10 MUST-HAVES TO KEEP EMPLOYEES SECURE AND PRODUCTIVE

ProofID

With a global shift towards a hybrid workforce, employees require a secure and productive environment whether they are working from home or in the office. If employees can't access applications and information securely from any location or device, their productivity will decrease, and the security of key corporate assets will be at risk. We help enterprises take an identity focused Zero-Trust approach and have devised 10-point plan for digital employee identity security that is both practical and actionable.

1 Single Sign-On

On average, employees spend 10.93 hours per year entering and resetting passwords.[4] This slows down remote employees as they sign on to applications to get their work done, like collaboration apps for instant messaging and video conferencing. Federated single sign-on (SSO) and self-service password reset gives employees back all those hours and lets them get back to work. Better yet, strong authentication methods, such as biometrics and FIDO2 keys, can make passwords a thing of the past. By implementing SSO and SSPR across the organization's application estate, user productivity will be gained, and an improved user experience will be achieved whilst improving the organization's security posture.

2 Multi-Factor Authentication

52% of data breaches are due to hacking, and of those, 80% are due to weak or compromised passwords.[1] Multi-factor authentication (MFA) can reduce password risk by 99.9%.[2] Putting MFA everywhere is a no-brainer, especially on VPN connections and for employees that use personal devices (BYOD) when they work from home. By adding MFA technologies, security is increased by reducing the risk of compromised passwords, forgotten passwords and a quick win with speedy deployment.

3 Adaptive Authentication

While there is a need to increase security and protect resources from unauthorized access, the user's authentication journey shouldn't be intrusive or frustrating. Adaptive Authentication provides a flexible authentication user journey by establishing rich security profiles that drive the authentication experience. Start with MFA for once per day and add additional rules relating to a recognized device, geo-location and build up with several variables. Adaptive Authentication is paramount to ensuring the workforce users are not compromised by malicious acts of account fraud and is widely adopted throughout financial organizations today.

4 Risk Profiling

Where there are advanced factors that drive the authentication journey risk profiling offers an additional level of authentication. Create policies based on risk factors such as impossible travel, device patching level, and anonymous networks, allowing these policies the ability to ultimately deny access. Where with risk profile passwordless authentication is the goal and when combined with Adaptive Authentication, provides a powerful tool to understand the threats to an organization and allow action to be taken.

5 Privileged Access Management

The reality is that despite the privileged access associated to these users many organization struggle to know how many privileged access accounts they might have and who/what is using them. As privileged accounts are the preferred target for hackers, enforce least-privileged access and establish Zero-Trust security for apps, APIs and data. More than 80% of breaches are due to compromised privileged accounts and by implementing Privileged Access Management (PAM) risk can be avoided and can be extended to endpoint device security for greater protection further reducing risk across local user admin and service accounts.

6 Role Modelling

Simplify the process of provisioning and deprovisioning by aligning with the business functions within an organization. Aim for a simple model and align your role calculation strategy within your existing identity governance solution.

7 Map Access to Roles

A fundamental function of Role Based Access Control (RBAC) and critical to a Zero-Trust security posture. Any organization that implements RBAC has complete control of the user provisioning and deprovisioning and the power to revoke access instantly, as required. Many organizations have hundreds or thousands of orphan accounts which can be a potential threat, where redundant but still active accounts have remote access to systems and data.

8 Audit & Access Review Strategy

As you venture towards Zero-Trust nirvana, auditability will be key, as you will be required to prove who is accessing what. A robust strategy of periodic review of access for each user with confirmation, amending request of approval will provide transparency. Excessive access not only compromises security but can also lead to unnecessary license costs. Many organizations face strict auditing requirements and by implementing a modern Identity Governance and Administration solution, reports can be provided to prove access in minutes not weeks and remedial action can be achieved quickly.

9 VPN

Organizations enable VPNs for remote access, but this often allows employees to access more than they need. Since 23% of sensitive data breaches are caused by internal employees,[3] someone shouldn't have access to everything just because they're on the network. All that said, if you don't have an identity-defined perimeter as described in the above bullets, at least do this (or VDI). And please...put MFA on it!

10 Audit & Access Review Strategy

Now that we've covered the key components of your workforce identity solution, which are critical to your hybrid workforce strategy, it's time to evaluate your business continuity. Identify what is truly critical and outline your disaster recovery strategy. Many organizations have the processes in place, fail to update as the digital ecosystem changes for both infrastructure and business requirements. This failing could ultimately compromise the business.
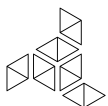
ProofID Workforce Identity Solutions empower users to access applications and data required seamlessly regardless of location whilst significantly improving the overall security of your IT estate. Take the next step and **connect** with the identity security experts.

[1] Verizon 2019 Data Breach Investigations Report
[2] Microsoft Security Intelligence Report, 2018
[3] Forrester Analytics Global Business Technographics Security Survey, 2019
[4] Ponemon 2019 State of Password and Authentication Security Behaviors Report