# Welcoming Our
# **New Bot Overlords**

**SailPoint**

Do you ever ask a device in your home what the weather will be like today or the score of last night's game? You're not alone – the explosion in virtual assistants in home environments underscores the reality that software applications are weaving themselves into the fabric of our lives.

This is not merely an innovation for the consumer market. Virtual assistants and other "bots" are enjoying a wave of popularity within the enterprise. From customer service chatbots and order fulfillment, to booking travel for employees, organizations are using bot technology to speed internal processes. As is the case with any new technology, bots are proliferating throughout the environment rapidly.

For organizations and their focus on identity, this new wave of bots presents both a security challenge and a powerful opportunity.

### A Security Challenge

With such a potentially large wave of adoption – Gartner estimates 73% of organizations will have some kind of "Internet of Things" (which includes bots) program in place by the end of 2018 – the potential for bots to be used without appropriate identity governance is significant. Businesses should ask the right questions of their organizations and be on the lookout for automation programs that might be creating bots ad-hoc. Being ahead of the curve is key to ensuring identity governance standards are met in the rush of early adoptions.

As these bot-based initiatives arise, businesses can pave the way to success by using models already proven in production. Most often, this will mean treating bots in the same manner as contractor-based identities. Just like contractors today, this will require the establishment of a repository dedicated to bots. As they are created, modified or eliminated, this repository must be updated, bringing that information into the identity governance solution.

This also means time-based access and the application of policy to ensure tight restrictions on their capabilities within the environment. Any access to privileged information must be restricted through appropriate separation of duties policies, and any use of privileged accounts must be performed through governable channels, such as a dedicated privileged access management solution.

Because their actions should be strictly within set boundaries, analytics may also be deployed to identify if bot activity includes anything outside of its originally intended function. Additionally, human oversight of bots is key to good governance, meaning

every bot must (once again, like a contractor) have a real-world person who is ultimately responsible for their governance. A high-level architecture highlighting the modifications to a mature identity governance program is shown below:
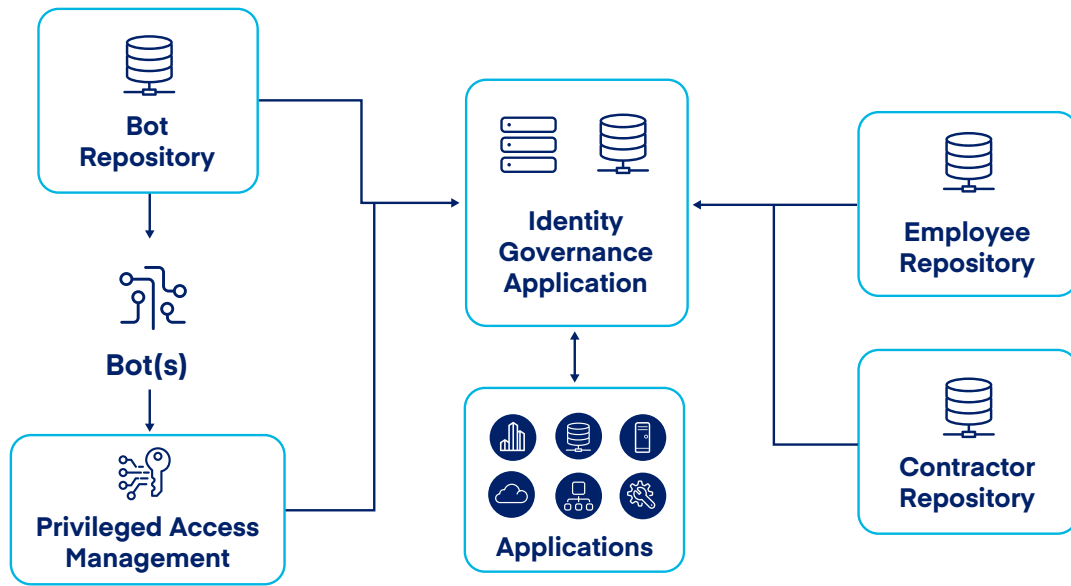


## A Powerful Opportunity

The wave of bot adoption provides an opportunity for identity to become more intuitive and pervasive within a business. Not only can bots provide efficiency gains and enhance customer service, bots can also be used internally to facilitate interaction between the business user and the identity infrastructure in the form of chatbots or other close-to-human processing of requests. This may allow business users to obtain reporting and analytics from the business more rapidly or check the progress of a project.

Users may also become more involved with the actual process of governance itself. An example of this might be using a bot-facilitated process for access request. This would allow for the governance to be customized further to the needs of the end business user. A bot could direct the user to the correct choice through context and other information at its disposal, and thus guide the user to a better outcome as a result. The actual process of identity governance would then be improved, just as other activities are seeing the benefit of bot adoption.

## Governing Our New Bot Overlords

The rapid rise in the use of bots throughout organizations grants identity programs a chance for enhancement, as well as a new class of identity to govern. By being proactive, asking the right questions and using proven governance models, identity can be utilized to retain governance and oversight, while still allowing for quick adoption of this new technology.

**SAILPOINT:
THE POWER
OF IDENTITY™**

**sailpoint.com**

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.