www.SeKON.com
11480 Commerce Park. Ste 100
Reston, VA 20191

The Enterprise-wide Data-Driven Operations Platform (EDDOP) – Zero Trust

Zero Trust Security - Never Trust, Always Verify

Zero Trust is a modern approach to cybersecurity that secures an organization by eliminating implicit trust based on network boundaries in favor of continuously validating every user and device at every stage of a digital interaction. Rooted in the principle of "never trust, always verify," Zero Trust is not a single technology but rather a framework consisting of strong authentication methods, network segmentation that prevents lateral movement, and granular, "least access" policies.

SeKON's **Enterprise-wide Data-Driven Operations Platform (EDDOP)** leverages Zero Trust Security natively via **Palantir Foundry's** dynamic, granular, modular, and layered security architecture that enables organizations to not only store their data securely, but to tailor access to their specific needs. Foundry has been developed to protect integrity, availability, and confidentiality by design and to work in conjunction with the customers' existing Zero Trust Architecture. The following are the core pillars of this capability:

- **Identity, Credentials, and Access Management (ICAM).** Foundry integrates with a customer's existing SAML 2.0 Single Sign-On (SSO) identity providers (IdPs) or can provide a dedicated Multi-Factor Authentication capability providing users with a familiar, secure sign-on experience. Additionally, it provides identity and access management administrators with a single source of control across their organization's applications. This means access management administrators can easily and effectively modify who has access to Foundry and use existing SAML SSO audit log systems to review access to Foundry. Foundry provides an integrated ICAM capability to modernize the security of your organization's data and transition from endpoint security to a data-centric model.
- **Roles.** Roles are a purely additive type of security. They are applied to resources in Foundry as the primary way to give access and capabilities to Foundry users. They represent a pre-defined collection of operations that define the specific actions a user or group can take on a given resource. Foundry supports both mandatory and discretionary role-based access controls. Roles ensure that all data are protected and only available to those users with authorization and appropriate need-to-know.
- **Projects.** Projects are the primary security boundary in Foundry and can be thought of as buckets of shared work. Because their boundaries enforce security, Projects are a key means of organizing data and enabling open collaboration within a secure space.
- **Security Markings.** Security Markings are solely restrictive, providing a legible and well-defined way of ensuring that sensitive resources remain restricted to the appropriate users. A user must satisfy all of the Security Marking requirements on a resource to have any access

(even discovery). Regardless of a user's role on a resource, the Security Markings must be satisfied first.

- **Granular Permissions.** Granular permissions are access controls that can be applied below the resource level in order to push access requirements into the data itself. These controls come in the form of access policies that can be evaluated differently at the record, row, or column level. These policies are highly configurable and can leverage a user's attributes or group membership against specific values in the dataset.
- **Access Auditing.** Data administrators need to fully understand permissions and how they work in practice. Foundry offers tooling to allow administrative users to audit the access of resources and data.

With an ever-growing hybrid workforce and continued migration to the cloud, the transformation of security operations to a Zero Trust approach has never been more critical. Done correctly, a Zero Trust architecture results in higher overall levels of security while reducing security complexity and operational overhead.

To learn more about EDDOP, visit www.SeKON.com/news/ or on LinkedIn at SeKON Enterprise, Inc.