Aporeto Zero Trust Cloud Security Platform

CLOUD NETWORK SECURITY ACROSS ANY INFRASTRUCTURE AND ANY WORKLOAD AT SCALE

Aporeto provides comprehensive cloud network security through microsegmentation and secure access to applications and infrastructure using workload identity rather than IP addresses. Aporeto's use of identity decouples security from the underlying infrastructure and enables network security policies to now be managed up the stack at the application level. With the Aporeto SaaS-based platform, security is implemented at layers L3-L7 with end-to-end authentication, authorization and optional encryption for an inherent Zero Trust security posture. Security policies remain portable and persistent no matter where they reside across any hybrid or public-cloud infrastructure and any workload including VMs, containers, Kubernetes, serverless or service mesh at any scale.

USE CASES

Distributed Firewall
Microsegmentation using workload identity not IP addresses to control E-W lateral movement

Kubernetes Network Security
Easily deploy distributed policies for multi-cluster and cloud environments at scale

Cloud Privileged Access Management
Eliminate SSH key management with just-in-time user access to infrastructure

Identity-Aware Proxy
Eliminate VPNs with SSO secure access to web apps

DIFFERENTIATION

- Define policy once and deploy across your entire infrastructure
- Authorize, track and audit user activity for easy proof of compliance
- Accelerate DevOps app deployment with baked in security policy-as-code

COMPONENTS OF THE APORETO PLATFORM

Aporeto Security Orchestrator - functions as the control panel and is responsible for application identity management and the policy engine. From here policies are distributed to all of the individual workloads in addition to the tasks of data collection and aggregation, analytics and incident response. The Orchestrator has powerful APIs that allow the Aporeto platform to integrate seamlessly with a broad set of enterprise platforms into the entire infrastructure, from CI/CD pipeline to user single sign-on (SSO) to security operations center.

Aporeto Enforcer - is deployed as either a container or as an enforcement node on an individual host or virtual machine (VM). Any workload outfitted with the Enforcer and working in conjunction with the Orchestrator, is enabled with automated issuance and management of security policy at different layers of the stack. Enforcers implement functions that include: threat monitoring, transparent network security, API authorization and authentication.
ABOUT APORETO

Aporeto, the leader in Zero Trust Cloud Security, provides comprehensive cloud network security through microsegmentation and secure access to applications and infrastructure using application identity rather than IP addresses. The Aporeto SaaS-based platform allows you to build and enforce distributed identity-based policies enabling authentication, authorization, and encryption across all workloads including VMs, containers, Kubernetes, serverless, service mesh environments. Aporeto protects against attacks and enables complete visualization, simplified proof of compliance, centralized management, and accelerated app migration. Aporeto future proofs your infrastructure, delivering stronger cloud security, operational agility to accelerate digital transformation, and better ROI for any infrastructure at any scale. Learn more about Aporeto by visiting AWS Marketplace.

WHERE APORETO FITS

KEY BENEFITS

Uniform Security Across All Hybrid & AWS Cloud Infrastructure
Aporeto's approach to cloud security is based on a Zero Trust security model. Aporeto automates security with policy-as-code and monitors and protects applications at L3 - L7 through whitelisting, allowing only authorized and authenticated interactions to occur. Policies remain portable and persistent across applications and workloads no matter where they reside in your infrastructure.

Simpler Operations - Reduce Network Complexity & Compliance Scope
Aporeto eliminates the constraints from traditional Firewalls, VPNs, Cloud Security Groups, SDNs and virtual appliances. All policies are managed for your entire cloud environment from a central console. Network segmentation and workload isolation helps reduce compliance scope. Easily meet regulatory compliance requirements such as HIPAA, PCI DSS, GDPR, SOC 2, NIST and FedRAMP as well as data encryption requirements with end-to-end visibility for easy proof of compliance in audits.

Better ROI - Save Developers Time and Reduce Overall CapEx and OpEx
Aporeto bridges the DevOps divide between network, infrastructure and security teams by offering a security automation platform that operates in context with the application and independent of the drag of heterogeneous infrastructure. DevOps teams can accelerate deployment with security and compliance already baked into the application policies. By using one tool to reduce overall security infrastructure complexity, security teams can remain agile experiencing significant ROI cost savings.

© Copyright 2019 Aporeto. All rights reserved. Other brand names mentioned herein are for identification purposes only and may be the trademarks of their holder(s).