

SOLUTION OVERVIEW

DELIVERING MORE HIGH-VALUE FINANCIAL SERVICES AT GREATER SPEED

The rapid adoption of smartphones, tablets and other mobile devices has created a sea change in how services are delivered and transactions are conducted in the finance industry. Employees from trading floors to corporate offices now rely on mobile devices to wirelessly access market and client data, communicate with customers, and collaborate with colleagues.

Customers are also banking on mobility. Nearly half of smartphone owners have used mobile banking apps in the last 12 months, according to a recent Fed study. Customers want to research, purchase, and manage financial services on-demand using mobile devices – just as they do with other products and services.

For the finance industry, mobility can expand revenue opportunities, increase customer satisfaction, and provide a competitive advantage as the industry undergoes rapid change. By taking a top-down approach to mobility, it's possible to boost employee productivity, improve customer engagement, and deliver a more personalized transaction experience.

As financial institutions consolidate retail branches, for example, they can leverage mobility at remaining sites to offer a digital café experience that lets customers conduct banking transactions and interact with tutorials on products and services while drinking a cup of coffee.

Supporting mobility means making Wi-Fi ubiquitous across your organization. Businesses must shift investments away from the legacy wired networks to building out the wireless infrastructure. Doing so has considerable benefits.

For example, static wired networks cannot adapt to the needs of a mobile workforce and must be constantly reconfigured every time there is a change in users and devices. Rightsizing your network infrastructure by eliminating wired ports can result in a windfall that can be redirected to Wi-Fi expansion and other critical IT projects.

There was a time when IT was justified in thinking Wi-Fi was difficult to implement and lacked the security capabilities required by financial institutions. But today it is possible to fully embrace mobility by adopting Mobility-Defined Networks from Aruba Networks®.

With Mobility-Defined Networks, financial institutions can provide workplace Wi-Fi that IT as well as users can trust, while ensuring business continuity across multiple locations and employees. Mobility-Defined Networks also enable secure access for personally-owned mobile devices and automate wired and wireless network access for guests.

Aruba Mobility-Defined Networks have been instrumental in transforming some of the world's largest financial institutions in investment management, asset management, brokerage, investment banking, retail banking, financial services, stock exchanges, and government central banks.

Mobility-Defined Networks enable employees, guests and contractors to use the technology they prefer, and enable financial institutions to take advantage of the dynamics of mobility to increase business agility, competitive differentiation, and revenue opportunities.

WORKPLACE WI-FI THAT EVERYONE CAN TRUST

Mobility demands dependable, high-performance, secure Wi-Fi that meets regulatory mandates, no matter who logs into the network or from where.

Executives, analysts, customer service associates, mortgage brokers, and other employees need a seamless mobility solution that lets them continue a phone conversation while walking to a meeting without losing the connection. And they must be able to login securely from an airport or other remote location, even their kitchen table.

With Mobility-Defined Networks, trust begins with a suite of wireless security technologies that offer greater protection than wired networks. Standards-based security includes 802.1X authentication, WPA2/AES encryption, and even U.S. NSA-approved Suite B cryptography.

Additionally, Aruba Mobility-Defined Networks feature an ICSA-certified Policy Enforcement Firewall™ that provides identity-based access controls to enforce application-layer security and traffic-flow prioritization.

Making the mobility experience trustworthy for financial professionals requires delivering stable, high-performance Wi-Fi that's more reliable than wired. With Mobility-Defined Networks, changes in mobility state automatically trigger security actions, performance optimization and more efficient workflows that adapt to the dynamics of mobility.

Aruba 802.11ac ensures consistently high performance for every client, better Wi-Fi range and the highest device-densities. Aruba further boosts performance and reliability with technologies like ClientMatch™ and AppRF™.

Patented ClientMatch technology puts the Wi-Fi infrastructure in control of client connectivity and roaming. It automatically matches clients to the right radio on the right access point (AP), eliminating sticky clients and boosting Wi-Fi performance by up to 50 percent in crowded locations.

Subsequently, user perception and satisfaction with the wireless network is greatly improved. The combination of 802.11ac APs and ClientMatch ensures users are always on the optimal AP as they roam, for example.

Aruba AppRF technology prioritizes the handling of cloud apps and unified communications and optimizes IP multicast video traffic to make sure users get the very best performance from delay-sensitive apps like Citrix Virtual Client and Microsoft Lync. AppRF can even identify and prioritize encrypted apps, making it easy for IT to apply quality-of-service and other policies as needed.

IT operations also benefit from Mobility-Defined Networks. Self-healing and self-optimizing, Mobility-Defined Networks automate many manual and time-consuming IT tasks, reduce IT helpdesk tickets and safeguard enterprise data.

Critical to Aruba Mobility-Defined Networks is the AirWave™ network operations platform. It lets IT manage tens of thousands of network-connected users, devices, access points, controllers and wired infrastructures across multiple geographies and generations of multivendor networks – all from a single pane of glass.

AirWave employs a user-centric approach to deliver a full range of management capabilities, including real-time monitoring and visibility into who's on the network and where they're accessing it; device discovery; automated configuration management; troubleshooting and diagnostics; and root cause analysis and event correlation.

In addition, the AirWave RAPIDS feature strengthens network security and enables IT to meet strict compliance requirements by detecting and locating unauthorized client devices and APs as well as attacks against the wireless infrastructure.

BUSINESS CONTINUITY ACROSS ALL SITES AND EMPLOYEES

Mobility can lead to increased revenue opportunities and improved customer satisfaction. But your mobility infrastructure of choice must be resilient enough so all employees at all locations have secure, reliable access to critical resources and applications on the corporate network.

Aruba builds redundancy and survivability into the Mobility-Defined Networks and, for added assurance, offers advanced protection against infrastructure attacks. As a result, road warriors and other remote workers get secure, consistent access to corporate data, regardless of their location.

Key remote networking enablers for Mobility-Defined Networks include Aruba Instant APs and a suite of Remote APs (RAPs). They deliver high-performance enterprise-grade Wi-Fi to branch offices and give your remote workforce secure access to corporate resources and backend systems.

If a WAN connection fails, Mobility-Defined Networks ensure that branch offices stay up and running, including the ability to authenticate new users or make security adjustments. Aruba Instant APs can accommodate Internet connections from two different ISPs, ensuring business continuity for mission-critical applications.

In addition, Instant APs support zero-touch provisioning, which means that financial institutions can predefine branch network settings and APs will self-configure on site without requiring IT involvement, greatly simplifying remote deployments.

To safeguard the mobility infrastructure against malicious activity and RF interference that can lead to business disruption and downtime, Aruba RFProtect™ features the industry's only integrated wireless intrusion protection and spectrum analysis system.

With RFProtect, Aruba APs can service Wi-Fi clients while also monitoring the air for interference sources and rogue devices. IT can even turn an Aruba AP into a dedicated air monitor to detect and contain unauthorized devices and APs.

RFProtect also stops wireless traffic from flowing into the wired infrastructure via rogue APs, which protects the wired network against disruptions from wireless security breaches. Robust rogue detection is critical to meeting PCI requirements at retail bank and brokerage branches.

SECURE ACCESS FOR PERSONAL DEVICES

Historically, financial institutions have only permitted employees and guests to connect personally-owned devices to a Wi-Fi network that's completely separate from the wired LAN. They often purchase a wireless solution from an ISP that directs mobile users to the Internet and then back into the corporate office through a VPN.

With Aruba Mobility-Defined Networks, financial institutions can provide secure, automate network access for personal devices, ensure regulatory compliance, and deliver a better user experience without the cost and complexity of having multiple, disparate infrastructures.

To achieve this, the Aruba ClearPass Access Management System™ enables you to centrally create and enforce differentiated network policies across wireless, wired and VPN infrastructures, which eliminates the burden on corporate IT.

ClearPass leverages contextual data about user roles, devices, application use, location, and time-of-day to streamline network operations, automate device onboarding, and even distribute device-specific certificates for stronger authentication security.

Mobility creates a host of new challenges around visibility, especially when employees use multiple devices or access network resources from a variety of locations. Contextual data lets IT create more granular policies that simplify mobility rollouts and give businesses stronger control over network resources.

ClearPass Onboard allows employees to self-register and securely onboard their own devices through a personalized self-service portal that detects a device's operating system, presents the appropriate configuration package, and installs unique device credentials.

This automated self-registration process provides differentiated access controls for personally-owned devices and ensures BYO policies are enforced. It also dramatically reduces helpdesk tickets and eliminates the need to have IT manually configure devices.

Aruba also designed *ClearPass Exchange*, which allows ClearPass to integrate seamlessly with third-party security and workflow systems. Through standard APIs, ClearPass Exchange swaps user, location, application and other contextual data with web-based systems and applications to automate new workflows and IT tasks.

ClearPass Exchange works with SEIM tools to provide user, device and location visibility into security events. With helpdesk ticketing tools, it can respond to an authentication failure by automatically creating a helpdesk ticket that includes information about the user, device, location, and cause of the failure.

ClearPass Exchange also leverages representational state transfer (RESTful) programming and data feeds like syslog to trigger business relevant actions for a variety of web-based systems – making it easy for IT to streamline processes and workflows.

For additional access security, Aruba RFProtect works with AirWave to provide spectrum visibility, event history and correlation, location tracking, and security reports to satisfy regulatory compliance, as well as to support the configuration and dynamic enforcement of network security policies.

AUTOMATED NETWORK ACCESS FOR CLIENTS AND CONTRACTORS

In addition to employee-owned devices, financial institutions are under pressure to offer secure network access to clients, contractors, and other guests. Mobility-Defined Networks achieve this by isolating different classes of traffic and leveraging the same network infrastructure for all users.

Automating secure network access for clients, contractors and guests eliminates the need to involve IT and enables business to redirect IT resources to solving more critical issues. With Mobility-Defined Networks, businesses can even engage onsite visitors with personalized, location-relevant push notifications.

The Aruba Policy Enforcement Firewall, with its stateful app-level visibility and granular user-based network access controls, lets IT specify and enforce who can access the network and where as well as what devices they can use. It can separate employee, client and contractor traffic on the same network by applying policies uniformly across wireless, wired and VPNs.

And with ClearPass, IT can automate many of the time-consuming tasks that the IT helpdesk has traditionally done manually. For example, *ClearPass Guest* enables contractors, guests and other users to self-register for wired or Wi-Fi access through personalized portals that automatically apply the appropriate user role and network access privileges.

Guest onboarding is further secured using a sponsor-approved workflow that only grants network access after an authorized user, or sponsor, approves the guest's request. This level of automation reduces helpdesk calls and provides a better guest experience.

Aruba automates guest and contractor access via self-service workflows and auto-delivery of user credentials via SMS and email, without compromising security. IT maintains full visibility and control to effectively manage users and devices on the network. And all guest network activity can be captured and logged for reporting and regulatory compliance purposes.

MOVING FORWARD WITH MOBILITY-DEFINED NETWORKS

Financial institutions that embrace Mobility-Defined Networks are better-able to respond quickly to changing market and client demands, expand revenue opportunities and compete more effectively.

Mobility-Defined Networks can be deployed without forklift changes to existing networks and transform wired and wireless into one cohesive and manageable system. The result is a mobility experience that IT and users can trust, business continuity across multiple locations and employees, secure access for personally-owned devices, and secure, automated network access for guests.

Perhaps the most transformative aspect of Mobility-Defined Networks is the ability to rightsize the wired infrastructure. This enables IT to free up their budgets and focus on mobility. Instead of maintaining static legacy configurations, IT cut costs by eliminating unnecessary wired ports and consolidating the fixed infrastructure.

The resulting rightsized infrastructure enables IT to dramatically reduce capital and operating expenses, eliminate network complexity, accelerate the delivery of network services, and provide a uniquely personalized mobility experience.



1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com

©2014 Aruba Networks, Inc. Aruba Networks®, Aruba The Mobile Edge Company® (stylized), Aruba Mobility Management System®, People Move. Networks Must Follow®, Mobile Edge Architecture®, RFProtect®, Green Island®, ETIPS®, ClientMatch®, Bluescanner™ and The All Wireless Workspace Is Open For Business™ are all Marks of Aruba Networks, Inc. in the United States and certain other countries. The preceding list may not necessarily be complete and the absence of any mark from this list does not mean that it is not an Aruba Networks, Inc. mark. All rights reserved. Aruba Networks, Inc. reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba Networks, Inc. uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba Networks, Inc. will assume no responsibility for any errors or omissions. SO_FinancialServices_030814