of our databases, we enforce strong logical separations and fine-grained authorization controls at the table, namespace, and row levels.
- **Dedicated Databases:** Specific classes of sensitive data are isolated in dedicated databases, ensuring that the multi-tenant environment does not compromise data security.

Continued...

- **Role-Based Access Control (RBAC):** This allows secure and efficient collaboration across different workflows and funds, enforcing strict adherence to access permissions based on user roles.

Enterprise Network Security

Anduin's network security framework is structured to provide robust protection against both internal and external threats:

- **Multi-Layered Firewalls and Virtual Networks:** We deploy advanced firewalls and utilize multiple virtual networks to create clear boundaries between different operational modules. This ensures isolated environments where traffic is strictly regulated based on predefined security policies.
- **Production Network Isolation:** All application servers are hosted within private subnets without public IP addresses, effectively segregating our production environments from less secure networks.
- **Regular Vulnerability Assessments:** To maintain a proactive security posture, we conduct regular assessments to identify and rectify network vulnerabilities and misconfigurations.
- **Perimeter Security Controls:** Enhanced security measures such as Network Access Control Lists (ACLs), Intrusion Prevention Systems (IPS), and Web Application Firewalls (WAFs) are implemented at critical points within our network. These controls serve as an additional security layer, preventing unauthorized access and monitoring for malicious activities.
- **Strict Access Controls:** Consistent with our Zero Trust approach, server access is stringently controlled. By default, no ingress traffic is allowed, ensuring that only explicitly authorized actions are permitted within our network infrastructure.

Endpoint Security

As a part of our Zero Trust strategy, a comprehensive endpoint security strategy is deployed:

- **Device and Application Controls:** Includes enforcing regular software updates, restricting external storage use, and implementing application control measures.
- **Physical Security Measures:** Automatic locking of devices, removal of admin privileges, and full disk encryption are standard to prevent unauthorized access.
- **Behavioral-Based Protection:** We deploy advanced anti-malware, always-on firewalls, host-based intrusion prevention systems, and extended detection and response systems to actively monitor and respond to potential threats.

Encryption

Ensuring the security of data, both in transit and at rest, is a critical priority:

- **In Transit:** We use HTTPS and TLS 1.2 or higher to secure all data transmissions to and from our systems.
- **At Rest:** Data is stored in environments that meet stringent standards, including SOC 1 Type II, SOC 2 Type I, and ISO 27001 certifications. Encryption of customer data, documents, and critical infrastructure configurations is performed using AES-256 encryption.
- **Key Management:** We ensure the security of encryption keys via industry-grade secret vaults with regular rotations of master keys to further bolster security.

SECTION 3

Product Security

This section highlights security features offered in our products. The features are designed to allow customizations that align with your standards and regulatory requirements.

Authentication

At Anduin, we implement a robust authentication system that ensures the identity verification of each user from initial login to every request. Our comprehensive approach includes several layers of security to meet industry standards:

Two-Factor Authentication (2FA)

Users can enable 2FA, which requires not only a password but also a verification code generated by authenticator apps like Google Authenticator or Microsoft Authenticator, or sent via SMS or phone call. Administrators have the option to mandate 2FA for accessing specific environments, enhancing security for sensitive operations.

Single Sign-On (SSO)

We support SSO through OpenID Connect (OIDC), OAuth 2.0, and SAML 2.0, allowing users to seamlessly and securely use their existing credentials from other systems to access the Anduin platform. Our SSO solutions have been extensively implemented across various customer systems, providing both enhanced security and user convenience.

API Key Authentication

Secures public API interactions, ensuring that only authorized entities can access our services.

Strong Password Policies

Minimum 10 characters, must have numbers, capitalized letters, special characters and must not be similar to 3 previously used passwords.

All user passwords are hashed using the PBKDF2 algorithm, ensuring robust protection against unauthorized access.

Session Management

Idle sessions are automatically expired after a set period, which can be adjusted by administrators according to internal security policies.

Authorization

Anduin's authorization framework is designed to tightly control data access within our multi-tenant platform, ensuring users can only access data for which they have explicit rights:

- **Role-Based Access Control (RBAC):** We implement a detailed RBAC system where access privileges are defined by specific user roles, such as deal owner, deal participant, data room owner, and data room participant. This structure provides users with flexible yet controlled access to their data.
- **Pre-Authorized Access Tokens:** For operations that do not require a full login, such as e-signing documents, completing tasks, or viewing reports, our system utilizes pre-authorized access tokens to streamline access while maintaining security.

Audit log

Anduin maintains a rigorous audit system that captures all users' actions in an immutable audit trail, accessible only to authorized system administrators. We employ advanced tools that enable:

- **Log Analysis:** A comprehensive suite of tools is available to search, filter, and report on system activities to ensure transparency and accountability.
- **Secure Log Storage:** All logs are encrypted using AES-256 and stored securely in the cloud, ensuring their integrity and confidentiality.
- **Long-Term Retention:** We retain logs over extended periods, facilitating thorough audits and detailed forensic investigations whenever necessary.

Anduin Product Security

Data Residency

At Anduin, we're aware of the regulations you face to ensure the privacy and security of personal data. Often, these regulations include guidelines on data residency, or where this data is physically processed and stored.

We offer a simple way to set up and maintain data residency within your chosen geographic location. By having data centers located in both the U.S. and EU, we can offer customers the ability to choose where their data should be processed and stored.

SECTION 4

Operational Security Practices

These operational security practices underscore our proactive approach to safeguarding sensitive data and maintaining trust with our clients and partners. Each component of our security operations is crafted to address specific risks and ensure that Anduin remains at the forefront of data security and privacy standards.

Personnel Security

At Anduin, our commitment to security permeates every level of our organization. We ensure that all employees are continuously educated and vigilant about protecting customer data through comprehensive security training and regular awareness programs:

Cross-Functional Security Team

Experts from various departments collaborate to uphold our security and privacy standards.

Background Checks and Policies

Each employee undergoes thorough background checks and must adhere to our code of conduct and acceptable use policies.

Continuous Training

We conduct annual security and privacy training for all employees to reinforce our security-first culture.

Phishing Awareness

Regular phishing simulation tests are conducted to enhance awareness and preparedness among staff.

InfoSec Council

This group oversees our risk management strategies and the implementation of security protocols across the company.

Secure Coding Practices

Engineers receive specialized training to ensure secure coding practices are maintained throughout the software development lifecycle.

Internal Data Access

Anduin adheres to strict data access guidelines to ensure customer data is handled securely and ethically:

- **Principle of Least Privilege:** Access to customer data is strictly limited to what is necessary for employees to perform their duties.
- **Data Pseudonymization:** Where applicable, personal data is pseudonymized to enhance confidentiality.
- **Continuous Control Evaluation:** Our data access controls, including separation of duties, are regularly reviewed and updated to prevent misuse and ensure compliance with the latest security standards.

Data Loss Prevention Controls

Anduin's Data Loss Prevention (DLP) system is a cornerstone of our strategy to protect sensitive information:

- **Data Classification:** We categorize data by its level of sensitivity and business importance, ensuring it is handled appropriately.
- **Technical Controls:** Our layered security strategy includes sensitive data matching across all platforms and preventive measures against data leaks in production environments, cloud storage, and email systems.
- **Encryption and Security Measures:** Foundational security measures such as data encryption, full disk encryption, and remote wipe capabilities are implemented to secure data across all devices and platforms.

Secure Code Practice

Our development process is designed to produce secure and reliable software through rigorous testing and continual improvement:

- **Code Review and Deployment:** All code is thoroughly reviewed by qualified engineers before merging into production. We employ a continuous deployment model to streamline this process.
- **Automated Security Analysis:** Automated tools analyze our code base for vulnerabilities, unsafe practices, or sensitive data inclusions, ensuring issues are identified and addressed early.
- **Environment Segregation:** Development, testing, and staging environments are strictly separated from production environments to prevent cross-contamination.
- **Penetration Testing:** External security experts conduct annual penetration testing on our systems, with all identified issues addressed promptly to mitigate any potential risks.

SECTION 5

Resilience and Recovery

This section demonstrates Anduin's commitment to maintaining a reliable and resilient service, ensuring continuous availability and preparedness for any potential disruptions.

Business Continuity and Disaster Recovery

At Anduin, we emphasize resilience and robust response capabilities to handle unforeseen disasters efficiently. Our business continuity and disaster recovery strategies are anchored in several key practices:

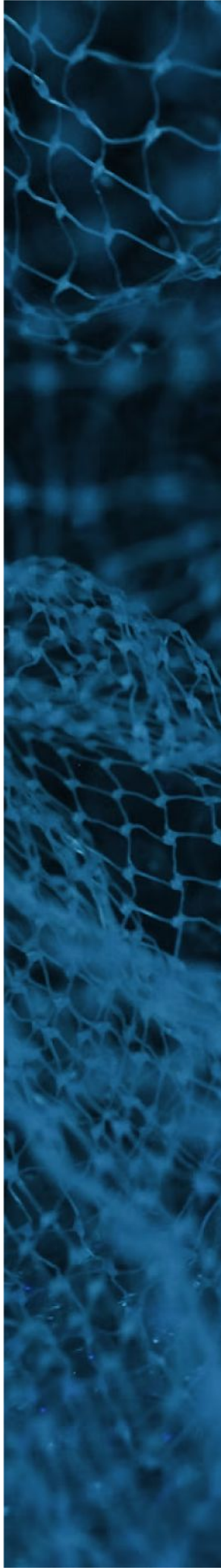
- **AWS Redundancy:** We utilize AWS to ensure redundancy across multiple geographically dispersed data centers, enhancing our ability to maintain operations under various scenarios.
- **Annual Plan Review and Testing:** Our comprehensive disaster recovery plans are meticulously reviewed and tested each year to ensure they are effective and up-to-date.
- **Offsite Backup:** Essential data is backed up in secure, remote locations to minimize risks associated with physical disruptions.
- **Proactive Communication and Response:** Our engineers and customer support teams are equipped with multiple communication channels to ensure swift notification and response during a crisis.

Reliability

Anduin's infrastructure is designed to ensure high availability and resilience:

- **High Availability Architecture:** Our systems are engineered to maintain operational performance with an uptime exceeding 99.9%. This is achieved through a robust infrastructure designed to handle both planned and unplanned disruptions.

Continued...



- **Multi-Layered Resilience:** We implement a multi-layered resilience strategy that addresses:
    - **Application Resilience:** Safeguards against user errors and software failures.
    - **Data Integrity:** Measures to prevent data corruption and ensure data recovery capabilities.
    - **Infrastructure Stability:** Precautions against environmental risks such as hardware malfunctions and network disruptions.
- **Availability Monitoring:** Real-time monitoring of our infrastructure's status is available to our users via our dedicated status site, providing transparency and up-to-date information on our operational status.

Monitoring, Alert, and Response

Anduin's security infrastructure integrates sophisticated monitoring and response mechanisms to manage and mitigate risks proactively:

- **Comprehensive Monitoring:** We utilize both native cloud services and select third-party solutions to achieve extensive visibility across all our systems and environments.
- **Advanced Threat Detection:** Our systems continuously correlate and analyze logs from various sources to detect, identify, and understand network and application-based threats promptly.
- **Automated Alert System:** Security alerts are configured to automatically notify our Infrastructure and Security teams via email and instant messaging, ensuring quick action and response to potential security incidents.

SECTION 6

Additional Resources

The scope of security we provide extends beyond the details presented in this whitepaper. For further resources, please refer to the links below:

- **Trust Report**
- **CCPA & CPRA Notice**
- **Cookie Policy**
- **Privacy Policy**
- **Terms of Service**

Other resources are available upon request.

For more information, email: security@anduintransact.com