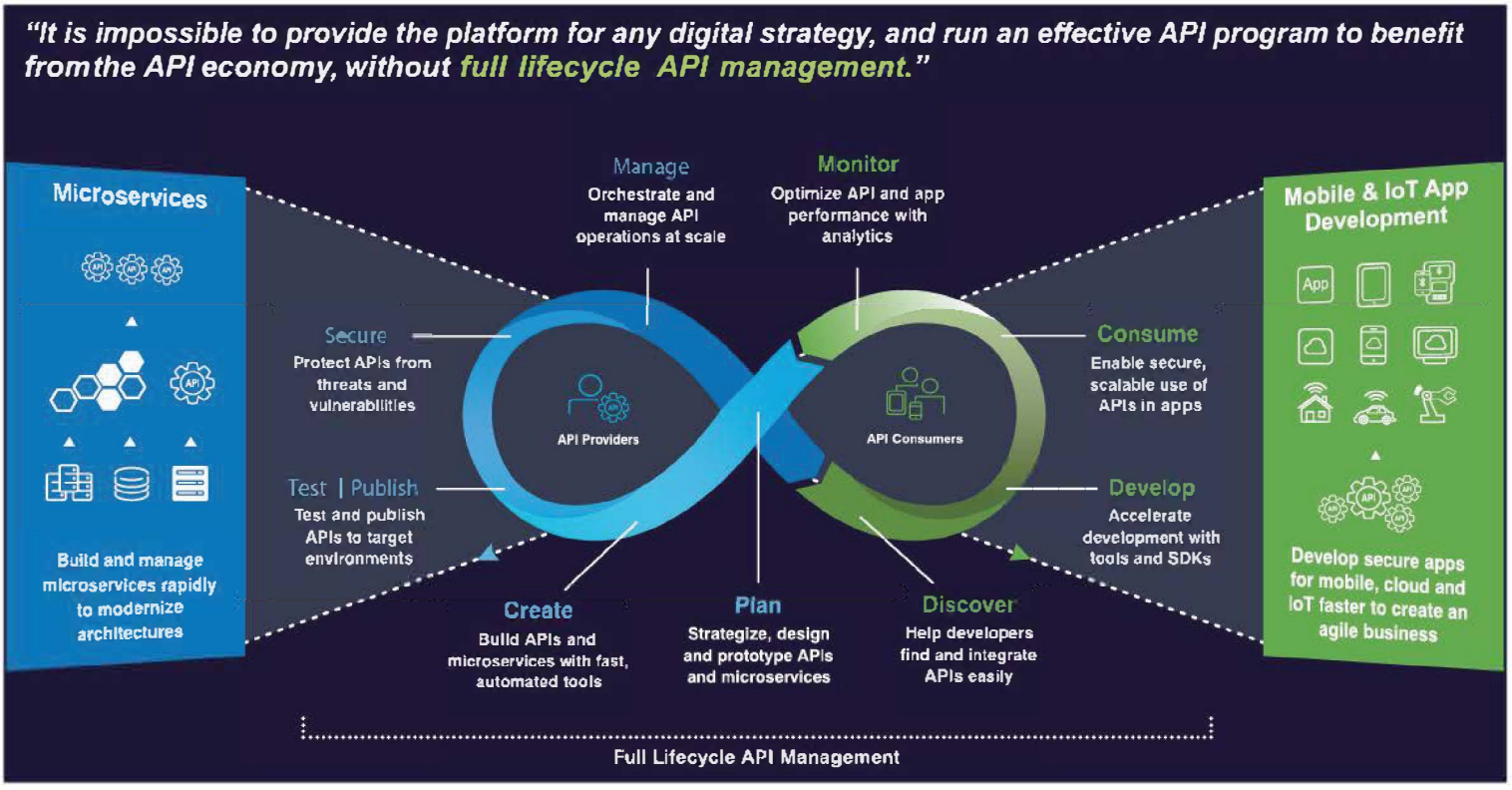
API-Centric Security Model as a Critical Component for Success in the Continuous Diagnostics and Mitigation Program

CA's API products accelerate technology modernization efforts, while at the same time provide gap fill for CDM requirements. Some reasons to consider an API-centric security model are:

- To integrate systems- whether legacy or not - all the way through to the CDM Dashboard, rapidly, consistently, and in a cost-effective manner.
- To meet NIST 800-53 and NIST 800-63 compliance standards.
- To accomplish CDM Functional Requirements (BOUND-F, PRIV, Design and Build in Security, PEP)
- To address immediate gaps in an agency's security posture, for example, Open Web Application Security Project (OWASP) vulnerabilities.
- To allow legacy and modern systems to rapidly and securely communicate via API, even if they do not have REST and SOAP native capabilities.
- To enable the management of all API communication interfaces within and beyond a system boundary.



How does the use of CA API Gateway improve results on the Department of Homeland Security (DHS) CDM program?

- SCIM is one of over 100 protocols supported by the CA API Gateway and is a critical component to enable identity and access provisioning from the SailPoint Master User Record to the CyberArk and privileged access management solutions from CA. The SCIM-based approach makes dynamic real time provisioning and deprovisioning possible, and prevents the risks associated with a daily sync-based approach currently used by many privileged access management systems and identity management systems.
- Allows agencies and DEFEND integrators to rapidly, securely, and consistently build API wrappers for applications and data sources in a standardized method that follows and enforces best practices by taking advantage of the CA API Gateway's ability to:
  - Normalize data – Standardize the schemas so developers can create APIs more quickly and with better quality, and more accurately monitor APIs to ensure content, format and schema does not deviate beyond KPIs.
  - Provide protocol transformation- to only allow policy-approved protocols to reach your network. This results in a common security posture for API connections and makes it easier to document, audit, and achieve an Authority to Operate (ATO).
- For CDM BOUND F:
  - CA API Gateway can sit between enclaves to apply filters, rules and policies to regulate the flow of traffic between trusted and less trusted sites as an enterprise policy enforcement point (PEP).
  - Encapsulation filter element – CA API Gateway can be used to create centralized standards for policy creation, enforcement and monitoring for protocol transformation processes following the best practices.

CA API Gateway is an appliance that can be delivered in many form factors, including hardened physical appliances, Docker container-based appliances, Microsoft AZURE™ and AWS appliances, and more. The ability to quickly implement and deploy the appliances makes it an achievable "first step" in developing your agency's API security strategy.

For more information about API management from CA Technologies, please visit ca.com

CS200-398422_1018