The Mobile App is the New Endpoint

The landscape of enterprise endpoints has shifted dramatically in the last few years, as typical endpoints have evolved from laptops to mobile devices—a shift that's likely to grow as mobile devices offer increased screen sizes and resolutions, better onscreen keyboards and more processing power.

Recently, Apple CEO Tim Cook was widely quoted as saying that he doesn't even travel with a laptop anymore; he gets along fine with just an iPad and an iPhone. Cook can leave his laptop behind because software is evolving, too, from desktop applications to self-hosted web applications, to SaaS, and now to mobile apps. Using the apps on his two iOS devices, Cook can do everything he needs to do when he's on the road.

BYOD and Mobile Security

In this new enterprise environment, more data flows through mobile devices and their applications than through many other systems in the organization. The crucial factor in this evolution is that it's no longer the device that really matters—Cook could use a Surface Pro and a Galaxy and still get his work done. What's important now are the applications on the device—native apps, third-party apps, custom apps and integrations among them. These mobile apps are the new interface between the enterprise and its end users. These apps contain corporate data, and provide access to back-end systems, which is critical to get work done —and why employees from CEOs to transportation drivers are moving to them for day-to-day use in business.

Security Considerations

As the perimeter of the enterprise erodes and devices exist in a more distributed environment, enterprise teams have the complicated task of figuring out what they can still manage. In this day of BYOD devices and zero-trust operating environments, IT and security professionals gain nothing from trying to manage the unmanageable—which is just as well, because the device is no longer the endpoint that matters.

The new endpoint is the mobile app: it's our interface with the user and the point at which data and transactions come into the enterprise, or service provider or retailer or financial institution. It's the new focus of users' interactions and the workflows they rely upon to make themselves more productive. It's the new vault for the things that matter in their lives—their organizations' proprietary information and their own HR records, the private health information they share with their doctors and their kids' social security numbers for school. Mobile apps have quickly become where all of us store our most vital data.

And attackers know that the money is where the data resides. They know that security is often overlooked in the rush to release mobile apps, leaving an open door to data. So now we're all mobile app enabled, attackers are starting to go after a wide variety apps to extract data—travel apps, dating apps, mobile payment apps and others. Some of the biggest brands on the planet—from T-Mobile to Walmart—have been found to have security flaws in their applications.

All of us—end users and IT professionals alike—must begin to think more about how we use mobile applications. What data are we putting into our apps? What data are we sharing among apps? What are the developers of those apps doing with our data? And further: What are our contacts doing with information we've shared with them? Are they uploading it to insecure mobile apps or via mobile app to some backend service? What if one of those organizations is compromised, and then compromises the data of people who aren't even customers or users of that application? Even when enterprises deploy apps that are secure, poor practices by users can expose the enterprise to external risks.

Strategies for Mobile Security

For too long, IT and security professionals have relied on closed ecosystems of managed devices to implement security that may be hard to penetrate from the outside but once in had little to no real protection. But ecosystems are no longer protected by a hard shell: they're open, highly distributed and alarmingly susceptible to attack. We don't control the devices—too many of them are BYOD. We don't control the mobile operating systems—we can't get low enough to defend the OS level from threats. What we can do is get security controls and risk mitigation technologies as close to the data and access as possible. This goal is the logical one we've been working toward for many years with database security, desktop security and web apps security.

In this new mobile world, our best chance is to protect applications, and we have a real duty—a real responsibility—to manage them, secure them and use them to safeguard the data that end users consume and produce. The application is an endpoint that enterprises can manage, much as we manage APIs and other endpoints. We can put security frameworks into our apps to defend against threats. We can enforce secure coding. We can utilize mobile app management products to enforce policies or to remove offending apps.

Realizing that mobile apps are our new endpoints forces us into a more mature strategy for data protection. Forward-leaning companies are embracing this challenge as a new opportunity to ensure that no matter where an application goes, no matter what mobile operating system or device its users employ, data and users are protected—as is access to the things that matter.