imprivata®

Make security the easy choice

A practical identity security assessment

Strong security shouldn't make critical work harder. Use this assessment to find where identity security creates friction, where that friction may introduce risk, and where making access easier could also make it more secure.



When security gets in the way

For mission-critical organizations, increasing IT complexity can create security and operational challenges.

Employees move between applications, workstations, mobile devices, and cloud services. Privileged users and third parties need access to sensitive resources. AI agents and other non-human identities create additional challenges.
More complexity increases risk, leading to more security controls. But controls that don't fit the way people work can create their own problems: repeated authentication, manual processes, inconsistent workflows, excessive access, security exceptions, and workarounds.

Security is a critical component, but it shouldn't get in the way of work. The secure choice should be the easy choice for all users. We've created a simple assessment to help you identify the friction points you're facing that may be negatively impacting efficiency and productivity – all while creating risky workarounds. It focuses on four areas:

- Workforce authentication
- Access across your technology environment
- Privileged and third-party access
- Non-human and AI agent access



How to use this assessment

This isn't a security score, but rather a way to identify friction points and decide where to investigate further.

For each question, select:
Yes | Sometimes | No | Not sure

Then consider:
What creates the friction?
Technology | Process | Policy | User behavior | Lack of visibility | Other

What happens because of it?
Lost time | Workaround | Service desk request | Excessive access | Shared credentials | Security exposure | Manual security work | Other

Pay particular attention to Sometimes, No, and Not sure. They may point to inconsistent experiences, security gaps, or areas where you need greater visibility.

When you're finished, you'll have a comprehensive summary of where you're truly experiencing friction, which you can then use to build a plan for addressing them.

1 Make security easier for the workforce

Is secure authentication the easiest way for your workforce to get to what they need?

Authentication is a frequent point of contact between users and security. When employees repeatedly enter credentials, reset passwords, or interrupt their workflow to authenticate, friction adds up.

Assess your environment

Can users:

1. Get through common workflows without repeatedly entering passwords?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

2. Authenticate securely without relying primarily on passwords?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

3. Authenticate in a way that supports high-frequency or time-sensitive work?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

4. Use shared workstations and devices without shared credentials?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

5. Get authentication/access support without generating significant service desk demand?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

What to look for:

Repeated login prompts, password resets, credential sharing, unattended sessions, password reuse, and workflows designed to avoid authentication.

What to consider:

Passwordless authentication, single sign-on, biometrics, badges, passkeys, phishing-resistant authentication, and authentication matched to workflow and risk.

Secure and easy:

Where could removing one unnecessary authentication step make access both easier and more secure?

2 Make secure access work across your technology environment

Does the secure experience follow the user?

Users rarely work in one technology environment. They move between shared and personal devices, legacy applications, cloud services, mobile workflows, and specialized systems.

When identity works differently in each environment, users face inconsistent security experiences and security teams inherit gaps and exceptions.

Assess your environment

Can you:

1. Give users a consistent way to authenticate across the systems they use?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

2. Support movement between devices without unnecessary reauthentication?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

3. Include shared mobile devices in your identity strategy?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

4. Apply appropriate security controls without creating exceptions for difficult-to-integrate

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

5. Modernize without creating new identity silos?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

6. Quickly revoke access when the business need changes?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

What to look for:

Standing privileges, shared administrator credentials, broad vendor access, manual provisioning, inconsistent identity verification, and limited session visibility.

What to consider:

Adaptive authentication, identity verification, least privilege, time-bound access, privileged credential management, third-party access management, and session monitoring.

Secure and easy:

Where could you apply stronger controls more precisely instead of adding friction for everyone?

3 Apply stronger controls where risk is greater

Can you increase assurance without increasing friction for everyone?

Routine workforce access doesn't carry the same risk as privileged administration, third-party access, credential recovery, or access to sensitive resources.

Instead of adding maximum friction everywhere, consider where stronger verification and tighter access controls are actually needed.

Assess your environment

Can you:

1. Adjust authentication requirements based on risk or context?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

2. Verify identity appropriately before issuing or recovering credentials?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

3. Separate privileged access from routine user access?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

4. Limit privileged and third-party access to the resources and time required?systems?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

5. Monitor and investigate privileged and third-party sessions?

◯ Yes ◯ Sometimes ◯ No ◯ Not sure

What to look for:

Separate credentials, inconsistent authentication, duplicate identity processes, legacy security exceptions, and controls that work for office users but create friction for frontline workflows.

What to consider:

Integrated access management, identity-aware application access, interoperability across legacy and modern environments, shared device access, and context-aware authentication.

Secure and easy:

Where does changing technology force users to change how they interact with security?

4 Prepare for non-human and AI agent access

If an AI agent takes action, can you identify it and control its access?

Service accounts, applications, and automated processes already require access. AI agents introduce new questions because they may access information or take actions on behalf of people and systems.

The access model should make appropriate behavior the default from the start.

Assess your environment

Can you:

1. Identify the non-human identities accessing critical systems?
   ◯ Yes ◯ Sometimes ◯ No ◯ Not sure
2. Give each AI agent or automated process a unique identity?
   ◯ Yes ◯ Sometimes ◯ No ◯ Not sure
3. Determine who or what authorized an agent?
   ◯ Yes ◯ Sometimes ◯ No ◯ Not sure
4. Limit access to the resources and time required for the task?systems?
   ◯ Yes ◯ Sometimes ◯ No ◯ Not sure
5. Distinguish an agent's actions from those of the human the agent represents?
   ◯ Yes ◯ Sometimes ◯ No ◯ Not sure
6. Monitor activity and immediately revoke access when needed?
   ◯ Yes ◯ Sometimes ◯ No ◯ Not sure

What to look for:

Persistent credentials, broad permissions, shared service accounts, unclear ownership, limited monitoring, and AI initiatives where identity requirements are addressed after access has already been granted.

What to consider:

Unique identities, least privilege, time- and task-bound authorization, credential and secret management, activity monitoring, traceability, and rapid revocation.

Secure and easy:

Are you designing AI access guardrails so appropriate access is built in from the start?

Map your friction

Now turn your answers into priorities.

For each workflow, capture where you found friction, what happens because of it, and what might make the secure path easier.

Access workflow	Where is the friction?	What happens?	Security concern	What could make access easier?
Workforce authentication				
Shared device and application access				
Cross-environment access				
Privileged and third-party access				
Non-human and AI agent access				

Circle the three areas you want to investigate first.
Don't choose based on an arbitrary score. Look for frequent friction, meaningful consequences, or areas where lack of visibility makes the risk difficult to understand.

Turn insight into action
Choose one priority from your friction map and answer three questions.

1. Where is access hardest?
Identify a workflow where people or systems work harder than they should to access resources they're authorized to use.

2. Where does friction occur and what behavior does it create?
Look beyond the documented process. Talk to the people who use and support it. Does the control encourage the intended behavior, or has another path become easier?

3. What would make the secure path easier?
Consider authentication, policy, identity verification, privilege, interoperability, automation, or changes to the process itself. What would have to change for the secure path to become the obvious path?

Make the secure choice the easy choice

Imprivata delivers Zero-Friction Security for high-stakes organizations where every second matters and work never stops. Our identity, access, and privileged access security platform secures every identity from human to AI, and across shared and dedicated devices, complex workflows, and modern and legacy environments. Imprivata helps organizations embed intelligent, context-aware access into the flow of work, protecting against threats, reducing operational complexity, and improving productivity and cost efficiency.

Talk to Imprivata about making security the easy choice for your organization.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

Copyright © 2026 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.

7818-2026_WP-Make security easy