White Paper

Does Your Method for BYOD Onboarding Compromise Network Security?

By Bob Laliberte, ESG Senior Analyst

September 2018

This ESG White Paper was commissioned by Ruckus Networks and is distributed under license from ESG.

Contents

Abstract

The number of devices and sensors connecting to corporate wired and wireless networks is poised to skyrocket. But are default network onboarding mechanisms up to the task to keep your environment secure and your employees more productive, as well as deliver a great customer experience? To ensure you can accomplish all three of these goals in a modern digital environment, organizations should consider deploying digital-certificate-based network onboarding and authentication solutions that support complex, heterogenous environments.

Overview

To stay relevant in this fast-paced digital economy, organizations are embarking on digital transformation initiatives to enable the business, provide higher levels of customer satisfaction, and mitigate risk. ESG research shows that, while 13% of organizations have mature digital transformation initiatives, the majority (61%) of respondents report that their digital transformation initiatives are in process or just beginning.[1]

A big part of any organization's digital transformation effort is to ensure that users have the ability to easily and securely onboard in order to connect to the appropriate applications, devices, and other users over the wired and wireless network. This is increasingly relevant, since bring-your-own-device (BYOD) initiatives continue to proliferate and users connect multiple devices, which means organizations have to contend with and defend a growing attack surface. In addition, most users will have a certain level of expectation (high) for access and delivery of services based on their experience at home (consumerization of IT).

Another area that organizations need to consider as part of the onboarding process is the Internet of Things (IoT). Just as personal devices are expanding, IoT devices and sensors have the potential to far exceed the BYOD numbers. Now is the time to think about this, with ESG research showing that 25% of respondents have IoT initiatives underway and another 43% plan to deploy IoT in the next 12 to 24 months.[2] This has the potential to create an even bigger attack surface, so establishing a simple, secure, and auditable onboarding process will be imperative.

Network onboarding is the mechanism by which BYOD, guest, and company-owned devices initially connect to the network. To be successful, the wired and wireless network onboarding process for authorized users and devices needs to be efficient, as well as easy to implement and manage—ideally without any hands-on involvement by IT (once deployed and configured). However, many organizations still rely on rudimentary onboarding methods that are built in to their network infrastructure (such as pre-shared keys and MAC authentication via captive portal) that can both impact user experience and create security risks.

Challenges with Default Mechanisms for BYOD and Guest Onboarding and Authentication

Many organizations leverage onboarding mechanisms that are built in to the network infrastructure currently deployed in their environment (such as pre-shared keys and MAC authentication). However, given the rise of BYOD, IoT, and the need to provide guest access to Wi-Fi, this can lead to a number of challenges for organizations, including:

1. **Pre-shared keys.** Probably one of the most pervasive techniques for protecting access to wireless networks, this method allows for the key to be easily shared with users you don't want connecting to the network, such as disgruntled employees, corporate spies, hackers, etc. This sharing may be inadvertent, as many employees write these pre-shared keys on whiteboards or sticky notes in their offices or cubes, making them visible to all who pass by, including those outside the building. This is also true for guest network access.

[1] Source: ESG Master Survey Results, *2018 IT Spending Intentions Survey*, December 2017.
[2] ibid.

2. **Unencrypted data.** In many cases, the data traversing the network is not encrypted (in the case of MAC authentication or open SSIDs), which leaves organizations vulnerable to being spied on by attackers if they are able to intercept the traffic. In this case, an attacker might simply sit in the lobby or parking lot and intercept unprotected data traffic.

3. **Lack of granular network access policies.** It is very difficult to create a policy specific to each department, individual role, type of device (IoT), etc., using these built-in mechanisms. (For example, the default mechanisms for granting network access may not provide an easy way to grant the HR department a different level of access than the call center.)

4. **The need to continuously re-enter pass keys.** In organizations with sprawling campuses or a number of buildings, it is common to find different SSIDs that may require different pass keys or multiple entries of the same key, which can impact user productivity. Consider that, with BYOD, a user may have multiple devices and need to connect each of them to different SSIDs as she moves about the environment. This could also be an issue for IP-enabled mobile IoT sensors or devices. Consider that each occurrence represents a new opportunity to mistype the key. Users trying to type complex passwords on small devices are prone to error.

5. **Overburdened support desk resources.** Another issue prevalent with these models is that users will either lose or forget their keys on a regular basis. This is quite common—users will enter the key when they connect for the first time but may forget it (or lose their sticky note) when they upgrade to a new device or bring in a new phone, and generate a trouble ticket with the support desk to gain access. Depending on the number of employees in your organization, this can consume a lot of time, especially around new device launches or just after the holidays when users are adding new devices.

6. **Lack of visibility.** These built-in default models don't provide insight into who the user is—making it impossible to create user-specific access policies and, even more concerning, prohibiting the organization from tracing anomalous, illegal, or dangerous activity to a person, since the organization can't identify the user associated with the device.

7. **Lack of auditability.** These default methods don't provide the ability to perform a health check on the device prior to joining to ensure compliance with corporate policy, such as password protection, virus detection, etc.

8. **User satisfaction or experience.** The impact of forgotten, changing, or continuous re-entry of keys to the support team and employee productivity has already been documented, but organizations should also consider how this impacts the user experience. Forgetting or regularly having to change keys can be extremely frustrating for end-users and may drive them to bad behavior, like posting keys on a sticky note or writing them on a whiteboard.

How to Overcome These Onboarding Challenges

If your organization is still using a legacy network onboarding mechanism, it could make it more attractive to attackers and put you at greater risk. To start, organizations need to understand what the current capabilities are and ask the difficult questions, like:

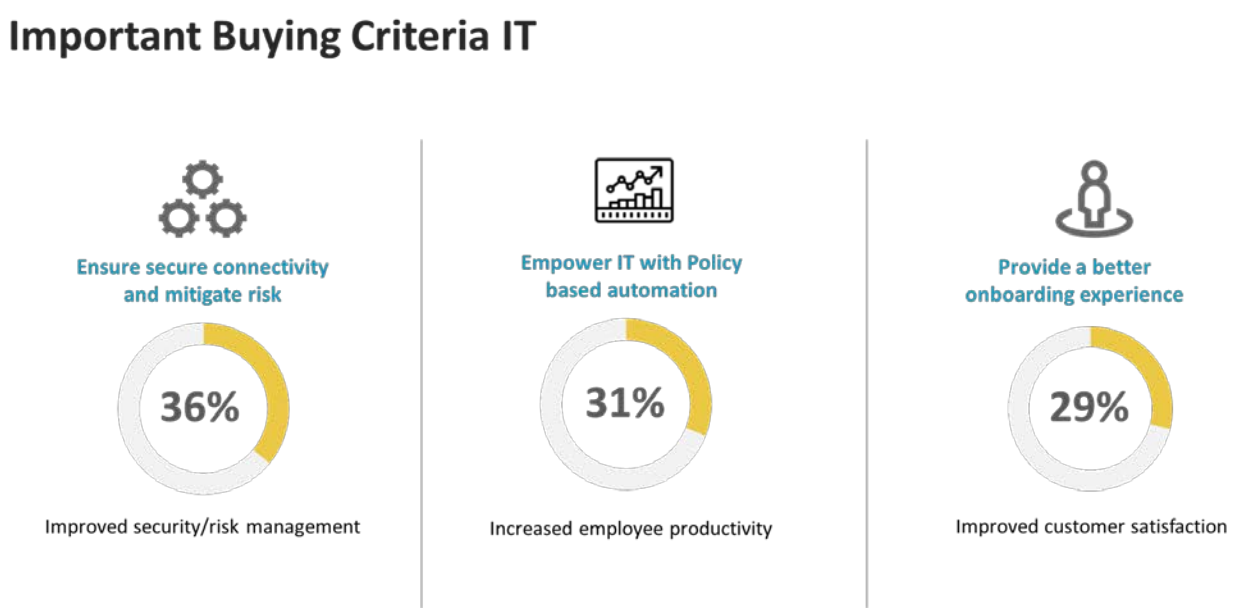
- Are we still using a pre-shared key model or MAC authentication for network onboarding? How long ago was it implemented? What level of protection does it provide?

- What is the impact if the network is hacked? Cost? Reputation? Careers? Have we completed a business impact assessment to determine how it will impact the business?

- How much time is spent supporting and troubleshooting network access issues? Using this information, along with a business impact analysis, can help to justify upgrading the network onboarding solution.
- What is the experience for end-users/guests? How can it be improved? What do our employees think of the current model? Does it provide a good experience for them or our guests? Use data from the support team.
- What are the potential risks of not changing? With an increasing attack surface and more aggressive attacks, can we afford to leave a known vulnerability in place?
- Are we underestimating the risks of insufficient security measures around network access, especially with increased BYOD and a potential tsunami of IP-enabled IoT devices about to be deployed?

The answers to these questions will help organizations provide the justification required to move off a legacy solution. ESG research reveals that the three considerations most reported by respondents as most important in justifying IT investments to their organizations' business management teams in 2018 were improved security, enhanced employee productivity, and improved customer satisfaction, as illustrated in Figure 1.[3]

Figure 1. Most Important Considerations When Justifying IT Investments to Business Management Teams



Source: Enterprise Strategy Group

Secure Network Access and Onboarding Solutions Requirements

Focusing on the three top criteria for justifying new IT purchases, organizations looking to improve the network onboarding process need to leverage solutions that utilize digital certificates. By deploying digital certificates to authenticate employee devices, organizations can significantly improve visibility, mitigate risk, and improve productivity. Solutions with digital certificates can ensure a smooth user experience regardless of location, reduce the workload for IT, and address important security holes by:

[3] ibid.

- Creating a much stronger security posture by:
  - Performing health checks on devices prior to onboarding to ensure a minimum level of security per device and mitigate the risk of onboarding infected devices. Ideally, this would leverage a dissolving agent to reduce overhead in all devices.
  - Providing the ability to deploy security policies based on role, department, or type of device, so users/devices only have access to what is appropriate for them.
  - Authenticating valid users to connect to legitimate access points via digital certificates. This eliminates the possibility of attackers gaining access via pre-shared keys.
  - Providing the ability to ID the user of any device on the network quickly and easily and revoke access if required to ensure improved risk management and/or incident response.
  - Fully encrypting data over the air. Ideally this would be using the latest WPA2 (or WPA3 as this protocol becomes mainstream) to secure wireless data in flight. This mitigates the risk of attackers intercepting traffic.
  - Integrating with the existing security ecosystem. Solutions should provide APIs to tie into third-party next-generation security solutions, thereby enhancing their effectiveness and creating a more robust defense-in-depth strategy.
  - Providing an alternative mechanism for secure onboarding when digital certificates do not make sense. For example, often even IP-enabled IoT devices cannot accept a certificate and it's not practical to expect a guest user to install a certificate when he is only in your environment for a short time. Look for solutions that have the potential to leverage dynamic keys for guests, which can provide similar security benefits.
- Enhancing employee productivity. With the frequency, severity, and sophistication of cyber attacks increasing, it will be imperative for IT to focus their time on architecting and building the appropriate defense posture, secure in the knowledge that device onboarding and authentication processes have automated workflows.
  - Reduce the number of trouble tickets. Certificate-based systems eliminate the need to remember and/or continually enter keys, so IT staff can focus on architecture and strategic initiatives rather than user connectivity issues.
  - Policy-based automation. Automated role-based access policies ensure that users have access to only what they need. The policies need to be easy to create and change to accommodate dynamic environments.
  - Reduce time spent troubleshooting. Rapidly map suspicious devices to a user to mitigate risk and take corrective action immediately.
- Providing a better experience. This includes enabling users to set up their own devices once and get access across all wireless APs or wired locations regardless of manufacturer or geographic location, without having to remember one or many keys. This essentially ensures that users will have a seamless experience at work, similar to that which they experience at home.

Ruckus Networks Can Help

Ruckus Networks, an ARRIS company, offers a solution named Cloudpath Enrollment System. This is a software- or SaaS-based solution designed to provide a simple and secure onboarding and authentication process for heterogenous wired and wireless networks. The Cloudpath offering utilizes digital certificates to provide easy, secure connectivity and also leverages dynamic guest keys for situations where a certificate-based approach is not practical.

Role-based policies ensure that users only have access to what they are authorized to access. Cloudpath software also provides the ability to customize onboarding workflows by user (internal versus guest) and device type. This also ensures that operations has the ability to completely map devices to specific users should anomalous or suspicious activity arise.

It is also critical that the Cloudpath system performs a precheck on each device to ensure baseline security and automatically remediate issues prior to onboarding. This capability leverages a dissolving agent to minimize overhead.

The Bigger Truth

Organizations with mature or emerging digital transformation initiatives need to start by ensuring that all the devices connecting to the network are properly vetted and authorized. Considering the wave of additional BYOD and IoT devices connecting to the corporate or guest network, it will be important for IT to have the appropriate visibility into all of these devices and the ability to act immediately if there is suspicious activity.

Security continues to be a top challenge for network and operations teams, and the rapidly expanding wired/wireless network environment presents an attractive attack surface that needs to be addressed. Organizations should not underestimate the risks of failing to properly secure network access and authentication in support of BYOD and guest users. While this may not be the first network security hole that comes to mind, it could be exactly where attackers may seek to focus.

In addition to providing a stronger security posture, leveraging automation to drive productivity, it is vital to remember that users expect a smooth experience with BYOD across an entire campus. Any solution deployed needs to provide a better experience for all users—employees and guests. Make sure that any solution you evaluate or select ticks all three justification boxes—enhanced security, improved employee productivity, and a better customer experience—to accelerate funding.

Network onboarding and authentication solutions that leverage digital certificates provide a number of advantages in an increasingly digital world. Organizations looking to upgrade should consider Ruckus Cloudpath Enrollment System to simplify their onboarding and authentication solution for complex heterogenous network environments.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188