



| Industrial Vulnerability Manager

Neglecting vulnerabilities means taking risks

Operative challenges

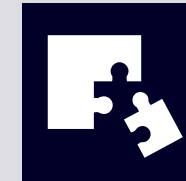
- Every day new software vulnerabilities get reported.
- Currently manufacturers and operators of automation technology with a multitude of different software components struggle to identify if their products are affected.
- Today's solution: Manual checking of different web pages from providers of automation technology (e.g. on the Siemens [web page](#)).
- The industrial security standard IEC 62443 2-3 recommends a broad patch management process.

Already known security vulnerabilities are one of the main entry points for cyber attacks. You need to keep on track with the vulnerabilities and react promptly.

Possible consequences



High manual effort and consequently neglecting already officially reported vulnerabilities



Stay unaware of real threats and consequently not trigger proactive measures (e.g. patching)



Significant financial loss due to cyber attacks exploiting existing vulnerabilities

Efficiently manage vulnerabilities to maximize availability with Industrial Vulnerability Manager



Solution

The Industrial Vulnerability Manager is an application that provides relevant security information to enable manufacturers and operators of automation technology to proactively manage their cyber risks – tailored to their system in a one-stop shop.

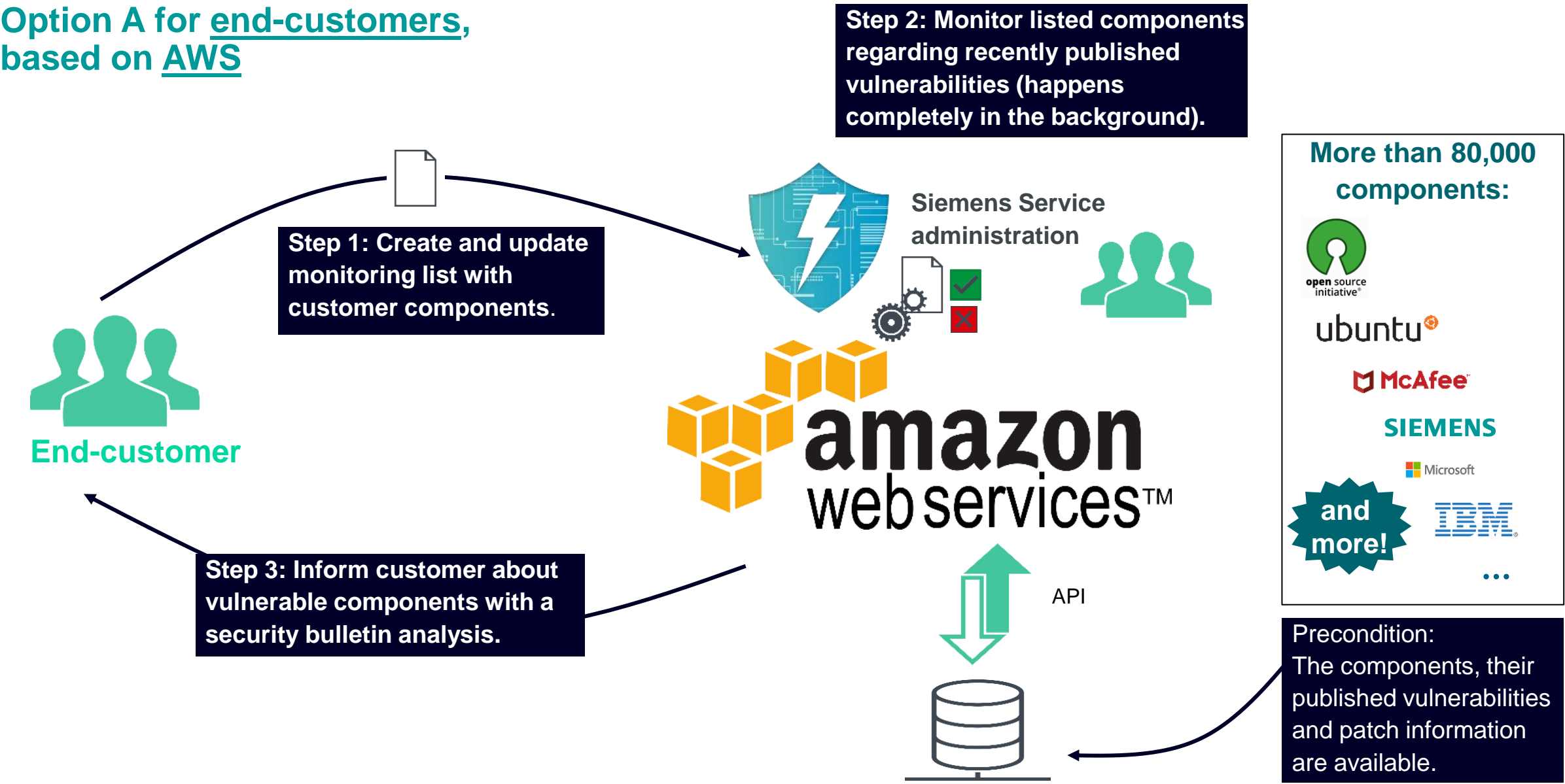
How does it work?

- Step 1: Definition of components to be monitored
- Step 2: Monitoring regarding recently published vulnerabilities (completely in the background)
- Step 3: Automatic generation of digital “Security Bulletins” in case of detected vulnerabilities and possible patches; overview via graphical dashboard

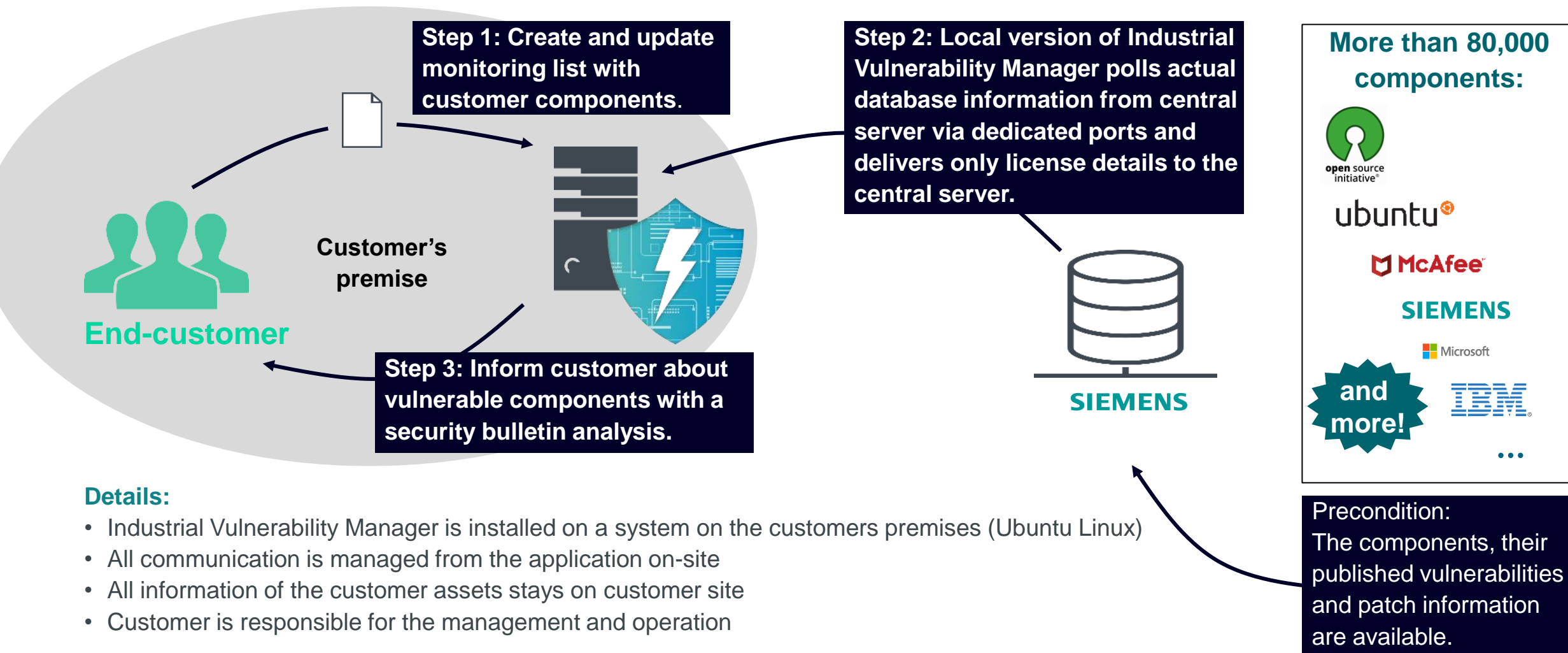
Several deployment options to meet different requirements:

- Option A: For **end-customers**, based on **AWS**
- Option B: For **end-customers**, **on premise**
- Option C: For **end-customers**, based on **Siemens Industrial Edge**
- Option D: For **OEMs**, based on cloud solution (incl. reporting to OEM’s customers)

Option A for end-customers,
based on AWS



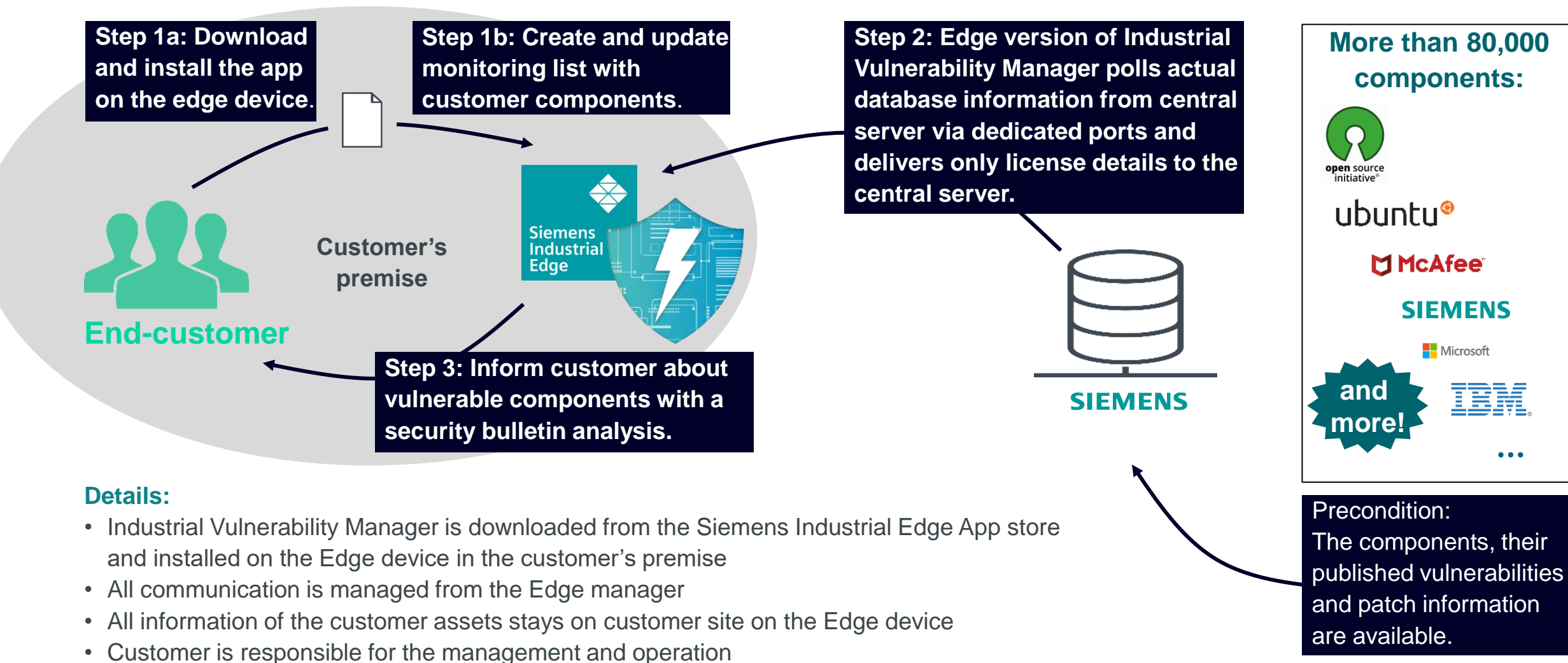
Option B for end-customers, on premise



Details:

- Industrial Vulnerability Manager is installed on a system on the customers premises (Ubuntu Linux)
- All communication is managed from the application on-site
- All information of the customer assets stays on customer site
- Customer is responsible for the management and operation

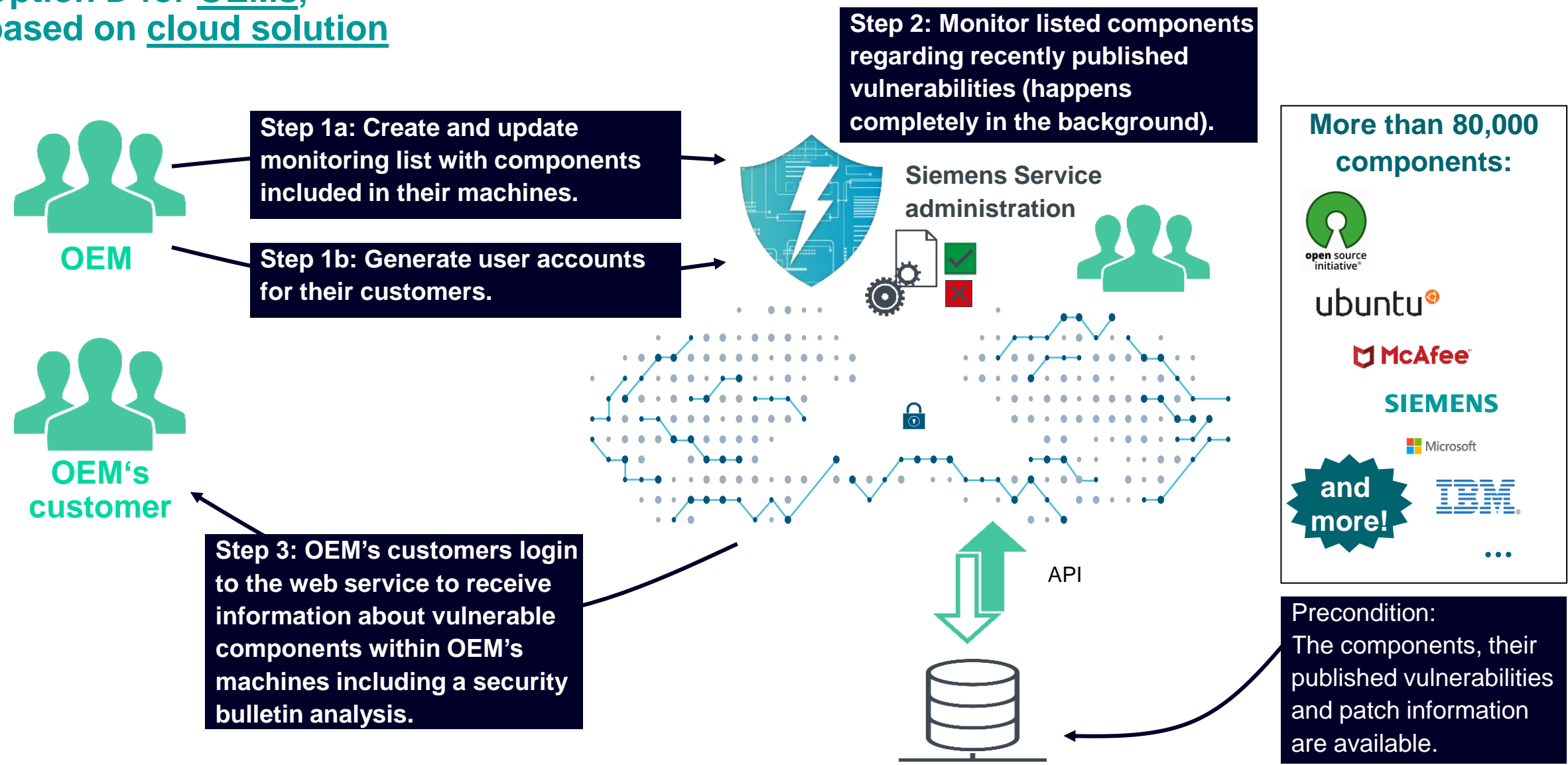
Option C for end-customers, based on Siemens Industrial Edge



Details:

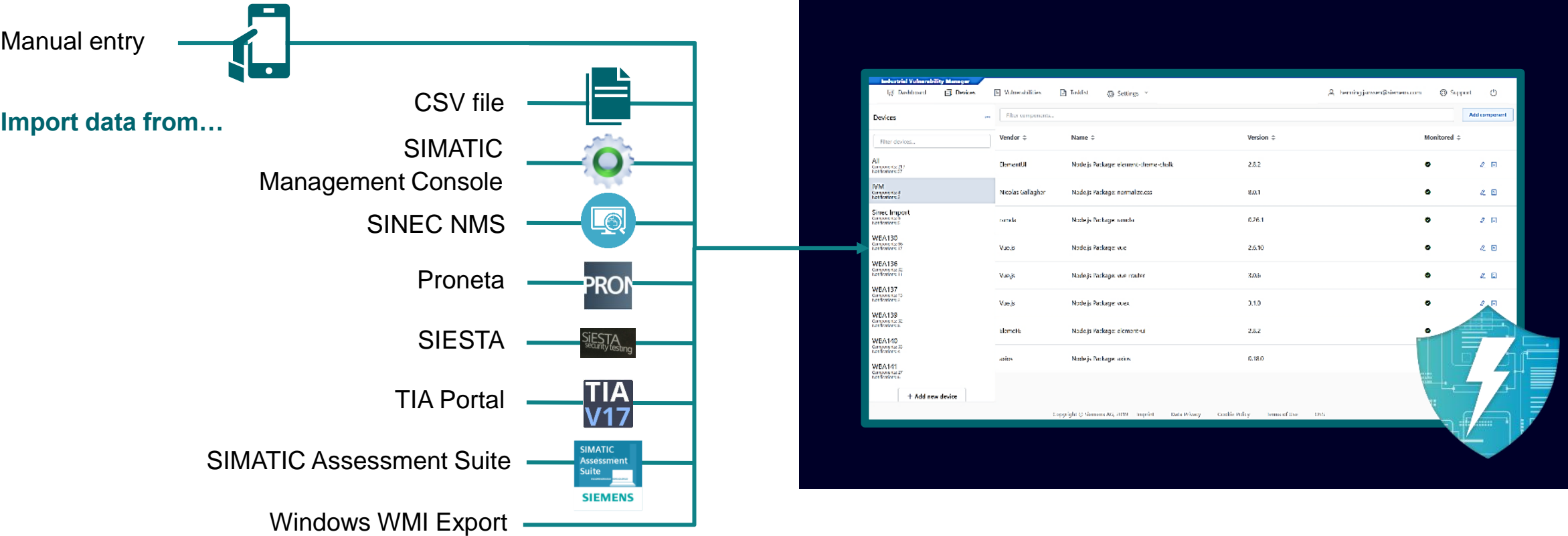
- Industrial Vulnerability Manager is downloaded from the Siemens Industrial Edge App store and installed on the Edge device in the customer's premise
- All communication is managed from the Edge manager
- All information of the customer assets stays on customer site on the Edge device
- Customer is responsible for the management and operation

Option D for OEMs,
based on cloud solution



Step 1: Definition of components to be monitored

Easy creation and update of component list through several import options



Step 2: Monitoring regarding recently published vulnerabilities

A sophisticated system as basis for the Industrial Vulnerability Manager

Unique monitoring infrastructure

- Gaining relevant vulnerability information from all over the internet, e.g.:
 - Official security advisories
 - Vendor support pages
 - Security communities
- Covering vulnerabilities affecting:
 - Open source software
 - Commercial software
 - Hardware components
 - Siemens and 3rd party



Security expert team

- Evaluates vulnerabilities with four-eyes principle regarding two rating scales:
 - Criticality scale
 - CVSS

Proven process

- Monitoring more than 80,000 components (constantly growing)
- Over 1,000 vulnerabilities per month, bundled in practicable packages



Step 3: Automatic generation of digital “Security Bulletins”

The notifications and the dashboard allow an easy management and reporting of cyber risks

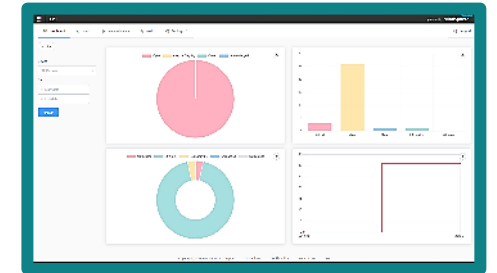


Security Bulletin

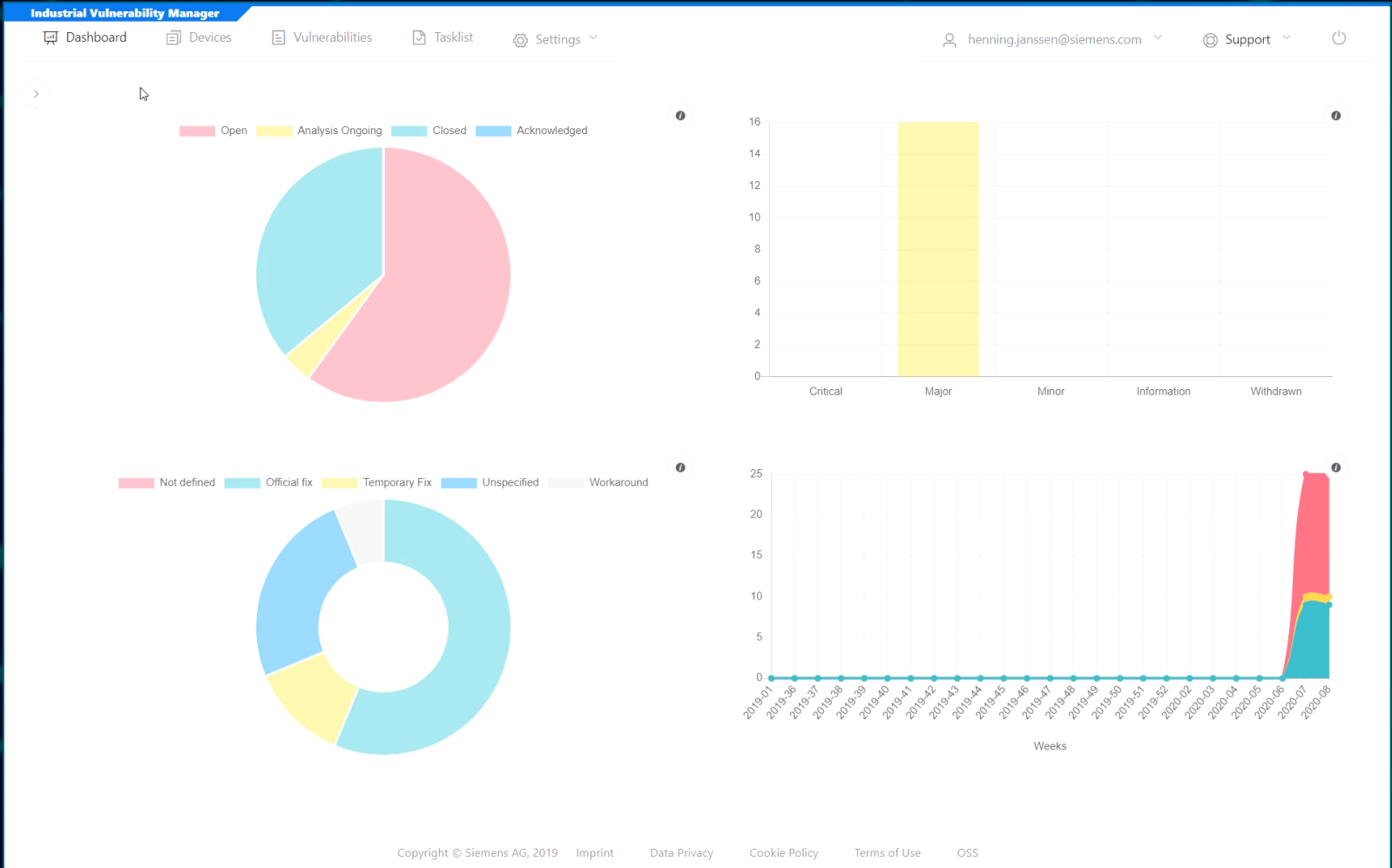
- Description of the vulnerability and affected components
- Real-time monitoring of available patches
- CVSS score
- Priority
- Link to the vendor web site

Graphical dashboard

- Overview of vulnerabilities including criticality
- Task list to check overdue and upcoming fixes
- Overview of patch status to follow and track the mitigation and closure of the vulnerabilities

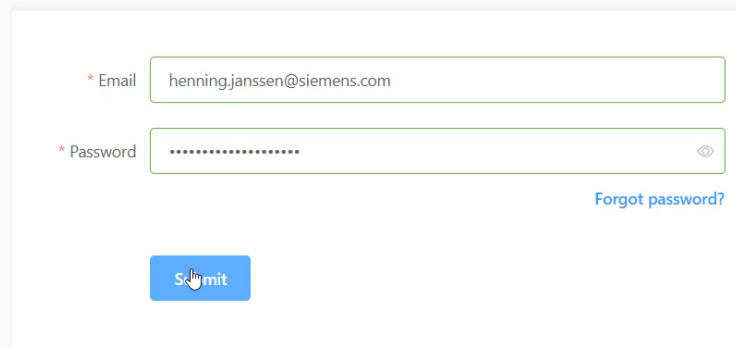


Application overview – short version



Application overview – long version

Industrial Vulnerability Manager



A login form titled "Industrial Vulnerability Manager". It contains two input fields: "Email" with the value "henning.janssen@siemens.com" and "Password" with masked characters. A "Forgot password?" link is located to the right of the password field. A blue "Submit" button is at the bottom.

* Email

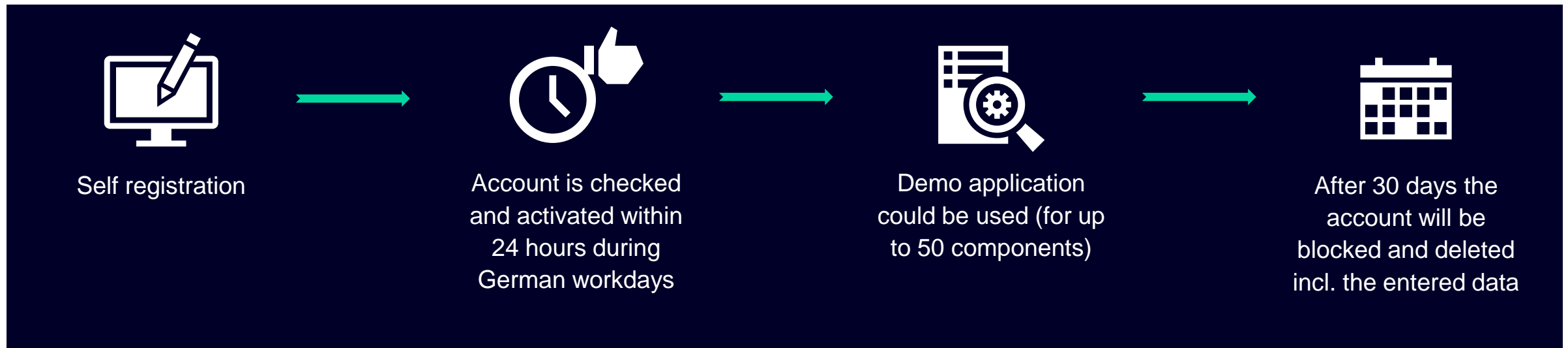
* Password

[Forgot password?](#)

Demo portal – access, workflow, restrictions

Demo portal can be accessed via the following link:

siemens.com/ivm-demo



Restrictions:

- The portal can be used to test the service for up to 30 days and up to 50 components. No new components can be added.
- As this is only a test portal, we will not guarantee any service level for the availability.
- It is only possible to register once.

Siemens as reliable partner for Industrial Security

We are the automation experts



We drive digitalization



We understand industrial security



We have specific industry know-how



We offer state-of-the-art technology and end-to-end services from a single source



“We make sure that you can focus on your core business.”

Why should you choose Industrial Vulnerability Manager?



Instant transparency on vulnerabilities and patches



Proactive management of cyber risks



Avoid downtime and save costs

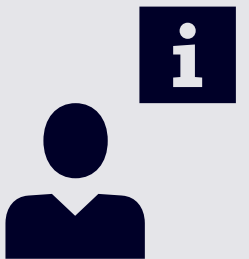
Let us know if there is anything we can support you with!



You want to find out more?

Contact the Siemens partner near you

[Siemens Contact Database](#)



Disclaimer

© Siemens 2022

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity>