aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

THE DIGITAL WORKPLACE

It's now an expectation, for businesses to succeed – they need to embrace mobility – allowing their employees to be able to work anywhere, on any device. With the explosion of smartphones and tablets, the way we communicate, consume services, and manage our personal lives has been transformed. The combination of mobile devices and cloud-based apps has also changed the very nature of our work environments, where collaborative open spaces and non-routine schedules are the norm.

But now IoT is driving an even larger transformation—one that will impact everything from the enterprise, business processes, and even customer experiences in healthcare, retail, and large public venues, to name a few. IoT may have once been thought to be a consumer phenomenon, but organizations are now realizing its huge potential in creating smarter, more efficient workspaces through intelligent meeting rooms, location services, and real-time monitoring. Combining IoT devices with contextual information—location, application, and policies—yields opportunities to lower costs, build loyalty, improve productivity and drive revenue.

While IoT offers potential rewards, the thought of all those devices connecting to the network is the stuff that keeps security and IT managers up at night. The BYOD phenomenon was bad enough—employee-owned devices and risky user behavior blurred the lines of a secure perimeter—but IT got a handle on this challenge by creating security policies based on known, contextual data that it could trust. Given their sheer number, IoT devices need to be an integral part of the conversation when planning the network infrastructure for the digital workplace. The network needs to be smart enough to classify, understand and react to the behavior of IoT devices automatically.

MOBILE AND IoT BRING CHALLENGES

Do you really know what's on your network?

Security starts with understanding what's on the network—unmanaged smartphones, rogue endpoints, and IoT devices that users may connect without consulting IT. Any of these can introduce new threats and broaden an organization's attack surface. A better understanding of what is on the network through granular profiling provides IT with the ability to identify every device that is connecting to the network, regardless of type, owner or where it's connecting from.

This becomes more important as unknown wireless and wired IoT devices flood the network. Constant profiling helps to accurately enforce policies based on a device's category type and attributes, to automatically grant or deny access privileges to internal and external resources.

ARUBA'S 6 STEPS FOR THE DIGITAL WORKPLACE

1. Identify and profile all devices on wired and wireless
2. Connect mobile and IoT devices with integrated wired and wireless
3. Protect the network with an integrated way to quickly detect and respond to advanced cyberattacks
4. Manage the network—on-premise or cloud
5. Personalize experiences with location and context
6. Speed up innovation to improve user experience and security

Increasing device density

The growing number of mobile and IoT devices is placing a burden on aging infrastructures that were not designed with these trends in mind. But it's not just the number of devices that's causing bottlenecks and congestion. Consider user behavior and new traffic demands. Employees and guests are using video more than ever before. These behaviors place unprecedented demands on the network. The infrastructure needs to support bandwidth prioritization features to understand disparate traffic types.

To help solve the problem, organizations need management tools that identify which applications are being used and that easily set up usage policies to prioritize voice and video over data for specific apps and users. It will be increasingly important to then monitor the performance of the network on a continual basis.

Wired is just as important as wireless

In organizations within enterprise and industrial spaces, the number of expected wired IoT devices can range from 35% to over 50% depending on vertical—HVAC, lighting, motion detectors, medical equipment, badge readers, process controllers on the factory floor, to name just a few. In the past, network access control discussions centered on how to secure the wireless network because that's how most devices were connecting.

The heavy focus on securing wireless networks meant that wired networks were left unprotected as switches sat behind locked doors. The perception was that they don't exhibit the same vulnerabilities as wireless. Unfortunately, as wired networks grew, consistency across many switches wavered, leaving ports wide open and accessible by anyone. Conference rooms and printer areas are a classic example where "hit or miss" security exists. With many IoT devices now connecting via wired, it's time for the same level of attention be given to securing the wired infrastructure.

Traditional wired infrastructure not optimized for IoT

Legacy switching environments were designed before mobility and IoT were prevalent. Assets lived behind the firewall and IT needed to make sure that the perimeter kept out external threats. Now enter IoT—today's switches need to ensure that connectivity, security and smart network management complement each other so that all of these devices can connect, but are segmented based on their access and traffic needs. With IoT driving up wired device densities and introducing new traffic patterns, automation and analytics have become table stakes to support the network with constrained resources.

It's expensive to innovate and keep ahead of the hackers

As companies invest in technology and network security, it's almost impossible to keep ahead of the hackers by doing it alone. Partnerships are critical for success and IT needs solutions that work across multi-vendor architectures as well as being open to developers to encourage innovations that are easy to deploy and consume.

ARUBA'S BLUEPRINT FOR ENTERPRISE MOBILITY AND IoT

Aruba's solutions are designed to enable and capitalize on new digital experiences that harness the full potential of mobility and IoT for business, customers and employees.

1. Identify and profile all devices on wired and wireless

Mobile and IoT can improve workplace productivity and automate decisions that can be a catalyst for new products and services, but only when insights come from data collected through secure connections and trusted devices. Aruba ClearPass enables IT to automatically identify endpoint types and attributes of IoT and traditional smart devices across a multi-vendor wired and wireless access network. This solves issues related to connectivity, performance and the ability to accurately set and enforce granular policies.

2. Connect mobile and IoT devices with integrated wired and wireless

Device density demands, critical mobile applications, and the move to smart buildings mean that today's businesses need a smarter wired and wireless infrastructure. A highly mobile workforce, the surge in IoT devices and the increasing use of Wi-Fi bandwidth means that the wired infrastructure must be optimized for resiliency, security and scale.

Aruba's 802.11ac wireless APs provide the fastest gigabit data speeds to boost network performance in high-density environments with the intelligence to provide seamless roaming and app prioritization. That means that business critical traffic is prioritized and users enjoy a seamless experience without dropped calls.

Aruba's access and core switches provide an integrated wireless-wired foundation with scalability, security and high performance for campus networks. Programmable ProVision ASICs and ArubaOS-Switch software in our access switches enable fast wireless aggregation and simplicity with unified role-based access across wireless and wired networks using the ability to identify and assign roles to users and IoT devices to prioritize business critical applications while securing the network. Aruba's layer 3 switches are also capable of leveraging user and port-based traffic tunneling to a Mobility Controller so that policies can be applied, advanced services can be extended to users and IoT devices, and traffic can be encrypted to secure the network.

In distributed enterprises, the Aruba switches support Zero Touch Provisioning and optional cloud-based management to allow enterprises to simplify and slash network deployment and management costs.

The explosion of mobile and IoT devices, combined with the rise in traffic demands means all of this traffic needs a game changing core switch to meet the needs of today and into the future. The Aruba 8400 and 8320 core switches are founded on the next generation ArubaOS-CX with its Network Analytics Engine and full REST-based programmability to unleash the programmability and analytics that tomorrow's networks require to automate, secure and power the network.

3. 360 degrees of analytics-driven attack detection and response

Starting with core security capabilities embedded in the foundation of all of Aruba's Wi-Fi access points (APs), switches, routers, and controllers, Aruba builds on this foundation by integrating IntroSpect machine learning-based attack detection with access control systems like Aruba ClearPass in an open, multi-vendor platform. With the Aruba 360 Secure Fabric, security teams can now develop a seamless path from trusted network infrastructure, to user and device discovery and access, to analytics-driven attack detection and response – based on policies set by the organization – without being locked into a single vendor. Aruba provides the best elements of a unified security solution with the flexibility of an open architecture.

4. Manage the network—on-premise or cloud

Today's networks need to provide more than connectivity — they must deliver insights that clearly identify anomalies that affect network and application performance as well as user connectivity issues before they occur. Management dashboard visuals must be designed to allow for mobile users with multiple devices and those who bring IoT devices to work. Built-in policy management and analytics need to provide the ability for users to login from anywhere, and give IT the visibility to see when and where users are connecting from. And as budgets and IT resources dictate, organizations need the ability to choose between on-premise or intelligent cloud-managed networking solutions that deliver consistent levels of deployment and day-to-day management features — locally with Aruba AirWave or in the cloud with Aruba Central.

5. Personalize experiences with location and context awareness

Aruba's Location Services solutions enable any organization to leverage Bluetooth Low-Energy (BLE) technology to enable indoor location and wayfinding, and proximity-aware push notifications at enterprises, stadiums, hospitals and other public venues. Aruba Meridian software combined with Aruba Beacons and any wireless infrastructure turns smart devices into interactive wayfinding and notification endpoints. Now employees, guests or shoppers can easily book conference rooms, get to nearby amenities quickly and on time, learn about new products or points of interest, boosting venue revenue opportunities andcustomer loyalty via a personalized experience. With the addition of Aruba Tags and Meridian asset tracking, organizations can easily locate and retrieve valuable items. Increase staff efficiency and reduce costs associated with managing misplaced assets.

6. Speed up innovation to improve user experience and security

At Aruba, we are working with the industry's best technology partners and app developers to deliver solutions that are easy to deploy and consume. Together our efforts deliver innovative solutions that connect the dots between today's business and IT priorities. Depending on your business, our partner programs cover everything from secure connectivity to location-based services and mobile engagement.

To learn more about Aruba's digital workplace solutions, visit www.arubanetworks.com/digitalworkplace.

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com