WHEN ALL THE WORLD'S A WORKSPACE

IT leaders redefine strategies for mobile security as they adopt multiple, heterogeneous cloud services.

Mobile first is more than a marketing slogan; it's a workforce mentality. Thanks to mobile devices in multiple form factors, users work wherever they happen to be – in the office, at home, on the road. With around-the-clock access to apps and data behind an enterprise firewall, and increasingly, in the cloud, they're more adaptive, collaborative and productive.

In fact, the combination of mobile technologies and cloud computing multiplies the competitive opportunities for many organizations. But this benefit comes with a significant drawback: As opportunities for collaboration and productivity grow, so do security threat vectors. Consider the matrix of vulnerabilities: Most users have at least two mobile devices, and some carry everything from smartphones to tablets, notebooks and wearables – all potentially running different operating systems. Many of these devices run personal apps alongside business apps or are used to access any number of cloud-based applications. Many organizations allow users to connect their personal devices to enterprise networks in what are commonly known as bring-your-own-device (BYOD) programs. And IT leaders also must accommodate a growing number of partners, contractors and guests who expect some level of network access in the course of daily operations.

You Are the Weakest Link

In the minds of CISOs, the characteristics that make the mobile device such a powerful business tool also make it among the weakest links in an organization's security posture. It's not just that users have more control over these devices than they do traditional PCs, but they're also connecting to different resources over wired and wireless networks, so the clearly defined perimeter that was a first line of defense has given way to IT environments with no clear borders.

"IT departments are used to having a boundary to work with, and it's always been around the data center," says Jay Kelley, senior product marketing manager at F5 Networks, whose portfolio includes products that help customers secure access to apps wherever they reside. "The problem is, apps are no longer just in the data center. They can be virtually anywhere."

And increasingly, these apps reside in the cloud. In a 2015 survey conducted by SkyHigh Networks, a cloud access security broker, IT respondents from organizations of all sizes said that, on average, they're using more than 1,100 cloud services, with 73 percent comprising enterprise services. Across all mobile platforms, use of cloud services increased nearly 63 percent in 2015 over 2014. The majority of these are cloud-native collaboration

"IT departments are used to having a boundary to work with, and it's always been around the data center ... The problem is, apps are no longer just in the data center. They can be virtually anywhere."

—Jay Kelley, Senior Product Marketing Manager, F5 Networks

and content-sharing apps, but many respondents either have moved or are considering migrating legacy customer relationship management, human resources and other major systems to the cloud. Though 32.7 percent of IT leaders surveyed by the Cloud Security Alliance in 2015 cited better security capabilities as a benefit of such migrations, more than two-thirds said concerns over their ability to enforce corporate security policies are a stumbling block.

Further, in a 2015 IDG Research Service survey of IT leaders, 95 percent of respondents said they believe data accessed by or residing on users' mobile devices increases their risk of breach. These concerns aren't unsubstantiated: Nearly 75 percent said they'd suffered a breach attributable to a mobile security issue.

"Mobile devices are blowing up the idea of the fixed perimeter," says Trent Fierro, director of security solutions marketing at Aruba Networks, whose offerings include products that help customers provision and manage devices and enforce security policies for accessing applications running anywhere. To secure a mobile workforce today, he says, "you have to be more targeted, treating individual users as having their own perimeter." This requires what Fierro calls an "adapted trust" model, which lets administrators define granular policies that map to how specific users work.

Moreover, the focus for mobile security initiatives should be on applications rather than data, according to Kelley. F5 treats the application, wherever it resides, as the perimeter. "The application is the gateway to all the data sources that feed it," Kelley says. "By securing the application, you automatically secure the data that's behind it."

From MDM to EMM

Mobile devices introduce risk in a number of ways. A lost or stolen device is a major threat, but it's far from the only one that organizations face. The number, skill and sophistication of cyberattackers continue to grow, and those who focus on attacking mobile platforms are no exception.

If a device is stolen or lost, the ramifications vary. If policies successfully restrict device usage to basic functions such as browser-based email, risks are lower. Using mobile device management (MDM) software, IT teams can remotely lock a device or wipe it clean of all enterprise data.

Today, IT departments with mature mobile security programs don't allow much choice in anything that could affect security — the potential damage caused by ignoring policies, indulging in shadow IT activity, or making bad decisions far outweighs concerns about irritating employees. In the cloud realm, security efforts are aided by enhanced encryption from cloud providers, which encrypt data at rest and in-transit and increasingly let IT administrators hold encryption keys. New enterprise-class security features in mobile operating systems also improve cyberdefenses.

In addition, the move from MDM to more advanced enterprise mobility management (EMM) suites puts more control in IT administrators' hands. Beyond securing and managing devices, EMM has a host of features for managing applications and content.

"MDM features have essentially been absorbed into the larger EMM feature set," says Eric Parizo, senior analyst for enterprise security at Current Analysis. The latest EMM suites better secure the device ecosystem through deployment and management features with more granular security controls. "You can deploy apps to all your mobile devices, regardless of operating system, but define different privileges for each based on users, user groups, location of device and more," Parizo says.

EMM suites also integrate with policy platform providers such as Aruba and F5 to enable provisioning of per-app virtual private network access, so that only a designated application gets through firewalls to access back-end systems. "Per-app VPN is an important security control. If you have only device-level VPN, everything on the device goes through the VPN," says Kelley. IT teams don't want to deal with the possible ramifications >

Double-Check Your Security Posture

As mobile device and cloud app usage grows, even large organizations with teams of security specialists have trouble accurately assessing the strength of their threat defense. Many organizations hire security specialists to conduct a thorough threat assessment and establish a security baseline, after which they conduct periodic security audits.

These audits should include penetration testing. Specialists that provide comprehensive pen-testing services can test systems from different perspectives. They can test internally to determine which systems are vulnerable to insider threats, externally to identify vulnerabilities at the perimeter and beyond, and even drill down to conduct app-specific pen tests to identify risky mobile applications.

of having, say, a user's Facebook info coming into the data center.

Centralizing Authentication

One of the biggest challenges IT departments face in enabling mobile access to multiple heterogeneous cloud applications is secure authentication. If an organization is migrating from on-premises Microsoft Exchange to Office 365 running in Microsoft's Azure cloud service, for instance, it needs two different methods of authentication. "A lot of times, a business has to provide its authentication database — the crown jewels of the company — to their cloud providers so they can duplicate it in their environment to secure user access to apps," says Kelley. "That requires a lot of trust."

Moreover, an organization with multiple cloud providers must deal with the identity silos created when each provider has its own authentication mechanism. The solution lies in identity federation, which connects different identity and access management (IAM) systems through identity service providers. Federated IAM systems serve as a trusted source for validating and tokenizing credentials so users can access multiple cloud applications through a single authentication point. By using technologies based on such identity standards as Security Assertion Markup Language, OAuth and the System for Cross-Domain Identity Management, IT organizations, security technology providers, identity service providers and cloud providers all share responsibility for securing mobile access.

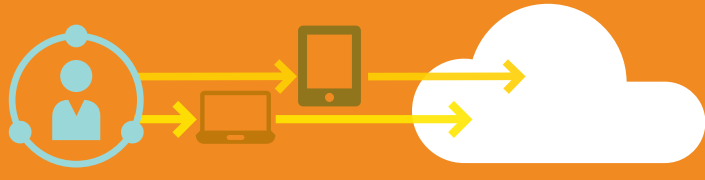
Federated IAM is offered as a service by cloud providers, as well as through comprehensive management services provided by cloud access security brokers (CASBs). These brokers integrate identity services, EMM and other hosted services, and provide compete visibility into mobile activity through monitoring, analysis and similar functions.

"CASBs provide the platform for managing access and privileges for a variety of different cloud services," says Parizo. They also scan environments for use of unauthorized cloud apps and alert organizations so they can take action.

Malware Protection

In today's threat landscape, according to Verizon's 2015 Data Breach Investigations Report, mobile malware doesn't yet register as a data breach problem. According to the report's authors, mobile devices haven't become a preferred vector for cyberattackers, with most mobile malware taking the form of "adnoyance-ware."

Nonetheless, IT teams need to deploy anti- malware as part of mobile protection and larger defense-in-depth strategies. When devices connect to the network,



Take Mobility Management to the Cloud

As the move to the cloud continues on all fronts, more IT departments are choosing cloud-based mobility management platforms to manage devices, apps and data, as well as mobile policies and provisioning.

"Cloud-based EMM makes a lot of sense because mobile devices are used not just off a company's physical premises but to access resources outside the corporate network," says Melanie Turek, a research vice president at Frost & Sullivan. The cloud is especially appealing for the large number of organizations that are just getting serious about EMM solutions. "If you don't have mobile management tools in place or what you have isn't enterprise-class, it's easy to go immediately to EMM in the cloud rather than figure out how to hybridize mobile security," Turek says.

Even today, EMM deployments can be complex. "That's why you don't see many customers using all the features in their EMM suites, and vendors starting to package offerings that target buyers based on where they sit on the mobile maturity curve," says Eric Parizo, senior analyst for enterprise security at Current Analysis.

On-premises EMM and MDM vendors are all moving toward hosted models, Parizo says. "Unquestionably, it's where the industry is going because it's so much easier than deploying and managing multiple appliances on-premises. Scaling that down by offering cloud-based solutions is a powerful value proposition for customers."

66%

The percentage of IT leaders who say they're very or extremely concerned about the security of mobile apps that access or transmit sensitive data

Source: IDG Research Service, "Buying into Mobile Security," October 2015

spearphishing presents the same problem it does on any computer. Further, more developers are creating malicious social and business apps, downloadable for free, and waiting until a device running a malicious app connects to a network. They then use the app as a gateway to prowl around for a place to plant malicious code. Enterprises should consider download policies, MDM controls, blacklisting and corporate app stores to mitigate this problem.

Bring Your Own? If IT Owns Security

If IT departments allow BYOD for enterprise use, they should apply the same security controls for any device that connects to their own and other networks, experts say. According to a 2015 Frost & Sullivan survey, 65 percent of U.S.-based IT decision-makers let users connect their own smartphones to an internal network. Further, Gartner predicts that by 2020, approximately 65 percent of organizations will require users to provide their own devices for work.

For BYOD, IT departments should dictate what enterprise applications devices run and monitor compliance via policy management tools. They should also secure these apps through containerization, which allows users to employ smartphones or tablets for both work and play because business apps are isolated from personal apps in their own container.

"Containerization has proven very effective," says Kelley. "If a device is lost or stolen, or an employee leaves the company, IT can just swipe the container and leave personal information untouched."

In addition, more organizations are creating security-smart configurations for mobile devices based on various job roles. If users refuse to accept implemented configurations, IT staff can use policy enforcement software to deny access to various internal and cloud resources.

When enrolling a new device, Aruba's ClearPass, for instance, uses an onboarding tool that takes a user's login and password to create a device certificate. It then pushes the certificate to the smartphone or tablet, obviating the need to use credentials to connect to a network. Further, administrators now have a detailed record of the device — information that plays into efforts to better secure, manage and analyze their entire fleet.

"You can improve security significantly by using contextual data and profiling to your advantage," says Fierro. For instance, if IT teams learn that a new device release has vulnerabilities in its OS, they can profile their fleet to determine how many of these devices are using internal and external network resources and take appropriate action.

Can IT See Clearly Now?

With security threats growing, private and public entities are joining forces to share cyber- and physical-threat information to get a better picture of what they face. Improved visibility into mobile activity is a key weapon in the larger security battle, and technology and cloud service providers are opening up through application programming interfaces and other means so customers can see what's happening with their users and data.

Many on-premises and cloud-based security technologies provide centralized views into mobile activities they're designed to manage. Today, security information and event management (SIEM) products are a leading way to bring together log and monitoring data captured by the diverse security tools, which they then present through a single dashboard. Using real-time analysis of trends and other indicators, SIEM systems also help administrators identify anomalies and incidents so they take action before they become catastrophes. ■

To learn more about strategies for protecting against threats, read the CDW Tech Insights Guide "Next-Generation Security" at CDW.com/next-generation-security-insights