Distributed Enterprise Networks Upgrade Consideration

More than Just Bandwidth Demands

Office networks designed 5 years ago are misaligned with these changes taking place. Distributed enterprises need to consider upgrades to their multi-office networks.

Introduction

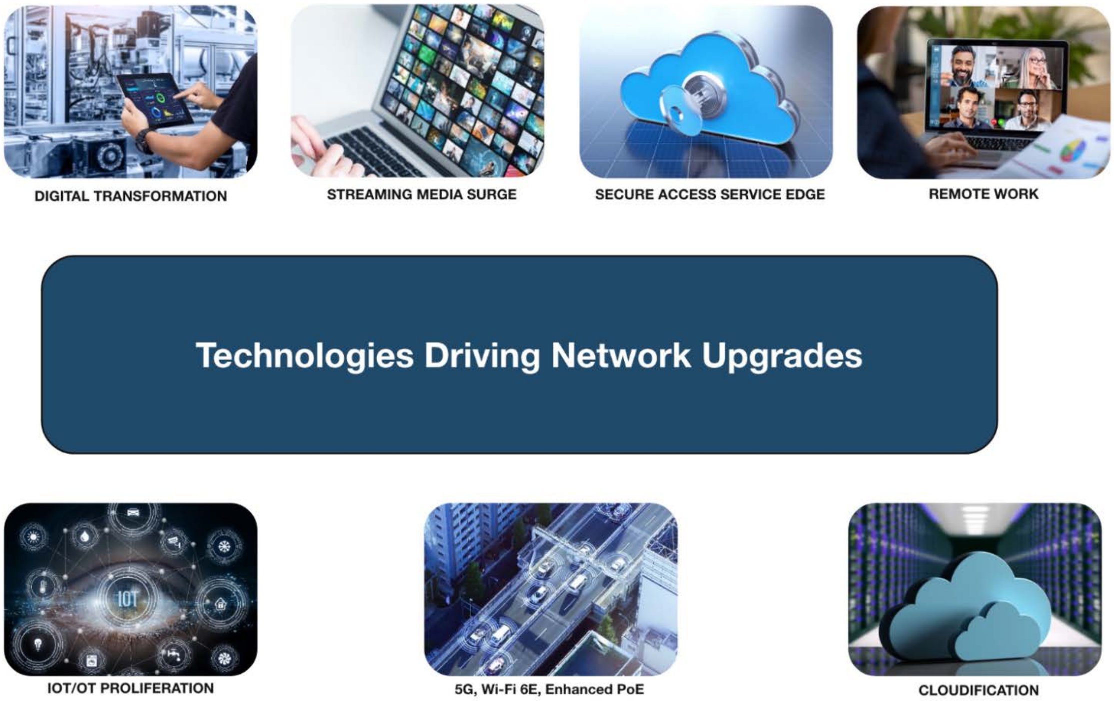
Major behavioral shifts in how often employees frequent their company office locations, coupled with the transition to cloud computing are driving the need for technology refreshes in distributed enterprise networks. Most enterprises however are hesitating on any changes to their networks as many office spaces remain underutilized. And while human resource organizations are rationalizing these changes ahead of infrastructure decisions, enterprises need to consider upgrades to their office and building networks, as there are a number of technology advancements that are closing in on them.

Technology Drivers

Where in the past, the majority of distributed enterprise network upgrades were driven by exponential bandwidth demands, there is a more gradual growth curve as application traffic patterns and office occupancy rates are much different compared to the patterns five years ago.

Office 365, Google's G-Suite, real time video driven collaboration, virtual desktops, diskless laptops, and 3rd party cloud hosting sites, are all shifting the traffic patterns within distributed offices. Traffic is multi-directional, not just north/south. Collaboration where files are viewed, modified and shared live within the cloud is the new normal. This results in fewer large file transfers, yet the need for lower latency real time connectivity, anywhere across the globe. And security at the edge is a must as offices, workers, applications and endpoints are numerous, diverse and distributed.

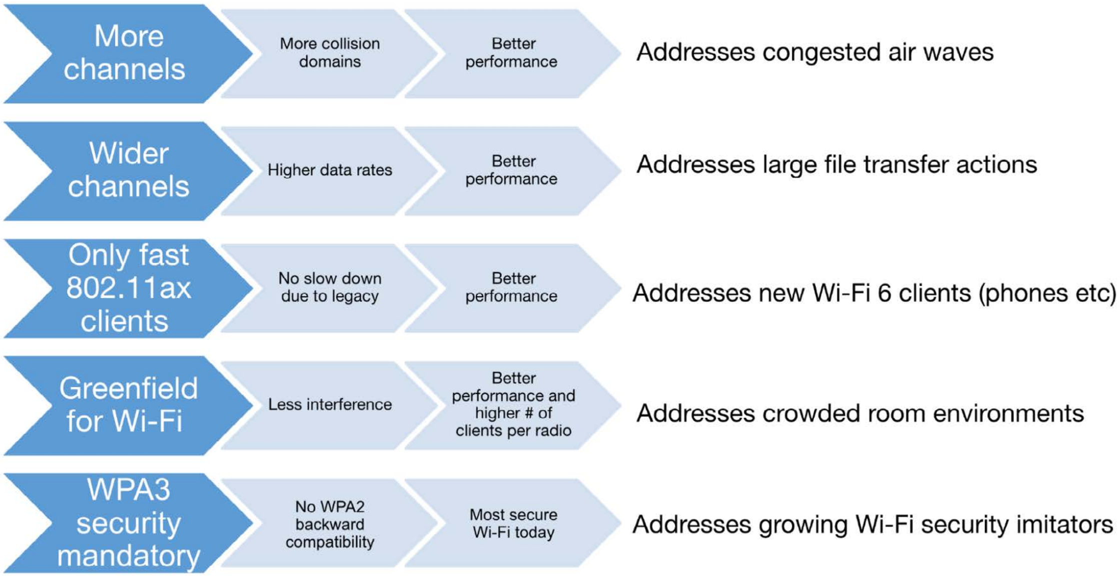
Distributed Enterprise Network Requirements



Office networks designed five years ago are misaligned with these changes taking place. Distributed enterprises need to consider upgrades to their multi-office networks. Here is a summary of use cases that are driving these upgrades.

- Newer endpoints including Wi-Fi 6E based laptop and cell phones, coupled with IoT devices that require battery preservation. While backwards compatible with older Wi-Fi Access Points (802.11ac based) the benefits of these employee, and office productivity devices are not being fully realized by these older Access Points.

Wi-Fi 6E Benefits



More channels	More collision domains	Better performance	Addresses congested air waves
Wider channels	Higher data rates	Better performance	Addresses large file transfer actions
Only fast 802.11ax clients	No slow down due to legacy	Better performance	Addresses new Wi-Fi 6 clients (phones etc)
Greenfield for Wi-Fi	Less interference	Better performance and higher # of clients per radio	Addresses crowded room environments
WPA3 security mandatory	No WPA2 backward compatibility	Most secure Wi-Fi today	Addresses growing Wi-Fi security imitators

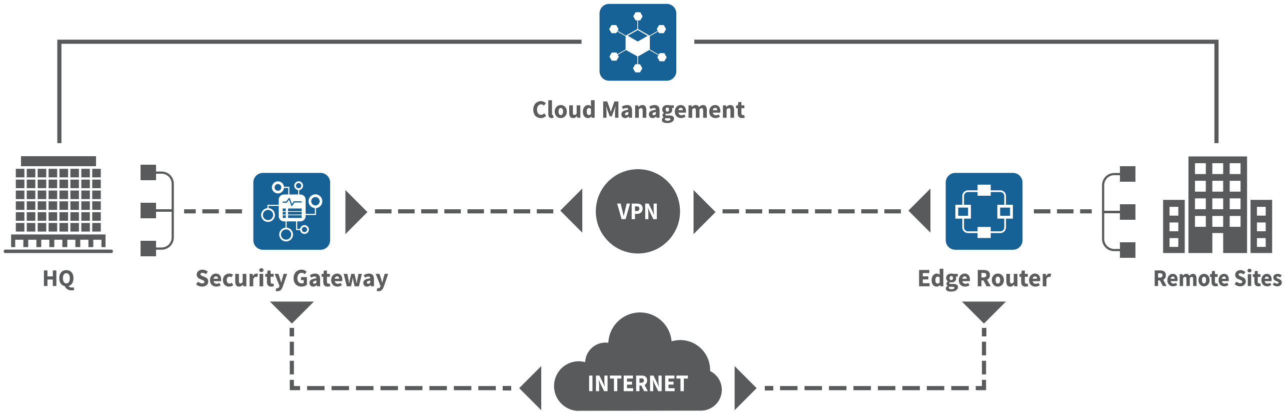
- The mature adoption of IoT devices including cameras, building controllers, speciality mobile devices, and real time multimedia. These devices are often unmanaged, with poorly engineered networking operating systems. IoT devices broaden cyber based attack surfaces. New security measures and systems must be deployed.
- Sophisticated security attacks based upon network vulnerabilities, especially with unsuspecting branch office workers and their bring your own device laptops and cell phones. Firewalls have to become more distributed out to the edge.

Network Security Building Blocks

Security Gatweay
Comprehensive Enterprise-grade Network Security Platform

Edge Router
Lightweight Network-edge Device for Branch Office Connectivity

Cloud Management
Cloud-based Centralized Management Platform



- Pop-up locations especially within healthcare, disaster relief areas, and multi-tenant buildings, where easy to mount, easy to cable, and easy to configure devices are common. These pop-ups typically have a 6-12 month life cycle where there are no equipment closets, designated mounting locations, ceiling plenum for cable runs, or UPS systems. Wi-Fi Access Points, software appliance based firewalls, and magnetic mounted switches address these ad-hoc office needs..
- More capable Wi-Fi 6E Access Points require higher speed uplink ports and higher Power of Ethernet (PoE) wattage as they have greater capacity. This requires switch, cabling, and Wi-Fi Access Point upgrades.
- Traffic pattern shifts where VPN and MPLS networks with tunneling to and through headquarters is inefficient and adds unnecessary overhead. Applications hosted within 3rd party clouds drive different traffic patterns and network designs. Office networks require flattened topologies with micro-edge Internet connections.
- Increased 7x24 reliance on the branch office network where any downtime impacts productivity, as more and more applications no longer run locally on workers laptops and desktops. Modern productivity applications are cloud hosted and 100% network dependent. Networks must be resilient with little to no downtime when making changes and upgrades.
- Congested Wi-Fi airwaves, within high density central business districts (CBD's) where the quality of the connections are impacted. Wi-Fi 6E access points are specifically designed to handle highly congested air waves.
- Operation cost savings where CIO's are minimizing the number of highly trained administrators by having a centralized IT staff that can manage these offices remotely. Enterprises cannot expand their offices with a linear increase in IT staff (experts on site)' they must leverage a cloud approach where administration is centralized with small technical staff.

- Supply and manufacturing constraints where chips and other critical components for aging switches, access points, and firewalls are either obsolete or are on older fab lines. Many older chips are simply not being manufactured. Wi-Fi Access Points, switches, firewalls, and Internet edge connectivity devices are being impacted here. Enterprises need to ensure supply continuity.
- Lower cost broadband services where 500 Mbps to 1 Gbp connections are the most affordable options. Bandwidth prioritization, rate limiting, and traffic controls are required to ensure these lower cost broadband speeds do not impact productivity.

Office Networks Must Evolve

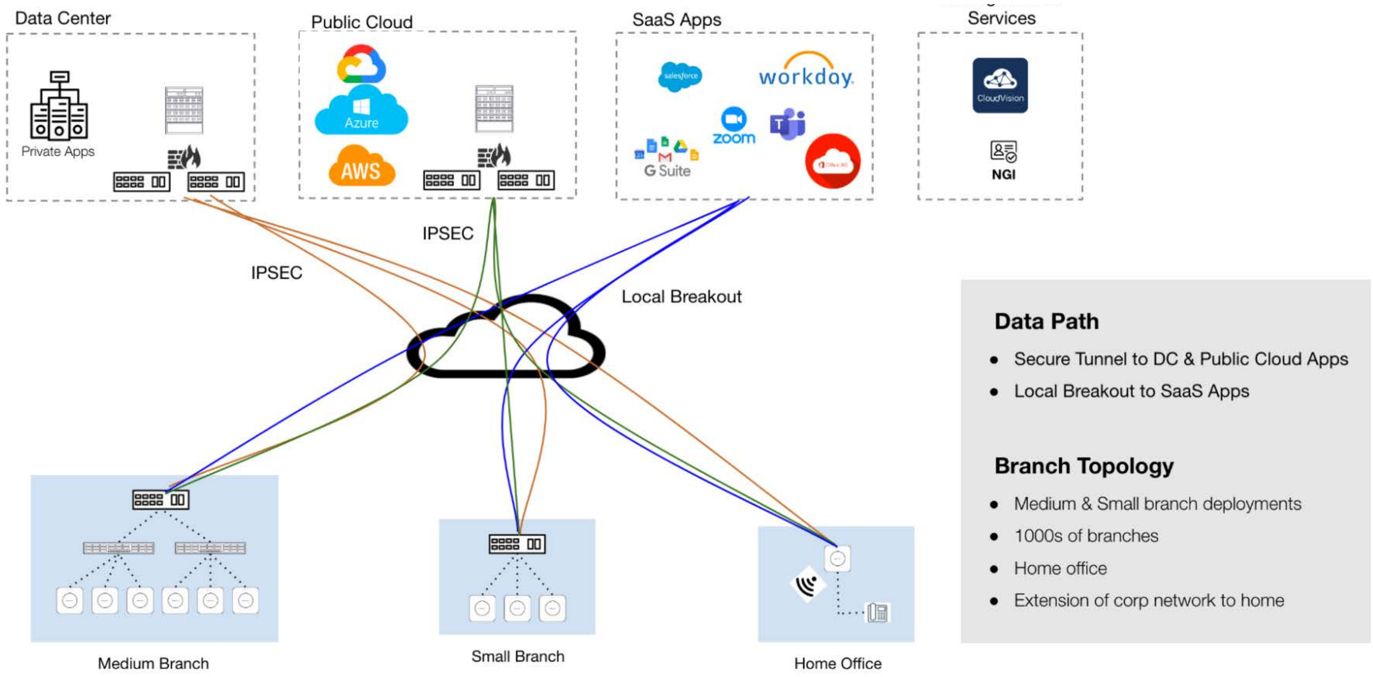
Many multi- office networks were originally designed for legacy productivity use cases including file sharing, emails, secured access to internal data centers, online transaction processing, voice over IP communications, and Internet browsing and search. These are use case artifacts pre cloud computing.

While the office of the future is open for interpretation it is clear that the best practice networking designs and operational tools, dating back 10 years ago, is not the way forward. There has been a major shift across all industries and applications, regarding how employees interface with IT applications. This in turn requires a shift in network designs, network platforms and network operations management.

Enterprises are becoming more distributed, with offices located based upon regional talent pools, flexible leasing options, global labor rates, and working remote policies. This often means smaller offices, where enterprises cannot afford networking specialists on site.

Offices are no longer managed as long term decisions, with 5 or 10 year lease options. Shared spaces, collaboration, bringing your own devices, lights out security systems, interconnected building controllers, flexible cubicles/offices, virtual lobby ambassadors, hoteling, and applications with no boundaries are just many of the IT changes taking place. All of these endpoint and application changes require secure networks, at the edge.

Distributed Enterprise Architecture



Data Path

- Secure Tunnel to DC & Public Cloud Apps
- Local Breakout to SaaS Apps

Branch Topology

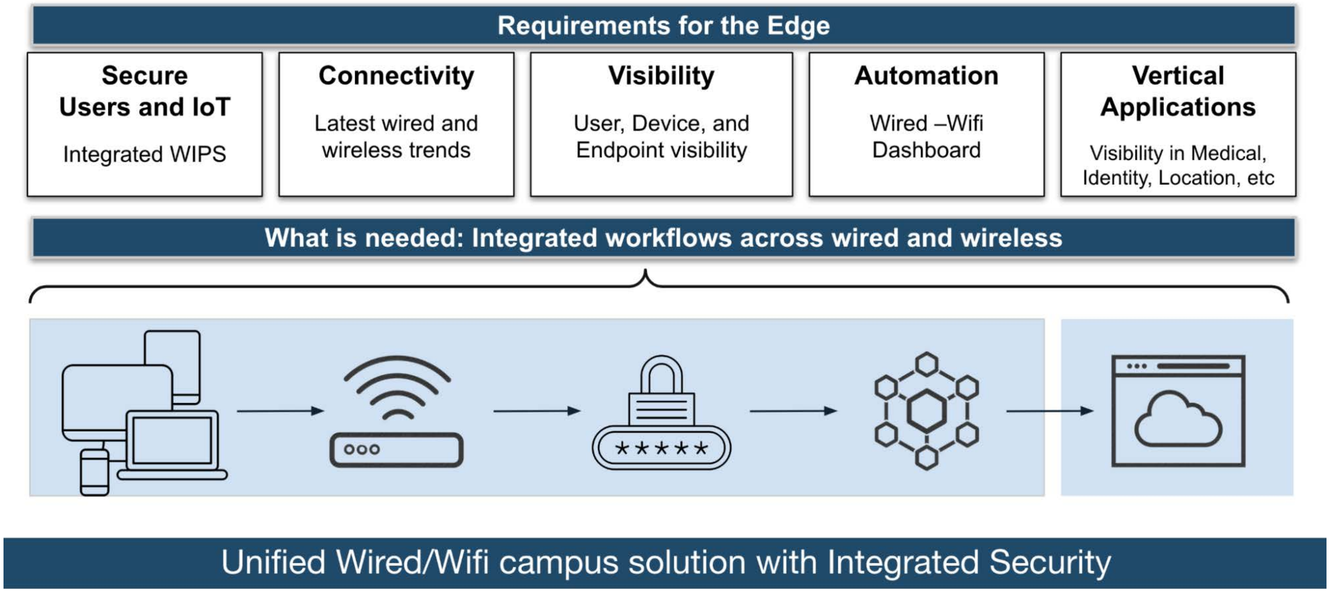
- Medium & Small branch deployments
- 1000s of branches
- Home office
- Extension of corp network to home

Edge-As-A-Service

Enterprises need to view their distributed office networks as an intelligent edge. Instead of a loose collection of ad hoc wireless, wired, security, tunneling, telemetry, and monitoring products, the combination thereof becomes a set of integrated services, ie. Edge-as-a-service. And while Edge-as-a-service is seemingly a simple concept, it is a significant change and transition from the predominant views 10 years ago (i.e legacy networking) where products were developed, sold, deployed and managed in fixed configuration, topology silos, and domain specific form factors.

Edge-as-a-Service embodies all of the distributed office networking requirements (wired, wireless, security, firewalls, internet connectivity) as an integrated, tightly orchestrated and managed ecosystem. Instead of a loose collection of networking appliances, or some sort of a super appliance that gets outdated every 18 months, Edge-as-a service integrates services across highly optimized appliances holistically.

Edge-as-a-Service



Requirements for the Edge

Secure Users and IoT	Connectivity	Visibility	Automation	Vertical Applications
Integrated WIPS	Latest wired and wireless trends	User, Device, and Endpoint visibility	Wired –Wifi Dashboard	Visibility in Medical, Identity, Location, etc

What is needed: Integrated workflows across wired and wireless

Unified Wired/Wifi campus solution with Integrated Security

Edge-as-a-service addresses many of the technical challenges that most companies with legacy networking solutions are struggling with. Many enterprises require network experts as they manage the interdependencies of VLANs, subnets, SSID's, VPN's, Guest Networks, endpoint authentications, firewall rules, DNS services (the list goes on and on) across multiple platform silo's (Wi-Fi, switches, firewalls). Any mis-configurations across these silo's can open up security holes, break communications, impact performance, in other silos with negative impacts to employee productivity, or protected digital assets.

Edge-as-a-service addresses these challenges where experts are no longer required within each site, or within each technology silo. Security, connectivity, bandwidth optimization, and other infrastructure policies are determined centrally, and are deployed locally.

Offering complete Edge-as-a-Service distributed enterprise networking solutions requires an intelligent management plan, with a rich real time data repository and relationship models where the dataplane stretches from the Wi-Fi Access Points, through the wired switch ports, through the firewall, and out to the Internet. And within this inter-related dataplane there are a rich set of QOS, security, bandwidth, authentication, authorization, self healing, configuration, and auto deployment features, again all managed as Edge-as-a-service. And all of these services are driven by a common data model with real time telemetry hosted in the cloud.

Offices must transition away from silo's as networking technologies are outpacing human capital, including the cost of labor and the cost of management tools (that commonly fall short).   Edge-As-A-Service is the way forward.

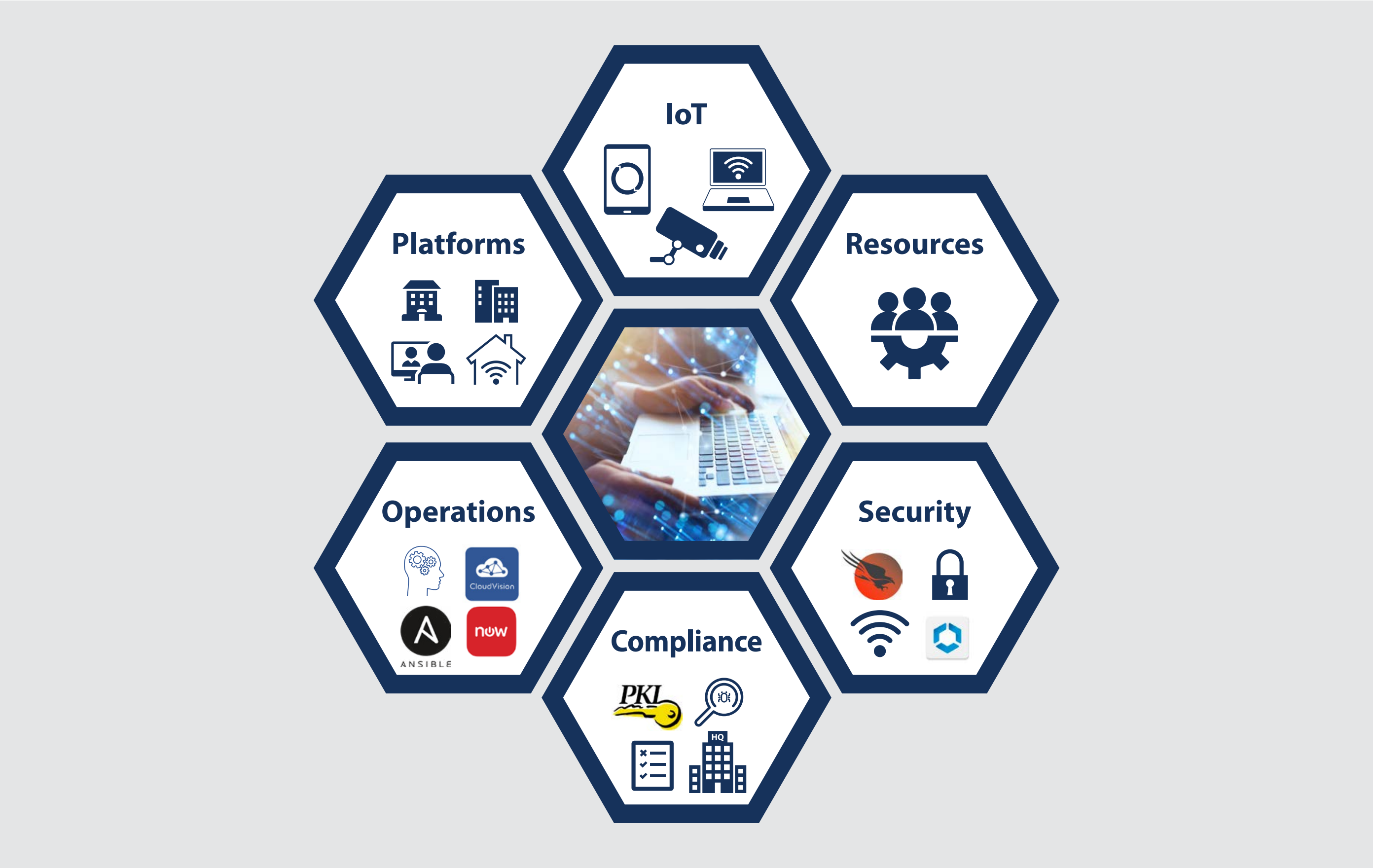
Picking the Right Solution?

There is no shortage of office communication features or products available for enterprises to choose from. And there is a continuum of products from consumer grade to enterprise grade that decision makers need to filter through. As employee productivity, security, and multi-year operations management (cost of maintaining the network) are the top-of-mind business deliverables, companies need to look beyond the upfront purchase price of any product, and focus on enterprise class offerings, as these better address the productivity, high availability, and security business needs.

Simply stated enterprise products have better chip sets, power supplies, operating systems, security features, and operation tools. And while these products are higher in price, the cost of downtime, and the other risks associated with consumer grade products have a far greater financial impact than the higher upfront cost of enterprise class products.

Evaluating distributed enterprise networking solutions can be daunting as true due diligence requires hands-on testing. Most customers lack the lab space, resources and time to extensively review these offerings. The good news here is that we live in a virtual reality world. Decision makers can now easily, and at no cost (except for their time), do hands-on proof-of-concept evaluations remotely.

Picking the Right Solution



Many virtual labs closely mirror real networking infrastructures. Virtual labs can demonstrate at scale the most important features, like Wi-Fi roaming, root cause analytics, wire rate firewall rules, segmentation tagging and encryption, intrusion and protection, automated RF tuning, lights out operations mgmt, hitless patches and upgrades. Essentially all features that drive Edge-as-a-service.

About Arista Cognitive Unified Edge (CUE)

Arista's CUE solutions help distributed enterprises optimize their networks while safeguarding their data and devices. CUE redefines enterprise networks with enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network.

Centralized Cloud Based Management

Centralized management is key for network administrators to be able to efficiently manage multiple networks remotely. All CUE products can be remotely deployed and managed providing network administrators the tools required to ensure that the network is running flawlessly.

Next Generation Firewall

NG Firewall simplifies network security with a single, modular, software platform that provides an intuitive interface enabling you to quickly gain visibility into traffic on your network. NG Firewall delivers a comprehensive, network security platform including content filtering, threat protection, VPN connectivity, application-based shaping for bandwidth optimization.

WAN Optimization

Micro Edge with advanced routing capabilities and WAN Optimization, provides the ability for businesses to build a comprehensive, secure network. Micro Edge provides interoffice connectivity, optimizes the internet over existing infrastructure, and prioritizes business critical applications to maximize employee productivity.

Wired Connectivity

Small to medium size offices require one or several switches that can be deployed flexibly based upon building limitations such as no equipment closets. Smaller offices often require power distribution from these small form factor switches for connecting access points, phones, IoT devices, IP cameras, and building controllers. These switches form the core of smaller offices and must be secure, manageable, easy to install and smart on how they deliver power to the edge devices.

Wi-Fi 6 Access Points

Arista's enterprise class access points have multi-radio offerings for ensuring the best floor coverage, intrusion protection, zero touch deployment, auto RF re-tuning, cloud manageability, and integrated wired/wireless cloud based centralized management. This product line is based on a controlless architecture, where management data is managed centrally, yet the data and control planes are local, ensuring no single points of failure.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989