Meta Networks

Case Study

Via Takes the Network to the Cloud with Zero-Trust NaaS

> With Meta NaaS, we are centrally managing a zero-trust network that covers all of our applications and data, and our employees, contractors and customers. We're growing quickly and the solution is robust and flexible enough to grow with us - it's easy to onboard new customers and assure the granular security that we need."
>
> Amir Mehler, Cross-Tech TL, Via Transportation, Inc.

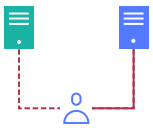
Via is a New York-based company that is changing the way people get around cities by building a Ride Sharing platform. Via is on-demand transit on a mass scale; it's smart transportation that's friendly to our planet. The company operates its own shared ride service in New York, Chicago, Washington DC, London, Berlin and Amsterdam. Via licenses its technology to companies building transit systems in Paris, Sydney, and Tokyo, and is expanding rapidly to other locations around the world.

Challenges of a Growing, Cloud-Native Company

Via takes the same innovative approach to IT as it does to ride-sharing. The company is completely cloud-native and has a widely distributed workforce with more than 400 employees and contractors including developers, DevOps, data analysts, sales reps, customer success, support and QA. Rather than build a legacy-style site-based WAN, Via's tech team provided users with direct access to cloud resources using OpenVPN. Their vision was a zero-trust, user-centric network security architecture that would be enforced consistently whether users were at the office or on the road.

A second group of users was Via's partners - transportation operators based in different countries and cities. This group required more controlled access to specific portions of Via's software platform to manage rideshares.

Providing secure access to these two groups presented Via with several challenges:



Segmenting and securing access

Each employee, contractor, and customer role required access to a limited subset of Via's cloud-based applications. Managing the network segments and access rules became increasingly difficult as the company grew, creating a potential security risk as well as operational overhead.

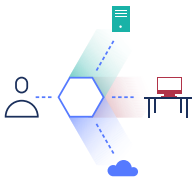
Complex onboarding

Installing and using the OpenVPN client was a real issue for partners. Via's team had to step in and help with configuration and troubleshooting, which wasn't sustainable because they didn't manage the devices. As a result, fully onboarding a new customer could take weeks, presenting a real obstacle to Via's ability to rapidly expand its business into new cities.

Via's team looked for a better solution than their homegrown network, that would provide granular, zero-trust security, and allow it to scale up and support the company's growth. They preferred a managed service so they would be certain that their security was in expert hands, while they focused on their own line of business.

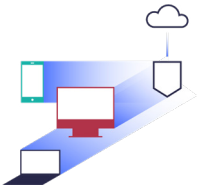
Solution

Via's team deployed Meta NaaS™ (Network-as-a-Service) as the secure platform for managing access to their cloud infrastructure.



Always-On User Experience for Employees

Via employees with managed devices connect using the Meta client, which replaced OpenVPN, and are authenticated via Okta and a certificate. Once they connect, they continue to work normally using any type of desktop or web-based application, and all traffic is protected.

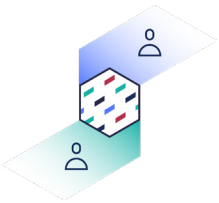


Browser-Based User Experience for Customers

Via contractors and customers use MetaConnect, a browser-based access solution. It requires no installation or setup, so it's optimal for devices that Via doesn't manage.

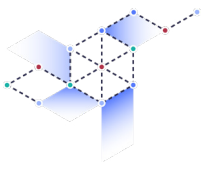
Identity-Based Access Policies

In minutes, Via's administrators onboard new users and assign granular access policies depending on their role, for example, to the production environment, the development environment, analytic stores, etc. The platform is fully integrated with Okta.



Software-Defined Perimeter

Users are protected by a software-defined perimeter. Once they connect, they can see only the applications and network resources that their policy allows - everything else is invisible. All access is monitored and logged.

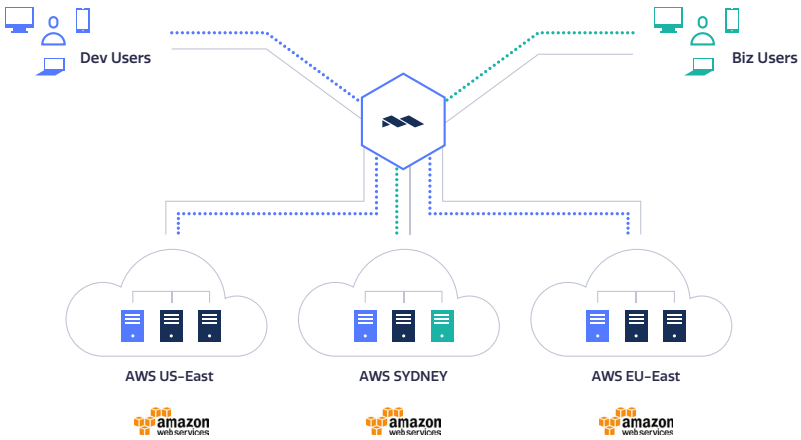


Cloud-Native Network

In addition to user access, Via used Meta's NaaS to connect their many cloud deployments to each other, replacing the site-to-site VPN and enabling convenient, central management of all of their networking.

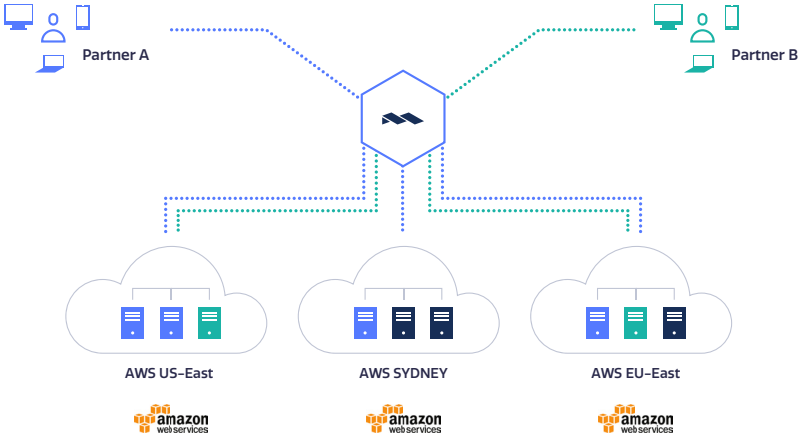
Via Users

Via employees access network resources located in different AWS regions as well as customer sites in specific subnets. Access is set by policy.

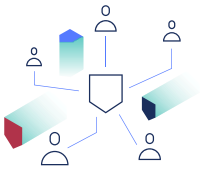


Via Contractors / Partners – MetaConnect

Via partners and contractors access dedicated Via web services in different AWS regions, using a clientless, browser-based solution.



Benefits

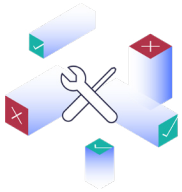


Enhanced security

Via's network is now protected by a software-defined perimeter per-user that is dynamically enforced, verified and logged. Policies effectively restrict access for employees, customers and contractors to exactly what is required.

Rapid customer onboarding

New customers and their users can be onboarded within minutes. Administrators import a new user into the Admin console, add him/her to a policy group and then send the user a link to the MetaConnect portal.



Efficient, simplified cloud network management.

Instead of spending time on firewall configurations to microsegment networks in Amazon, administrators can onboard a VPC or region in minutes. Such tasks are fully automated using the Meta API and are an integrated part of DevOps.

"With Meta NaaS, we are centrally managing a zero-trust network that covers all of our applications and data, and our employees, contractors and customers. We're growing quickly and the solution is robust and flexible enough to grow with us - it's easy to onboard new customers and assure the granular security that we need."

Amir Mehler, Cross-Tech TL, Via Transportation, Inc. VIA

About Meta Networks

With Meta's Network-as-a-Service, you can instantly provide secure remote access to corporate applications and the internet. As applications move to the cloud and employees, contractors and partners are increasingly mobile, companies need a better solution than the conventional, site-centric VPN. Meta NaaS implements the principles of a software-defined perimeter to ensure zero-trust, identity-based access. Leveraging a cloud-native global backbone, it delivers a great user experience along with always-on corporate and internet security. It's fast and simple to deploy and manage, even in complex, hybrid environments. Meta Networks is reinventing the secure enterprise network for the cloud age.

Learn more at metanetworks.com