

SOLUTION OVERVIEW

Aruba ESP (Edge Services Platform)

HARNESSING THE POWER OF THE INTELLIGENT EDGE

Every decade or so, we've seen the technology market undergo major shifts. Over the past few decades, those shifts have been driven by mobility and the cloud. Now we're entering the next big shift: the era of data—but we're not talking about data that's generated in a cloud or a data center. We're talking about data that is available where business is done—where users, devices, and things all come together. We call that the Edge.



So where exactly is the Edge? It could be a workplace environment, a hospital, a large sports stadium, or a factory floor. In these environments, massive amounts of data is generated by users, devices, and things, and that data is analyzed and acted on in real-time at the Edge. Businesses that successfully harness that data and turn it into new services to delight their customers or produce better outcomes, will ultimately win. Those that are not able to harness the data at the Edge, will likely lose.

So, the stakes are high. And the question becomes—do you have the right foundation in place to successfully win at the Edge? The network is critical in making use of all this data and will be what separates business leaders from the laggards.

CHALLENGES AT THE INTELLIGENT EDGE

Like every technology transition that has happened in the past, shifting to the Edge changes the role of your infrastructure and introduces new challenges. Corporate networks play a pivotal role in moving data and connecting people to their apps and services—just as they always have. However, with the Intelligent Edge, network requirements go far beyond standard connectivity and access technologies of the past.

Consider the sheer quantity of things now connecting to corporate networks. According to IDC, 55 billion devices will be connected within the next two years and are expected to generate 79.4ZB of data by 2025. In this data-driven era, the increased velocity and volume of data and actions occurring at the Edge requires a network and IT organization that can keep pace. Yet today's networks are bound by human capacity and experience—they are only as agile and secure as the operators that manage them. With the huge volume of data at the Edge, today's networks can't keep up.

BUSINESS OUTCOMES AT THE EDGE

Outcome	Example
New revenue streams	Retailers can create personalized experiences that make shoppers feel welcome and their unique tastes understood. By using context-aware apps, retailers can present customers with special offers, boosting revenue.
Improved customer experiences via personalization	Imagine people at a large public venue like a sports stadium or a museum. Their mobile experience can be improved with turn-by-turn navigation.
Business agility	Businesses that are able to harness real-time data are able to adapt and change quickly with market changes. The data is key because it can analyze and predict shifting customer needs and preferences.
Operational efficiency	In Manufacturing, sensors detect potential malfunctions before workers or production are endangered. This can also reduce equipment downtime and maintenance costs.
Employee productivity	In the office environment, connected conference rooms allow for seamless employee collaboration via voice and video—regardless of where everyone is located.



IT leaders need to carefully assess their infrastructure and operational models to ensure the network, tools and operator experience and functional capacity are poised to support business success in this new era. They need to consider the following challenges:

Siloed management

Independent management of WAN, wired, and wireless networking domains across campus, branch, and data center locations create communications delays, and silos of skills that include IT knowledge, as well as provisioning, monitoring, reporting and troubleshooting tools. Nearly half of organizations use 11 or more tools, which translates to a greater likelihood of service problems or outages.

Lack of visibility and insights

In these hyper-distributed environments, performance issues can pop up anywhere. Unfortunately, IT's visibility into existing or potential problems continues to diminish as more infrastructure moves outside of their direct control. The information that IT can gather from the network via third-party monitoring and reporting tools is often not actionable—either because data granularity is poor or because operators must manually correlate it to possible root causes. This is particularly problematic at the Edge, where there's often no on-site IT personnel to troubleshoot issues.

Highly manual processes

IT must tackle day-to-day network operations and attempt to ward off performance issues using personal experience, outdated tools and tedious workflows. According to Gartner, more than 65% of network operations activities in enterprises are manual, leading to human errors and downtime. Gartner also found that "automation reduces manual errors by more than 75% while increasing operational efficiencies." So in the data era, with an explosion of devices and things connecting to the network, it becomes challenging for IT to keep up with it all.

Security threats are everywhere

New and advanced security threats are emerging every day. In 2019, security breaches increased over 11% from 2018 resulting in 33B records being stolen, which is expected to cost businesses \$6T annually by 2021.¹ IoT devices aren't equipped with stringent security measures and are easy for hackers to exploit. Meanwhile, workforce mobility continues to expand the IT perimeter, as employees often access corporate resources on personal devices and from public Wi-Fi networks that aren't secure. Lastly, cloud-destined traffic that goes directly over the Internet is more vulnerable—particularly those from shadow IT apps.

ARUBA ESP: YOUR EDGE FOUNDATION

Given the importance of capitalizing on the opportunities at the Edge, it's critical for businesses to ensure that they have a solid network foundation. They need to prepare their IT infrastructure for today and future-proof it for the next big technology shift.

That's where Aruba ESP comes in. It's the industry's first platform with an AI-powered "sixth sense" that is designed for the new requirements of the Intelligent Edge. Aruba ESP uses the principles of AIOps, Zero Trust security, and unified infrastructure to help IT and the network cope with the:

- Velocity and volume of data generated and processed at the Edge
- Advanced threats from a vanishing security perimeter
- Operational challenges from an increasingly complex network architecture

Aruba ESP offers services at the Edge that include onboarding, provisioning, orchestration, analytics, location, and management, which can all be accessed using Aruba Central—the cloud-native single-pane-of-glass console for Aruba ESP. Central provides unified management, AIOps, and security for wired, wireless and SD-WAN operations across campus, branch, and data center locations. Through Central, network admins can use AI Insights to reveal and troubleshoot issues before users complain or the business suffers. Central can also help network admins accomplish tasks quickly with intuitive workflow-centric navigation, and provision and manage infrastructure remotely (with very little technical knowledge needed).



Aruba ESP focuses on three areas to build your network foundation:

1. AIOps

Aruba ESP uses AI, machine learning (ML), and network- and user-centric telemetry data capabilities that focus on revealing network issues before users notice them, helping the IT professional to move faster, and ensuring that service level expectations of users and devices on the network are met. For example, in a single glance, network operators can see a list of all the users, devices and APs experiencing high DHCP issues that will prevent users from connecting. Clicking on these insights will reveal likely causes and, in many cases, will recommend or automatically take prescriptive action.

This use of AI, analytics, and automation helps IT keep up with the massive amount of data and traffic on the network, by surfacing these hard-to-see issues and in many cases, taking action automatically. By making all of these capabilities available via APIs, Aruba ESP also allows for extensibility to 3rd party solutions, which means organizations can further their automation goals within other business processes.

2. Zero Trust Security

Zero Trust is a broad industry term that describes a security framework based on the concept that organizations should not trust any entity inside or outside of their network perimeter. Aruba ESP embraces the principles of Zero Trust by ensuring the identity of an endpoint, enforcing the policies applied to those endpoints with an application aware firewall, and being able to adapt to new threats by sharing information with other security platforms and dynamically adjusting policies to endpoints on the network. By using “role-based policy,” network administrators can embrace Zero Trust without adding to the complexity of their network.

In an era where IoT devices are proliferating rapidly, managing security policies with static VLANs, ACLs, and subnets are slow, error-prone, and only increase the likelihood of issues down the road. With Aruba ESP and our networking and security portfolio, organizations can now virtually eliminate the need for VLANs and control traffic using centralized policies that are based on device and role.

3. Unified Infrastructure

Aruba ESP is managed using Aruba Central. Compared to competitor’s solutions that require up to five different platforms and interfaces, Aruba Central and Aruba ESP unify all network operations across wired, wireless, and WAN; branch, campus and data center under a single cloud-native pane-of-glass and platform. This capability allows administrators to eliminate the time-consuming manual process of moving information from place to place or trying to correlate information across multiple views.

And by using a common data lake in the Aruba ESP platform, Aruba Central correlates and displays multiple dimensions of information in context, unlocks powerful capabilities around automated root cause analysis, and provides more robust analytics. This means faster deployments, shorter time-to-resolution, contextual presentation of information, and more efficient operations.

CONCLUSION

In this era of data at the Edge, it’s clear that today’s network architecture needs to be AI-powered and predictive—to cope with the massive amounts of data and decisions required in near real-time. By architecting an Intelligent Edge infrastructure with security, connectivity, insight, and automation, Aruba ESP can help you improve business agility, build new revenue streams, and create compelling experiences that delight customers and employees, while achieving new business outcomes. To learn more, visit arubanetworks.com/ArubaESP.