expertware CIDRE

Continuous IT Assets Discovery and Risk Evaluation

Automate, Integrate, Corelate, Graph Inference, Advanced Analytics, Trigger Updates. Device lifecycle audit

expertware.net

The needs

Automatic IT asset discover and management

ITSM processes rely on fresh, accurate information regarding the IT assets (laptops, workstations, servers, mobile devices), their ownership and activities, their last seen locations, security posture.

Traditionally organization maintain manual uploads of devices lists collected via various other solutions or had a 1-to-1 integration with a management/monitoring toolset like Azure/VMware/SCCM/Intune/ManageEngine/Nexthink/etc.

Alternatively, they acquired an IT Asset Management solutions outside the ITSM and build a system-to-system integration to feed device data to ITSM CMDB.

All these manual/semi-automated steps are time consuming and error prone.

Drawbacks

Information regarding devices, ownership, status was not accurate missing assets or having stale data.

Obsolete information leads to increased efforts from support teams.

Asset attributes were gathered from a single source. If the source system or integration had an issue ITSM was not being updated, processes run based on old or incomplete data.

No possibility to create intelligent automation rules based on device status, location, history was not possible.

Conflict resolution, assets reconciliation was time consuming, being done manually by a CMDB team.

Solution

Automatic IT asset discover and management

Develop an intelligent, automated multi system integration capable of detecting duplicates, of extending (multi joins) IT assets data originated from different systems (IT management, monitoring and the ITSM itself).

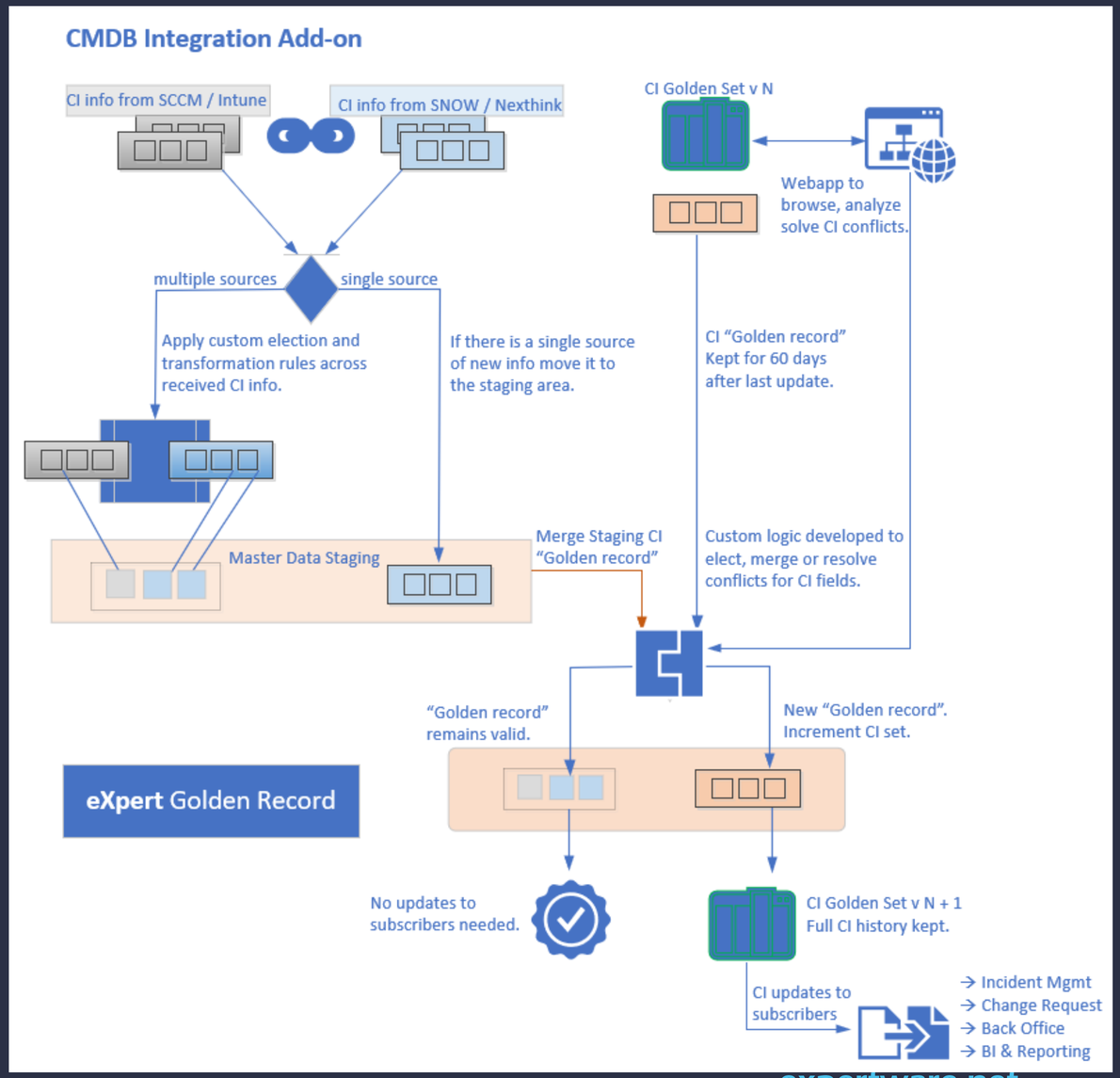
IT asset data is collected via Webservices from multiple sources (Microsoft Azure, VMware vCloud, Active Directory, Intune, System Center, monitoring tools, software licensing tools) and imported to a master data staging area. Solution ensures delta imports only to optimize the loads and costs.

In the staging area election and enrichment rules are applied ensuring that the best CMDB golden set is generated.

CMDB golden sets are pushed to subscribers ensuring validation of automatic reconciliation rules.

Update BI live dashboards, historical reports, custom queries for Cis, statuses, ownerships, changes.

It can be deployed as an Azure PaaS solution or in customer's private data center.

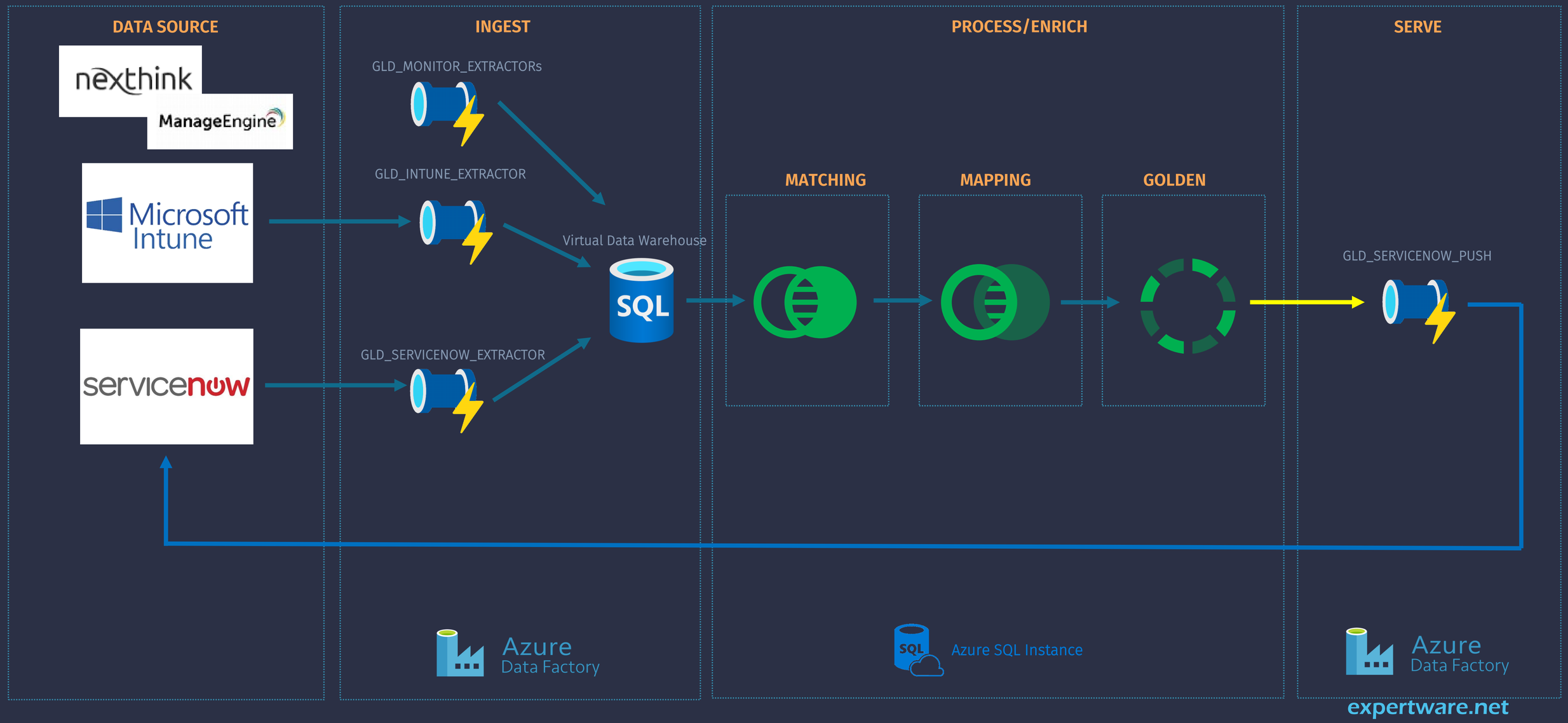


The Process

Technical deep dive

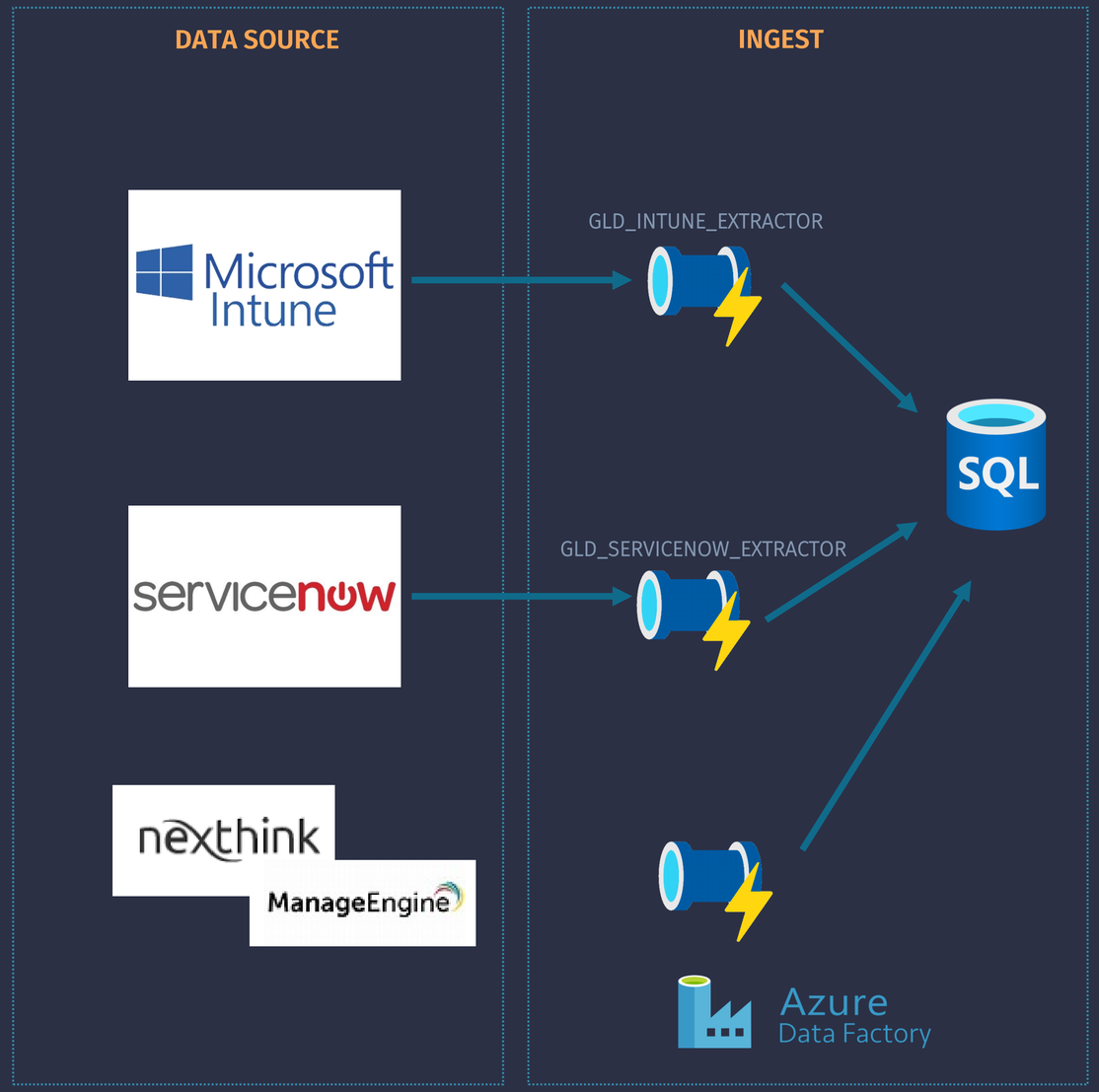
Architecture

Technical deep dive



Architecture

Technical deep dive



IMPORT

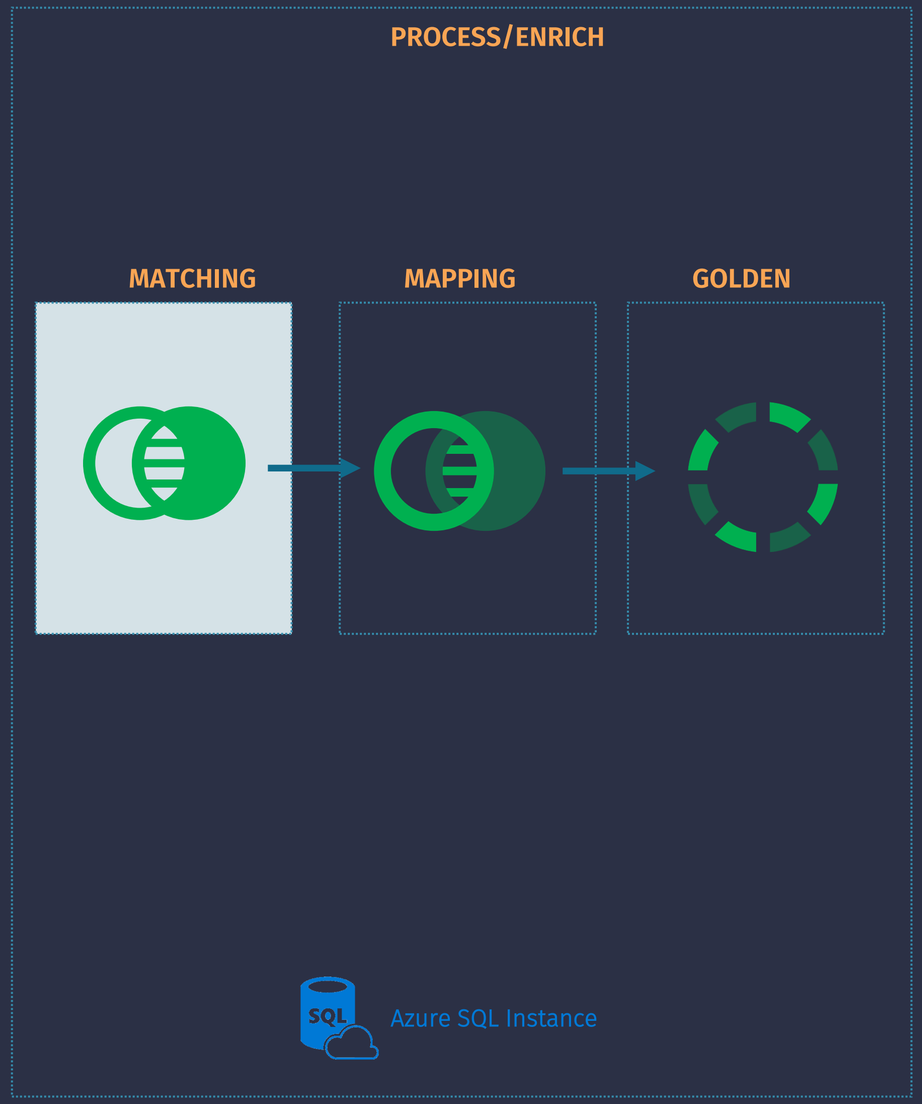
Step 01

Extract and Import data from external sources based on “delta” mechanism and store it to Golden Record master data

- **Extract data from sources (Devices, Users, Vendors, Models, Companies)**
- **Delta import mechanism**
- **Stage data and apply transformation rules**
- **Merge items in virtual data warehouse**

Architecture

Technical deep dive



MATCHING

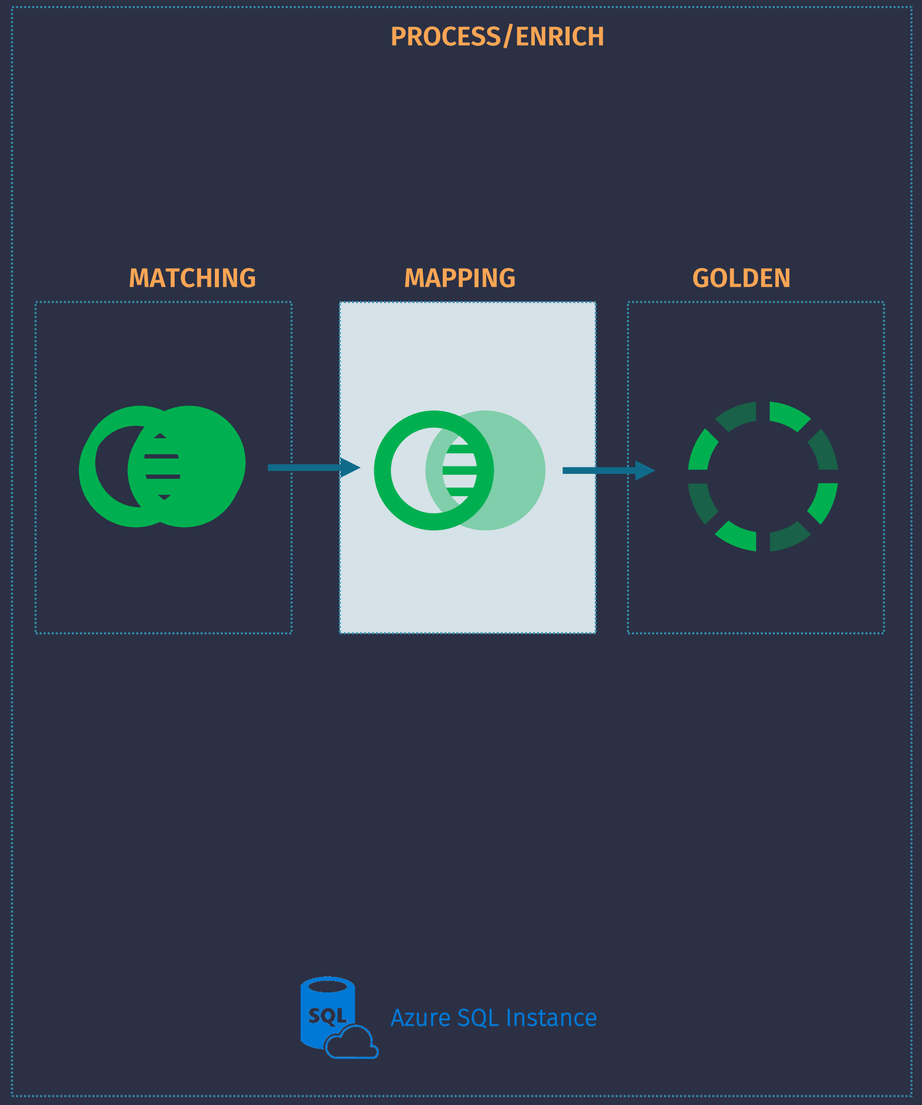
Step 02

Group together entities based on 1 or multiple fields and rules.

- **determine unique attribute(s)**
- **similarity score threshold**
- **generate unique group**
- **enrich records with attributes merged from different sources**

Architecture

Technical deep dive



MAPPING

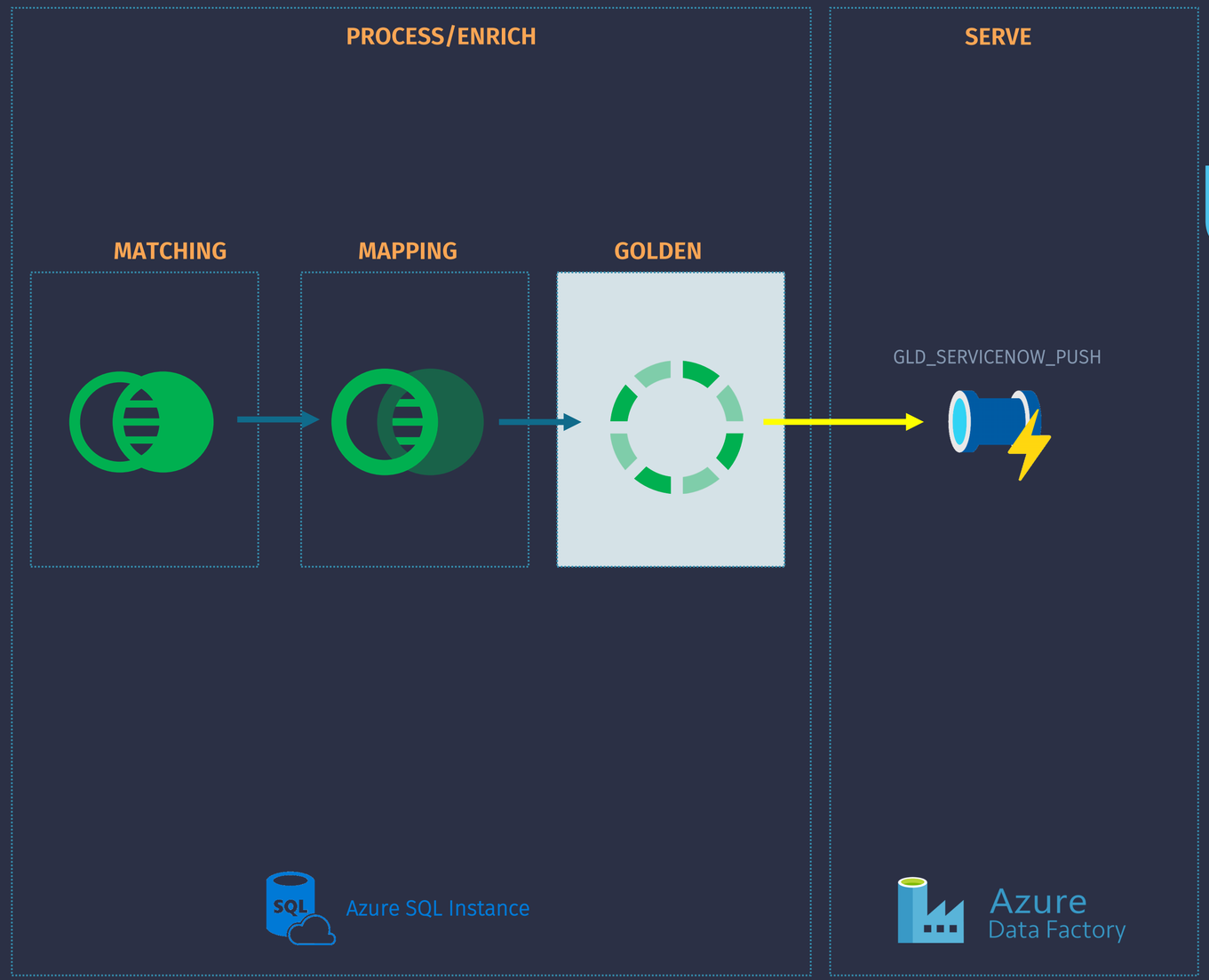
Step 03

Generate a single source of truth record (golden record) based on matching groups and selecting attributes from different sources

- **Determine mapping rules**
- **Detect last version of data**
- **Store changes in history**
- **Prepare update sets**

Architecture

Technical deep dive



Update subscribers

Step 04

Push latest details to subscribers

- **For each subscriber :**
  - **evaluate update rules**
  - **Push latest modifications**
  - **Push hierarchically newly detected records (e.g. new vendor → new model → new device)**

Technology

Release 1.0

Security

- All credentials stored in Azure Key Vault
- Data transfers are secured
- Data at rest is encrypted.
- Access to dashboards based on AAD
- MFA/2FA

Performance/Resources

- Cloud scalability using Azure components.
- High availability out of the box;
- DR possible with low investment.
- Optimized code for performance.
- Start small: SQL resources (1 vCore / 5 GB)

History Snapshots

- All changes on main entities(CI/Users/customers/models) are preserved to view the complete history tracking

Technologies

- **ETL:** Azure Data factory
- **Sources:** Microsoft Graph, Service Now
- **SQL:** T-SQL
- Azure Cloud PaaS
- Web services

Monitoring

- Azure monitor and notifications configured for continuous monitoring (imports, jobs, transformations.
- Integrations are monitored and alerts are sent in case of failures.

Management

- Power bi reports are available to view details about data.
- Manual corrections and failures will be processed by a technical team.

Results

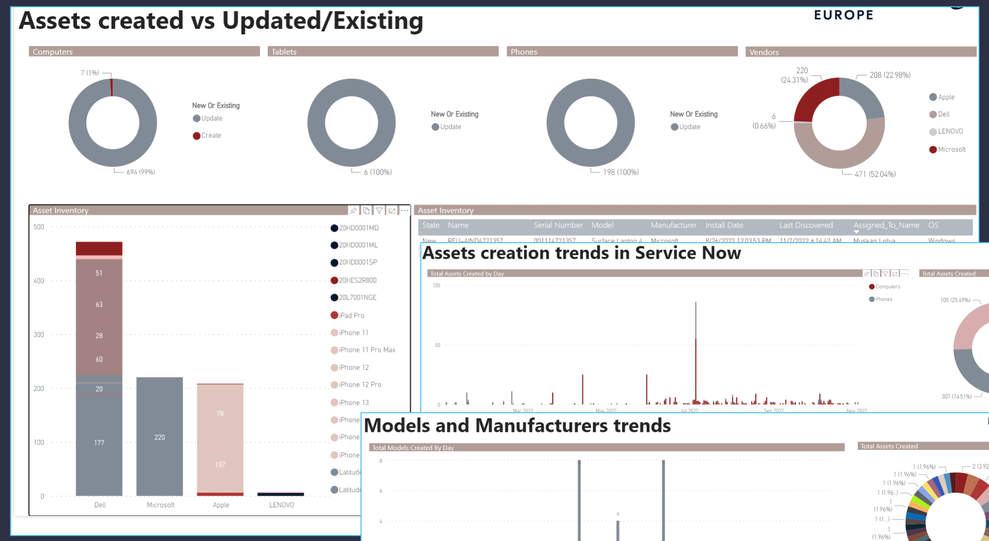
Release 1.0

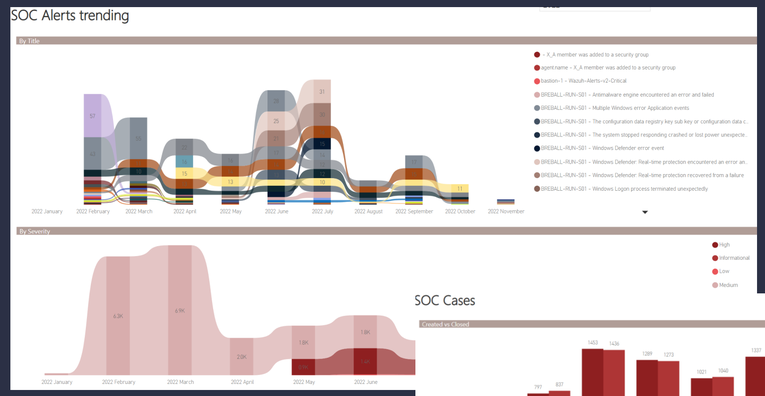
CDMB master data

- Multi-cloud Real time updates
- Push to subscribing systems

Continuous risk exposure evaluation

- Threat intelligence feeds evaluated against discovered assets
- NOC and SOC automations





Benefits

- Always fresh, validated assets, statuses & ownerships.
  Automates discovery of workstations, laptops. Servers, mobile devices via Intune / SCCM

- Unmatched records from sources are marked as new records to be pushed to ITSM CMDB.

- All Intune/SCCM/Azure/Vmware monitoring attributes are pushed to ITSM, NOC and SOC.

- Automatic hierarchical update to ITSM CMDB and NOC / SOC based on dependencies.

- Capability to customize for each subscriber the update rules (when to update, when to insert, when to freeze certain fields).

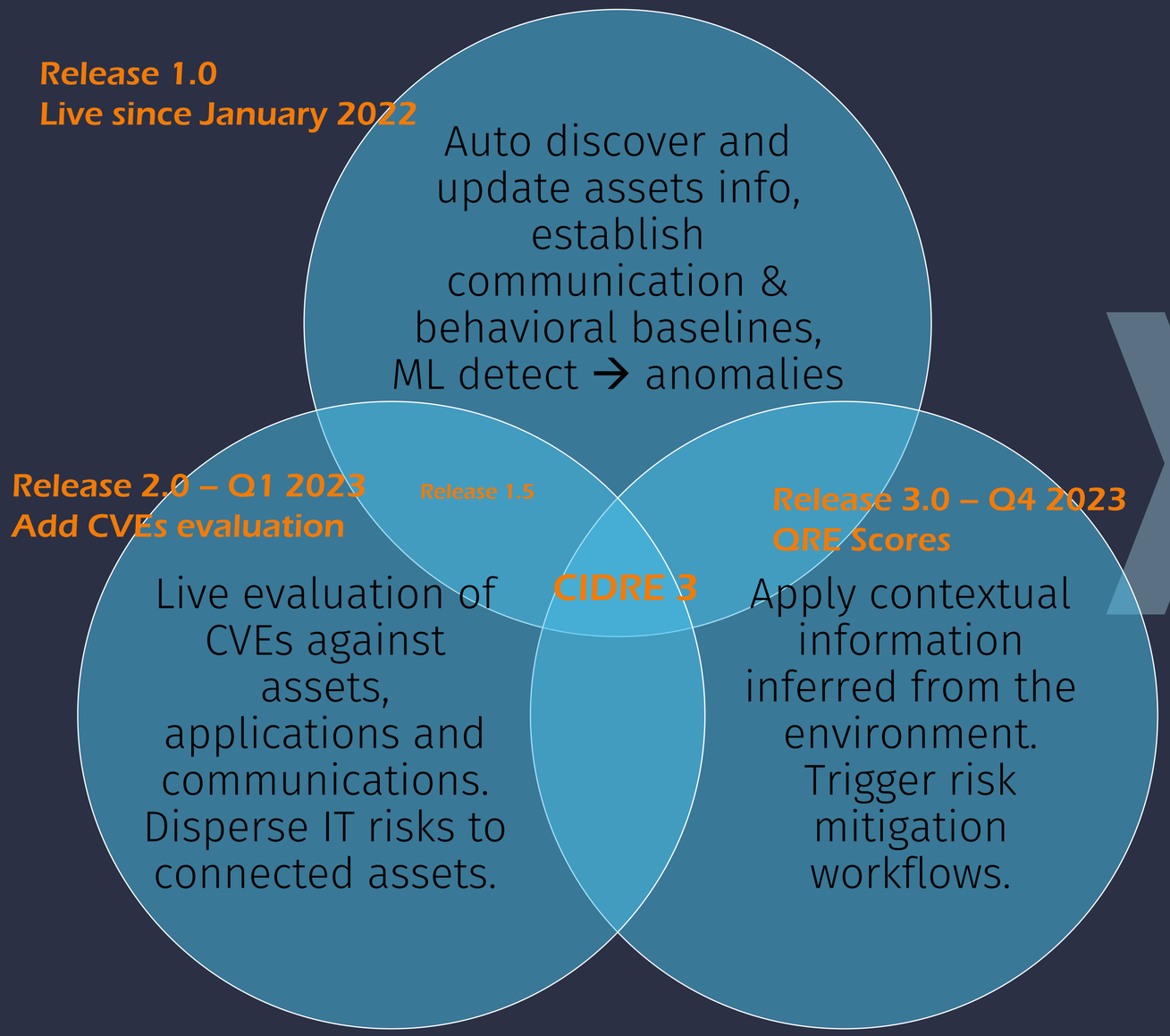
- Cloud scalability, no need for additional licenses, ROI in the first 6 months.

Benefits

- Empowers access to real time CMDB information to make faster, safer, and better decisions.
- Facilitates swifter and more accurate support activities.
  (Agents always have fresh accurate technical information regarding the company's assets at their fingertips).
- Full device history and audit recorded allowing point in time reports, audit changes , device lifecycle reports.
- Surfaces hidden Insights into performance, trends, and anomalies across the asset base. (Useful in global threat monitoring and performance monitoring).
- Fosters continuous improvement for the ITSM processes (incidents, problems, tasks, change requests).
- Improves business performance reducing response time and increasing customer experience.

Next Steps

Next Steps | Roadmap



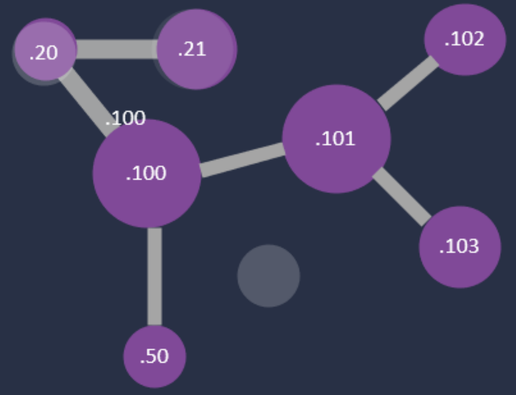
Expand the platform to bridge the GAP between Vulnerability Management process and IT Risk Remediation and Mitigation.

Automate, provide real time Generate Quantitative Risk Exposure Scores (QRE).

expertware CIDRE

Trigger automatic investigation for new connections, new assets

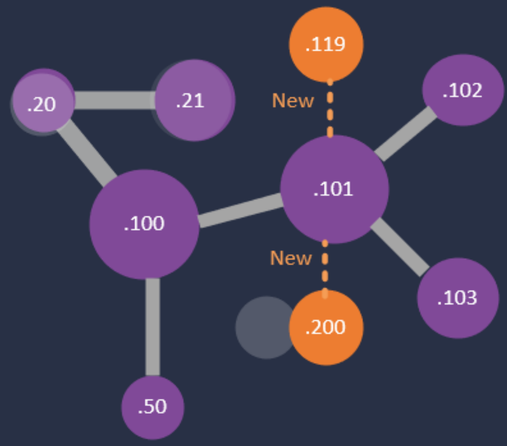
Baseline servers communication (graph)



Add to the baseline

Compare with baseline

Live (5min) servers communication Map



Apply ML models to tag connections

Countinous detections based on ML models
Identify anomalous connections (continuous comparison with the baseline)

Identify anomalous processes opening new connections (not found / added into the baseline)

New communication pattern detected

.101 TCP 134, 145, 3389 .119

.101 TCP 134, 145, 3389 .200

Validated

Not validated

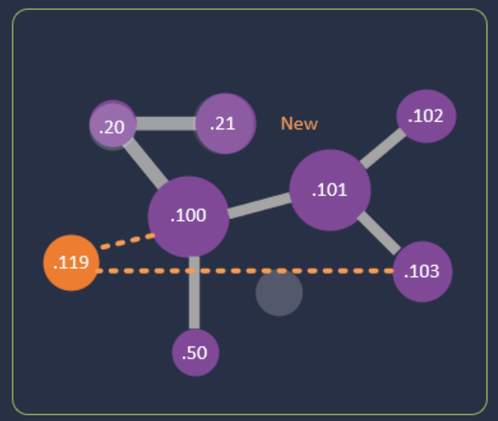
Log security incidents
Initiate remediation

Generate Security incidents, initiate notifications and remediation processes

expertware CIDRE

Intelligent detection and tagging for new assets

Centralize asset info across multiple locations and clouds

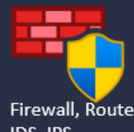


Hypervisors, system management , MDM

Identify new objects created in hybrid clouds,device management, MDM apps

AD, AAD, LDAP, Federations

Identify new objects in LDAP, AD, AAD



Firewall, Routers, IDS, IPS

Identify new communication paths continuously monitoring firewall logs

Server to server connections logs

Identify new server to server communications, detect/infer running applications.

Contextual infomration

Enrich, suggest asset role, properties, criticality

Type, creation date, owner, OS, (optional) department, resource group, locaiton

Container, hierarchy, location, business attributes

IPs, open ports, OS, browser fingerprints

IPs, open ports, applications communicating

Suggested Tags
ENV, Location, Role, Application, Criticality

Election, survival and enrichment rules

Update sets

Auto-update subscribed systems: CMDB, ITSM, SOC, NOC

Assets Criticality Review
Quantify Asset Risk Exposure,

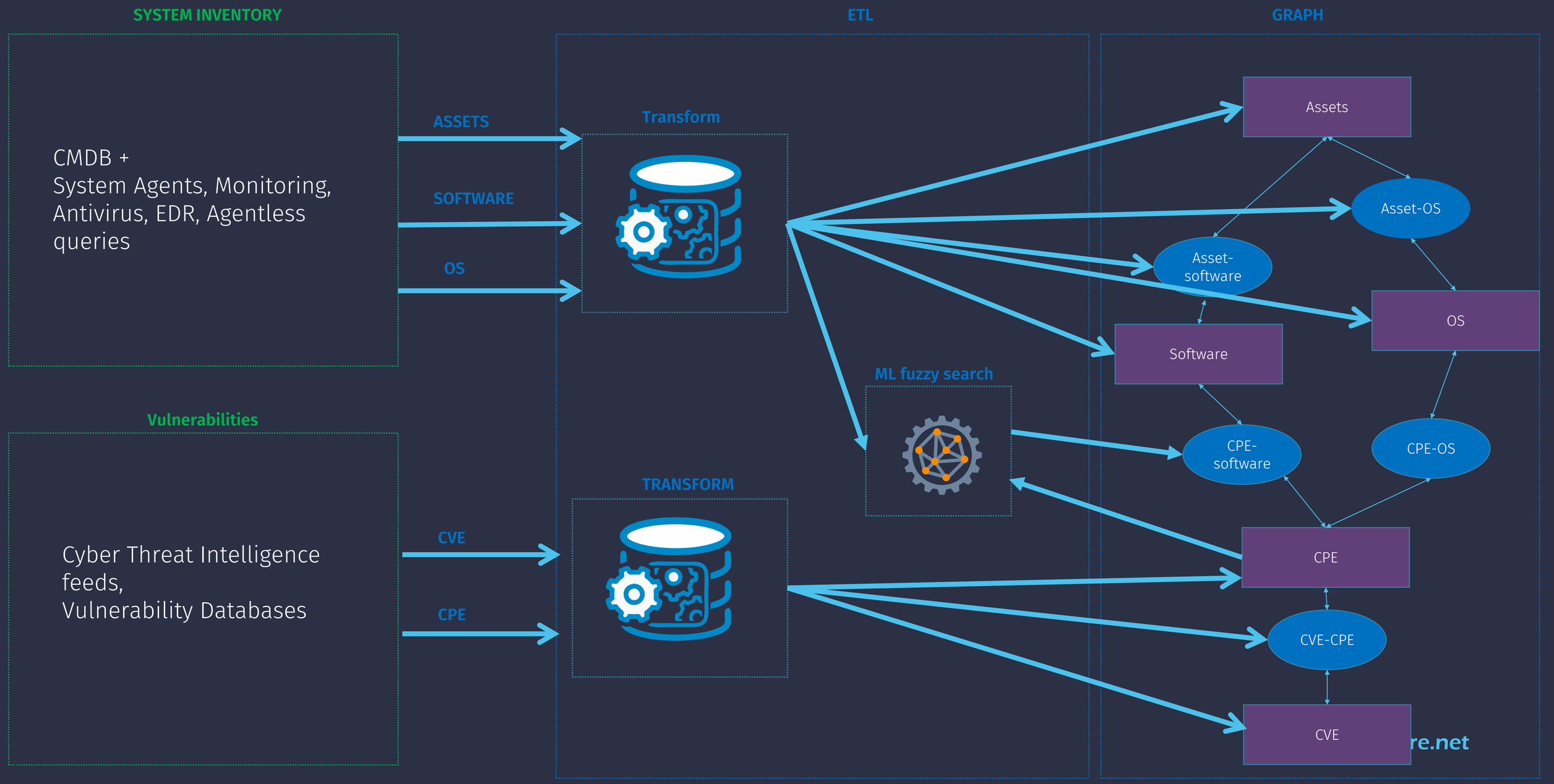
Push accurate information to subscribers, trigger review workflows.

expertware.net

expertware CIDRE

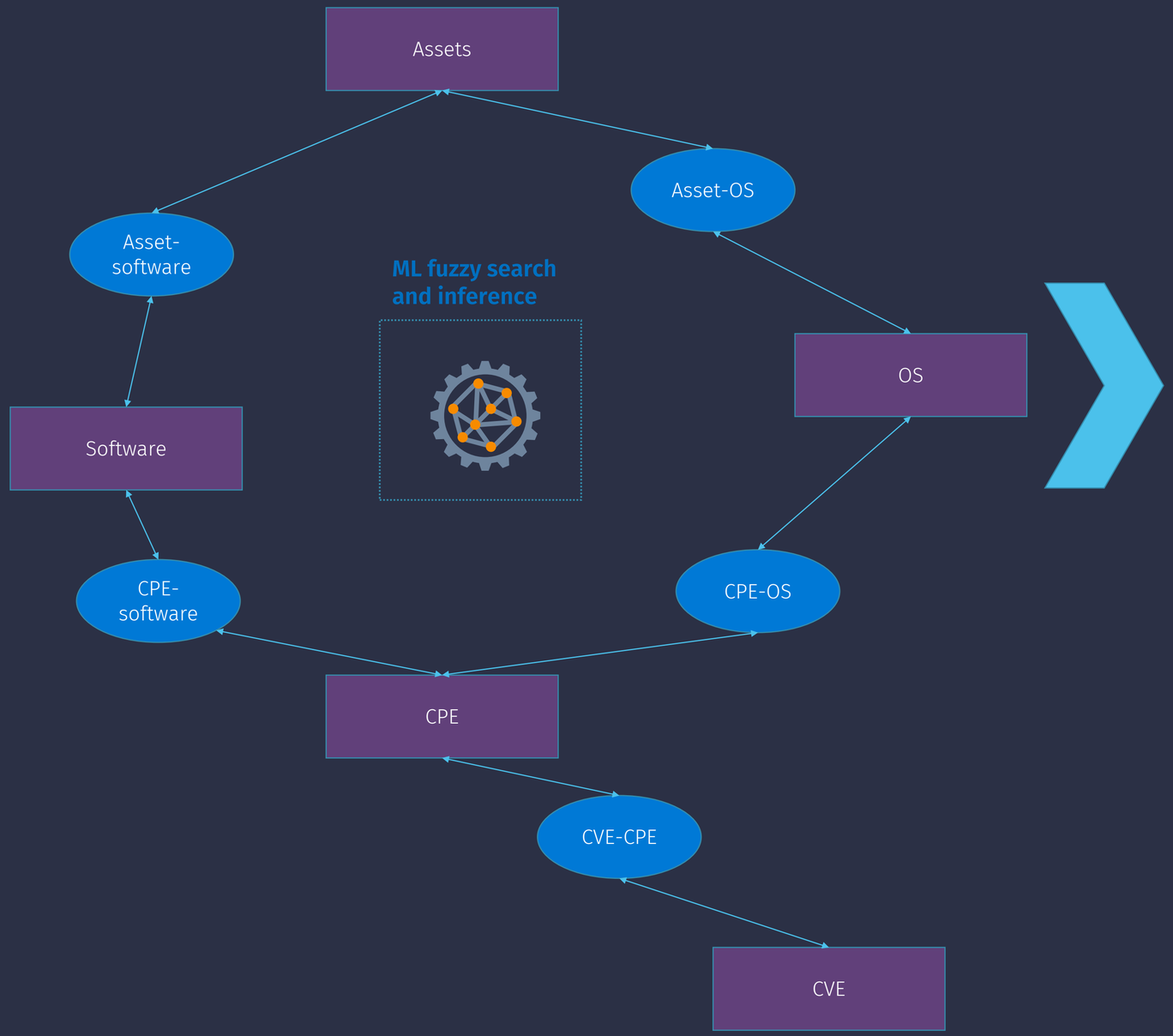
Architecture

Release 2.0

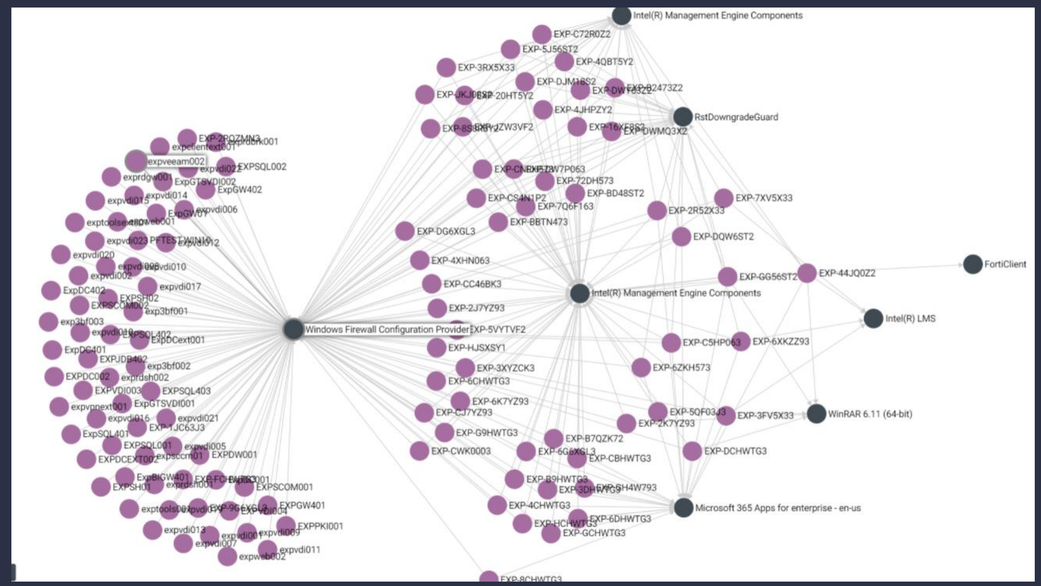


Architecture

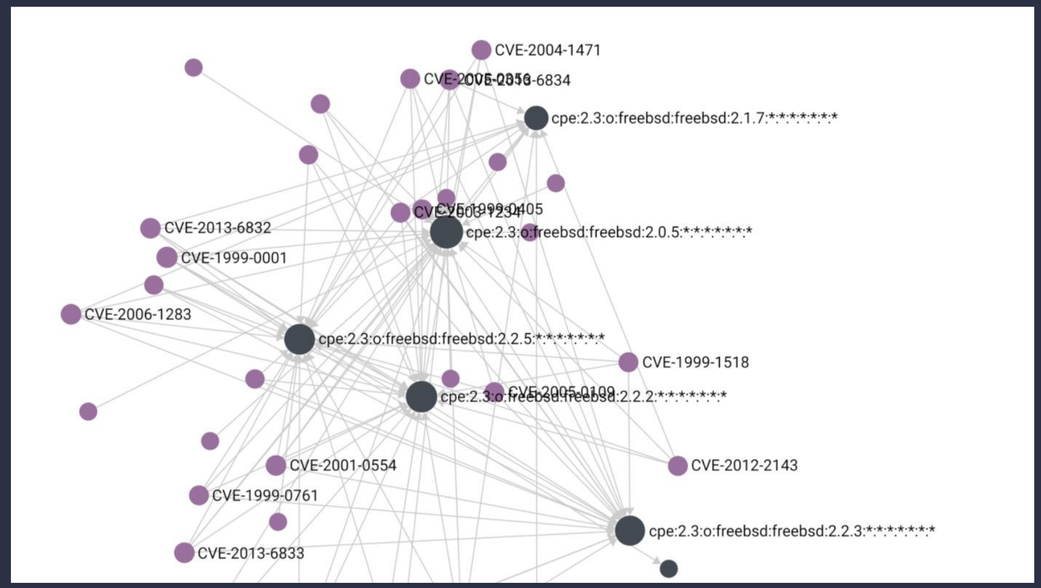
Release 2.0



Continuous evaluation CVEs and CPEs against assets

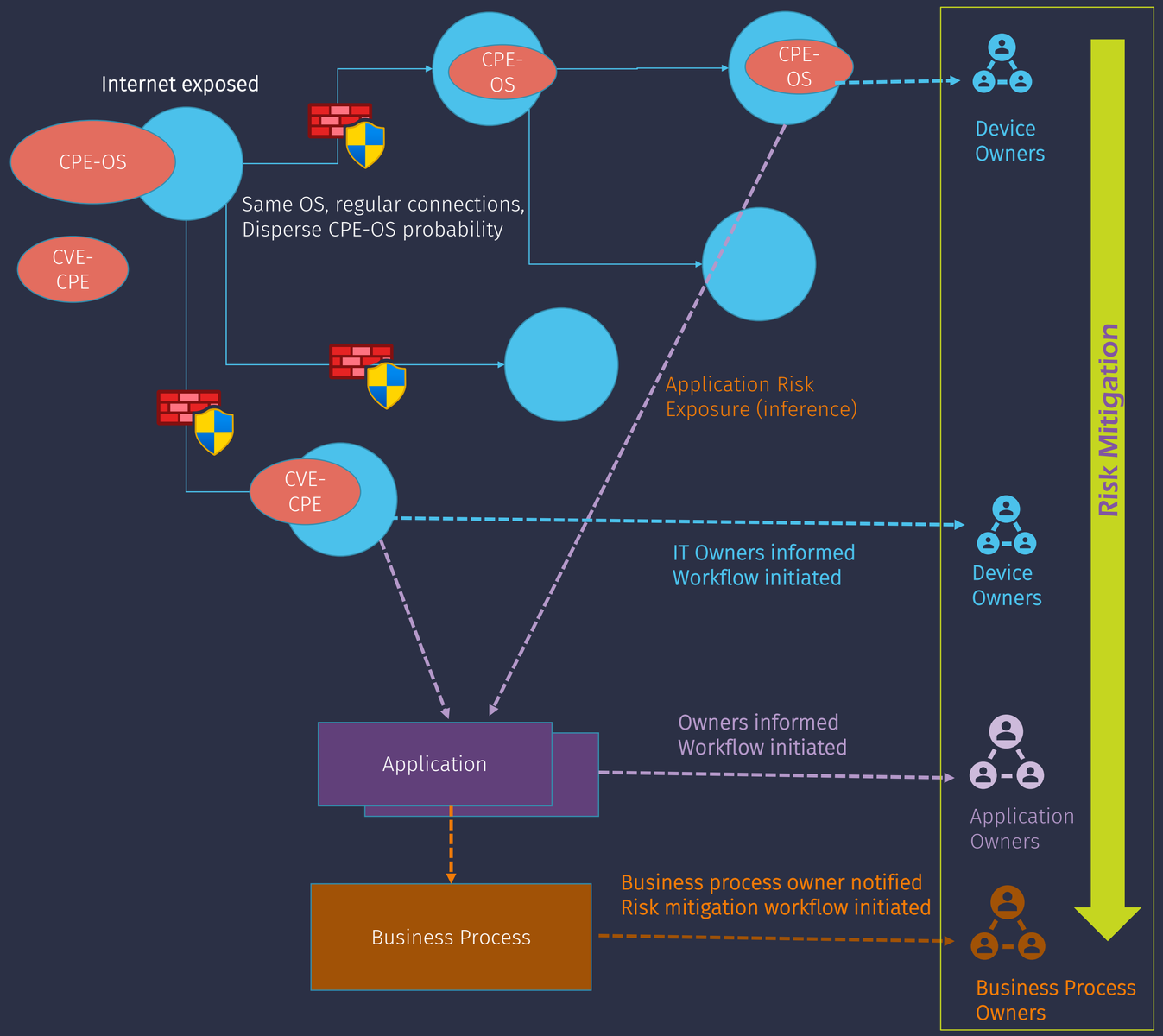


Dependencies CVEs, CPEs, OS



Architecture

Release 3.0



Based on detected communication patterns disperse risk exposure to assets located in different security zones.

Establish risk dependencies, quantify the risk exposure .

Auto-Map assets to business processes based on contextual data (location, department, users connecting manual labeling).

We hope we make you curios.

Contact us!