influxdata®

AN INFLUXDATA CASE STUDY

Securing Cloud-Native Workloads with Aporeto and InfluxDB

Don Chouinard
Product Marketing Lead, Aporeto
Bernard Van De Walle
Engineering/Product, Aporeto

Aporeto

JANUARY 2018

Company in brief

Based in San Jose (California), Aporeto strengthens security and simplifies operations for enterprises with cloud-native and legacy applications in hybrid and multi-cloud environments.

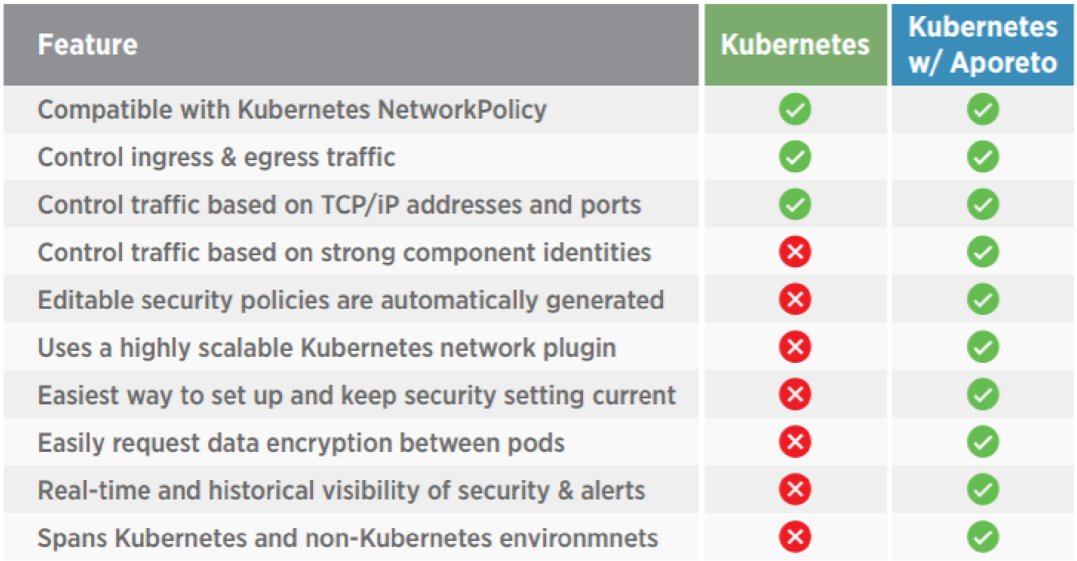
Aporeto is a Kubernetes network plugin that enforces the security policies specified by Kubernetes NetworkPolicy resources in a scalable way. It goes further to extend and strengthen the security of Kubernetes workloads with automatically generated trusted identities for workloads; automated creation of editable security policies; distributed enforcement for scalability; security policies that request AES-256 encryption; real-time and historical visibility of security; alerts for anomalous behaviors; and reduced complexity for DevSecOps whose applications can span Kubernetes and non-Kubernetes environments.

Aporeto believes the best security model enables your developers to move fast with microservices and untethers your team from “walled” network infrastructure. Aporeto is committed to building trusted relationships with people and between applications.

Case overview

Aporeto wanted to overcome the problems inherent in traditional perimeter security to provide an unsurpassed security posture for enterprises. In migrating legacy and cloud-native workloads to hybrid and multi-cloud infrastructures, enterprises were straining traditional security practices to the breaking point.

Aporeto’s solution secures cloud-native workloads without complex network gymnastics by attaching security to individual application components, through a new security model that uses InfluxDB to ingest and store longitudinal data for visualization and troubleshooting. InfluxDB secures the history of all flows and workload events for Aporeto’s solution, thereby providing visibility into security metrics and events and delivering improved security for Kubernetes and other cloud environments.



Feature	Kubernetes	Kubernetes w/ Aporeto
Compatible with Kubernetes NetworkPolicy	✓	✓
Control ingress & egress traffic	✓	✓
Control traffic based on TCP/iP addresses and ports	✓	✓
Control traffic based on strong component identities	✗	✓
Editable security policies are automatically generated	✗	✓
Uses a highly scalable Kubernetes network plugin	✗	✓
Easiest way to set up and keep security setting current	✗	✓
Easily request data encryption between pods	✗	✓
Real-time and historical visibility of security & alerts	✗	✓
Spans Kubernetes and non-Kubernetes environmnets	✗	✓

> *“With our product, which uses InfluxDB, people can achieve much stronger security than they otherwise would. The operations become simpler rather than more difficult. When this is used, no changes need to be made to the source code.”*
>
> ***Don Chouinard,*** *product marketing lead*

The business problem

Aporeto wanted to meet enterprises’ need to secure their hybrid cloud and multi-cloud environments. Adoption of the cloud, microservices, and containers in modern IT architectures has created new security concerns, for which existing security methods and tools are inadequate as they were designed for working on-prem with monoliths at a slow pace. Trying to secure all these dynamic application components using traditional IP address range rules was not useful. As architectures become cloud-native, and as they break apart and decompose the monolith, a new security model is needed where protection — rather than being tied to IP address ranges — is instead tied to the application components themselves. Such a model would work consistently across sites and clouds, provide real-time and historical visibility, and decouple security from the network infrastructure. It would follow the application components even in large numbers, anywhere anytime. Based on that model, Aporeto set out to create a solution that would meet DevSecOps' cloud-native security requirements:

- No IP address range gymnastics (over 50% of rules could be obsolete)
- Protect application components (assume zero internal or external trust)
- One consistent model (span sites and clouds)
- No changes to source code (to avoid slowing down developers and innovation)
- Codify security (integrate into customers' CI/CD toolset)
- Auto-generate Security Policies (observe running application)
- Clear security visibility (real-time & historical for debug)
- Zero touch end-end encryption (applied with a security rule)

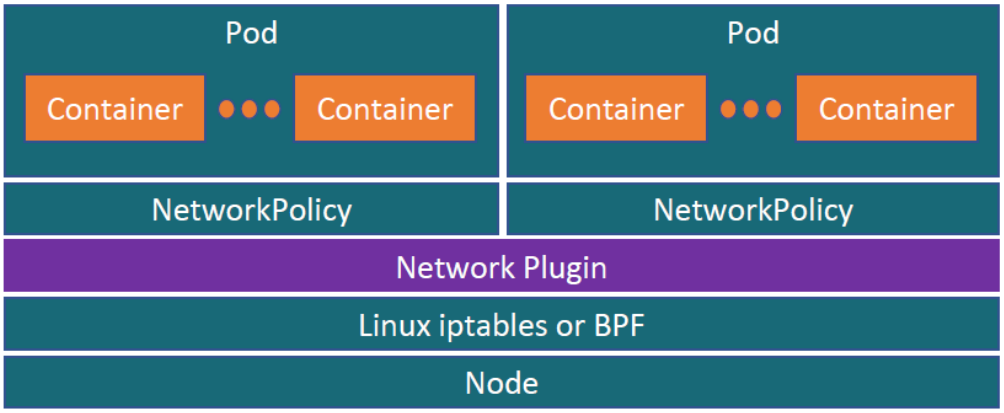
Aporeto realized that in today's highly competitive world, developers need to be able to just plow forward, developing new capabilities that fuel the business and its success factors — not be concerned with having to pepper code throughout everything they're doing in order to address security.

Technical journey

> *"Imagine if security were just attached to the application components. All of the problems go away. Now, security is always current, it's easy to keep up, security follows the application components wherever they run, however many of them there might be at any given time."*
>
> ***Don Chouinard,*** *product marketing lead*

To solve its business problem, Aporeto needed to provide an alternative to IP Address based Security, which does not work due to numerable unintended access routes, zero visibility, and the difficulty of figuring out which IP-address rules need to be changed. Instead, Aporeto sought a solution that provides fine-grained security for each application component, wherever it runs. This would provide stronger security that is always current, provide no unintended access paths, would be easy to administer, and would require zero changes to code.

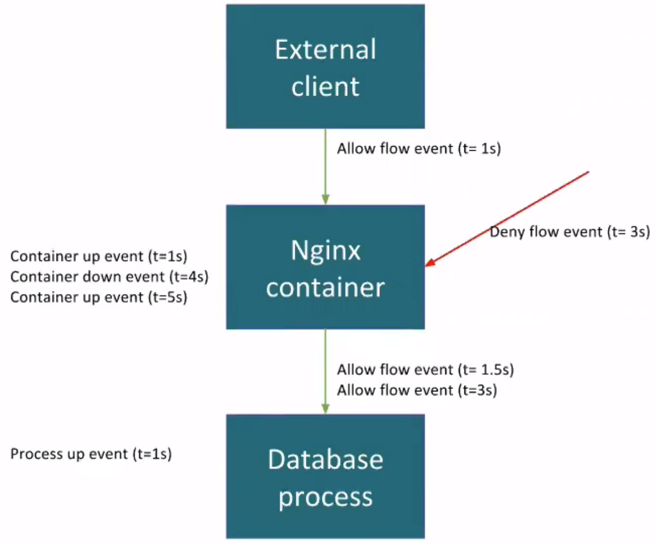
Kubernetes Network Access Control



Yet monitoring and enforcing every single event into your cloud or cluster (for example, Kubernetes cluster) generates a lot of different events. So Aporeto needed a time series database to monitor and record those events, and then replay them for auditing and logging purposes. They sought to record two types of events:

- Process/container events (containers going up or down)
- Flow/connection events between different components (the web client generates an HTTP request to the frontend at a specific moment, which also generates a request to the database in backend, with each flow event being accepted or rejected and generating a full point in time into the time series database).

Why a Time Series Database?



Aporeto needed to record all these events to show what happened in a given cluster over a given period as well as to see which container or processing unit was trying to connect to which other processing units. Every new TCP or UDP connection occurring would generate an event and push it to the time series database. Given the critical role of such a database to actualize Aporeto's solution, the database had to meet certain requirements.

The solution

> *"When we decided to use a TSDB to do this, the biggest requirement for us was to have a very high ingestion rate. By the end of the day, we chose InfluxDB, mainly because it was very easy to set up in HA, and also because it was written in Go."*
>
> ***Bernard Van De Walle,*** *engineer*

Why InfluxDB?

Aporeto's selection criteria for a metrics database were:

- Time series with fast ingestion rate
- High Availability
- Easy to use

Based on these criteria, and after considering Cassandra, MongoDB, HBase, KairosDB, and OpenTSDB, Aporeto chose InfluxDB because of its:

- High Availability model
- Performance
- Low complexity
- Licensing model
- Extensibility
- As-a-service and on-prem editions

Leveraging the properties of InfluxDB for its solution, Aporeto delivers:

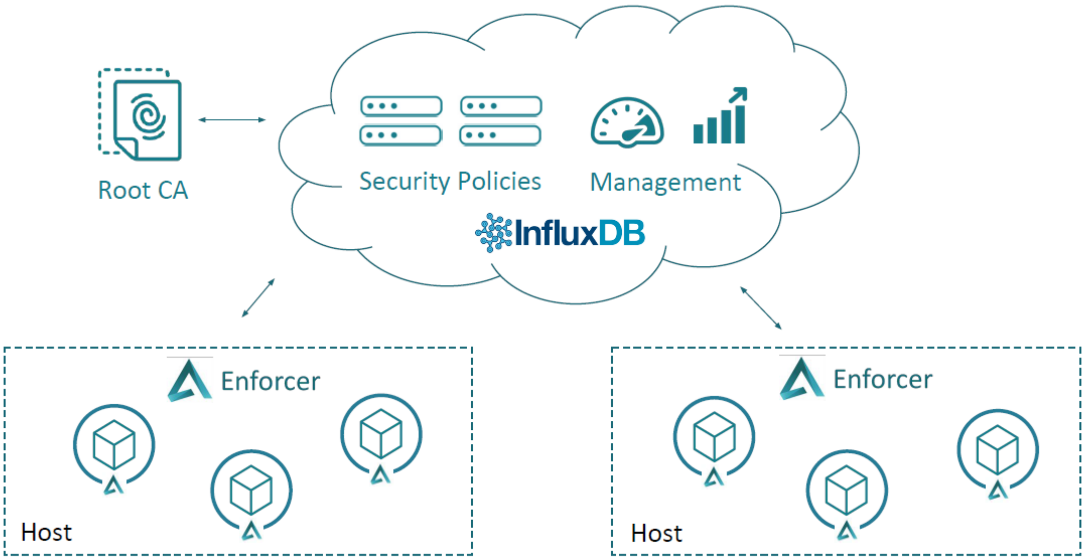
- Security based on identities of application components
- Authorization process enforced by Aporeto enforcer + access policies
- One consistent security model

- Fine-grained security for individual services
- Access based on multiple factors beyond user ID
- Security solution that's easy to administer and keep current
- Unrivaled security posture visibility

Aporeto's solution decouples security from the source code and underlying network infrastructure. Because security policies are associated with workload identities rather than being implemented with a patchwork of network settings and IP-oriented rules, they are more natural for DevSecOps to use and always remain current, even for large dynamic runtime environments where workloads are frequently spinning up, shutting down and moving. Protecting individual application components with fine-grained, automatically generated security policies protects organizations from security breaches that originate from within due to malicious intent or human errors. Aporeto provides one consistent security model that works uniformly across data centers, public clouds, private clouds, availability zones, VMs, and bare-metal servers that may be using any infrastructure or orchestrators, without requiring changes to source code.

Technical architecture

InfluxDB Monitors and Records Aporeto's Time-Stamped Security Events

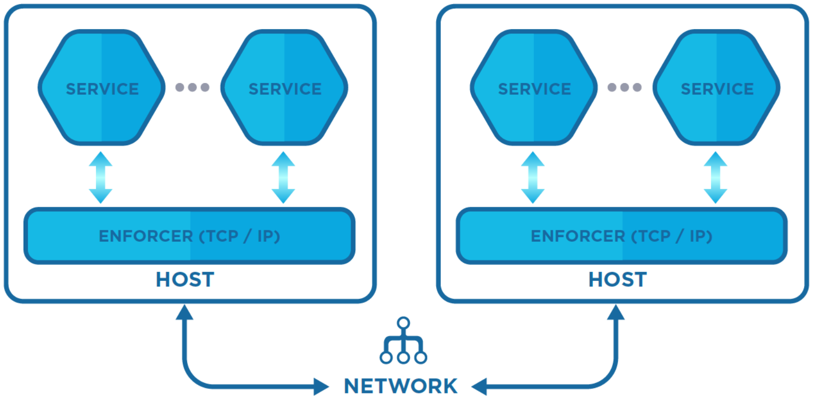


> *“InfluxDB is absolutely central to the Aporeto solution...It gives us the awesome performance profile that’s required for the huge-scale environments that our customers are putting us to use in, and the complexity is very low.”*
>
> ***Don Chouinard,*** *product marketing lead*

Aporeto uniquely identifies each application component, then uses enforcers and auto-generated security policies:

- The Aporeto Enforcer is a proxy, sitting in front of the TCP/IP services, and is easy to deploy onto each host under your control — be it physical, virtual, on-prem or in a cloud.
- The Enforcer oversees and optionally blocks traffic per the security policies.
- Using the Zero Trust Model, no services are permitted to communicate with any other services or access any resources unless explicitly allowed by an Authorization Policy. This changes the security perimeter from being around the application to being around each service and resource, providing fine-grained security and addressing the “M&M” problem (the land-and-expand attack where hackers get past the hard outer shell and then gorge on the “gooey” inner center to get all the privileged credentials they’re seeking).
- Using artificial intelligence methods, Aporeto makes establishing Authorization Policies easy and intuitive, enabling new application components to have the same level of security around them as older components, so that the overall application is protected. Security policies are auto-generated as the enforcer observes the running application. Because they are patterned after human language, security policies are easy to understand and edit.

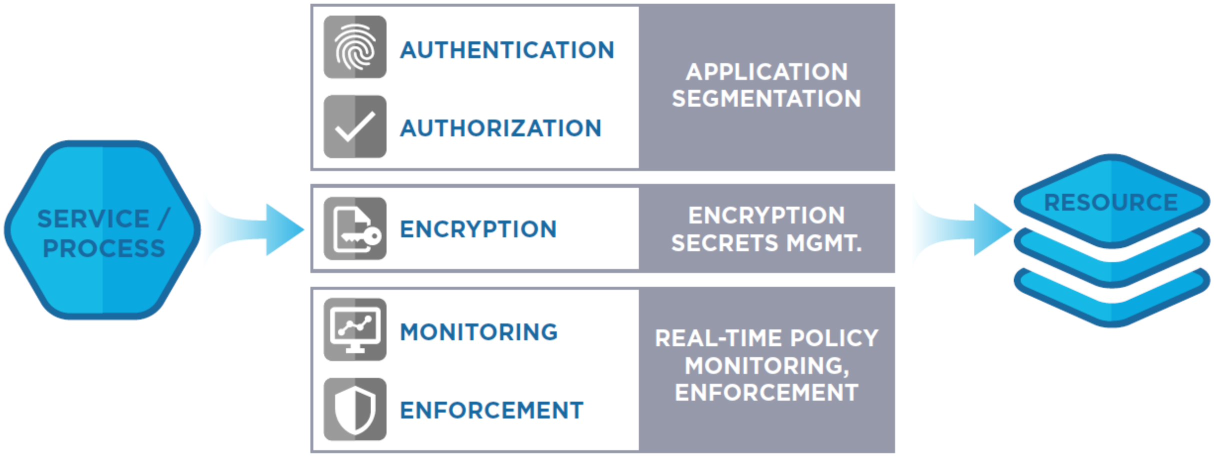
Aporeto Enforcer must explicitly allow all interactions within the distributed application



- Each of the enforcers sends detailed monitoring information to a centralized, scalable analytics engine (InfluxDB time series database) — in the cloud — that provides analysis, alerting, and application security dashboards.
- InfluxDB is queried with all the events that all the enforcers are pushing to it, and displays the metrics and flows for the chosen time intervals.

Aporeto's architecture enables it to provide great dashboards, good visibility into application components and their security, and advanced analytics to protect against potential events in the horizon that may not yet be visible. This clear visibility of the real-time and historical security posture is easy to understand and maintain, regardless of where workloads are running. Just by creating a security policy, workload traffic can be encrypted by Aporeto with AES-256 encryption with no key management burden.

Services Provided by the Aporeto Solution



Results

> *"A lot of people have no idea what's going on in Kubernetes' cluster or Docker set of hosts or containers. With this solution, what you can do with InfluxDB is push all that information and get inside, and then apply security rules on top of it."*
>
> ***Bernard Van De Walle,*** *engineer*

With Aporeto, security can now be codified and built into the CI/CD pipeline. The Aporeto solution was designed with cloud workloads in mind: it automatically enforces sound security policies, solves the "M&M" problem, and allows enterprises to leverage open source without opening themselves up to unnecessary security risks.

The Aporeto solution enables enterprises to:

- Confidently, securely and effectively leverage hybrid cloud resources to meet business objectives
- Move beyond the flawed perimeter security model to the state-of-the-art Zero Trust Model recommended by National Institute of Standards and Technology (NIST), which is ideal for cloud workloads

Further, the insufficient role-based access control (RBAC) model is supplemented with contextual information to deliver the highly effective Attribute Based Access Control (ABAC) model, which NIST also recommends.

By delivering stronger security, simpler operations, and zero-touch for developers, Aporeto's cloud-native solution bridges the "new" and "old" IT worlds, creating pathways to growth that start wherever enterprises are in their cloud journey.

With Aporeto, the velocity of innovation is no longer impacted by security, and the historical view made possible — which provides the ability to go back in time for forensic purposes — reveals what is happening with an enterprise's security posture at all points in time. Using InfluxDB, Aporeto is fulfilling its promise of "Security Transcending Clouds."

About InfluxData

InfluxData is the creator of InfluxDB, the leading time series platform. We empower developers and organizations, such as Cisco, IBM, Lego, Siemens, and Tesla, to build transformative IoT, analytics and monitoring applications. Our technology is purpose-built to handle the massive volumes of time-stamped data produced by sensors, applications and computer infrastructure. Easy to start and scale, InfluxDB gives developers time to focus on the features and functionalities that give their apps a competitive edge. InfluxData is headquartered in San Francisco, with a workforce distributed throughout the U.S. and across Europe. For more information, visit influxdata.com and follow us @InfluxDB.