Govern user and identities

*Silent Security — the best security is the kind you don’t know is there.*
Contents

3 Striking a balance: Reducing tensions between users and organizations

4 What is Silent Security?

5 Secure your business

6 Enable digital transformation

7 Prove compliance

8 Case study: The Silent Security approach in action

9 IBM Security is here to help you achieve Silent Security

Key points

User behavior analytics powered by AI enable greater trust for those who deserve it

Least privilege and granular data access don’t have to slow users down

Great user experiences that also protect critical business assets

Business activity-based entitlements streamline governance and compliance
Since most organizations’ IAM policies are not black and white, it’s helpful to visualize the landscape upon which these challenges occur. At one end is the “no privileged access” approach that sacrifices speed and usability for higher security and compliance. At the other end of the spectrum is the “overprivileged access” mentality, which prioritizes convenience over taking adequate measures to securely govern user access.

Ready for the good news? There is a way to strike the just-right balance between overreactive, no-privileged-access strategies that slow down business and casual, overprivileged-access approaches that sacrifice security for convenience and usability. And the solution is as straightforward as addressing those top three challenges to governing the users and identities that have access to your organization’s assets.
What is Silent Security?
Organizations need the ability to efficiently secure assets and respond to market and regulatory changes to stay competitive. Fortunately, most employees have good intentions. This means you can start building an effective strategy to govern users and identities that doesn’t sacrifice speed or security. We call it Silent Security — where the best security is the kind you don’t know is there. This is not security that’s invisible or ineffective, but that remains in the background, facilitating seamless and fast access, and only intervenes when risks are elevated.

How can you achieve Silent Security?
It turns out that the three most significant challenges to governing users and identities reveal exactly where you should focus your attention when building the firm, yet flexible, anchors for your governance plan:

- Secure your business
  To answer the challenge of growing enterprise complexity, you need a silent way to know that the right people — and only the right people — have the right access to the specific data they need, and only the data they need, at the right times.

- Enable digital transformation
  To answer the challenge of increasing demand for convenient access, you need to create exceptional, seamless experiences for users that enable the growth of your business while still keeping information secure — silently.

- Prove compliance
  To answer the challenge of changing regulatory requirements, you need to continuously and silently get ahead of compliance with evolving mandates and company audits.
Now that the foundation is laid and the pillars have been raised, ready for the rest of the Silent Security success blueprint? Below are some helpful checklists for key capabilities that enable each of these three strategic components.

**Secure your business**

While it’s true that most users can be trusted with sensitive company data, organizations still need accurate ways to pinpoint suspicious activity to help uncover malicious behavior as quickly as possible. User behavior analytics is the most efficient and silent way to give human analysts a running start in their efforts to protect data from insider threats without disrupting productivity. With artificial intelligence helping to identify and monitor the riskiest users, and automatically enforcing step-up challenges like multifactor authentication as needed, security analysts have more time to focus on the most critical investigations and make judgment calls.

Another key component of an intelligent governance strategy is applying and enforcing the principle of “least privilege” across the enterprise. Put simply, “least privilege” refers to giving individuals only as much access to data and apps as they need to do their jobs — no more and no less. In the discussion of the next pillar, you’ll see how least privilege doesn’t actually have to limit productivity at all. Security and usability begin to balance out when you can give employees exactly what they need to get things done, with seamless user experiences enabled by Silent Security.

**Secure your business checklist**

- Deploy user behavior analytics to detect insider threats
  - Identify risky users over time with machine-learning algorithms
  - Monitor highest risk users and offenses based on data access and actions
  - Dynamically update risk scores
- Consistently enforce the principle of least privilege
  - Apply granular access control to sensitive data elements
  - Restrict entitlements and access based on demonstrated need
  - Discover, manage and audit privileged accounts and authentication secrets
- Protect with multifactor authentication
  - Automate your authentication framework to step up and challenge users as needed
  - Verify identity or automatically shut down bad actors in an instant
  - Require users to prove identity with something they know, something they have and something they are
Enable digital transformation

Given modern workers’ expectations of mobility and convenience, organizations are allowing unprecedented levels of access to sensitive data, and that access is often neither secure nor compliant. Chances are you’ve identified some serious gaps in your own asset protection strategy — shadow IT, for example — and are looking for ways to silently tighten security without sacrificing productivity.

Enabling single sign-on (SSO) and a choice of authentication methods for users is a great place to start.

By allowing your users to sign on once to access web, mobile and cloud apps and be able to choose the authentication method they feel most comfortable with, you eliminate the need for them to remember multiple complex passwords while still giving IT an effective and silent way to manage user access. You also reduce the risks associated with employees choosing unsafe passwords and storing them in unsafe ways. The more choices users have, the less likely they are to circumvent access controls and potentially jeopardize network or data security.

These user experiences don’t have to be clunky to be adequately secure, either. Another way to silently secure data access while focusing on user outcomes is to apply the principles of design thinking to help develop frictionless experiences. This approach to designing seamless user interactions takes into consideration the ways that users actually engage with technology. With creative ideation, rapid iteration and diverse organizational input across lines of business, IT, security and more, design thinking fosters continuous improvement with the user always in mind.
Compliance and regulatory demands are complex and always in flux. That’s why it’s critical to simplify compliance-related activities wherever possible. One of the best ways to start streamlining your governance — especially as it informs your need to prove compliance — is to adopt an approach that governs users at the level of entitlements rather than roles.

Instead of relying on arbitrary groupings of access privileges that are authorized for particular roles or teams, a business activity-based strategy enables greater visibility and granularity of your employees’ data access privileges. This, in turn, makes it easier to silently enforce segregation-of-duties policies, manage orphan accounts and automate controls and reporting ahead of an audit.

---

Enable digital transformation checklist

- Log in once, access everything with single sign-on (SSO)
  - Bridge the access control gap between on-premises and cloud
  - Delegate access administration to the line of business
- Improve user experience with seamless authentication
  - Give users a choice of how to authenticate, such as biometrics, hardware tokens, one-time passwords, knowledge questions and mobile apps
  - Use mobile as a second authentication factor
  - Adopt user-centric authentication methods, such as biometrics
  - Authenticate users into lower-risk apps without passwords
- Create user experiences with a design thinking approach
  - Focus organization on user outcomes and seamless experiences
  - Encourage fast iteration and cross-functional collaboration
  - Create an environment based on continuous improvement

---

Prove compliance

Compliance and regulatory demands are complex and always in flux. That’s why it’s critical to simplify compliance-related activities wherever possible. One of the best ways to start streamlining your governance — especially as it informs your need to prove compliance — is to adopt an approach that governs users at the level of entitlements rather than roles.

Instead of relying on arbitrary groupings of access privileges that are authorized for particular roles or teams, a business activity-based strategy enables greater visibility and granularity of your employees’ data access privileges. This, in turn, makes it easier to silently enforce segregation-of-duties policies, manage orphan accounts and automate controls and reporting ahead of an audit.
With this example of an activity-based approach as your guide, you can then use the following checklist of key capabilities to build out the rest of your plan for supporting continuous compliance across your enterprise.

**Continuous compliance checklist**
- Delegate and simplify access recertification for lines of businesses
  - Better understand entitlement policies and impact on user access
  - Review entitlements with templates and business language
  - Ease communication between lines of business and IT for access decisions
- Map roles and entitlements to business activities
  - Govern access at the entitlements level to help pass audits
  - Avoid assigning a toxic combination of entitlements to users
  - Simplify access management and governance
- Manage user data for GDPR and secure transactions for PSD2
  - Make informed decisions about user access using insights
  - Employ algorithms for role mining, modeling and optimization
  - Discover personal data in your databases and see who has access
  - Allow users to access account info and transactions in one place

**Case study: The Silent Security approach in action**
An international retailing group secures its web and mobile applications against threats while delivering seamless user experiences on the go.
IBM Security is here to help you achieve Silent Security

IBM Security offers market-leading solutions to help you govern users and their identities, and these solutions can be configured to meet your needs wherever you are on the journey to achieving Silent Security.

- IBM Security Identity Governance & Intelligence
- IBM Cloud Identity/IBM Security Access Manager (ISAM)
- IBM Security Secret Server
- IBM Security Guardium
- IBM QRadar User Behavior Analytics (UBA)

Products

Managed Services

Consulting Services

IBM Managed Identity Services

IBM Managed Guardium Services