Hewlett Packard Enterprise

Solution brief

Check if the document is available in the language of your choice.

PROJECT COSIGNO—SERVICE IDENTITY FABRIC FOR THE CLOUD-NATIVE ENTERPRISE

OVERVIEW

Project Cosigno provides a web-scale, unified service identity platform that enables security and infrastructure engineering teams to standardize, scale, and accelerate service-to-service authentication across cloud, container-based, and on-premises platforms. Unlike other approaches, Project Cosigno allows you to issue and broker scalable-, cryptographic-, and platform-agnostic identities based on open standards. As a result, it enables you to boost security operations and developer productivity, reduce application on-boarding times, and accelerate cloud or container adoption while strengthening your overall security posture.

CHALLENGE

The last five years have witnessed a seismic change in how applications and services are architected, built, and deployed. Led by cloud and containerization, services are being built more quickly by semi-autonomous teams and deployed on a wide and growing range of platforms. As this development accelerated, these systems are becoming increasingly interdependent and interconnected.

Strong security and defense in depth for inter-service communication is increasingly critical in such a heterogeneous operating environment. Yet, existing security products such as network/application firewalls and authentication protocols such as Kerberos and OAuth are struggling to keep up with the elastic, dynamic, and hybrid services. Services credentials spread across platforms are becoming a risk for theft while at the same time are increasing operational complexity and reducing deployment velocity.

BENEFITS

Strengthen your security posture and protect your existing investments: Multifactor policies establish greater trust in provisioned identities. Short-lived credentials reduce the threat radius. The ability to broker identities across your existing on-premises identity providers (IdPs)—such as Active Directory—to cloud and container services strengthens your security posture, reduces the risk of compromise, and helps eliminate the need to rewrite code or rearchitect for cloud and container platforms.

Boost staff and developer productivity: API-driven, automated controls mean that your developers spend less time writing code for security controls or waiting for tickets; and operations teams can deploy, operate, and scale authentication easily across dynamic, heterogeneous infrastructures.

Speed cloud and container adoption: Leverage a common, scalable identity model that works with your existing IdP and is designed for cloud- and container-based environments to seamlessly and securely authorize services across any platform.

Reduce time to market from weeks to minutes: Helps eliminate manual processes and development efforts to authorize a service across multiple platforms. Automated, uniform service identity management reduces application onboarding times from weeks to minutes.

KEY FEATURES

Scalable-, cryptographic-, platform-agnostic service identity based upon an open standard (SPIFFE): Deploy standard service identities across heterogeneous platforms including cloud, containers, and on-premises infrastructure. In contrast to traditional authentication mechanisms such as Kerberos and OAuth, Project Cosigno service identities are based on automatically provisioned, short-lived asymmetric keys. These are more resilient in distributed systems, not subject to replay attacks, and can be used to help ensure confidentiality using mutual transport layer security (mTLS). Applications can authenticate directly without relying on the availability of a trusted third-party during authentication. These identities are based an open-standard—Secure Production Identity Framework for Everyone (SPIFFE)—backed by the Cloud Native Computing Foundation (CNCF).

Multifactor service authentication: Instead of authenticating service-to-service communication with long-lived credentials that must be provisioned and rotated with the workload, Project Cosigno identifies services through real-time multifactor authentication policies. Project Cosigno's real-time attestation engine leverages a union of trusted third parties, including cloud provider control planes, container orchestrators, signatures from CI/CD pipelines, trusted OS kernels, hardware security modules, and existing machine identity frameworks. It provides a strongly trusted authentication for cloud and on-premises services. This helps eliminate long-lived credentials and mitigates credential exfiltration attacks.

Dial tone authentication: Authentication can be deployed and governed by infrastructure and operations teams, and made available as a consistent dial-tone API to any engineering team. Project Cosigno, since all developers have to do is call an API for real-time identity and authentication, helps eliminate the need to configure and manage credentials manually, and avoids potential outages caused because of engineers deploying the wrong credentials to the wrong environment.

Unified service directory and credential: Delivery encapsulates complexity by unifying service identities across IdPs spanning cloud, container, and on-premises identity providers through a single service-facing API.

Identity brokering: It enables you to extend your existing identity providers and authentication infrastructure (such as Active Directory) to the cloud and containers, and allows services running in one cloud to assume identities in others. For example, Project Cosigno can deliver Kerberos service tickets from an on-premises Active Directory installation.

Comprehensive auditability: It ensures compliance and precisely identifies where and when service credentials are generated and delivered with granular tracing, even in highly elastic and dynamic environments. By leveraging the service metadata collected for multifactor authentication, Project Cosigno can provide a comprehensive picture of where tokens are delivered and avoid ephemeral identifiers like IP address.

Scales to next-generation architectures: Project Cosigno is designed for hybrid and multicloud deployments. It also caters to elastically scaled and dynamically scheduled workloads. It has been built and maintained by a team with deep expertise in distributed architectures. It helps protect legacy identity providers from overload burst and scale.

LEARN MORE AT

hpe.com/us/en/software/service-identity-management.html

Get updates

Hewlett Packard Enterprise

a50002185ENW, August 2020