Security FAQs

Last Modified on 05/21/2024 8:38 am EDT

The Exalate Approach to Security

At Exalate we base our security approach on three dimensions:

- **Security by Design**
  Security vulnerability scanning has been implemented at every stage of the development, deployment, and operation of the solution. This scanning is based on the solutions provided by Snyk, which allow highlighting the security problems from the moment a developer types a line of code.

- **Advanced Endpoint detection and response (EDR) monitored by a 24/7 SOC**
  EDR is implemented through a combination of the Palo Alto Cortex XDR solution, a 24/7 manned SOC for addressing incidents and vulnerabilities, and the Security Command Center to guard the Exalate cloud environment.

- **Process and policies focused on increasing the security awareness of the whole team**
  All policies related to the ISO27001 standard have been implemented and are controlled by various processes. Roles and responsibilities are defined and assigned to various people in the team.
  These policies include:
  - Acceptable use
  - Privacy and Employee privacy
  - Security awareness training for all the employees
  - HR recruitment
  - The Incident, Vulnerability, and Change management
  - Risk management

While we can address the specific security concerns customers might have based on their use cases, the following is a list of the most commonly asked questions.

Is Exalate ISO certified?

Exalate is ISO27001:2022 certified. This means that all the conditions for achieving this certification have been implemented. Evidence of the auditing process and the certificate can be provided upon request.

Is Exalate SOC2 compliant?

As part of our ongoing improvements to our security program, we will soon proceed with the SOC2

certification.

Is Exalate GDPR Compliant?

Exalate has its HQ in Europe (Belgium) and therefore complies with all GDPR-related legislation.

Is Exalate a data processor?

Exalate is NOT a data processor as defined in GDPR Art 4. Exalate can be compared to an email system, which processes synchronization transactions as fast as possible. Exalate has not been designed for processing PII data (ie., there are no tables with user-related information). Exalate can fully operate, even if there is no PII data in the messages.

Can Exalate be integrated with an SSO Solution?

Exalate performs authentication through the underlying platform (e.g. Jira). Whenever there is a need to log into the application, Exalate will check with the platform if the authenticated user is authorized to perform configuration tasks or not. The authentication protocol is either 'Basic Authentication' or 'Oauth' based. Since Exalate doesn’t have a user directory concept, there is no need for an SSO Solution integration.

What is the benefit of Exalate's single-tenant architecture compared to a multi-tenant one?

A single-tenant application, in the context of integration software, is an application that is related to only one system. A multi-tenant application on the other hand allows using one infrastructure to connect with multiple systems. So, whenever considering an integration solution, one should pay attention to the tenancy of the proposition.

All software has bugs, either because of improper development, configuration mistakes, or any other reason. The recent breaches at LastPass and Octa show that protecting information is a Herculean task. Integration software is more complex as it needs to take care of many diverse aspects and information paths.

To minimize the risk of information leakage, a single-tenant architecture is a much better option as it allows us to contain information leaks at the infrastructure level.

When an Exalate node is deployed on the Exalate Cloud, it is running inside a 'Kubernetes pod' that is configured to ensure no information can leak. The maintenance of this Exalate Cloud is fully based on the principles of 'Infrastructure as Code'. There is no manual configuration for the environment.

How is Exalate Cloud protected?

All clusters are protected by state-of-the-art Endpoint Detection and Response (EDR) systems, specifically the 'Cortex MDR', from Palo Alto. This infrastructure is monitored round-the-clock by a Security Operations Center (SOC) staffed by Cyber Security engineers. The monitoring service, provided by NVISO, has been validated by a MITRE ATT&CK test.

How does Exalate encrypt my data?

Any customer data in the Exalate cloud is encrypted in transit and at rest. Offline backups are encrypted for each tenant. Furthermore, Exalate Cloud ensures that every node is totally separated from any other node, including computing resources, file storage, database storage, and network path.

What encryption method does Exalate use?

Exalate uses the Transport Layer Security (*TLS*) Protocol Version *1.3. If the issue tracker does not support this version, we use TLS 1.2.*

What information is exchanged between instances?

Once the Connection setup is finished, Exalate generates the shared secret. The secret is used to define a secure connection between both Instances. It is shared only once to generate a JWT token. The token is temporary and is generated for every communication request between Exalate in both Instances.

The following information is exchanged between Instances:

- shared secret
- information about the type of connection with the Destination instance
- Connection name
- information about the Connection initiator
    - Exalate app version, including supported features
    - Instance type and version (JIRA Server, JIRA Cloud or HP ALM/QC)
    - Instance URL and Exalate URL
    - Instance UID, which is a unique instance identifier

Where is my data hosted?

Depending on the deployment model, there are several models of data hosting. In case the node is deployed on-premise, data will be hosted on-premise. There is no need for an Exalate node to be connected to the Internet to fully operate.

When the node is deployed on the Exalate Cloud, all data resides on the Google Cloud datacenter in Europe-West1 (Belgium) or on Exalate Cloud that is hosted in Tier 4 datacenters, located in Belgium. Backups of that environment are stored offline in the data center of Rsync.net in Zurich (Switzerland).

Does Exalate store any of my data?

Exalate stores the metadata required for the integration functionality, such as the relation between an incident and an issue. This metadata consists of unique identifiers, such as numbers or strings, without any meaningful content.

Furthermore, it stores the payload of the synchronizations in flight. It does this through an

advanced transaction-based synchronization engine where every stage of the transaction requires queueing this payload. Once the transaction is fully processed, no payload information is stored in the database.

What information is stored locally?

The following data is stored locally: Instance URL, Instance version, Exalate URL, a unique instance identifier.

Does anyone have access to my data?

Access to the application is defined by the underlying system and is fully configured by the administrator of that platform. When deployed on Exalate Cloud, our support engineers and cloud operators can have access to the data, but only after explicit approval by the customer. All our staff goes through background checks, and only a well-identified list of employees with appropriate clearances can access your information.

Do you use any production data for testing?

We do not use production data for testing unless explicitly approved by the customer in case of a root cause analysis (RCA) of a defect.

For how long do you store audit logs?

Audit logs are kept for 30 days.

Is there a solution in place for endpoint detection and response, in addition to protection against malware and viruses?

The entire Exalate infrastructure is protected by the Palo Alto Cortex XDR solution, which provides, next to malware and virus protection, an extensive set of cyber security capabilities, including vulnerability and incident management.

How do you deal with vulnerabilities?

Vulnerabilities are handled according to the ISO27001 standard. Customers are notified of critical vulnerabilities.

How do I report a security vulnerability to the Exalate team?

If you notice a vulnerability in one of our products, please notify us immediately so we can address the issue as quickly as possible. Any vulnerability, concern, or incident can be reported either on the support portal or by email to security@exalate.com.

Do you notify customers in case security vulnerabilities have been detected?

Yes, in case of critical security vulnerabilities, all Exalate users, including evaluators, are notified within 48 hours after we detect the vulnerability.

Does Exalate have Business Continuity and Data Recovery Processes?

Business continuity processes are defined in the context of policies and procedures.

Do I need to list Exalate as a sub-processor?

No. Exalate does not store any PII data directly.

Product

About Us

Release History

Glossary

API Reference

Security

Pricing and Licensing

Resources

Subscribe for a weekly Exalate hack

Academy

Blog

YouTube Channel

Ebooks

Still need help?

Join our Community

Visit our Service Desk

Find a Partner