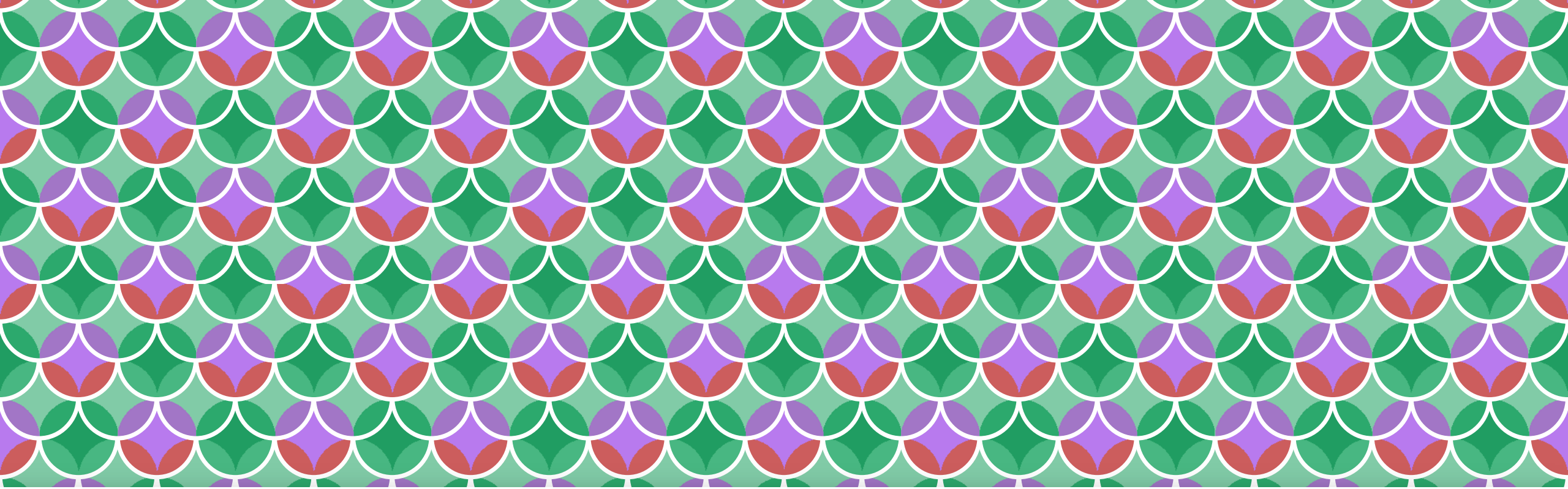

SYNC FISH

High Level Overview

CI Sync (Enterprise Edition) for Defender for Endpoint to ServiceNow

CI Sync (Enterprise Edition)

Platform Architecture and Security Overview

CI Sync (Enterprise Edition) is a modern SaaS-hosted integration platform that implements robust security mechanisms to ensure to protection of customer IT asset information.

The scope of this deck is the CI Sync (EE) connectors for Defender for Endpoint (as the source system) and ServiceNow (as the destination system).

Other CI Sync connectors include:

- Lansweeper OT
- Lansweeper Cloud (for on-prem data augmentation)
- Azure
- AWS (MVP)
- GCP (MVP)
- Microsoft 365
- Intune
- SCCM
- JAMF
- Nutanix
- Vmware (virtualisation)
- Vmware SD-WAN
- Palo Alto SD-WAN
- BeyondEdge SD-LAN
- SolarWinds Orion
- LeanIX
- and more coming on regular basis.

General Overview

CI Sync (EE) for Defender for Endpoint to ServiceNow

Key Points

1. The Microsoft Defender for Endpoint Vulnerability Management dashboard within the Microsoft Defender portal provides security administrators and security operations teams with security recommendations, software vulnerabilities, remediation activities and exposed endpoint devices.
2. The CI Sync Microsoft Defender for Endpoint connector retrieves endpoint devices and their associated vulnerabilities (CVEs) and populates this information into Configuration Management Database (CMDB) enabling organisations to visualise their endpoint exposure. In addition, organisations can use ServiceNow to generate remediation tasks to create end-to-end CVE remediation workflows.
3. The integration requires minimal configuration to connect to your Defender for Endpoint Portal. All that is required is an Azure Application Registration (service principal) with access to your Defender for Endpoint portal and you are up and running.

For further information visit:
www.syncfish.com.au

Important Characteristics of CI Sync (EE)

CI Sync (EE) for Defender for Endpoint to ServiceNow

Key Points

- **Each customer is provided their own dedicated instance** of the CI Sync (EE) SaaS application. There is **no sharing of processing or storage between customers**.
- **Each CI Sync (EE) customer decides where their SaaS instance is located**. The CI Sync (EE) SaaS application (for each customer) is deployed to any Azure Data Centre with the required services (so almost all Azure locations across the globe).
- **CI Sync (EE) does not store a copy of the Defender for Endpoint resource data** after it has been processed and persisted into ServiceNow.
- **All authentication and authorisation is controlled by the customer's own Azure AD**

- There is **no requirement for any of the following in ServiceNow** :
  - **No ServiceNow** Mid-Server
  - **No** need for any **Service Graph connector/s**
  - **No** need for any **Integration Hub components**
  - **No** need for any **ITOM Discovery components**
- **Only the following is needed within ServiceNow:**
  - **A least privileged user/system account** for CI Sync (EE) to authenticate to ServiceNow.
  - **One/two simple settings** (a timeout and some CMDB CI dictionary settings). **performance**
- **The CI Sync (EE) Agent** (lightweight Windows service)
  - It can be installed on any VM in the customer environment.
  - The agent is installed using an installer wizard (MSI).
  - Multiple source systems are supported by a single agent (e.g. Azure, InTune, VMWare, etc).

The customer installation of CI Sync (EE) usually takes 60 to 90 minutes!

After this short time the customer is sync'ing into their non-prod CMDB

Contact Syncfish for further information

PHONE
+61 (7) 3532 4097

EMAIL
info@syncfish.com.au

ONLINE
www.syncfish.com.au