ADVANCED SECURITY FOR CLOUD WI-FI AND ON-BOARDING

> Enterprises are developing intuitive self-service workflows with streamlined network onboarding so bring-your-own-device (BYOD) users, guests and IT-issued devices can gain network access simply and securely without IT intervention.

The global BYOD market is expected to register a compound annual growth rate of over 15% between 2019 and 2024 with Asia-Pacific witnessing the highest growth rate. BYOD adoption is being driven by increasing adoption of mobile devices in everyday life to access information anywhere and everywhere, be it work related or personal information; rising IT expenditure across diverse sectors; work-from-home culture; and government Smart City initiatives.

Moreover, failure to secure network access is a risk that many organisations cannot ignore. Aligned with simple ways to improve security related to wired and wireless access, the CommScope-Ruckus portfolio of solutions bolsters data security with increased visibility and control over devices and users allowed on the network.

SECURE ON-BOARDING

Expectations of enterprise end-users, especially for self-service, have been shaped by their experience as consumers. Users are familiar with the common set-it-and-forget-it experience of activating a new cell phone at the carrier retail outlet or connecting to a home Wi-Fi source.

But in the enterprise environment, IT organisations typically rely on cumbersome methods for network on-boarding and authentication, like MAC authentication and conventional pre-shared keys (PSKs) that are built into their networking infrastructure.

A better fit for network on-boarding is self-service with the right mechanism in place so that it is easy and intuitive for users. This calls for a purpose-built system for secure network on-boarding where users only have to go through the on-boarding process once without IT intervention.

CLOUDPATH ENROLMENT SYSTEM

The CommScope Ruckus Cloudpath Enrollment System software or software-as-a-service platform streamlines network on-boarding for BYOD users, guests and IT-owned devices. It enables IT teams to define and manage policies for role-based access; delivers visibility and granular control over what devices users can access on the network; and dramatically reduces help desk tickets related to network access.

Cloudpath secures every connection with WPA2-Enterprise, protecting data in transit between the device and the access point (AP) with powerful encryption. Internal users can self-provision any device for network access using their existing login credentials. A digital certificate for network authentication ensures that after the initial connection, users do not need to hassle with Wi-Fi passwords.

Guest users access a self-service login portal and receive credentials for internet access via email or SMS. Be it cloud-based or virtualized on-premises deployment, the solution supports any user, any device, and any network infrastructure.

IOT ENDPOINT ON-BOARDING

Secure device on-boarding is also a challenge for organisations seeking to deploy IoT solutions in the face of a fragmented ecosystem of standards, devices and services. Common IoT access addresses these issues by consolidating multiple physical-layer networks into a single converged network.

This common network establishes uniform security protocols and converges IoT endpoint management and policy setting. The CommScope Ruckus IoT Suite simplifies the creation of such an access network through the reuse of LAN and WLAN infrastructure, thus shortening deployment duration and reducing cost to support multiple IoT solutions.

This concept is applied across various verticals such as manufacturing, hospitality, healthcare and education. In hotels, an increasing number of wireless devices and systems for both guests and staff connect to Wi-Fi as well as other forms of wireless protocols such as Zigbee, LoRa or Bluetooth Low-Energy (BLE). Unifying these wireless protocols within a single AP enables hotels to save physical space and streamline secure device on-boarding.

Additionally, a converged AP, such as the CommScope Ruckus R730 Access Point, allows IT staff to easily view, manage and secure an entire wireless infrastructure. This facilitates network automation, generation of actionable analytics, and creation of custom dashboards with open APIs.

In addition, a converged AP can support Citizens Broadband Radio Service (CBRS), which enables hotels to create their own private LTE networks and provide reliable mobile coverage in support of guest experience.

CLOUD WI-FI

The CommScope Ruckus Cloud Wi-Fi wireless LAN management-as-a-service, coupled with Cloudpath subscription, takes complexity out of the secure on-boarding of new users and guests in Wi-Fi-enabled buildings and campuses.

With Cloudpath software's 802.1X certificate management and Ruckus cloud-managed Wi-Fi, even small IT departments can remotely and easily add new users and wireless APs; administer guest networks; and manage entire Wi-Fi-enabled buildings and campuses or any multi-site deployments.

Ruckus Cloud Wi-Fi enables IT departments to provision, monitor, optimise and troubleshoot an enterprise-grade Wi-Fi network with intuitive simplicity via a single web dashboard or mobile app. This has helped retailers easily capture detailed analytics; hotels enhance the overall guest experience; and retirement and nursing homes monitor health data in real time, among other use cases.

SUCCESS STORY: ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION, MALAYSIA

FAST, SECURE CAMPUS WI-FI ELEVATES LEARNING EXPERIENCE

The Asia Pacific University of Technology & Innovation (APU) aims to provide access to the best learning and teaching experience. To this end, the institute wanted a high-performing Wi-Fi network that is easy to deploy and maintain.

With smart devices already widely used on campus, enabling secure and simple on-boarding for faculty, staff and students was a critical requirement.

Students need to reliably and securely access all the server-side applications needed for their lessons and tutorials, whether from campus or off-campus. The network also supports a wireless environment across multiple platforms including computers, telephones and projectors in lecture halls and university labs.

SOLUTION

With CommScope Ruckus APs providing seamless wireless network roaming across the campus, a virtual SmartZone (vSZ) controller, which can scale up to 300,000 devices, enabled administrators to expand and adapt the network to the changing needs of the university.

Additionally, the CommScope Ruckus ICX switches simplified network set-up, management and upgrades; enhanced security; and minimised troubleshooting. The ICX switching architecture ensured excellent throughput for the most demanding video, unified communications, VDI and mobile applications.

BENEFITS

The CommScope Ruckus solutions have allowed APU to deploy an affordable and highly resilient wired and wireless network to support BYOD, media-rich applications, and the Internet of Things (IoT). Its network now easily handles approximately 7,000 connected

devices at any one time, and with capacity to spare.

The solutions also feature the Dynamic Pre-Shared Key (DPSK) and Ruckus Zero-IT Activation. The DPSK distinguishes lecturers' and students' networks, which makes Wi-Fi usage more secure. The Zero-IT feature, on the other hand, allows lecturers and students to directly conduct authentication using their user ID without IT intervention.

Granular role-based policies for wireless clients enable the creation of policy groups segmented by user role, domain, location, and OS type, among many other factors. Roles are assigned during the authentication phase of new user on-boarding, along with other policies as desired.

APU plans to apply analytics and insight into functions such as indoor location tracking to help administrators track student movements within campus buildings in case of emergencies, or to enable lecturers to track attendance without requiring students to manually tap in using their student IDs.

APU is planning ahead for future technological and infrastructural needs. Moving forward, Wi-Fi 6 is well poised to support the capacity and reliable connections required by future digital learning tools as well as emerging IoT applications.