assistedge | Discover

edgeverve
An Infosys company

AssistEdge Discover

Security Overview

TABLE OF CONTENTS

AssistEdge Discover – Security Overview

AssistEdge Discover is a critical tool in the enterprise automation toolkit that helps business leaders gain deep visibility into their processes and make optimal decisions around process reengineering and automation.

AssistEdge Discover unlocks the hidden business value trapped in your processes. It acts as a powerful foundation for enterprises seeking cutting-edge technology, to drive intelligent automation and process excellence. From non-intrusively capturing human-machine interactions to leveraging AI to creating actionable process insights, AssistEdge Discover sets you on the right path to embrace continuous improvement with relentless focus on creating a hyper productive enterprise.

Key security principles

AssistEdge Discover is used by large G2K enterprises to discover processes for automation. Given the nature of data handled by Discover, information security and user privacy have been given prime importance while designing and developing this product. This has manifested into the following core principles across data collection, storage and processing:

- Encryption as default (both in rest and in motion)
- Data minimization (both during initial capture and in retention)
- Access limitation (data access is limited strictly on need basis)
- Defence in depth across layers of security

Topic covered in this document

AssistEdge Discover analyses enterprise systems and manages their critical data to provide process insights. Through this document, we provide an overview of how we have kept very high security benchmarks for this product

- Security Philosophy
- Multi layered Security Assessment
- User and Access Controls
- Cryptography
- Data Privacy
- Auditability
- Separation of concerns

Annexure on AssistEdge Discover on cloud

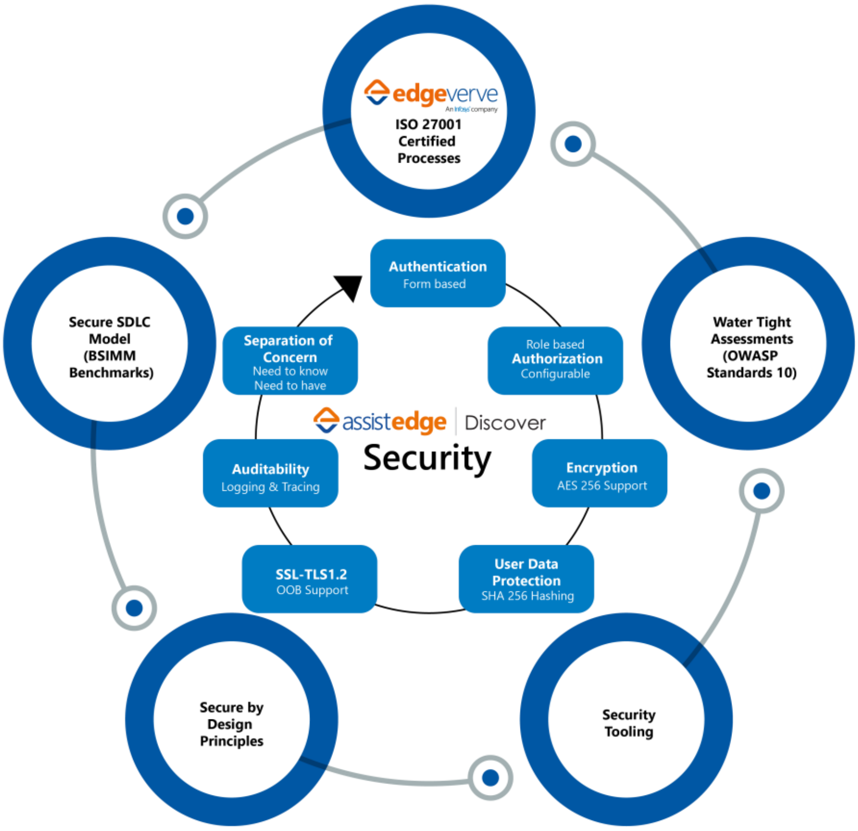
Security Philosophy

Security is not a gate at the end of the product release. The Defence in Depth approach to security ensures implementation of the right controls at each stage of product design and development. Security considerations begin with release planning. The process is extremely well-defined with all product engineering teams required to follow the Secure Development Lifecycle.

The process is well researched and established to make it consistently repeatable and measurable. It is well supported by investments in industry leading tools and the holistic approach from threat modelling to vulnerability assessments make the product secure and trustworthy.

In addition, the developer security awareness campaigns and training in different programming languages ensures defence in depth. A well-qualified and adequately certified Security Team that works independent of product engineering teams brings in the assurance of a dispassionate emphasis to the security activities and ensures consistency.

Holistic approach to Product Security



Security is a shared responsibility across the product engineering teams and the security organization with a leadership focus. The Security organization has dedicated teams for enterprise security and product security.

Multi-layered Security Assessments

In line with the Defence in Depth philosophy, various appropriate reviews and assessments are conducted on AssistEdge Discover. Investments in industry leading tools support the holistic approach towards security and continuously elevate product security benchmarks

Here is a view on the security vulnerability assessments done as part of product security checks

- Secure Architecture Analysis
- Static Analysis
- Dynamic Analysis
- Manual Security Assessment
- Open Source Security Analysis
- Vulnerability Assessment & Penetration Testing
- Data Privacy Assessment

Following tools and repositories are used to support these assessments

A gamut of industry leading tools assists in carrying out pre-release assessments for each product. Apart from commercial and open source tools in the areas of static and dynamic application security testing (SAST & DAST), toolsets for penetration testing, software composition analysis, open source vulnerability checks, container image scanners, interactive application security testing software are also employed. Some of the tools used as part of security testing are Coverity, Checkmarx, Seeker, Blackduck Hub, Prisma Cloud Compute and Burp suite to name a few. In addition, there are Secure Coding Guidelines for various programming languages and curated repositories for popular images.

Access Controls

AssistEdge Discover enforces strict access control on the all the users that interact with the product. The access is strictly role based and each role is provided access only to the extent of requirement. Discover has four key roles and one additional responsibility

Roles:

1. Product Admin – Product admin administrates the product and has access to all the product modules except privacy management
2. Business Analyst – Business analyst is the process specialist and has access to product modules except privacy management for areas under his responsibility.
3. Business Leader – Business leader is the head or owner of the department and has access to analysis and insights modules only for areas under his responsibility.
4. Process Executive – Process executive is the one who executes the process and has access only to his/her data in analysis module

Responsibility:

1. Security Admin: Specific users can be chosen and assigned an additional responsibility to handle security aspects and ensure the configurations are in-line with the organizational security and privacy policy. Any privacy configurations in the product can only be changed by Security Admin.

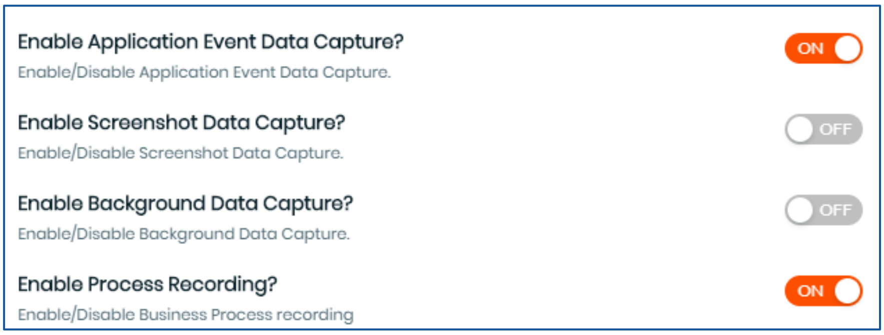
AssistEdge Discover also follows a strong form-based authentication approach. It supports integration to active directory or industry standard identity management solutions.

Data Privacy

AssistEdge Discover has undertaken significant strides in ensuring total compliance to GDPR regulation. As a processor of data, we have ensured maximum privacy measures and an overall holistic security approach to handling customer data.

The product has implemented a 7-step methodology envisaging a secure environment for our users to realize maximum potential out of our offering:

- **Data Minimization**
  AssistEdge Discover, as a data processor, captures only relevant fields or elements which are required as a minimum to realize the value of process discovery. Product captures the granular keystrokes and click data which is enabled by default. The additional data fields (like screen coordinates, screenshots etc.) or data elements (like USB, Network) are disabled by default. These can be altered as per data controller's organizational requirement. Discover also allows the capability to allowlist/blocklist specific application or data touchpoints



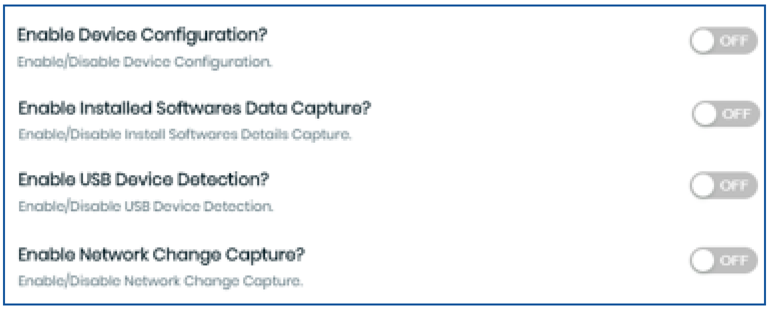
Enable Application Event Data Capture? ON
Enable/Disable Application Event Data Capture.

Enable Screenshot Data Capture? OFF
Enable/Disable Screenshot Data Capture.

Enable Background Data Capture? OFF
Enable/Disable Background Data Capture.

Enable Process Recording? ON
Enable/Disable Business Process recording

- **Purpose Limitation**
  AssistEdge Discover clearly defines the purpose of data elements it captures through various touchpoints in the product like Configuration Screens, Help page and User guides. These data elements will be used for the defined purpose only and is configurable by user with appropriate privileges.



Enable Device Configuration? OFF
Enable/Disable Device Configuration.

Enable Installed Softwares Data Capture? OFF
Enable/Disable Install Softwares Details Capture.

Enable USB Device Detection? OFF
Enable/Disable USB Device Detection.

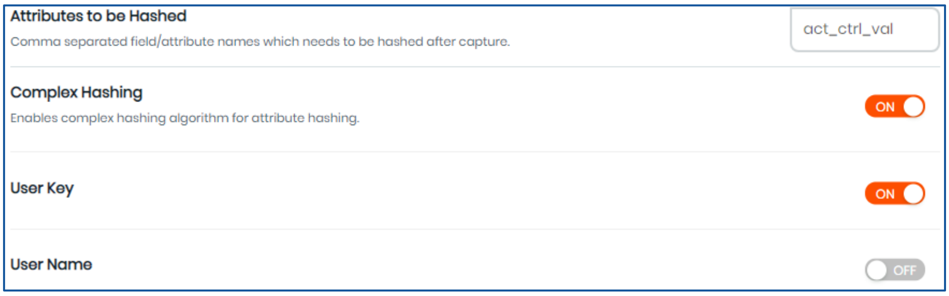
Enable Network Change Capture? OFF
Enable/Disable Network Change Capture.

- **Data Security**
  AssistEdge Discover has implemented a holistic approach to Security principles. It ensures data security using below approach:

  - Role based authorization
    AssistEdge Discover follows the authorization concept which allows roles-based access to product features. It has a security admin role option that enables access for authorized users to privacy configurations like allowlist/blocklist data hashing or masking

- Data Hashing
  AssistEdge Discover hashes the data directly during data capture using SHA256 algorithms and stores them. This pseudonymizes the data and it is not readable for humans, in case users with product roles or database administrator attempts to view the same.
- Data Masking
  Security admin can further add additional layer of security by masking sensitive PII data
- Data Encryption
  AssistEdge Discover implements data encryption at rest and in transit using HTTPS with TLS 1.2. In case of cloud offering, the encryption capabilities provided by database services such as RDS are used.

Note: In cases where user inputs are necessary for deducing process flow information such as command strings in case of mainframe applications or menu commands in SAP etc., the inputs are identified by using a configuration file where human readable commands are listed which are forward hashed to be compared with the collected data. This ensures, at no point in time, the user input data is converted into a human readable form.



Attributes to be Hashed
Comma separated field/attribute names which needs to be hashed after capture.
act_ctrl_val

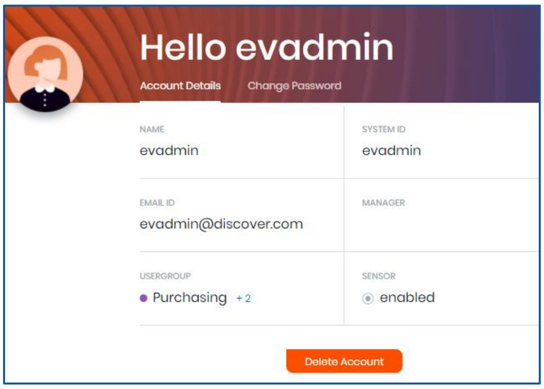
Complex Hashing
Enables complex hashing algorithm for attribute hashing.
ON

User Key
ON

User Name
OFF

- **Data Transparency**
  As a processor of the data, AssistEdge Discover ensures complete transparency on our modus operandi and safety of PII data. It has complete visibility to Terms of Use and Privacy Statement at multiple touchpoints of the product vis-à-vis the Discover Insights hub and Discover Sensor. User can view the Terms and Privacy Statement at any point of the user-journey and from any module of the product.

- **Data Retention**
  AssistEdge Discover Enterprise Version ensures that client information, of any type, is not retained in the product infrastructure. For Discover Trial, which is hosted on cloud, Discover as controller of the data keeps a maximum retention period of 60 days as communicated in Terms of Use document. In case a Trial user wants to delete their PII data before the stipulated time of 60 days, product has an option of deleting the account which will erase all access and account information of the user immediately.



Hello evadmin

NAME
evadmin

SYSTEM ID
evadmin

EMAIL ID
evadmin@discover.com

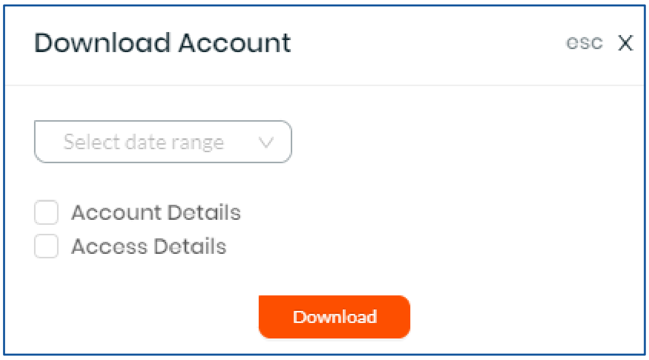
MANAGER

USERGROUP
● Purchasing +2

SENSOR
◉ enabled

- **Data Transfer**
  AssistEdge Discover clearly governs the data transfer guidelines in its privacy statement.

- **Data Subject Rights**
  Trial users can download the personal data in a machine-readable format. Users can manually choose the timeframe for which data needs to be downloaded while choosing the data elements that they wish to download.



AssistEdge Discover has gone through a mandatory review for GDPR compliance by EdgeVerve Data Privacy Office underlining the emphasis that it places on Data Privacy and Security concerns.

Cryptography

For the purposes of secure information transfer and storage, AssistEdge Discover users some of the most secure cryptographic algorithms.

Some of the algorithms used are:

TLS with strong ciphers
AES_256 for encryption
SHA 256 for hashing

These algorithms are used for purposes such as password encryptions, data hashing and secure communications. User passwords are one way hashed using SHA256 with secure random salt. Other passwords like Database, SMTP are encrypted using AES256. Microsoft DPAPI support to encrypt client-side data

Auditability

In order to maintain traceability of user actions, including administrative actions, AssistEdge Discover supports appropriate logging. Log files typically contain information about the actions carried out by a given user, time stamp information etc. The product also captures information about agent process enable, disable and the names of applications monitored.

The log files are stored in secure location with access control to eliminate any possibility of tampering.

Separation of Concern

The product has ingrained application user-level access control features both on premise and enforced in the cloud deployment model as well. The access to the application and data stores are provided to administrators based on need-to-know and need-to-have.

AssistEdge Discover on Cloud

AssistEdge Discover is also available as a Software-as-a-Service (SaaS) solution delivered through EdgeVerve’s secure cloud offering called EVonCloud.

It is a highly scalable and secure service-delivery platform based on AWS and Azure public cloud infrastructure. The cloud infrastructure is spread across multiple availability zones to ensure uptime and resilience. Specific contracts and SLA agreements with both AWS and Microsoft help deliver consistent and reliable service to the consumers of AssistEdge Discover as a service. Certified by ISO 27001 for security processes and controls and ISO 22301 certified for business continuity provides confidence to clients that consume services from EVonCloud.

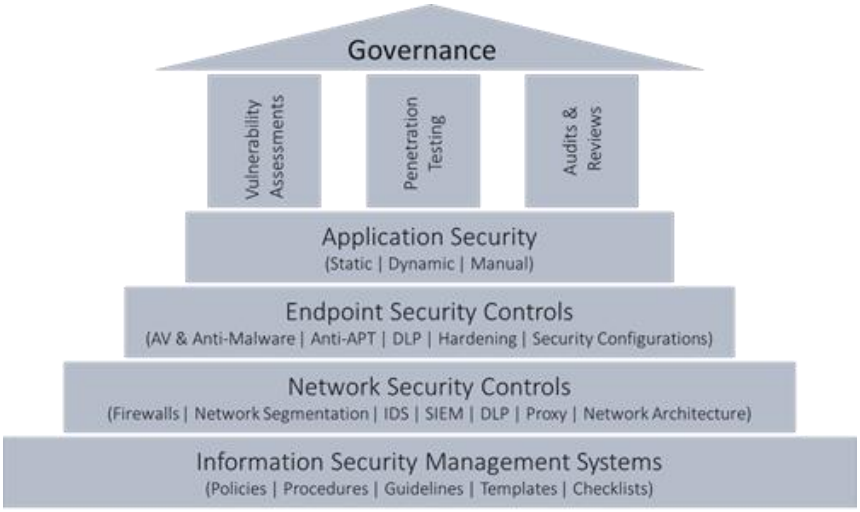
Network and Perimeter Security

EVonCloud is secured tightly with industry leading firewall and stringent security policies. The cloud is safeguarded from threats with APT protection, Intrusion detection system, Antivirus, Anti malware and DLP software have been deployed to prevent critical data loss. All the appliances and servers hosting the security defence systems are deployed in high availability mode to ensure that at no point in time the defence is debilitated.

A dedicated Security operations centre monitors our cloud infrastructure 24x7 and follows a well-defined security incident, event and response management process.

Infrastructure Security

The cloud infrastructure security is a critical aspect in ensuring the systems, the applications as well as the data in the system is protected. System Vulnerability assessment and system compliance audits are performed on all the virtual machines on a quarterly frequency.


Governance
Vulnerability Assessments
Penetration Testing
Audits & Reviews
Application Security
(Static | Dynamic | Manual)
Endpoint Security Controls
(AV & Anti-Malware | Anti-APT | DLP | Hardening | Security Configurations)
Network Security Controls
(Firewalls | Network Segmentation | IDS | SIEM | DLP | Proxy | Network Architecture)
Information Security Management Systems
(Policies | Procedures | Guidelines | Templates | Checklists)

Each virtual machine in the cloud has hardened images of Operating systems. The access to the systems is strictly controlled through an active directory setup.

EVonCloud provides an integrated active directory-based identity and access management capability. Access is provided to any subscriber of the cloud service and administrators strictly on a need to know, need to have basis. All the access is logged and audited. User lifecycle management is in place to ensure granting and revoking of access in case of employee rotation.

A strong foundation of policies and standard operating procedures combined with overarching governance mechanism ensures smooth, secure and continuous operation of the cloud offerings hosted on EVonCloud.

Conclusion

AssistEdge Discover has been engineered with stringent security controls through the development process, and compliant with data privacy regulations including GDPR and other data privacy requirements.

More information

To learn more about AssistEdge Discover: https://www.edgeverve.com/assistedge/assistedge-discover/

For Demo / Enquiry: https://www.edgeverve.com/contact/?source=assistedge

To learn more about AssistEdge products: https://www.edgeverve.com/assistedge/

assistedge | Discover

AssistEdge Discover unlocks the hidden business value trapped in your processes. It acts as a powerful foundation for enterprises seeking cutting-edge technology, to drive intelligent automation and process excellence. From non-intrusively capturing human-machine interactions to leveraging AI to creating actionable process insights, AssistEdge Discover sets you on the right path to embrace continuous improvement with relentless focus on creating a hyper productive enterprise. https://www.edgeverve.com/assistedge/assistedge-discover/

edgeverve

An Infosys company

EdgeVerve Systems Limited, a wholly owned subsidiary of Infosys, is a global leader in AI and Automation, assisting clients thrive in their digital transformation journey. Our mission is to create a world where our technology augments human intelligence and creates possibilities for enterprises to thrive. Our comprehensive product portfolio across AI (Infosys Nia), Automation (AssistEdge) and AI enabled Business Applications (TradeEdge, FinXEdge, ProcureEdge) helps businesses develop deeper connections with stakeholders, power continuous innovation and accelerate growth in the digital world. Today EdgeVerve's products are used by global corporations across financial services, insurance, retail, consumer & packaged goods, life sciences, manufacturing telecom and utilities. Visit us to know how enterprises across the world are thriving with the help of our technology. https://www.edgeverve.com/

contact@edgeverve.com www.edgeverve.com