

“ZERO TRUST” FOR ENTERPRISE MOBILITY: THE BRAKES THAT HELP YOUR USERS GO FASTER

November 2019

Derek E. Brink, CISSP

Vice President and Research Fellow, Information Security and IT GRC

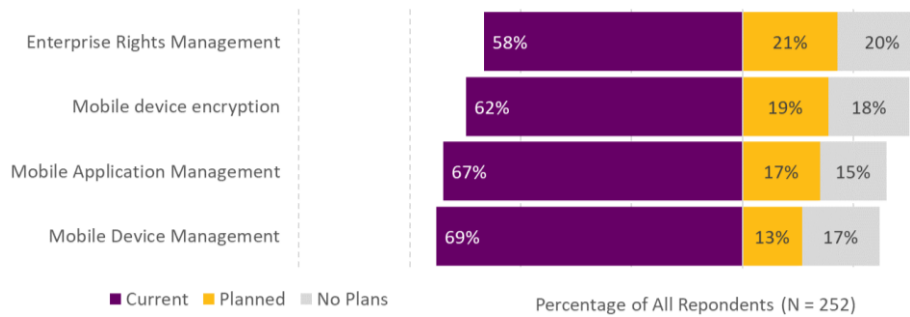
Aberdeen’s research shows that mobile security solution categories, which are consistent with the principles of **zero trust** — such as *mobile threat defense, device monitoring and analytics, and adaptive access controls* — are among the highest for planned deployments over the next 12 months. In this report, Aberdeen describes how **business objectives, security risks, and user expectations** for enterprise mobility initiatives are all better addressed by mobile security solutions that incorporate these capabilities.

Under the principles of **zero trust** security, access to enterprise resources is always *conditional* on establishing a level of assurance for devices, users, and normal behaviors and locations, both before and after the initial connection.

Zero Trust Security for Enterprise Mobility: Déjà Vu, Redux

Organizations are increasingly embracing the use of **mobile devices** (e.g., *smartphones, tablets*) to achieve their strategic goals for *digital transformation, collaboration, productivity, and operational efficiency*. At the same time, however, they must also address the associated **risks** related to *security, privacy, and regulatory compliance* from their use of mobile devices — as well as rapidly evolving **user expectations**.

Figure 1: A Common Response to BYOD was Implementation of Controls Designed to Bring Mobile Devices “Under Management”



Source: Aberdeen, November 2019

Initially, a common enterprise response to the pressure of supporting *Bring Your Own Device (BYOD)* was to just say no, followed by implementation of a variety of controls designed to bring all mobile devices “under management.” For example, Aberdeen’s research shows

that **mobile device management**, **mobile application management**, **mobile device encryption**, and **enterprise rights management** are widely deployed, by more than 3 out of 5 respondents (see Figure 1).

More recently, **massive user adoption** of mobile devices for personal use has quickly and irrevocably changed our collective **expectations** regarding their dual use in the enterprise. Today, access to enterprise resources — from any device, at any time, from any location, over any network — is widely considered to be table stakes for user productivity and convenience.

Enterprise users are also more apt to expect that “my device, my data” also implies “my privacy, and my control.” Said another way, enterprise users increasingly feel that their employer has every right to manage its own applications and data on their personal devices...but not theirs.

Your Mobile Security Capabilities Should Support Both Goals

Traditionally, mobile security capabilities have focused on the **technical** aspects of *protecting* against the negative business impact that may result from a loss of *confidentiality*, *integrity*, or *availability* of your enterprise computing resources. These can be referred to as “**unrewarded**” **risks** — i.e., primarily about the *downside*.

Today, mobile security capabilities should also focus on the **business-oriented** aspects of *enabling* the positive business impact that’s desired from the organization’s strategic initiatives — including high-profile areas such as *digital transformation*, *productivity*, and *collaboration*. These opportunities can also be referred to as “**rewarded**” **risks** — i.e., primarily about the *upside*. Both sides of the coin, upside and downside, involve inherent **uncertainties** (this is what makes them **risks**).

Enter the Principles of Zero Trust for Mobile Security

The notion of “zero trust” is anything but new. On the contrary, it’s a topic that both solution providers and security practitioners have been talking about for at least the last 15 years. For example, from the mid-2000s onward:

- ▶ **Network access control (NAC)** was designed to enforce pre-connection policies for **traditional endpoints** (e.g., *PCs*, *laptops*) based on establishing a level of assurance by way of *known users*, *known devices*, and *device posture / health*.

Massive user adoption of mobile devices for personal use has quickly and irrevocably changed our collective **expectations** regarding their dual use in the enterprise.

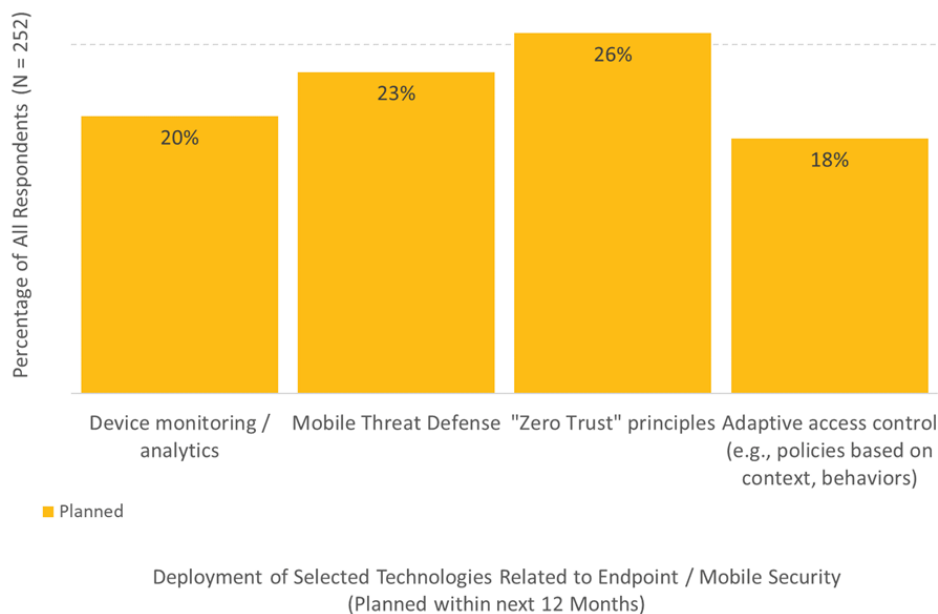
- ▶ **Adaptive authentication** was designed to provide the vast majority of online users with friction-free access to web-based resources, by using dozens of under-the-covers indicators to make a real-time evaluation of the current risk — and to require a higher level of assurance for user identity, as needed.

In the context of current trends in mobile security: Whether or not owned directly by the enterprise, mobile devices are increasingly being assessed for threats and vulnerabilities *before* being granted access to enterprise infrastructure and data — and being continuously monitored for device posture / health and normal user behaviors while connected.

In Aberdeen’s research, solution categories consistent with the principles of zero trust are among the highest for planned deployment over the next 12 months (see Figure 2), such as:


- ▶ **Mobile threat defense (23%)**
- ▶ **Device monitoring and analytics (20%)**
- ▶ **Adaptive access controls (18%)**

Figure 2: Directionally, Enterprises are Moving Towards Mobile Security Controls Consistent with the Principles of Zero Trust



Source: Aberdeen, November 2019

Most organizations have already deployed a **large and complex portfolio** of security tools, products, and services. In Aberdeen’s study,



individual respondents had deployed *between 12 to 45 different solution categories* in the context of mobile and endpoint security, with a *median of 29*. These realities highlight an often-underappreciated challenge, as well as an important opportunity for leading solution providers to help organizations drive incremental investments in mobile security — e.g., by increasing the degree of *integration* and *automation* between solutions.

Making Mobile Security a Priority: What's the Risk?

In Aberdeen's view, **ineffective communication about risk** — in *business terms*, as opposed to *technical details* — is among the most impactful obstacles for faster, broader deployment of mobile security.

Consider the perspective of the organization's senior leadership team, which typically sees a *significant allocation of resources* towards security but an *unclear connection between activities and results*:

- ▶ **Companies worldwide are investing tens of billions of dollars per year on security**, with a forecasted [increase](#) of more than 9% per year
- ▶ **Security solution providers number in the thousands**, a [superabundance of controls and countermeasures](#) which underscores the *importance* of the problem — but also highlights the *complexity* of managing a large portfolio of solutions
- ▶ **Regulatory compliance requirements for data privacy and data security are numerous and complex** — e.g., 6 out of 7 (86%) of respondents in Aberdeen's research have to deal with the complexity of *multiple* types of data and / or data-related processes subject to compliance; 100% have at least one type
- ▶ **Attackers are consistently outperforming the defenders**, with [attacker dwell times](#) — i.e., the time it takes defenders to detect a successful compromise by the attackers — *improving* to a global median of 78 days (still, 10 to 11 weeks) in 2018, but with 25% of compromises still going undetected for one to four years
- ▶ **Data breaches continue unabated**, with [public disclosures](#) of more than 3,200 in 2017-2018 — and while 75% of these were less than 10,000 records, the run rate for mega-breaches of 1M records or more was more than 2 per week

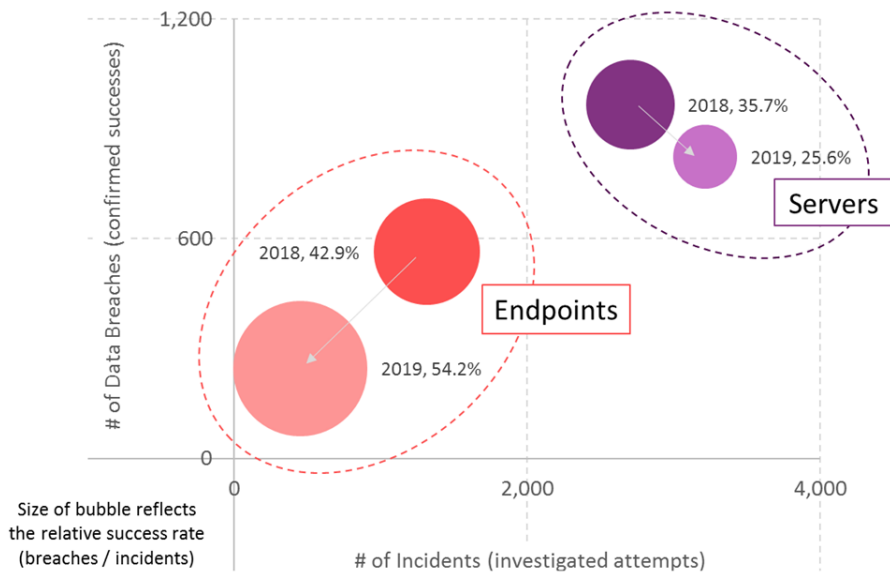
Ultimately, the primary objective of security professionals is to help senior leaders to understand the organization's mobile security-related risks —

In Aberdeen's view, **ineffective communication about risk** — in *business terms*, as opposed to *technical details* — is among the most impactful obstacles for faster, broader deployment of mobile security.

in terms of both *how likely* and *how much business impact*, as risk is properly defined — and to take appropriate steps to help manage those risks to an acceptable level.

For example, Aberdeen’s analysis of data breaches by asset type — based on empirical data on thousands of investigations shared in the Verizon *Data Breach Investigations Report (DBIR)* series — shows that **servers** are more frequently under attack, but **endpoints** are *more than 2-times more likely* than servers to be successfully compromised (see Figure 3). Although back-end systems are typically where the organization’s most valuable assets (i.e., the “crown jewels”) are located, vulnerabilities at the endpoints are attractive targets / points of entry for attackers.

Figure 3: Empirical Data Shows Servers are More Likely to Be Attacked, But Endpoints are More Likely to Be Compromised



Source: Empirical data adapted from Verizon *DBIR* 2018 (N = 4,020) and Verizon *DBIR* 2019 (N = 3,667); Aberdeen, November 2019

Example: The Risk of Mobile Phishing Attacks — How Likely?

As an illustration of how to communicate more effectively about risk in business terms, let’s be even more specific and consider the risk of **mobile phishing attacks**.

Empirical data provides ample evidence that the *likelihood* aspect of mobile phishing attacks is **higher for Android devices than for iOS devices**, as summarized in Table 1.

The Responses to Risk

Not all security-related risks need to be addressed! Risks can be:

- ▶ **Avoided** (e.g., by not undertaking a given initiative at all)
- ▶ **Accepted** (e.g., proceed as planned)
- ▶ **Transferred** to other parties (e.g., contractually, or through insurance)
- ▶ **Managed to an acceptable level** (e.g., through an investment in an appropriate mix of security controls and countermeasures)

The response to risk we should strive to avoid, by communicating more effectively about risk:

- ▶ **Ignored** (which has the same effect as acceptance, except without appropriate consideration)

Table 1: Empirical Data Shows the Likelihood of Mobile Phishing Attacks is Higher for Android Devices than for iOS Devices

Factors of Likelihood	Android devices	iOS devices
Mobile phishing link <i>encounter rates</i> , for every 1,000 mobile devices	50 to 570 (median: 270)	20 to 570 (median: 220)
Mobile phishing link <i>user click rates</i> , for every 1,000 mobile devices	20 to 360 (median: 150)	0 to 250 (median: 80)
<i>Window of vulnerability</i> : Time for installed base to upgrade to the most recent mobile device OS version	<i>Enterprises using MDM</i> are faster to upgrade than <i>Consumers</i>	<i>Consumers</i> are faster to upgrade than <i>Enterprises using MDM</i>

Source: Empirical data adapted from Lookout 2Q19-3Q19; Aberdeen, November 2019

With regard to how long the window of vulnerability is open, Aberdeen’s research is consistent with the empirical data. For respondents in Aberdeen’s recent study, **time to patch** (in total calendar days) ranges from 1 to 2 weeks to more than 3 months, with a median of about 6 to 7 weeks. In addition, **mobile devices are generally out of sync with the latest updates for slightly longer** than traditional endpoints.

Example: The Risk of Mobile Phishing Attacks — How Much Impact?

With respect to the *business impact* aspect of mobile phishing attacks, we can consider factors such as:

- ▶ **Data breaches:** About 4 out of 5 (80%) respondents in Aberdeen’s recent study experienced at least one data breach, with a median of six. As previously noted, 75% of publicly disclosed data breaches over the last two years are relatively small (less than 10K records), but there’s still a non-trivial likelihood of mega-breaches (more than 1M records).
- ▶ **Non-compliance issues:** About 6 out of 7 (86%) respondents in Aberdeen’s recent study experienced at least one non-compliance issue, with a median of six. Even setting aside the possibility of *fines and judgements* for non-compliance, the identification and remediation of non-compliance issues can result in significant *operational expense*.

Aberdeen defines a **non-compliance issue** to be a finding / observation identified as an audit deficiency, or another instance of non-compliance that is substantial enough to require prompt remediation, or a committed plan for remediation — i.e., not an issue that can be deferred or ignored.

- ▶ **Productivity losses:** Respondents in Aberdeen’s recent study report spending between 11% to 86% of their annual IT Operating Expense on mobile devices and endpoints, with a median of 48% — a figure which still doesn’t fully account for the productivity loss for enterprise *users* as a result of mobile phishing attacks.

Example: The Risk of Mobile Phishing Attacks — Quantifying Risk

Pulling together selected factors of both how likely and how much impact, Aberdeen has developed a simple **Monte Carlo** analysis to *quantify* the risk of mobile phishing attacks:

- ▶ In a Monte Carlo analysis, each variable in a calculation is expressed as a *range* (lower bound, upper bound) and a *shape* (probability distribution) — as opposed to as a single, static amount. The relevant calculations are then carried out based on a randomly selected value from the probability distribution for each variable, over many (say, 10,000) independent iterations.
- ▶ In doing so, the result is also expressed as a **range of possible outcomes, along with their associated likelihoods** — as opposed to a single, static amount such as “the average cost of a data breach is \$201 per record.” Most importantly, the result can then be represented in terms of both *how likely* and *how much business impact*, i.e., in terms of *risk*, as risk is properly defined.

For the purposes of this illustrative example, Aberdeen’s quantitative model focuses on the *biggest* factor of business impact from mobile phishing attacks (i.e., data breaches) — which simply means that as is, it represents a *conservative, understated* estimate of the total risk.

A quantification of the risk of mobile phishing attacks — based on the following input parameters: North America; private sector; MDM not deployed; 10K mobile devices (80% iOS, 20% Android); up to 10M data records — is shown in Figure 4. For this scenario, the annualized business impact from mobile phishing attacks ranges from \$0 to a “**long tail**” of more than \$200M, with a **median of about \$500K**.

When talking about risk, “**exceedance curves**” such as the one shown in Figure 4 are pretty standard, and can be read as follows:

- Given the status quo for security policies and controls,
- There is a *Y% likelihood* that the total business impact will exceed *\$X per year*.

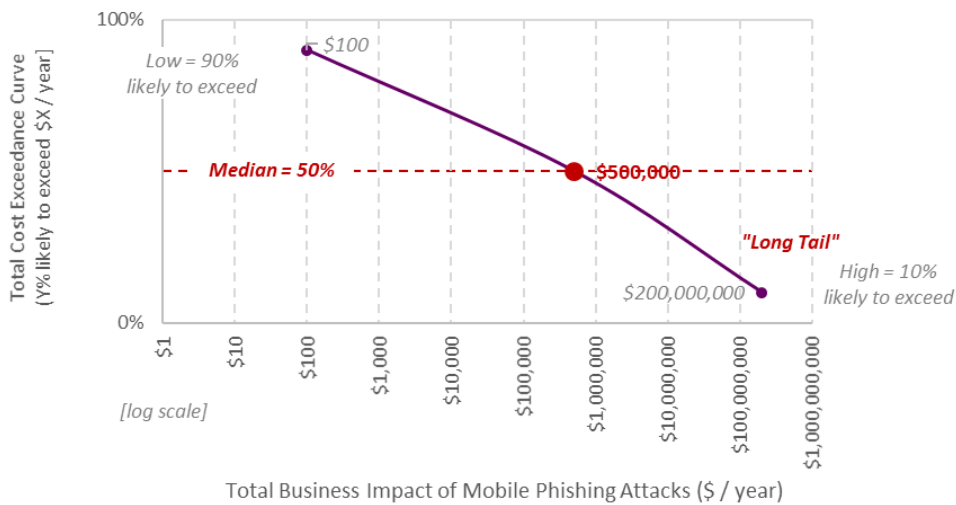
Qualitative risk assessments represent selected factors of likelihood and business impact in terms of *high / medium / low* or *red / yellow / green* — which are sometimes transformed into **pseudo-quantitative** assessments by assigning numeric ranges, such as *1 to 5* or *1 to 100*.

These methods are widely perceived as being easy for senior business leaders to understand, but a moment’s thought makes it clear that their value for making better-informed decisions about risk is dubious at best:

- ▶ Doing math on these values is meaningless
- ▶ Leaders are still asked to make important business decisions about risk based merely on an assessment of “yellow” or “72”

In their dual roles as **subject matter experts** and **trusted advisors** to the senior leadership team, security professionals need to learn how to communicate about risk in ways that move the dial away from the default of mere *intuition* and *gut feel*.

Figure 4: Quantifying the Risk of Mobile Phishing Attacks



Source: Monte Carlo analysis; empirical data adapted from Lookout (*mobile phishing link encounter / click rates*) 2Q19-3Q19; Verizon DBIR 2018; Thales eSecurity www.breachlevelindex.com 2017-2019; Ponemon *Cost of a Data Breach* 2018; Wombat *State of the Phish* 2019; Aberdeen, November 2019

The most important feature of risk exceedance curves is that they properly describe risk not as a single, fixed-point outcome — but as a **range of possible outcomes**, along with their **associated likelihoods**. If we could actually calculate a precise, specific value it wouldn't be a *risk* at all; it would be a *fact!*

Referring again to Figure 4, look at the following points:

- ▶ **90% likely to exceed \$100:** Senior leaders obviously won't care that much about this end of the exceedance curve, which basically says that mobile phishing risks are almost certain to cost the organization *something*.
- ▶ **50% likely to exceed \$500K:** If we only talked about the **median** business impact of mobile phishing risks (please, don't fall into the trap of using the *average*, which conveys *nothing* about the corresponding *likelihood*), it may or may not get the attention of the senior leadership team. While \$500K is a meaningful amount, depending on other priorities and available resources this may well be a risk that senior leaders are willing to accept.
- ▶ **10% likely to exceed \$200M:** Most business decisions about how much risk from mobile phishing attacks is acceptable are going to be made at this, the *"long tail"* end of the risk exceedance curve.

Most business decisions about how much risk from mobile phishing attacks is acceptable are going to be made at the *"long tail"* end of the **exceedance curve**.

On an annualized basis, there's a **10% likelihood** that the total business impact from mobile phishing attacks in this scenario will be **more than \$200M**; is this a risk the senior leadership team is willing to accept?

Ultimately, the job of security professionals — in their dual roles as both **subject matter experts** and **trusted advisors** — is to *advise* and *recommend*. It's then up to the senior leadership team (which *owns* the risk), to *decide* which response to take: avoid, accept, transfer, or take steps to manage to an acceptable level.

Zero Trust and Mobile Security: How Brakes → Go Faster

In an ideal application of zero trust security for enterprise mobility initiatives, the goal is not to slow your users down, but to **help them go faster** for normal use.

As discussed previously, your mobile security capabilities should support both of two important goals:

- ▶ **Protect against the “bad,”** i.e., the unwanted downside impact of *threats, vulnerabilities, and exploits* related to security, privacy, and regulatory compliance and the use of mobile devices
- ▶ **Streamline and fast-track the “good,”** i.e., the sought-after upside impact of *collaboration, productivity, convenience, and higher scale at lower cost* related to the use of mobile devices

Zero trust principles for mobile security can be used to help **eliminate unnecessary friction** for your users in carrying out their normal daily activities, while offering essential protections in scenarios of higher risk. In Aberdeen's view, here are three foundational capabilities to include (see also Figure 5):

- ▶ **Mobile Threat Defense** — to provide mobile devices (regardless of ownership) that are authorized to access enterprise resources with protection, detection, and remediation from the large and growing landscape of mobile threats, vulnerabilities, and exploits.

These capabilities can help to provide enterprise users with the desired access to enterprise resources from any device, at any time, from any location, over any network, and maintain visibility and control over enterprise resources — while respecting user privacy and control over their personal devices, apps, and data.

“It is amazing how many drivers, even at the Formula One level, think that the brakes are for slowing the car down.”

– Mario Andretti

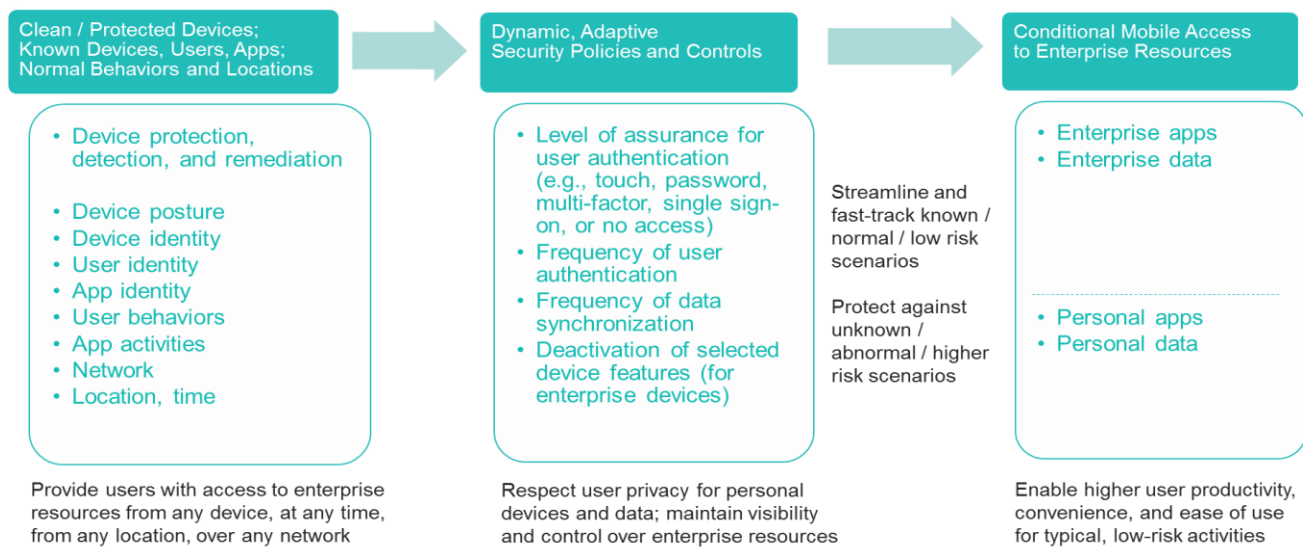
► **Adaptive Policies and Controls** — to replace traditional *one size fits all* policies in favor of dynamic policies based on an intelligent, real-time assessment of risk factors such as:

- Device identity and current posture / health
- User identity and behaviors
- Application identities and behaviors
- Current context (e.g., network, geolocation, time of day)

These capabilities can help to *automate* flexible, adaptive security policies and controls based on the current assessment of risk, including the *level of assurance* required for user authentication (e.g., touch, password, multi-factor, single sign-on, or no access), *frequency* of user authentication and data synchronization, and potential *deactivation* of selected device features (e.g., camera, Bluetooth) for enterprise-owned devices.

► **Conditional Access** — to enable the upside opportunities of higher user productivity, convenience, and ease of use by *streamlining and fast-tracking access* for typical, low-risk activities, and to help protect against the downside of unknown / abnormal, higher-risk scenarios.

Figure 5: Zero Trust and Mobile Security — Mobile Threat Defense, Adaptive Policies and Controls, and Conditional Access are the Brakes That Can Help Your Enterprise Mobile Users to Go Faster



Source: Aberdeen, November 2019

Readers should establish their **mobile security solution selection criteria** with consideration for the above.

Related Research

- ▶ *Mobile Device Security: No Perimeter? No Problem*; November 2019
- ▶ *Email Security is Ineffective, and Getting Worse: What You Can Do About It*; June 2019
- ▶ *Reducing Cyber Security Risk for SMBs: How Security Awareness and Training Programs Deliver Big Returns*; May 2018
- ▶ *Enterprise Email: Are You Adequately Addressing Your Risks?*; August 2017

About Aberdeen

Since 1988, Aberdeen has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen is headquartered in Waltham, Massachusetts, USA.

This document is the result of primary research performed by Aberdeen and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen.