EXECUTIVE BRIEF

MAKING #GENMOBILE SECURE

Mitigating risks associated with enterprise mobility

Mobile devices now dominate our workplaces, thanks to a new generation of worker known as #GenMobile. The flexibility to use just about any number of personal devices for work keeps everyone connected to vital information.

But the freedom to work from anywhere at any time exposes enterprise IT to a variety of unforeseen risks. To maintain a high degree of security, organizations need to understand associated risks and implement proper techniques to help mitigate the loss of devices and data.

IDENTIFY RISKS VS. GOALS

Creating mobility policies without an overall plan can hurt the security posture of a network. Defining a tolerable level of risk based on business needs is an important first step in determining how and where to implement policies that support users' mobility needs.

In the past, security required a strong defensive perimeter to protect the network from outsiders. Mobility brought about a zero-trust approach from traditional security vendors because that well-defined perimeter no longer exists. Security from the inside out is now equally important.

Moving forward, an adaptive trust approach – one that uses access policies based on a range of contextual data – is the best way to ensure secure mobility. Contextual data can include user roles, device types, application usage, location, time-of-day, and even Active Directory status.

When employing an adaptive trust approach, it is also important to identify acceptable risk levels for users and devices. Users authenticating at their desks using valid Active Directory credentials does not necessarily mean they can be trusted.

Knowing what devices are connected and where they're connected allows IT to make better-informed decisions. In addition to identifying and assigning risk levels to users and device types, these critical factors should be considered in adaptive trust approach to network access:

- Location, time-of-day, day-of-week.
- Health assessment of a device.
- Wi-Fi vs. wired connections.

By combining policy management, traditional security solutions and risk assignment for mobile users and devices, enterprise IT can ensure strong access protection for today's mobility infrastructure as well as for the #GenMobile workforce.

POLICY ENFORCEMENT: BEYOND AUTHENTICATION

Legacy authentication, authorization and accounting (AAA) grants basic network access privileges but is unable to deal with the unique traits of mobility. These older AAA solutions can't use all of the contextual data available today to allow or restrict access based on user roles, multiple devices and types, access method, or location.

What's more, legacy AAA is prohibitively expensive and technically difficult to integrate with mobile device management (MDM), firewall and other threat protection solutions. This integration is essential for strong access security across the entire infrastructure.

USER AND DEVICE RISK CATEGORIES

	Users	Devices
High risk	Security positions, road warriors, engineers, executives	Mobile phones, tablets, laptops
Low risk	Clerks, order entry, administration, marketing	Desktop computers and IP phones, printers, cameras
Compliance oriented	Doctors, nurses, financial analysts, legal, retail associates	Medical devices, Point-of-sale systems, safety equipment
Public facing & M2M	Guests, fans, shoppers	Asset tracking, environmental sensors, meters

It's equally difficult to enforce network-based policies using device-specific attributes – such as jailbroken status – without a tightly-integrated solution that can leverage critical information provided by leading MDM/EMM solutions.

IT now needs a robust policy engine, with next-generation AAA capabilities, device profiling, and the ability to leverage information from the existing security infrastructure. IT can then create policies that fortify network defenses and mitigate risks based on trusted contextual data.

STRONG DEVICE AUTHENTICATION

A user's identity and role are vital to the creation of policies and IT must consider this when differentiating access privileges for IT-issued and personal devices. Active Directory attributes alone are insufficient and creating the same policies that apply to all is a recipe for disaster.

Providing unique credentials or device certificates for all authenticating devices adds a layer of control, especially for smartphones and tablets. Certificates ensure that devices are authorized to access the network and eliminate the need for usernames and passwords.

In addition to eliminating the risks associated with brute-force password attacks, this is the most beneficial path to ensuring a secure and productive enterprise mobility experience for your #GenMobile workforce. And if a device is lost or stolen, access by that device can be revoked instead of revoking access of the user's Active Directory account.

DEVICE MANAGEMENT AND APP PROTECTION

Enterprise data access and storage by personal devices exposes organizations to a host of new risks. In addition to potential loss and theft of these devices, regulatory compliance mandates, privacy laws, and other legal issues must be weighed.

Careful planning and proper risk assessments should occur before allowing personal devices to connect. MDM and enterprise mobility management (EMM) can mitigate risks associated with lost devices, as well as the applications and data stored on these devices.

MDM/EMM and policy integration give IT a wide range of controls over where and how devices are used for work. When devices are not connected to the enterprise, IT can enforce PIN protection, secure access to work apps, and remotely wipe content from lost or stolen devices.

CONTEXTUAL DATA FOR ADAPTIVE TRUST POLICY ENFORCEMENT

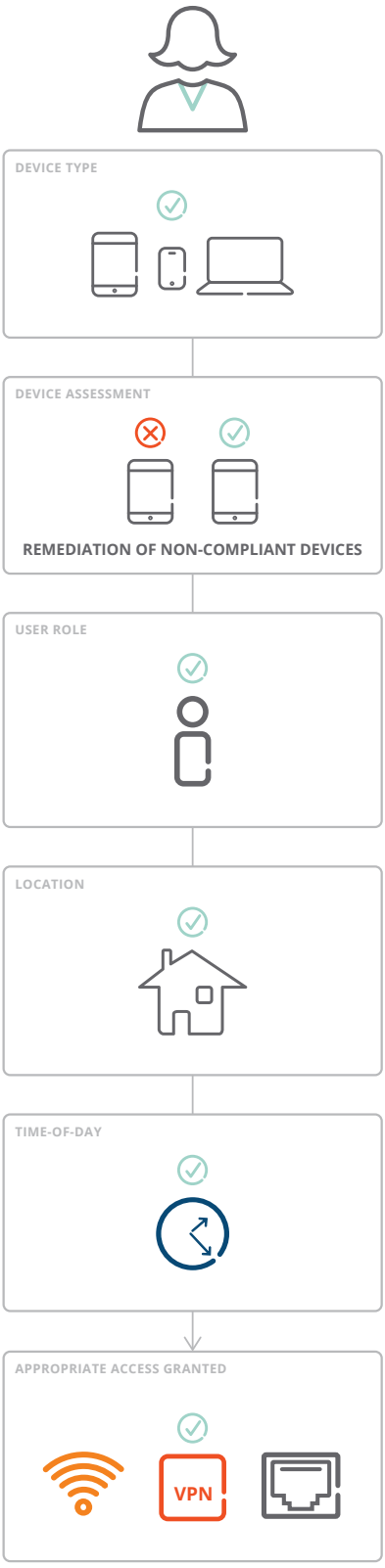

figure 1.0_10064_mobilityrisk-eba

CONCLUSION

Unfortunately, the security perimeter that used to prevent attacks from the outside no longer applies since users can connect from anywhere with any device. The biggest threats now come from within. Embracing zero-trust thinking is one approach, but may not be adequate for today's fast changing mobility needs.

Fortunately, an adaptive trust approach to secure enterprise mobility enables IT organizations to turn zero-trust inside out. These critical steps leading to adaptive trust can mitigate the risks associated with enterprise mobility:

- Go with adaptive trust and rely on contextual data about user roles, devices and location.
- Identify and assign acceptable risks and assess them against overall security goals.
- It's time to give up the old legacy AAA in favor of modern policy enforcement.
- Require unique credentials and certificates for all authenticating devices.
- Integrate policies with MDM/EMM for device management and app protection.

With adaptive trust, IT can make smarter decisions about how users and devices connect and how access privileges are enforced. Consequently, a centralized policy enforcement engine that integrates with MDM/EMM becomes the central nervous system for everything that connects.

aruba NETWORKS

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com