Aporeto

Zero Trust Security Solution for Microservices, Containers and Cloud

Zero Trust Security Solution for Microservices, Containers and Cloud

Microservices, containers and cloud are allowing enterprises to build and deploy applications with ever increasing speed. However, security teams have diminishing control and visibility into what is happening with these applications, especially as they become distributed across public, private and hybrid cloud infrastructures. Enabling the business to move fast to the cloud requires rethinking of static, perimeter-centric security and moving to a Zero Trust security model.

The Zero Trust security model is particularly effective for cloud-based applications because it is based on the principle that everything in an application is accessible to everyone and could be compromised at any time. Deploying a Zero Trust model puts the security team back in control of applications by making security automated, scalable and infrastructure agnostic.

Aporeto provides:

- **Uniform security decoupled from the underlying infrastructure**
- **Workload isolation without changing the network**
- **Threat detection and vulnerability management across the entire stack**
- **Granular API access control for microservices without writing code**
- **Out-of- the-box identity management for microservices**

Aporeto Overview

Aporeto is a Zero Trust security solution for microservices, containers and cloud that uses identity context, vulnerability data, threat monitoring and behavior analysis to build and enforce authentication, authorization and encryption policies for applications. The Aporeto security solution provides critical capabilities required for secure inter-network microservices and cloud applications across network security, API-level access control, runtime threat detection and identity management. These security capabilities are powered by the Aporeto application identity, a multi-attribute contextual identity for any application component created and managed by the Aporeto platform. Unique identities for each application resource allow Aporeto to automatically create custom protection policies and enforce security at a granular process level regardless of where the application runs. At runtime, the addition of behavioral and vulnerability data enriches the resource identity to create dynamic security visibility and protection capability.

"Aporeto is accelerating our expansion to the cloud. With Aporeto, we can secure our Linux workloads on any infrastructure with end-to-end encryption and have a path for modernizing with a security layer that is future-proofed."

Alec Chattaway

Director of Cloud Infrastructure Operations

Informatica

Powered by Application Identity

Contextual identity automatically created for every service

Each time a resource – which can be a container, VM, process, or external service – attempts to access another resource, a userland process that resides on each host, automatically creates application identity which travels along with the I/O request. The application identity includes information such as:

- **User-ID as verified by authentication**
- **Network address of requester**
- **What service or resource is being accessed**
- **Metadata from Linux processes, Dockerfiles, Docker containers, Kubernetes labels, etc.**
- **Threat, vulnerability and risk scoring**
- **Behavior from past history running in the environment**

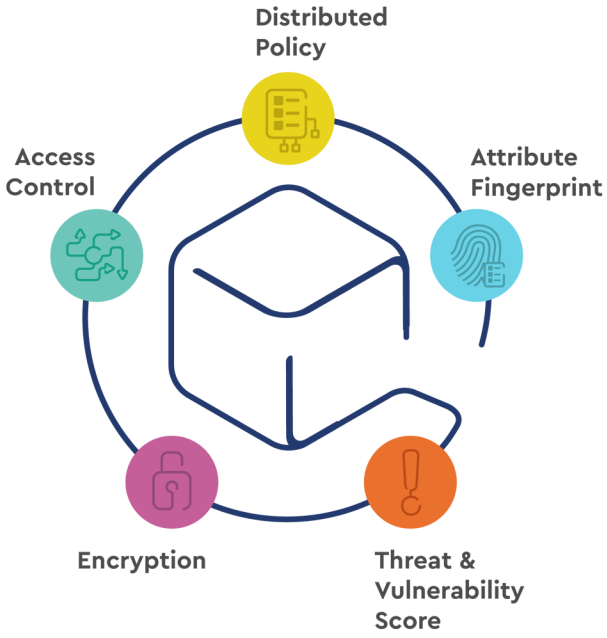
Application identities are hashed and cryptographically signed by Aporeto, to ensure they are genuine and cannot be tampered with. Each application identity is registered and granted a signed certificate to create a "chain of trust".

Distributed security enforcement

An Aporeto security policy controls what a resource can do within the system. Aporeto automatically generates security policies for all resources based on their unique application identity. To refine the security of the application, security policies can be easily inspected and edited. If encryption of data in flight is specified in a security policy, Aporeto automatically encrypts the traffic with no changes required for source code and no key management required.

Security visibility and orchestration

During runtime, Aporeto orchestrates authentication, authorization and encryption for all application resources. All access and behavior to the resource is controlled via policy. System level run-time protection is achieved through inspection of all communication, and if suspicious behavior is found – an alert is issued or a policy action is taken. Automated remediation can be orchestrated through a variety of actions like resource quarantine or container snapshot. Vulnerability and behavioral data is fed back into the resource identity to enrich the identity profile and dynamically influence policy. Cloud-native security automation and orchestration is achieved without writing code or changing the network.



The Aporeto Security Platform

The heart of the Aporeto platform is the Aporeto Security Orchestrator, which includes the automated application identity management infrastructure and the policy engine for defining and operating the policy that is distributed to all of the individual workloads. Powerful APIs allow the Aporeto platform to integrate seamlessly into the entire infrastructure, from CI/CD pipeline to user Single Sign-on to security operations center incident reponse.

The Aporeto Enforcer is deployed as either a container or as an enforcement node on an individual host or virtual machine. Any workload instrumented with the Enforcer and working in conjunction with the Orchestrator, is enabled with automated issuance and management of security policy.

Key Features

Microservices & API Security

- Zero touch service-to-service authentication, authorization & encryption
- Uniform API access control policy across services in public or private cloud
- Composite user and app identity policy enforcement
- CI/CD, VA integration for rich contextual service identity

Network Security

- Network micro-segmentation and workload isolation, reducing compliance scope
- Protection against malicious application discovery
- Automated flow, telemetry logging
- Transparent encryption offloaded from application

Identity Management

- Automated service identity creation, validation, attestation, and assignment
- User identity & Single Sign-on integration
- PKI infrastructure for microservices
- Certificate issuance, verification, rotation, and revocation
- Secrets management

Threat & Vuln Management

- Continuous vulnerability analysis of container images
- Runtime threat detection and protection based on behavioral analysis
- Advanced analytics and correlation of identity, network and application context
- Integration into SecOps workflows (SIEM, SOAR, ITSM)

Use Cases Powered by Aporeto

Workload Isolation for Compliance and Security

Aporeto efficiently segments and isolates workloads of any type in any environment for stronger security and simpler regulatory compliance. A workload may be an entire server, a VM, a classical n-tier application, a container, a microservice, and an OS process or a serverless function. Using persistent & attested application identity coupled with distributed policy enforcement, Aporeto protects and controls assets across multi-cluster or multi-cloud environments while providing coherent visibility into their operations. Aporeto's approach to workload micro-segmentation and isolation offloads encryption from applications, abstracts away infrastructure complexity, does not require any complex network operations or firewall rule permutations, and even works on top of flat networks.

Threat Detection & Remediation

Aporeto provides real-time threat detection and container vulnerability management across the entire microservices technology stack by analyzing and correlating behavior from network, identity, vulnerability and application context. Aporeto embeds vulnerability information about workloads running in the environment into application identities through scanning container images or importing vulnerability data from market-leading vulnerability assessment platforms. Aporeto also monitors runtime behavior by analyzing workload network communication patterns and lower-level system call activity against security benchmarks and observed baselines. Out-of-the-box and custom orchestration policies provide automated response action against specific CVEs or threat behaviors to quarantine containers, stop communications, and snapshot them for further analysis. Threat monitoring logs and alerts may be readily integrated with external SIEM, SOAR, or ITSM system APIs for better integration into enterprise-wide security operations and incident response programs.

API & Microservices Access Control

Aporeto transparently secures enterprise applications by authenticating and authorizing user-to-service, service-to-service, and service-to-external-resource API and microservice interactions. Aporeto provides this granular control and visibility whether your enterprise is using new microservices architectures or simple API interactions in brownfield environments. By implementing this standards-based authentication and authorization independently of the applications' business logic, Aporeto captures originating user and service context and identity to enforce authaorization policies. To enable this unique, high-value functionality, Aporeto provides complete PKI and identity management infrastructure for applications, saving developers' time from the onerous and error prone tasks of designing in security features into the application logic.

For more information, visit:
www.aporeto.com