SailPoint

WHITE PAPER

SailPoint Extensibility: Automate and Embed Identity Security Across the Business

Ensure Identity Security Keeps Pace with Your Digital Ecosystem

Organizations continue to accelerate their adoption of cloud infrastructure and apps (such as SaaS, iPaaS, or PaaS), shifting to a digital-first, anywhere approach to enable their users in the virtual workforce to work faster and more securely.

Not only are there more cloud-based applications and platforms than ever before but these are also increasingly dependent on – and interconnected with – essential digital ecosystems (e.g. business, IT and security).

So there is no doubt that your existing policies and methods for identity security must keep pace — to guard against data theft or loss of IP, disruption to business operations, potential damage to your brand, as well as penalties for non-compliance.

But how are you currently extending core identity security policies and practices to applications and platforms?

- If you are using or adding IT resources that employ legacy, manual, or quasi-automated script-driven techniques, what is that costing you — either directly or in opportunities lost?
- How much more visibility and control over identity in business processes are you gaining?
- Is your current methodology helping you accelerate the adoption of cloud infrastructure and applications?
- If you're considering investing in a development project to further automate this process, what will it take to do the complex coding that extends security to interconnected applications while also keeping it simple to use?

This white paper will present a more cost-effective alternative for building the kind of automated workflows you need. Using APIs and event triggers can reduce integration development from months to days (or even hours). And taking advantage of an extensible framework of a core identity security platform will automate and infuse identity security into your critical business processes and workflows.

Why Extensibility:

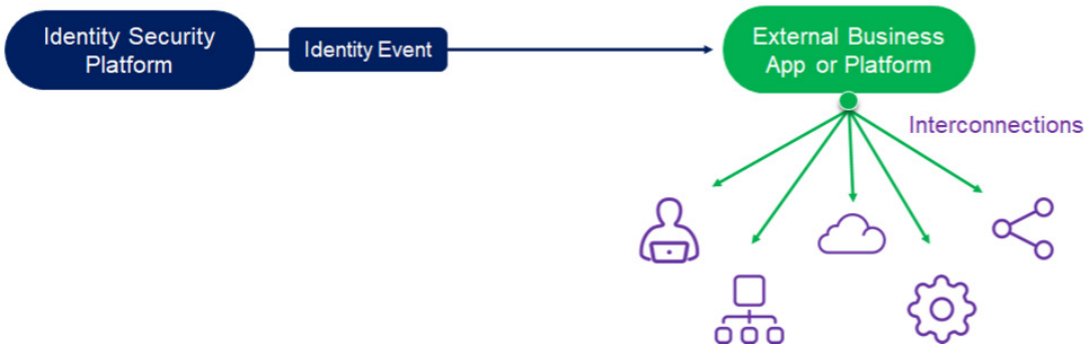
- Shift to a digital-first, anywhere approach
- Accelerated adoption of cloud infrastructure and apps
- Need to extend identity into business processes for greater visibility and control
- Requirement for tailored business processes and workflows

The Dynamics of Embedding Security in Cloud-based Resources and Workflows

Many modern software architectures are implemented using event-driven programming, especially integration use cases between SaaS applications from different vendors.

An event-driven architecture is designed to receive and react to events such as user clicks in a UI, object changes in a database, or messages originating from other subsystems in a distributed architecture.

For example, a core identity security platform broadcasts predefined events when something in the system changes; downstream applications listen to those events and update accordingly. This allows decoupled, highly reactive, independent subsystems to all work in concert.

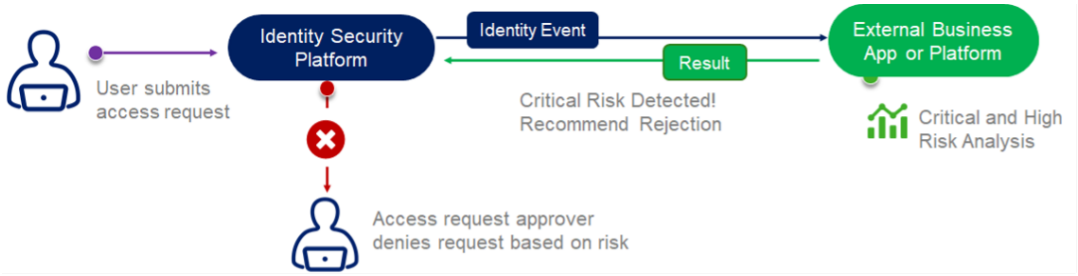


For example, when an identity attribute changes (e.g., the approving manager for a user changes), the event is sent to an iPaaS system like a workflow orchestration engine. This triggers custom business logic within the iPaaS system. The appropriate cloud systems and applications connected to the iPaaS system may be directed to perform an action (e.g., to generate a certification campaign or send an automatic notification).

But to be cost-effective, this process needs to be foolproof — easily integrating with virtually any workflow platform. With access to SDKs and open-source tools, these integrations can be designed to support an organization's unique business requirements. Thus, identity security becomes fundamental to the business as opposed to a hurdle to overcome.

Bidirectional Integration: The Next Level

In a more interactive integration, the trigger from the identity security platform gives the receiving application the ability to respond in order for the interaction to be considered complete and successful.



For example, when a user requests access, the identity security platform automatically knows that for this type of request it needs to pass the event on to a critical, high-risk analysis application for evaluation. Thus, when the identity security platform receives the analysis recommendation, the interaction is complete and the access request approved or denied.

The external business app or platform needs to respond to the request with a result as specified in the trigger's output schema. Responses may be framed as:

- **Synchronous** – a response within 10 seconds to the trigger invocation with the output payload
- **Asynchronous** – an acknowledgment (2xx Success) that it has received the trigger invocation request and will complete the invocation at a later time
- **Dynamic** – a determination whether to respond to the trigger invocation synchronously or asynchronously

Examples of core events that trigger actions on an integrated external application or platform

- Identity Created
- Identity Deleted
- Identity Attributes Changed
- Saved Search Complete
- Identity Aggregation Completed
- Access Request Submitted
- Access Request Dynamic Approval
- Access Request Decision
- Provisioning Action Completed

With this level of integration, workers can request access to an application or approve access right within these collaboration tools, eliminating the continuous distraction of switching between multiples apps to get work done.

Build New Integrations Faster to Meet Unique Business Needs Securely

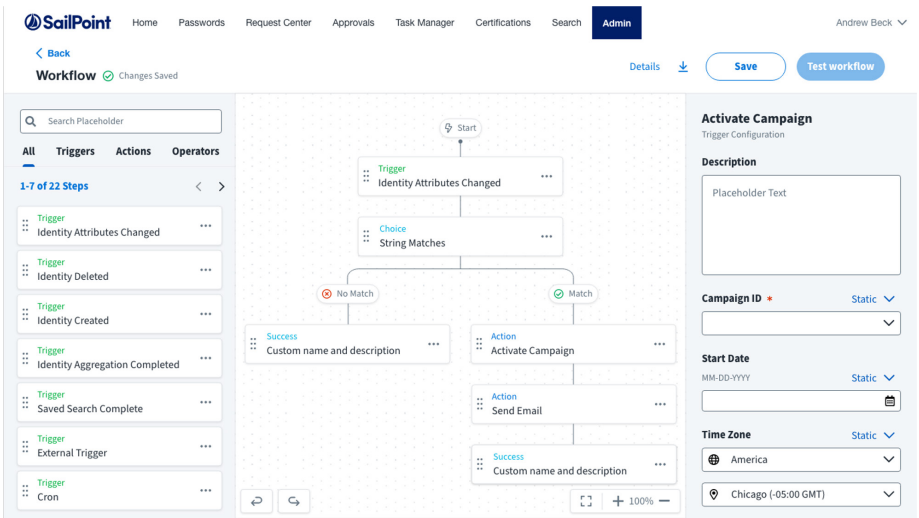
Using an extensibility framework unleashes productivity. Instead of tasking an entire team with building integrations, the framework streamlines the creation of integrations via a toolkit of event triggers, APIs, and drag-and-drop workflows. This interface is not only far more efficient but provides deeper insights and control of user access lifecycles, and triggers automated processes across the business.

Event triggers are the perfect vehicle for communicating changes in an identity security platform. Event triggers emitted from the platform can be received by a multitude of downstream applications, for example, receiving a Slack notification every time a Jira ticket changes, or auto-inviting new employees to your #welcome Slack channel every time a new user is added to your directory.

REST APIs allow organizations to build their own applications, websites, and tools to take advantage of data, features, and workflows from identity security solutions. The APIs follow a familiar, simple RESTful standard, using standard query and path parameters, request/response headers, and JSON request/response bodies.

These options – together with a drag-and drop-workflow interface – enable the creation of automated no-code workflows that connect to a virtually limitless number of external applications and platforms, allowing you to scale while also creating tailor-made integrations that fit your unique requirements.

An easy to use, drag-and-drop workflow UI simplifies automation and accelerates the development of integrations. This also enables the non-technical business user to tailor workflows to fit their business needs.



By incorporating workflows, you can:

- Reduce the burden of managing SaaS sprawl
- Make sure nothing falls through the cracks
- Automate with other business applications and systems
- Securely manage identities many times faster than a manual, human-based approach

Take the Next Step with SailPoint

SailPoint's Identity Security Platform features a built-in extensibility framework that provides event triggers, APIs, and a drag-and drop-workflow interface to quickly and seamlessly integrate identity security into your existing business processes and ecosystem of applications.

Build automated workflows rapidly and with little to no code. SailPoint's extensibility framework easily integrates with industry-leading iPaaS providers and incorporates identity into the applications users rely on every day.

And with the SailPoint Developer Community, you'll have everything you need to get started, including:

- **The SailPoint Developer Community Forum**, hosted by Discourse.org — a rich source to exchange experience and insights around building integrations.
- **APIs and event triggers** are comprehensively described on the API Reference page. When learning and working with a new API, for example, you'll learn what data can be sent in and what data to expect back.
- **Documentation** – API Docs provides a deeper dive into more advanced topics surrounding your API, including best practices and in-depth conversations on when to use a particular input.
- **Tools** – In addition to our APIs and event triggers, SailPoint also provides tools to help developers realize value with them more quickly (e.g., Postman collections and language-specific client libraries). Check here regularly for open-source tools.
- **Blog** – Links to our engineering blog at https://medium.com/sailpointtechblog.

SailPoint's extensibility capabilities make your organization more connected and in turn–more protected. You'll gain deeper insights and control of user access lifecycles and trigger automated processes where once an entire team was needed for manual processing.

The possibilities that extensibility provides are limitless. So take control and embed identity within your digital ecosystem with the SailPoint Identity Security Platform.

ABOUT SAILPOINT

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.

WP1992-2108