Moving from Mobile-First to Mobile-Only

In this Q&A, the BlackBerry Sales Engineering team lays out key considerations for state and local governments as their mobility programs expand and morph to take advantage of emerging technologies and accommodate new use cases.

What does mobility look like in state and local governments today?

The definition of "mobile device" now encompasses not just phones but any non-stationary computing system, including laptops, vehicles and vehicle charging stations. As technology continues to advance at lightning speed, mobile is becoming the norm rather than a luxury, with individuals owning multiple devices. Along with this movement and society's acceptance of work-from-home models (where appropriate), we'll see desktop use give way to a mobile-first approach, which will soon take us to a mobile-only approach.

What trends are you seeing as reliance on mobile devices increases?

COVID-19 created an awakening that a high percentage of historically office-only jobs could be shifted to mobile-only. Personal devices must be protected at the same level as organization-issued devices to maintain security, protect users, and prevent the compromise of personal and enterprise data. CISOs can no longer afford to secure only the network. They must secure the operating system, mobile applications, browsers, access controls and digital signatures. Mobility of the future will expand device protections by converging capabilities such as mobility management, mobile threat detection, data security and Zero Trust — all of which have been a patchwork of apps across vendors.

What challenges do these trends present?

Cost, staffing and the balance between security and user experience all play critical roles in mobility protection. Today's mobile-generation users demand easy, innovative ways of getting the job done. This has driven an influx of third-party software attempting to tie into an agency's infrastructure, databases and existing websites — which weren't designed for the security demands of mobile access. To meet mobile security requirements without sacrificing the user experience, organizations need to update back-end infrastructure as well as security at the user's fingertips. Using a suite of products from a single vendor — along with software as-a-service or a managed services approach — frees staff resources and licensing budgets for use in other areas.

What should organizations consider when they integrate mobile apps with the rest of their enterprise?

Mobile apps introduce exponentially more risk than desktop applications. They're created by countless developers — some professional and some amateur. Historically, mobile apps have not received the same penetration testing, vetting and inspection as desktop applications. Loading mobile apps onto a user's device without that scrutiny opens the flood gates for undetected back doors, insecure transmissions, database access and other vulnerabilities. Mobile threat detection solutions that employ AI and machine learning provide prevention rather than the detection and response methodologies of traditional solutions. Using these next-generation solutions along with mobile device management platforms lowers the risk as much as possible.

What would you recommend for creating a strong, secure foundation for mobile initiatives?

Organizations must secure all devices that process enterprise data. It's important to look past "industry standard" protections of yesterday and embrace newer technologies that employ AI and machine learning to provide smarter, quicker and lighter-weight ways of protecting assets. In addition, it's best to implement mobile-first architectures, 5G (as well as the anticipated 6G release) and cloud architectures simultaneously with their non-mobile infrastructure counterparts. Non-negotiables include yearly penetration testing, programs to review and test third-party applications within agency environments, and securing mobile devices as strongly as desktops. It's also wise to ensure the security posture of cloud environments is equivalent to on-premises environments. Of course, securing data in transit and at rest is essential. Finally, end-to-end security can't take a back seat to appeasing users' demands.

What do you foresee in the near future for mobility?

The successful roll out of 5G and the anticipated 6G development get technology closer to mobile-only. Mobile devices of all kinds will continue to emerge in new and unexpected places. Technologies for access control and to protect against hacking, ransomware and malware will continue to improve, diminishing risks to near zero.