Changes in Mobile and Remote Work Require a New Security Model

More than ever before, enterprise employees are getting work done outside the traditional office perimeter while using mobile devices. A majority of U.S. enterprises say they support partial or full remote work for the foreseeable future.
Organizations now offer workers the choice of either using their own device or choosing the type of device provided to them with a wide range of security and management functions available. Many end users are still wary of traditional heavy-handed device management approaches to both corporate-owned or personal devices. Meanwhile, mobile devices have become a primary attack vector for targeted attempts to compromise data or steal sensitive information.

As a result of these shifts, businesses are rethinking their network access architectures. Doing so will help them support remote and hybrid workers using Android and iOS devices as a primary work device. In addition, the focus of cybercriminals and bad actors has shifted to the mobile vector as businesses see attacks and data theft attempts against workers’ mobile devices growing. The new model for securing this kind of environment must separate detection points, policy enforcement, and remediation actions from on-device functions.

They should also distinguish from technologies that rely on perimeter-based security tools. Modern cloud-centric security architectures put security controls, monitoring and remediation closer to the apps that workers use. This enables advanced security functions such as multi-factor authentication and continuous conditional access controls that are based on user and device behavior, health, and context.

In the near future, the “where” (location) and “what” (device type) factors of digital work will matter less. This will accelerate the need for compliance, strong security principles, and cloud-centric data protection strategies. Organizations looking to digitally transform operations and improve employee support in the wake of 2020 and looking beyond, must consider modernizing their mobile security, management, and overall app and data access strategies as an integral part of a broader movement towards organizational resiliency.

Message from the Sponsors

**Lookout** is the leading cybersecurity provider of integrated endpoint-to-cloud security. Our mission is to secure and empower productivity in a privacy-focused world, where work and play can happen anywhere. With everything now in the cloud, it’s critical that cybersecurity follows you wherever you go, securing your data from the endpoint all the way to the cloud.

Learn more

**Google Cloud** provides organizations with leading infrastructure, platform capabilities and industry solutions. We deliver enterprise-grade cloud solutions that leverage Google’s cutting-edge technology to help companies operate more efficiently and adapt to changing needs, giving customers a foundation for the future. Customers in more than 150 countries turn to Google Cloud as their trusted partner to solve their most critical business problems.

Learn more

© 2021 IDC Research, Inc.
IDC materials are licensed for external use, and in no way does the use or publication of IDC research indicate IDC’s endorsement of the sponsor’s or licensee’s products or strategies.
Privacy Policy  |  CCPA