Accelerating Private Mobile Network Adoption with Alef's Disruptive Approach

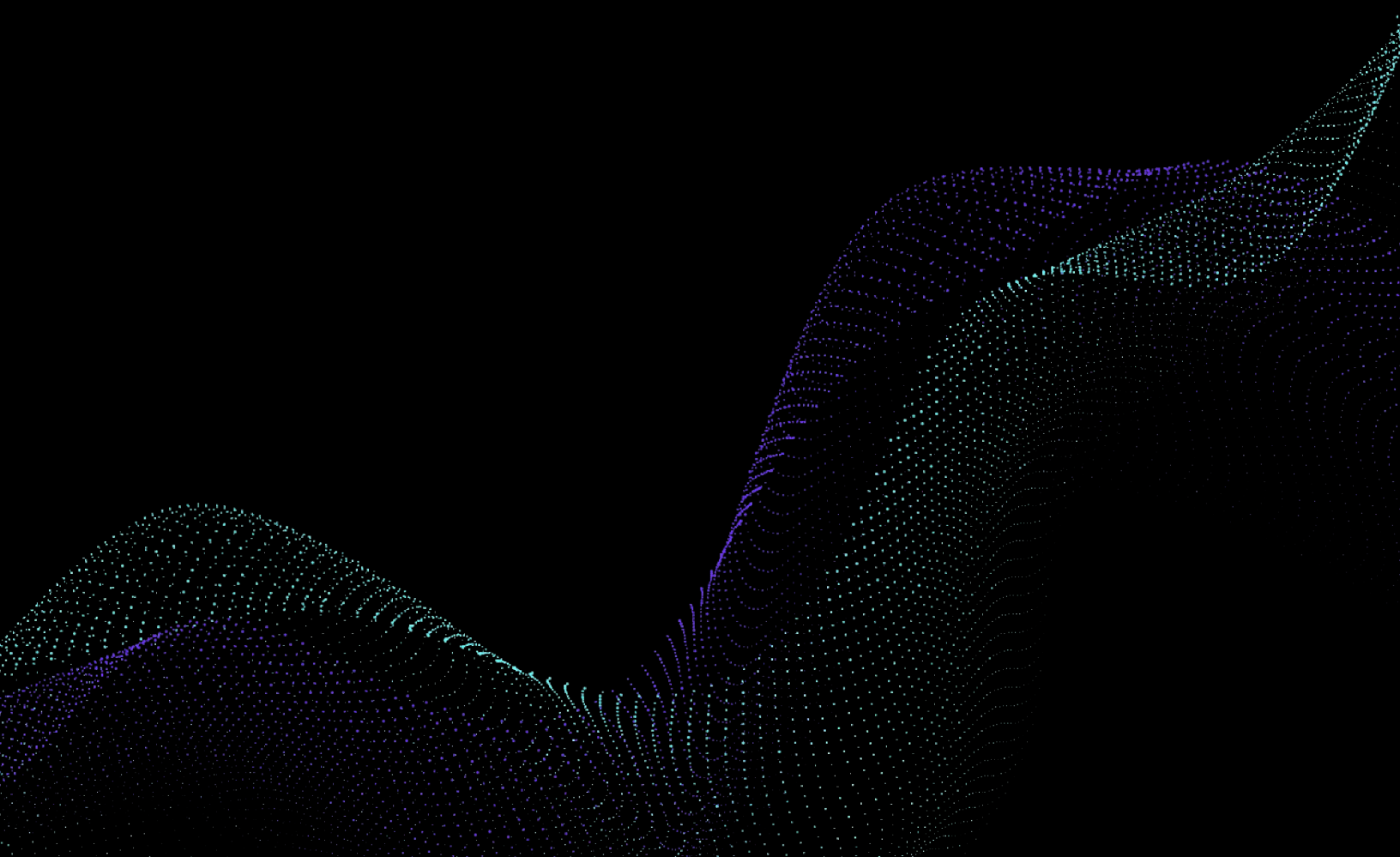


Table of Contents

1.0 Introduction

The growth of digital enterprise applications that require wireless connectivity with predictable performance and broad indoor and outdoor coverage is forcing CIOs to rethink their network strategy. Private 4G & 5G mobile networks are becoming critical to enterprises as they can provide deterministic network performance, uninterrupted mobility, indoor and outdoor communications, high network security, and complete customization and control of their mission-critical data. Private mobile networks allow for improved control over network access, which helps businesses comply with industry regulations and maintain a secure network environment. This allows for more efficient communication and collaboration, accelerating the process of the digital transformation that will integrate the IT and OT systems on top of the same IP network infrastructure.

Many enterprises are hesitant to adopt private mobile networks based on concerns about their benefits, cost of ownership, and complexities to efficiently manage and customize their private mobile networks. These concerns result in two meaningful questions for businesses:

- How can private mobile networks be deployed and controlled as simply as Wi-Fi and integrated with current enterprise IT systems?
- How can enterprises ensure network performance without the cost and complexities of deploying and managing private network equipment on-premises?

This paper will take you through how to navigate these concerns and how to bring down the cost and complexities of private mobile networks with Alef's Edge platform and APIs.

Benefits of Alef's Private Mobile Networks

- Exclusively Enterprise: With an IT-first mindset, not retrofitted carrier products, Alef delivers cohesive, secure, private 4G/5G solutions
- Integrates seamlessly into Enterprise IT & Security systems to ensure consistent device authentication and security policy
- Operates within Enterprise firewalls to ensure data security and privacy
- Designed for reliable performance, resilience, and latency expectations of business-critical applications
- Highly flexible Network APIs to meet any enterprise application needs
- Radio agnostic software to choose best-in-breed vendor to specifically suit current & future needs
- Flexible, transparent, low-cost Mobile Network as a Service with no CAPEX required

2.0 Understanding the Complexities of Deploying a Private Mobile Network

There are three key components in a private 4G or 5G mobile network:

1) The Radio Access Network (RAN), which consists of 4G/5G small cell access points. These access points broadcast signals for private 4G/5G wireless connectivity to mobile devices in the enterprise premises.

2) The 4G/5G mobile network core software, which performs two primary functions: 1) mobile device management, including authentication, registration, and mobility management, and 2) data processing, such as user data packet routing/switching and policy enforcement between mobile devices and applications on the network.

3) The network transport that connects 4G/5G RAN to the corresponding mobile network core.

Though there are a lot of similarities in the components of Wi-Fi and private mobile networks, cellular networks introduce new variables to enterprise IT operations. For instance, cellular and Wi-Fi networks use different approaches to authenticate the identity of a user and device. The two networks have different signaling and data flow architecture, impacting the enterprise network design and ensuring application performance. Additionally, the 4G/5G core network adds many more network functions and programmable capabilities, requiring enterprise IT teams to add new configurations and management processes.

These differences add three primary challenges for enterprises in integrating a private mobile network into their existing processes:

1) Managing a new Identity and Access Management (IAM) system

2) Optimizing network performance and cost of ownership

3) Integrating with existing systems & workflows

2.1 Managing a New Identity and Access Management (IAM) System

Adding a private mobile network to an enterprise can lead to possible duplication of Network Access Control systems for authenticating Wi-Fi and cellular devices. Private mobile networks authenticate and authorize cellular devices based on the SIM/e-SIM identity using a 3GPP-based authentication management function of the mobile network core. In contrast, Wi-Fi networks follow IEEE 802.1x-based Network Access Control (NAC) mechanism that involves a RADIUS server to authenticate the identity of an access client based on a username/password, certificates, or one-time-password. The authentication server interacts with the corporate directory to access the IAM policies. Maintaining two disparate systems for identity management adds complexity in maintaining consistent security policy across the entire network and ensuring uninterrupted mobility as devices move between Wi-Fi and cellular networks.

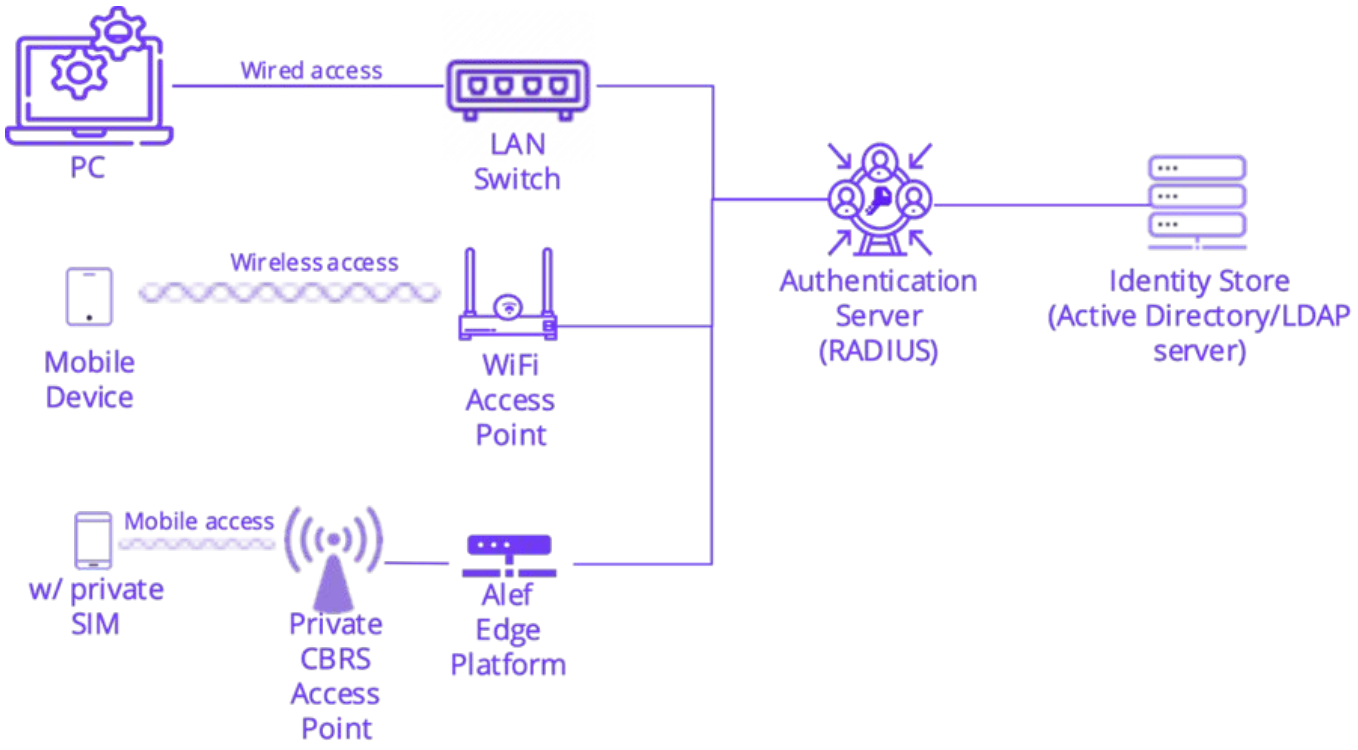
To simplify operations and reduce cost, cellular device authentication and authorization should use the same NAC & IAM system already in use for Ethernet and Wi-Fi networks.

As the use of converged networks grows, additional layers of automated self-acting security, enforced by centralized policies, are needed to defend against proliferating varieties of cyberattacks.

2.1.1 Alef's Solution

Alef provides an Edge Platform that is secure and scalable, allowing businesses to accelerate their digital transformation strategies with real-time analysis and insight. It empowers enterprises to create, customize, and control their own private mobile network, inside their firewall. It provides all significant functions needed in the enterprise network for the mobile devices accessing the Alef-enabled mobile network, making the mobile access technologies just one new type of connection to be managed by the same system already operated by the enterprise. For example, in the picture below, the user/device with a private SIM is added to an existing enterprise, which already connects online with wired PCs and wireless mobile devices via Wi-Fi. The new device connects to the network via a cellular access point (e.g., on CBRS), which connects in turn to an Alef Edge Platform. The Edge Platform uses the same authentication method - the RADIUS protocol that is used for authenticating WiFi access in the enterprise network, sending identity information, to verify network access via the authentication server and identity store, as do the pre-existing device types. The identity store can be either an Active Directory or a Lightweight Directory Access Protocol (LDAP) server, where the IAM and policies associated with the users and devices are managed.

The Edge Platform extends existing security policies and rules provisioning, providing carrier-class security and keeping data within the existing firewalls.



2.2 Optimizing Performance and Cost of Ownership

Private mobile networks can be complex and expensive to configure, manage, and maintain. The first step in building private networks is to make choices that address the design needs of the enterprise. This includes the use cases and the desired applications. Next are the decisions on the customization of networks to serve the application needs, such as latency, throughput, coverage, security, cost, and manageability requirements. This is followed by ensuring that the mobile network is set up to achieve the desired outcomes.

Private 4G and 5G mobile core provide the flexibility to disaggregate control plane (signaling) and user plane (data processing) network functions. This capability allows enterprises to scale signaling and data processing independently. Also, it provides the flexibility to deploy signaling and data processing network functions separately at optimal locations in the network (on-premises, near-edge, far-edge, or in the public cloud) to achieve desired application performance objectives at an optimal cost.

The decision on the placement of the data processing functions on the premises, at the near-edge or far-edge private cloud, or public cloud is critical for achieving their performance objectives. Enterprises must weigh the cost and quality of application performance. On the public cloud, latencies are likely to be higher, and a greater likelihood of its congestion constraining the actual throughput. Shared networks, such as at the cloud and the far-edge, cost less, while on-premise dedicated private networks have the lower latency needed by today's digital automation but cost more.

Furthermore, enterprises need an intelligent way to extend their existing intranet to the edge cloud securely, and control data flows from the near-edge, far-edge, on-premises, or cloud depending on cost and performance trade-offs.

2.2.1 Alef's Solution

Alef uses a distributed fabric of edge cloud (called Edge Points) to host private mobile networks and ensure required QoS including latency is delivered for industry 4.0 applications. Alef's Edge Platform, the key component of its private mobile network solutions, simplifies the deployment and management of edge computing networks, giving businesses more control over their data and reducing costs associated with hardware and infrastructure. With Alef's near-prem private mobile network as a service (MNaaS) solution, there are no on-premises hardware to maintain, no extra power requirements for servers or AC, and no training necessary for IT staff to learn how to manage new equipment. Alef's hosted Private Mobile Edge Platform empowers enterprises to take control of their mobile connectivity and total cost of ownership by not relying on legacy wireless networks. It ensures reliable mobility, robust security, deterministic performance for time sensitive data at the edge, and removes complexity through its suite of APIs.

Alef's hosted Private Mobile Network infrastructure is connected to the enterprise intranet via private links so that the Edge Point becomes a node in the private enterprise intranet. It provides enterprises with access to mobile networks over private connectivity or encrypted virtual links over the internet, allowing subscribers to use their applications and services without purchasing and managing their own mobile infrastructure. A MNaaS enables enterprise customers to deploy 3GPP-based private cellular systems just like they set up a Wi-Fi system. This type of service is becoming increasingly popular as well as more accessible and cost-effective due to the growth of cloud computing technology.

Alef's Private MNaaS:

- Removes CapEx and lowers OpEx
- Scales quickly and easily
- Is vendor-agnostic
- Provides intelligent orchestration of core network functions at the edge
- Offers quick onboarding of devices and IoT sensors inside the firewall

Private MNaaS enables a pay-for-play model, allowing enterprises a subscription service consumption model combined with minimal usage schedules. Alef's Private MNaaS abstracts private cellular network provisioning, mobile network control and management, device activities, and data usage reporting into APIs. This allows enterprises to manage their networks efficiently and cost-effectively and receive industry-standard reliability.

When used with a CBRS-based network, Alef's Private MNaaS is the most cost-efficient way to deploy and operate a private cellular network with deterministic performance.

2.3 Integrating with Existing Systems & Workflows

Private Mobile Networks for the enterprise today need tight integration with application controls and network orchestrations as they become part of distributed IT & OT networks with multiple service providers. Such networks integrate the near and far edges, multiple clouds, and data centers.

The convergence of multiple networks adds to their design and management complexity. The challenge is to seamlessly integrate private mobile networks into existing unified management systems without the burden of manual effort and excessive engineering. Most private network solutions today operate in a silo with their own dedicated GUI-based management system and limited APIs that require telecom expertise. In contrast, enterprises need simple-to-use web developer-friendly private network APIs to complete the integration without overly increasing costs, adding time lags in the deployment of the network, or being so inflexible that they don't adjust to future changes.

Furthermore, the enterprise needs an intuitive and easy-to-use means to control operations after the deployment of the private network. Application developers should be able to request on-demand network resources, monitor the performance of the network and adjust application behavior in real time if the outcomes fall short for individual enterprise applications. To react quickly, developers need APIs to get a visual snapshot view of its performance and act promptly to variances in performance.

Finally, networks need to be future-proof as they evolve rapidly with the fast pace of technological change. They should be able to make incremental changes in the network system, the gamut of applications, and the devices to achieve expected business outcomes.

97% of global IT leaders "agree that successfully executing an API strategy is essential to secure organizations' future revenue and growth." Rapid

2.3.1 Alef's Solution

Alef uses open APIs to provide an abstraction layer that alleviates the intensive work of having developers write code to communicate with each network function of the mobile system, creating an environment where enterprises can build their own mobile network at the edge.

Alef's Edge Platform allows customers to use their APIs to do all the core functions involved in creating and managing a private network in an easy-to-use model. These core functions include creating and modifying sites, creating and modifying connections between a given site and the core, managing SIMs, pulling usage and performance reports, and more. APIs allow easy integration of new functionality into an existing configuration/management console, thereby providing a single pane of glass view. In addition, Alef's APIs enable management of the cellular network from the enterprise customer's existing network management and policy framework and tools such as Identity Access Management (IAM) and Network Access Control (NAC).

On top of the connectivity management, Alef APIs allow enterprises initiate intent requests over the private mobile networks and orchestrate the network resources based on their mobile applications need, making Alef enabled private mobile network an intent based network supporting enterprises' dynamic application requirement in real-time.

Alef's approach is in contrast with other operator provided models that deploy the mobile network as a separate silo with its own 3GPP-based security and access policies. Alef accomplishes this by abstracting as much complexity as possible from the customer, thereby allowing them to manage the mobile network using concepts and terminology with which they are already familiar. Alef's method is also in contrast to other solutions that offer limited or no abstraction and require enterprises to learn the intricacies of cellular technology.

2.3.1.1 What Alef's Enterprise Mobile Connectivity APIs Do

Alef's APIs allow companies to manage their business workflows securely on near-prem edges from within the enterprise IT applications. They can integrate private mobile network capabilities without worrying about external hardware and software maintenance. Alef eliminates the need for a second management system, allowing enterprises to manage their private mobile network from their existing management systems, removing the need for your IT manager to operate two different systems that could cause them to become out of sync. Alef's APIs use industry guidelines and follow a consistent style guide with standardized API status codes, versioning, error handling, etc.

> "Alef's expertise in APIs, building strong developer relationships and solid track record of enabling enterprises' mobile applications with Edge Points serving as the mobile abstraction layer are helping to create the mobile network-as-a-service (MNaaS) market."
>
> VentureBeat

By taking advantage of Alef's APIs, organizations can deploy and manage private mobile networks more easily and cost-effectively.

There are four sets of APIs:

1. Network Setup
2. Account Management
3. SIM Management
4. Reporting

<u>The Network Setup APIs allow users to:</u>

- Create mobile networks
- Get all their orders of creation
- Get network provisioning details
- Update creations
- Cancel creations

<u>The Account Management APIs let users:</u>

- Get account details
- Update account details
- Add customer site address
- Get all customer sites details
- Update customer site
- Delete customer site

The SIM Management APIs provide users the ability to:

- Get all eSIM/SIM details
- Get eSIM/SIM status
- Manage eSIM/SIM status
- Enable eSIM download
- Disable eSIM download

The Reporting API allows users to generate customized reports for user status, time and data usage, connections, and network performance with real-time or historical views. Many filters are available, including time, granularity, and metric type.

3.0 How it All Fits Together
3.1 Alef's Solution Architecture

As businesses increasingly turn to edge computing to improve the performance of their applications and deploy 4G/5G networks, it is playing an essential role in enterprise digital transformations, providing near-real-time data to companies. By enabling data and applications to be processed and stored closer to where they are used, the edge cloud helps eliminate the on-prem data center build-out and operations while maintaining the required latency and other network performance. Data security is enhanced as enterprises own and have total control of the mobile security when Alef Edge Platforms let their own security systems manage mobile devices.. Additionally, the near-prem edge can provide cloud-like scalability and reliability to organizations, ensuring they have the capacity to meet their growing data processing needs.

Alef's service provides three components for an enterprise's private mobile network: Alef Edge Point, Alef Management Services, and Alef Cloud Services.

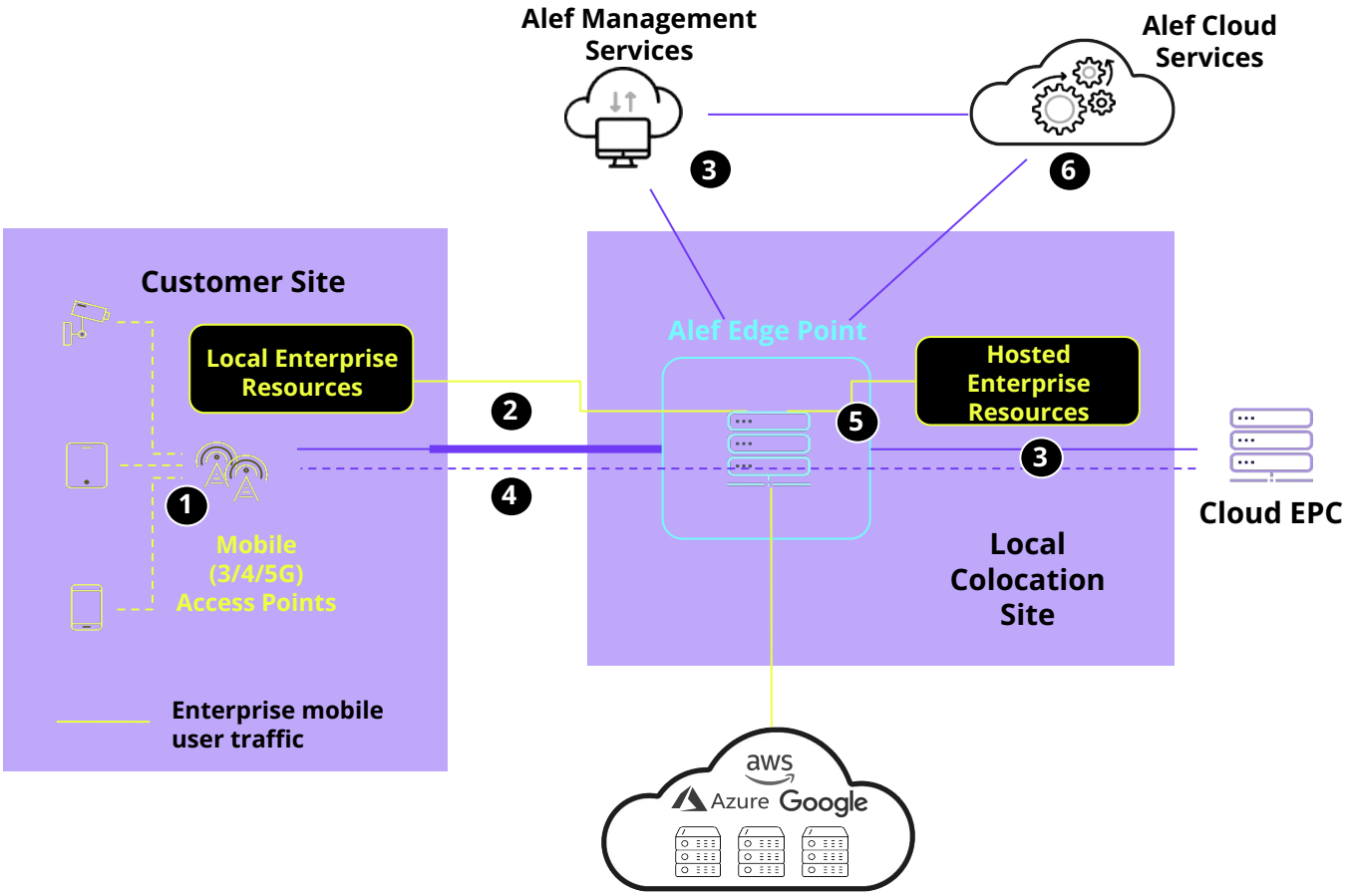
Alef's Edge Point hosts the Alef Edge Platform and software stack, usually in a near-prem site. Alef deploys Edge Points in a geographically distributed manner across many co-located facilities that are easy to reach by many network carriers, enabling the Edge platform to deliver mobile device user traffic directly to the enterprise network. It is a nearby Point of Presence (POP) that is usually located near the customer site to provide the low latency connectivity required by many enterprise applications. The Edge Point provides seamless mobility within a mobile network by allowing the enterprises' mobile devices to roam between access points while fixed to the same Alef Edge Platform that processes user plane data from mobile devices, providing a superior user connectivity experience.

The Edge Platform breaks out mobile user traffic in one of three directions: the enterprise private network, to customer resources at the edge colo, or to customer resources in public clouds. It communicates with the mobile core, forwarding control plane traffic for registration, authentication, authorization, mobility hand-off, and other session management signaling; with Alef Management Services, forwarding usage data for reporting and billing; and with Alef Cloud Services, letting customers provision, monitor, and manage their network.

Alef Management Services communicates with all edge points to achieve session management, accounting, and other management plane functions, providing the management function of monitoring service and proxy service.

Alef Cloud Services hosts the front and back end of the developer portal, manages subscriptions of Alef services, hosts customer lifecycle services such as license management, ordering, account management, and billing, and exposes customer-facing APIs. Customers provision, monitor, and manage their mobile network as needed via the Alef Cloud Services API.

3.0 How it All Fits Together
3.1 Alef's Solution Architecture (Continued)



Here is how different components come together to enable secure and high-performance Private Mobile Network for enterprise:

- Mobile devices communicate over the air with mobile access points (APs).
- Mobile APs send traffic to the nearest Alef Edge point. The connectivity between the enterprise network and the nearest Alef Edge points are provided by a dedicated managed link such as fiber (assuming the Edge Point shares a colo location with enterprise network equipment), MPLS, EVPN, or any other supported secure medium.
- Alef Edge Point forward control plane traffic to the mobile core and report usage data to Alef Management Services.
- Mobile core communicates with the mobile AP via the Alef Edge Point, authenticating and managing the user session in real time.
- Alef Edge Platform breaks out the mobile user traffic, which are routed onwards to its destination ensuring the network performance required by the mobile applications.

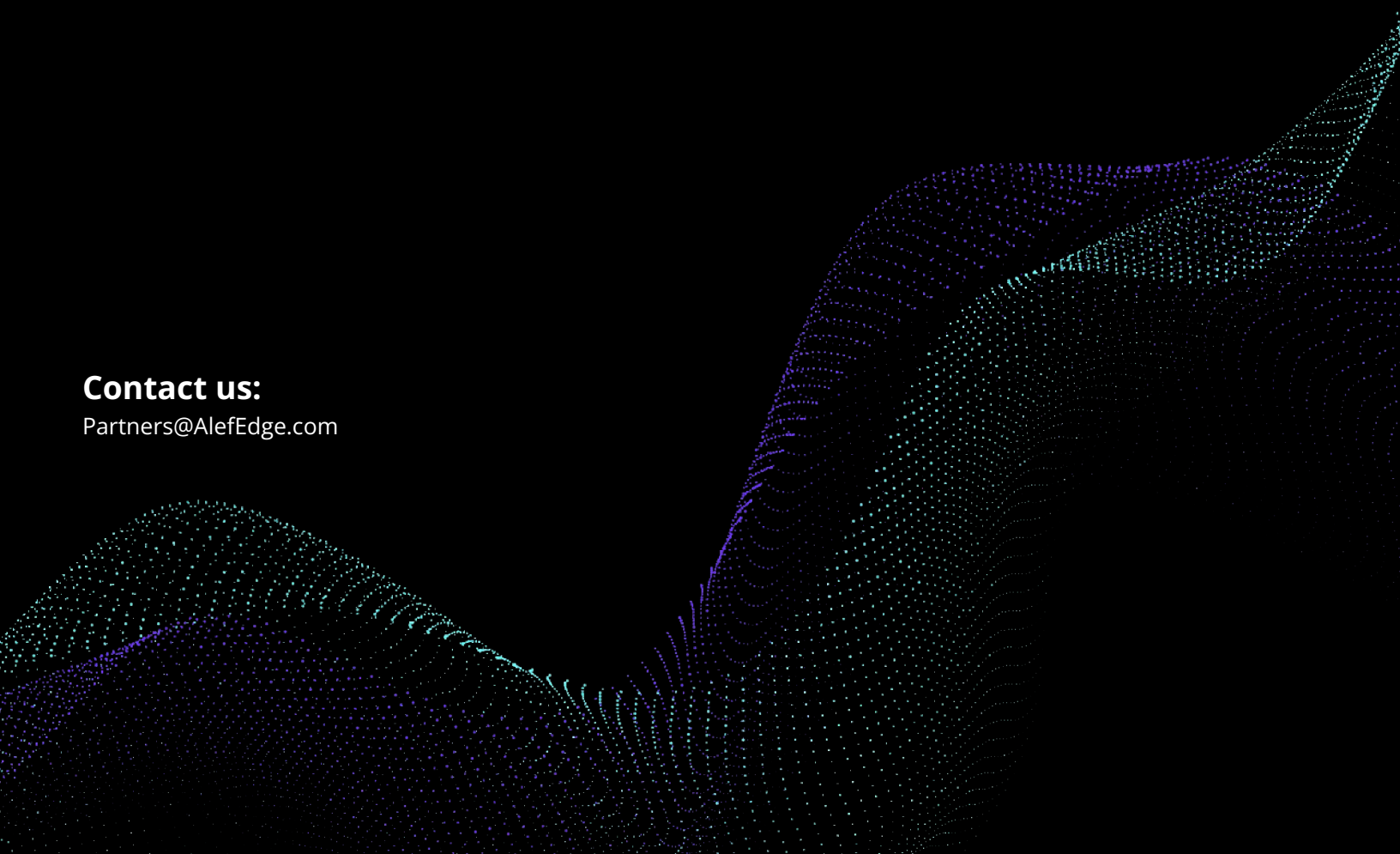
3.2 Use Cases

Alef's Private Mobile Network as a Service is suitable for many verticals, with numerous use cases, including K-12 and higher education, warehouse, healthcare, utilities, transportation, and agriculture. For example, in education, Alef's low-cost approach makes it easy for school districts, perennially short on funding, to minimize CapEx and pay on an as-you-go basis while expanding coverage to narrow the 'homework gap,' track school assets, improve student safety, and enhance the campus experience. Multi-dwelling units (MDU) can provide remote access to appliances and electronics, enable real-time notifications to residents, and enhance safety and security for occupants. Smart Cities using Alef's Private Mobile Network as a Service will find that they can use far fewer access points than Wi-Fi with less interference, track their assets, monitor traffic, use HD video cameras to increase public safety, and use predictive maintenance to determine if public equipment needs to be repaired.

Conclusion

The use of Private Mobile Networks is on the rise in enterprises, but impediments to adoption remain. IT leaders need to deploy systems that meet their existing challenges and stay effective in the future. To make the use of Private Mobile Networks more readily available, cost-effective, and understandable, Alef:

- Offers a Private Mobile Network as a Service solution that bridges the skill set gap and reduces the cost of ownership
- Easily integrates devices into an enterprise's existing NAC & IAM system
- Ensures application performance at a reasonable cost with a private network core at the distributed edge that ensures low latency for applications at all enterprise business locations
- Provides APIs that effortlessly integrate the new network's operations within existing business workflows.



Contact us:

Partners@AlefEdge.com