Information & Application Security

White Paper

Table of Contents

Introduction

This White Paper provides an overview of the security measures of Semantic Web Company undertaken on an organizational and product level. It shall support decision makers during their vendor and software evaluation process.

The Semantic Web Company headquartered in Vienna (Austria) is providing semantic metadata management consulting services worldwide. A certified partner network is complementing our technology services. PoolParty Semantic Suite is the flagship product of the company and at the core of graph data management solutions. The globally acknowledged and repeatedly rewarded semantic middleware is installed in over 150 companies and organizations such as Boehringer Ingelheim, Pearson, Credit Suisse and the World Bank.

Implementing Semantic AI in enterprise information management systems is an innovative and complex encounter. As we work with large, distributed and heterogeneous data sources, security questions are of special concern. PoolParty Semantic Suite is enterprise-ready and currently in the process of getting ISO 27001 certified. We embrace a transparent approach towards our customers in regards to internal security processes, applied technologies and third-party vendor relations.

You will find further resources at the end of the White Paper. Alternatively, you can reach out to our information security team at: security@semantic-web.com.

Andreas Koller	**Johannes Trippl**	**Michael Scharitzer**
CIO	Head of System Operations	Information Security Management

Our approach to information security

The Semantic Web Company has been established in 2004 and is a distinguished expert organization in the fields of semantic AI technologies and standards-based semantic metadata management solutions. Amongst our customers are government organizations and global organizations across multiple industries as financial services, e-commerce, pharmaceutical industry and media & publishing. These companies have complex data models at the core of their business and operate with sensitive data repositories ranging from customer, product and provenance data to intellectual property.

PoolParty Semantic Suite is implemented as a semantic middleware to enrich heterogeneous data sources with metadata and make it actionable across multiple platforms taking context dependency into account. Our technology solutions are deeply integrated in enterprise information architectures. With the growing demands in improved search, recommendation and dynamic content publishing services, the semantic capabilities of smart data platforms get increasingly more important over time.

Applying Semantic AI is an exciting journey. It might start out as an innovation project, but usually with a high awareness of its strategic importance for the whole enterprise. PoolParty customers use the semantic software in various ways and many different IT-systems can gradually merge into a cognitive computing platform. PoolParty is a technology suite based on W3C standards, which is thoroughly designed to stay integrable and state-of-the-art in the long term.

This has severe implications for our information security approach. We conform to security standards that fit with the compliance expectations of Fortune 500 companies. At the same time, we are aware that IT regulations shouldn't be too restrictive in a rapidly changing environment. Balancing security requirements with enough alternative choices for our customers is a core principle for our information security management committee.

Cybercrime is an actual threat that can't be solely prevented on a technical level. Building and sustaining security awareness and limit operational risk across the whole organization is key. The top management of the Semantic Web Company is actively driving information security measurements to protect critical assets and considers security questions at every relevant touchpoint.

Corporate Security

The Semantic Web Company is a globally acting organization in a highly networked business and knowledge ecosystem. An information security expert team sponsored by the top management ensures that all stakeholders comply with the code of conduct and consider potential risks in their daily work carefully. As the vendor of a semantic data management platform for data intensive industries, fulfilling high security standards is a critical prerequisite.

Background checks

Depending on the professional role of our employees, background checks on different intensity levels are performed. 80% of our employees are recruited internationally and have to go through severe national security screening of the Austrian government. Many of our consultants participate in international government projects, where security clearance is mandatory as well.

A partner certification program ensures that strategic partners for PoolParty Semantic Suite share the same quality standards along the whole value chain.

Security Awareness Program

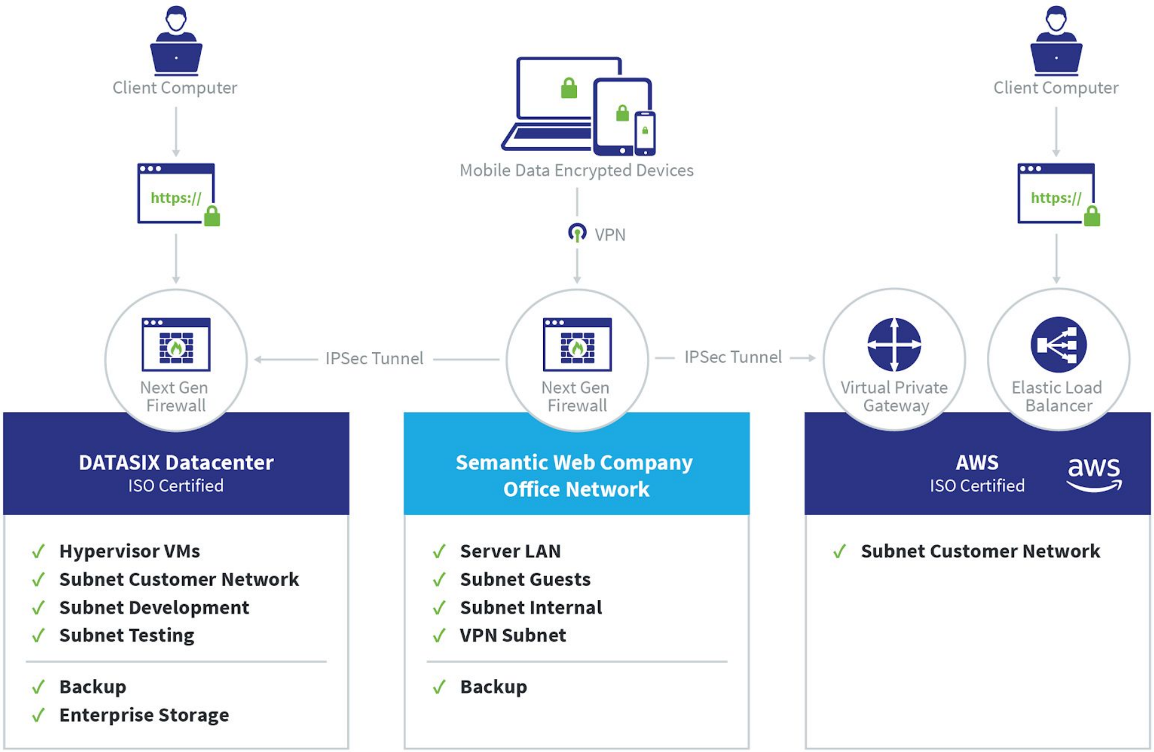
Security rules, regulations and guidelines affect all organizational processes and departments. A strong security culture depends on every employee and needs to be continuously screened and adapted. Every new employee gets a dedicated security onboarding. Regular updates of the corporate security framework are shared by the information management security committee. Besides, every department has a security commissary who ensures that teams act accordingly to regulatory compliance.

Data privacy

With GDPR (= General Data Protection Regulation) becoming effective in the European Union in May 2018, there is an extensive mandatory rule set for data privacy to follow. European companies have to document transparently which personal data is collected and how this data is processed. A business process inventory provides the underlying foundation to keep track of potential data breaches, which also strengthens the internal security awareness as a side effect. Having an overview of data flows is an important strategic asset for keeping the information security management program up-to-date. Non-EU companies benefit from legally binding data privacy regulations.

Network security

The rise of cloud tools, mobile devices and virtual working requires preventative measures to ensure improved data security. Only authorized users have access to the Semantic Web Company network. Remote access is strictly controlled with encryption and a strong password policy. Network traffic from and to the data center and AWS are secured via IPSec tunnels. At the data center the network is segmented. Customers and various company departments such as Infrastructure, Development and Testing have their own subnet. A next generation firewall prevents a broad range of security threats and a monitoring system immediately notifies about malicious activity. By performing regular audits potential security vulnerabilities are examined and considered in the strategic security roadmap. A multi-layered security approach is established for utmost protection of the organization’s IT assets, while still granting enough flexibility to ensure an agile business environment.



Semantic Web Company Network Security Architecture

System level security

All virtual machines use an operating system, which is hardened to reduce the surface of vulnerability. Every software package which is not needed by the server or the infrastructure gets removed. In order to secure all systems, every user gets only a specified set of commands with elevated rights. The system operations team reviews every request for access to a server as well as needed software packages. Malware detection and file integrity checks are deployed on all servers.

System Recovery Mechanisms

All company data is backed up daily to a separate data storage server in a data center at a different geolocation. Separate local copies of data are backed up to a mobile storage in a secure and locked location. All backups are highly encrypted and protected from unwanted access. To keep recovery times short, snapshots are made for every virtual machine which are kept for seven days backwards. Additional snapshots of data are made in the datacenter on an enterprise storage device. All data is kept for 50 days at the offsite backup location.

Physical Protection

Our major company servers are running in ISO 9001:2008 and ISO 27001:2005 certified data center. The data centers are under permanent video surveillance. All rooms are monitored around the clock seven days a week by a security firm. Checkpoints are used to log and record the regular scrutiny. Entrance is only possible by passing an RFID and a biometric access system. The data center has a fire alarm system with inert gas. The Very Early Smoke Detection is very sensitive and is already beating, when there are only a few smoke particles in the air.

Risk Assessment and Audit Arrangements

The Information Security Management System (ISMS) of the Semantic Web Company is based upon the ISO/IEC 27001 standard. A risk assessment and risk treatment methodology has been established to address unwanted events in the most efficient way.

Product Security

PoolParty Semantic Suite is a semantic data integration platform to be integrated with third-party enterprise information systems. The data processing capabilities and embeddedness in core business functionalities require high security measures along the whole software development lifecycle. PoolParty provides two major releases every year. Our software engineering and systems delivery team is following the OWASP (= Open Web Application Security Project) principles.

Cloud or on-premise installation

PoolParty Semantic Suite can be licensed as an on-premise installation or as cloud service. Depending on the IT strategy of our customers various deployment scenarios are feasible. In regards to security, it depends on the customer's preferences which alternative is most suitable. For all deployment options, support packages are available.

Customers usually decide for an on-premise installation, when PoolParty is heavily integrated with third-party systems and a mature IT environment is in place.

Many companies run their software services in the AWS (= Amazon Web Services) cloud and can easily add PoolParty to it. In this case, the customer will be responsible for hosting and updating PoolParty.

Alternatively, Semantic Web Company can host and update PoolParty in the AWS cloud or the DATASIX datacenter. Customers will always have the newest software version available. Shared security responsibilities with the cloud provider will be covered by Semantic Web Company, which significantly reduces the operational burden. The two datacenters provide equally high global infrastructure security, but provide different pricing models.

Secure Software Development Process

Our software development process lifecycle covers security issues stemming from customer security audits as well as regularly performed internal audits that are aligned with the OWASP Top 10 risks.

To increase security awareness and strengthen secure coding skills of the whole development team, regular trainings are organized. Peer-reviews of new features ensure high quality of code and mitigate the risks of security related issues during the design and development phase. Furthermore, legacy code and outdated functionality is regularly scheduled for redesign and refactoring.

Third-party components are reviewed exhaustively before used in the core product and are regularly scanned for common vulnerabilities. All security critical functionalities such as authentication, authorization and encryption are implemented based on well-established frameworks.

Highly customizable security functionalities

PoolParty provides default configurations for all security critical functionalities, which can be easily configured and extended for the customers' security policies. This includes the enforcement of secure user passwords, configurable session timeouts, and authentication methods.

New security configuration options are regularly included in the release cycles to meet the requirements of different security policies.

Authentication

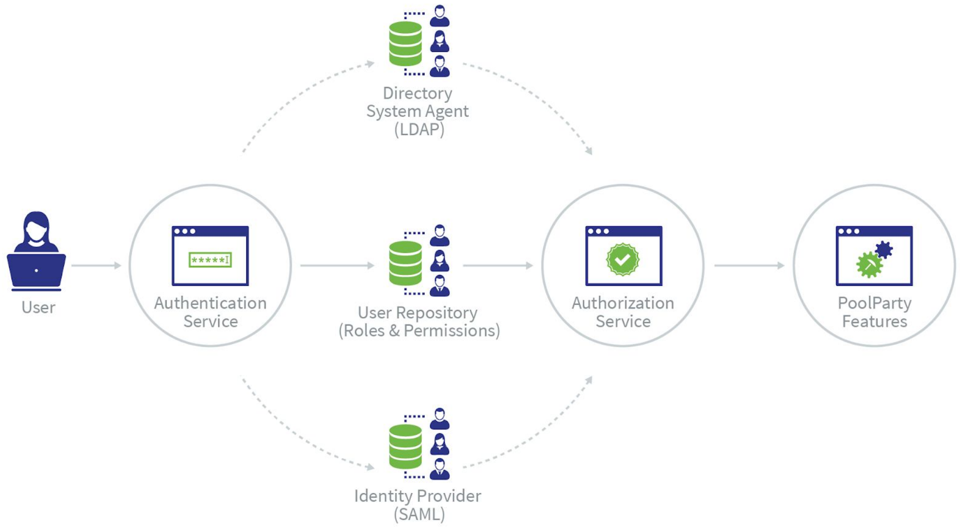
PoolParty provides various ways to authenticate users.

The default authentication method is password based verification. Administrators can configure a strong password policy by enforcing a minimum required password length and upper/lower case as well as digits and punctuation characters.

Some customers might prefer to use their existing authentication infrastructure, PoolParty's authentication can be enforced alternatively via:

- Lightweight Directory Access Protocol (LDAP)
- Single-Sign-On (SSO) using Security Assertion Markup Language (SAML 2.0)

Server administrators can also restrict access from predefined IP addresses or domain names.



PoolParty Authentication and Authorization

Authorization

Authorization determines the access rights to see, create and change data. The user management module of PoolParty Semantic Suite differentiates various roles. With release 7.0, the role-based system has been changed to permission-based access controls to allow more flexible and fine grained access rights.

You can for example:

- Differentiate access rights via the user roles: Superadmin, admin, user, API user, read-only user
- Set up appropriate access rights for different PoolParty projects by creating user groups
- Make projects publicly available by publishing them via the Linked Data frontend

Session management and secured API endpoints

Every successfully logged-in user is assigned a session that allows to identify the user and apply access control restrictions on subsequent requests. Server administrators can easily change the session timeout timespan to mitigate the risks of users leaving their workplaces while still logged in.

Every request to the provided Application Programming Interfaces (API) is secured by basic authentication. Secure endpoints must only be provided by HTTPS, which protects user credentials and guarantees integrity of sent data.

Monitoring and data recovery

System administrators set up different log configurations for the components of the product, which allows to monitor different events such as failed login attempts or current logged in users.

The project history allows to track changes to project data, providing the means for manual inspection or custom implemented analysis. PoolParty 7.0 allows to configure the maximal number of failed login attempts that are stored for each user. The notification management system allows to configure alerts for different user actions that can be communicated over different channels.

In case of data corruption, automatically created snapshots enable the recovery of the project data.

Further reading

Different stakeholders in your organization have various information needs when it comes to IT security. In this White Paper we provided you with a general overview of the security and risk management measures of the Semantic Web Company at a corporate and product level.

- You will find more product-related security information at: https://help.poolparty.biz
- For customer references, please visit: https://www.poolparty.biz/customers/
- Explore our partner network at: https://www.poolparty.biz/partners/
- Our information security team is happy to answer your questions: security@semantic-web.com