WISE ATHENA

Your Data and Artificial Intelligence: Wise Athena Security, Privacy and Trust

Wise Athena Security Team

Contents

Abstract... 3
Security, privacy and trust.. 3
Artificial Intelligence in the cloud and Information Security Governance....................................4
Wise Athena cloud platform security and privacy...5
Conclusion.. 6
More detailed information... 6
Contact us... 7

Abstract

The need for security to be included in the design of technological systems is nowadays consensual among responsible software companies. The maturity of the IT industry, and in particular the Software as a Service (SaaS) market, reserved for security a role of growing importance. Digital security is now a vertical discipline with connections to almost every aspect of a well designed product and represents a sizable share of R&D investment.

This document summarizes principles and processes implemented by Wise Athena on the development and maintenance of its Artificial Intelligence as a Service platform (AiaaS).

Security, privacy and trust

Customers of the SaaS market often present legitimate concerns regarding security. Being SaaS something relatively new and given the continuous trend of worldwide Internet access over ever growing bandwidth it is reasonable to question whether SaaS providers allocate appropriate effort to platform security.

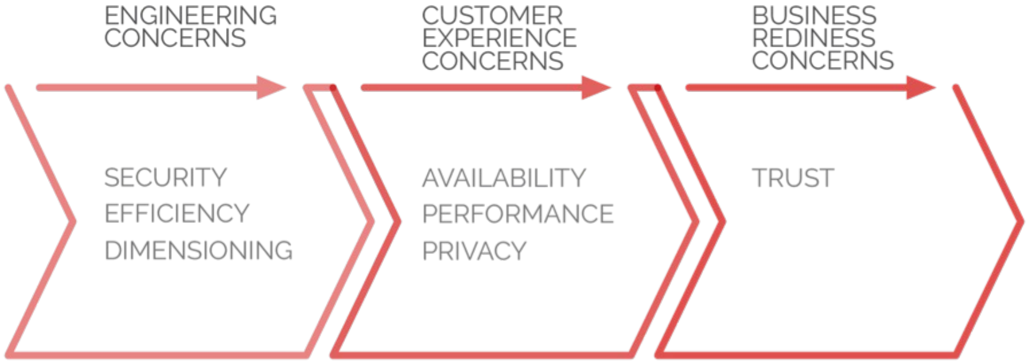
Special attention is usually paid by customers to data privacy, a critical concept for cloud operations. From a customer standpoint the assurance that business data is managed in a way that prevents unauthorized access is often the most important component in the definition of trust. And trust is, of course, the basis of every successful business relationship.

A reliable security process puts in place mechanisms that ensure resistance to data privacy threats, either internal or external to the company. Such process must be documented and clearly explained to customers so they can evaluate the provider's conformance to their own privacy standards.

But other less obvious components of security are also critical for long term customer trust: it is desirable that a SaaS platform is resistant to service disruption and service degradation threats that could otherwise affect users in different ways. For example, availability and performance issues could lead customers to sub-standard productivity levels and the provider's support team to overload situations. Preventing these kinds of threats protects customers and providers from troublesome road maps.

This means that a high security level is necessary at all fronts in order to deliver a platform of great availability, performance and data privacy. The relationship between security, privacy and trust, contextualized by other critical platform concerns is described on the diagram below. The end to end maintenance of security features and processes is usually called Security Governance.

How security impacts privacy and trust

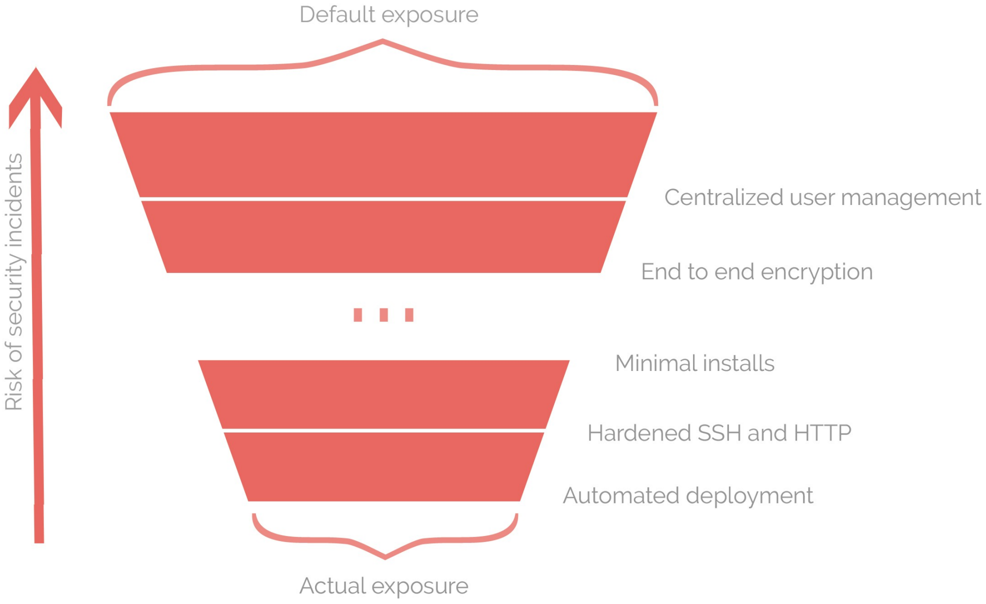


Artificial Intelligence in the cloud and Information Security Governance

The business of Artificial Intelligence as a Service (AIaaS) features many common properties of the SaaS model along with a small number of unique ones.

As with any SaaS scenario, the Security Governance of AIaaS is the art of managing all sides of security at all layers of the platform, such as the software layer (e.g., secure design, unit-tested functions, ...), the operating system layer (e.g., minimal viable package set, centralized authentication, scheduled installation of security updates, ...) or the human layer (e.g., employee role assignment and life role cycle). Security improvements at each layer contribute to minimize the platform's exposure to security threats.

How investing in security measures minimizes risk of incidents



The extent of areas to cover and the continuous nature of the corresponding effort have led to the well-known governance mantra, already hinted at the previous section: "security is a process".

What "security is a process means" is that, no matter how good the technical components of the system are at a specific moment in time, any fire-and-forget approach will statistically lead to security incidents: vulnerabilities can be found at OS components, employee roles can be abused, custom software can have bugs, etc. For each potential attack vector a mitigation process must be in place - this is how responsible suppliers should see security.
An AIaaS platform must deal with very large amounts of business data, such as sales records or customer activity logs, and moments very high processing loads intertwined with ones of mostly idle systems. This is caused by the periodic nature of customer data which needs to be processed at predefined time intervals.

One consequence of the above is the need for large amounts of encrypted temporary per-customer storage blocks. Another one is the need of built-in processing scalability that allows the platform to grow to hundreds of CPU cores in a matter of minutes, along with a secure method of communication between processing virtual machines and their controllers. The large amount of machines necessary imposes the use of fully automated system installation and configuration tools, which, on the other hand, prevent potential security problems that would arise from error-prone manual configurations.

Wise Athena cloud platform security and privacy

At Wise Athena we've built a platform based on the needs of AIaaS described above along with a careful selection of industry best practices including:

- minimal system installs
- fully automatic deployments
- enforced system configurations
- DROP by default firewalls
- end to end encrypted communication
- brute force login attack mitigation
- two factor authentication for user creation
- complex passwords
- centralized user life cycle management
- version controlled security configuration
- security event log
- data encryption
- ISO 27018 certified data center
- external auditing

Operations are aligned on a high level with the ISO 27018 standard in criteria such as:

- Organization of information security
- Access control
- Cryptographic controls
- Operations security
- Communications security

Specifically, we have paid close attention to the points described below.

Our team has well defined security responsibilities and clear segregation of duties (sysadmin, software developer, data scientist, business developer). Access to information such as source code, customer data, management interfaces and live applications depends on the person's role at the company. This is an important privacy safeguard that needs to be supported by appropriate technical means.

To make this possible our AIaaS Platform implements centralized user management and per application user and role assignment. For example, a user has access to none of the applications by default. After a user is created on the system it has to be explicitly assigned to specific applications - something which happens on a strict need-to basis. The act of assignment gets recorded on a central log for future review. On the topic of user management it is also important to point out that no storage of plain text passwords ever takes place - only salted hashes are stored.

Customer business information is encrypted and only accessible to our applications (automatic process), to data scientists (for the development of machine learning models) and to system administrators (only in very rare situations).

System administrators use secure administration tools such as SSH to work on remote systems. They are given scheduled time windows for security updates and ad-hoc moments for urgent security updates. The update policy is decided and maintained by the Chief Security Office (CSO) and performed by the system administration team.

Communications between Wise Athena's infrastructure and any user works solely via SSH and HTTPS (hardened configurations on both cases). This means that every exchange of information, including login data, is encrypted.

Conclusion

While no platform can claim 100% perfect security Wise Athena takes this matter very seriously allocating a considerable amount of time and resources to the implementation of security features and processes.

We believe that investing in security is much more cost efficient than dealing with the results of lack of security, besides being far superior in terms of engineering. Therefore, security is and will always be a major feature of Wise Athena's cloud products.

From our standpoint the privacy of customer data is as important as any business-continuity concern. We are confident that our investment in security translates strongly into to data privacy, service availability and sustained performance.

Our engineering team is available to jointly discuss any security matters that our customers find of special relevance to their businesses as well as to accept suggestions that might lead to future improvements in our systems.

More detailed information

More detailed security information, including technical documents and external audit reports, is available to our customers on request. Those documents provide an engineering level insight into the security and privacy of our systems. On the audit reports it is possible to check, among many other things, the strength of SSL configurations in use and the non-existence of known vulnerabilities on our Internet facing services.

Contact us

Wise Athena's security team can be reached at:

security@wiseathena.com

or via our website at:

http://wiseathena.com