



Managing modern identity complexity and reducing executive risk

How identity security can help support your organization’s continuous compliance goals

Cybersecurity regulations are increasing executive accountability while identity ecosystems continue to grow in size and complexity. Continuous compliance can require more than periodic audits. Organizations must continuously understand who — or what — has access to critical systems and data in order to reduce security risk and demonstrate ongoing governance.

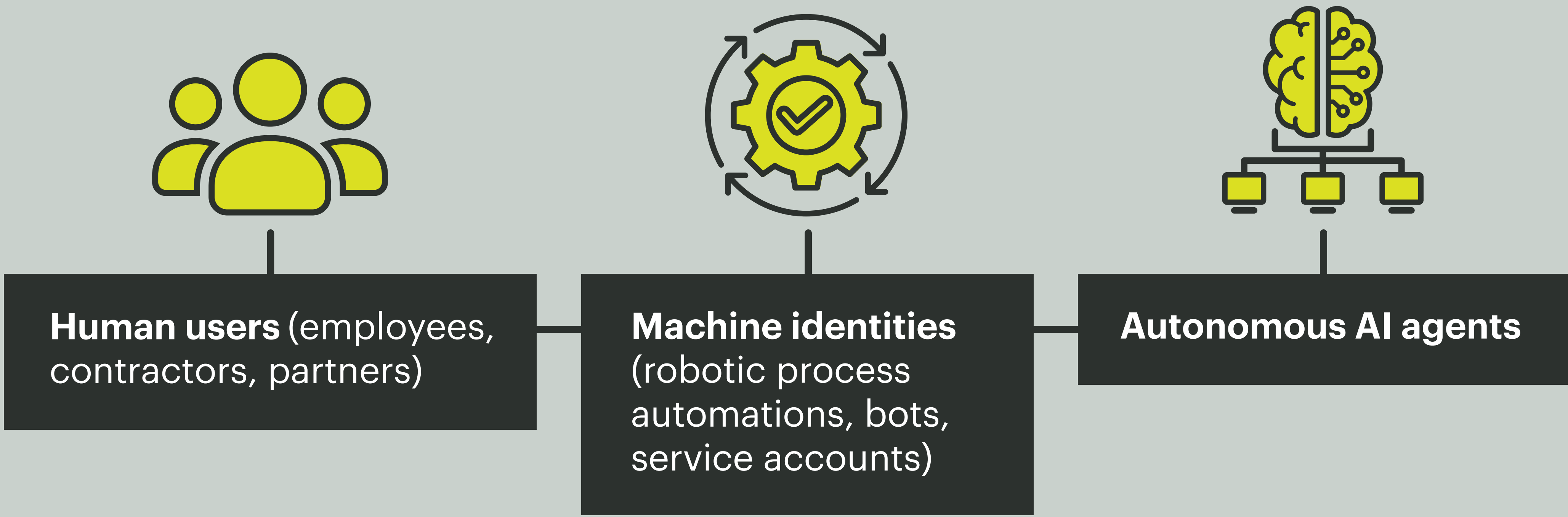
Why identity security is a top CISO priority

According to the most recent [Foundry Security Priorities](#) study, security leaders are managing increasingly complex identity environments while trying to improve their organizations’ overall security posture. To mature, security leaders must focus on:

-  **Strengthening** data protection
-  **Securing** your expanding footprint
-  **Streamlining** compliance and privacy efforts

The modern identity ecosystem is expanding

Today’s enterprise goes far beyond workforce users. To support compliance, security programs must be equipped to govern:



Without continuous visibility, unmanaged identities can introduce critical security and compliance risks.

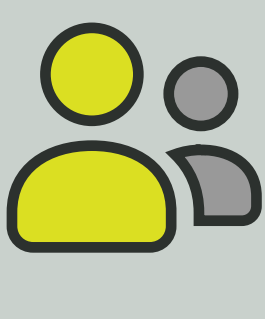
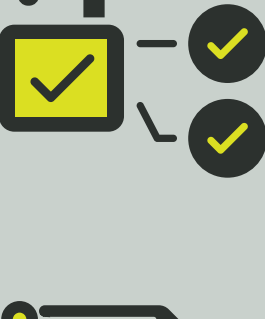
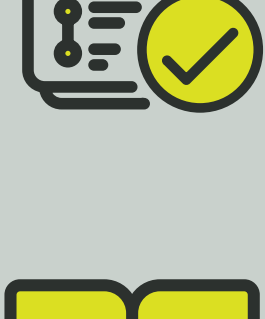
3 pillars of an adaptive identity security program

Organizations building continuous compliance share three core capabilities:

- 1 Discover and unify**
Continuously discover identities across the enterprise to help maintain a centralized system of record.
- 2 Govern continuously**
Apply policies consistently, automate lifecycle management, and continuously validate access as identities and business needs change.
- 3 Demonstrate and respond**
Produce system-generated reports to support audit requests, identify potential access gaps early, and respond before risks escalate.

5 identity security questions to test your readiness

Be ready to answer these questions:

-  **Do we have** centralized visibility over both human and machine identities?
-  **Can we show** who — or what — has access to critical systems at any given moment?
-  **Is our approach** to access static, or is it truly adaptive to changing risk?
-  **Can we quickly produce** the consolidated system records that auditors require?
-  **Are we equipped** to support evolving regulatory requirements?

Move beyond point-in-time audits

Establishing a unified, adaptive identity security program is a critical step toward strengthening security, simplifying audit prep, and supporting your organization’s risk management strategies.

Learn how a modern identity security platform helps organizations move away from fragmented, point-in-time audits and builds a foundation to support continuous compliance initiatives.

DISCLAIMER: THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY, AND NOTHING CONVEYED IN THIS DOCUMENT IS INTENDED TO CONSTITUTE ANY FORM OF LEGAL ADVICE. SAILPOINT CANNOT GIVE SUCH ADVICE AND RECOMMENDS THAT YOU CONTACT LEGAL COUNSEL REGARDING APPLICABLE LEGAL ISSUES.