SailPoint

WHITE PAPER

Cut Your Costs with a **Next-Generation Password Management Approach**

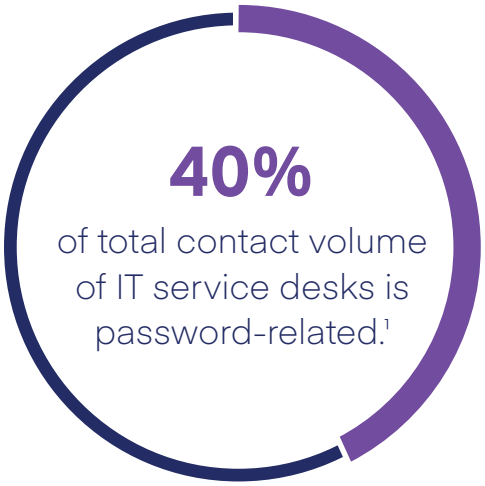
Legacy password management solutions are expensive to support and can't effectively address today's growing cloud and mobile requirements. This paper describes a next-generation approach to password management that is more comprehensive, scalable, and delivers a significantly lower cost of ownership.

Since the early 2000s, password management solutions have been used to automate self-service password resets and reduce the need for users to contact the helpdesk for assistance. Unfortunately, these decade-old technologies are expensive to support and maintain. In addition, legacy password solutions haven't adapted to address the rapid adoption of cloud applications and mobile device use in the enterprise. Organizations simply cannot assume that yesterday's password management technologies are the answer to today's complex requirements.

The fact is legacy password management solutions cannot meet the challenges facing today's hybrid (on-premises, cloud and mobile application environments) organizations and there is a more sustainable path forward by using a next-generation approach that is more cost effective, comprehensive and scalable.

Your Legacy Password Management Solution Costs More Than You Think

Legacy password management solutions were designed to relieve the internal burden of end user password reset requests on the helpdesk. Early password management solutions were viewed as technical initiatives that would streamline and centralize user password reset tasks while providing a higher degree of security by enforcing password policies defined by IT. As a result, many password management projects were focused on the technology and the internal integration aspects of coordinating password changes across different systems, rather than business user experience or requirements.



Gartner estimates that 40% of total contact volumes of IT service desks are still related to password change requests[1]. This means existing password management tools in the enterprise fail to address the main use case they were designed to support, which leads to higher IT costs, lost user productivity and security exposure. Simply put, legacy password management solutions cannot meet today's needs because they:

- Are more expensive to run and maintain
- Offer limited support for cloud-based applications
- Are not designed for the mobile workforce

Let's examine each of these barriers to success in greater detail.

Software Costs:

- Password Management software support and maintenance fees
- Operating system(s)
- Database/Directory(s)
- Application server(s)

Hardware Costs:

- Server(s)
- Router(s)
- Load balancer(s)

Day-to-day labor costs to run and maintain legacy password management solutions are another major component of overall costs:

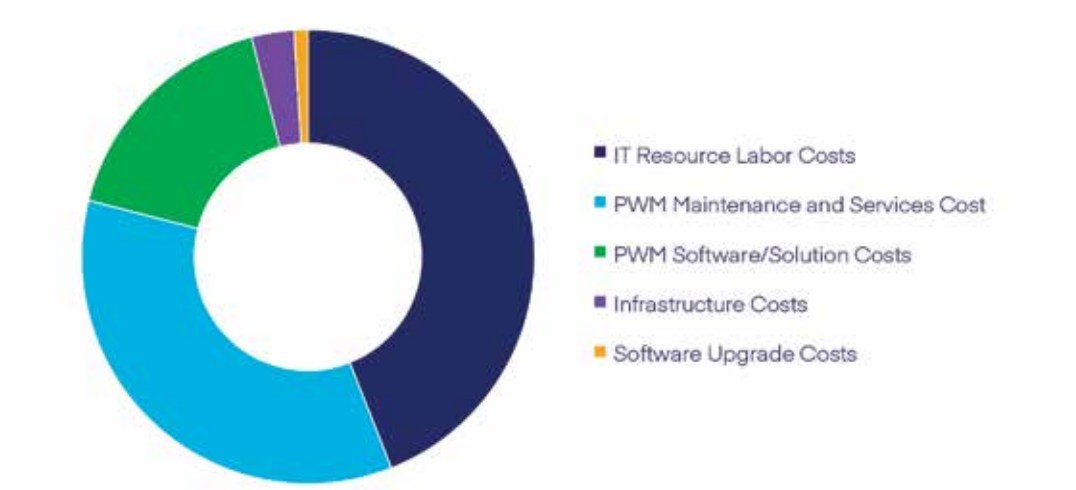
IT Admin Costs:

- Application owner(s)
- IT networking resource(s)
- IT database resource(s)
- Helpdesk resource(s)
- Professional services or consultants

[1] *Market Guide for Password Management Tools*, Gartner

Things to consider: How much does my password management solution cost to maintain every year? Does that number include the "hidden cost" of annual hardware and software maintenance fees?"

For an enterprise customer with 10,000 employees, the typical incremental "run" costs (e.g. software maintenance, labor costs, etc.) for a legacy password management solution are between $250,000 - $310,000 per year. This translates into a $750,000 to $930,000 three year total cost of ownership (TCO). With all the required infrastructure and labor to maintain an in-place legacy password management solution, it is easy to see how expensive it can get over time.



Another major concern companies have with legacy password management approaches are their lack basic governance-based policy administration and enforcement controls, as well as the ability to easily integrate into a governance strategy. In fact, to establish even a minimal level of governance within a legacy solution, customers had to custom-code workflows and complex rules within a completely separate provisioning product. Combined with product integration challenges, this dual product approach contributes to longer deployment cycles and skyrocketing project and maintenance costs.

Limited Support for Cloud-based Applications

Legacy password management solutions were designed to relieve the internal burden user self-service password resets for enterprise applications running on-premises in the data center. For example, enterprise applications and systems such as, Active Directory, Oracle E-Business, AS/400, RACF, PeopleSoft, SAP, Sybase, Novell eDirectory, ACF2, Remedy, AIX, and Red Hat, were generally considered target applications for password management solutions.

With the aggressive adoption of cloud-based resources, organizations must now address password management issues across both on-premises (internal) and cloud-based applications (external). End users expect the same level of service for their cloud-based applications such as Office 365, Google Apps, Salesforce.com, Active Directory, Concur, WebEx, Box, ServiceNow, Yammer, Workday, Dropbox, and GoToMeeting, as they do for on-premises systems. In addition, enterprises must be in a position to consistently enforce password policies across all applications, regardless on where the applications are running. Unfortunately, legacy password management solutions that lack the ability to support the growing use of cloud applications leave customers exposed to increasing helpdesk calls and security risks.

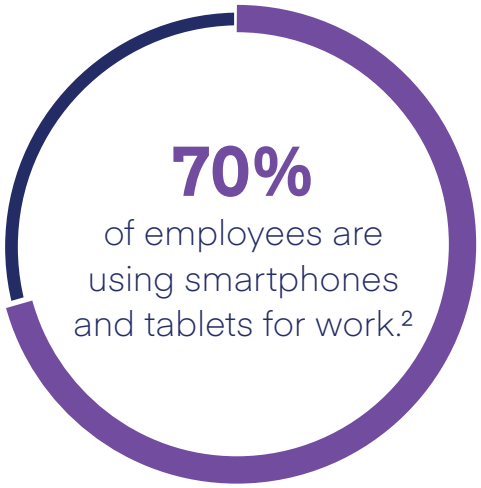
Things to consider: Is my current password management solution covering all applications? How do I control password policies for applications being introduced by organizations outside of IT?

Not Designed for the Mobile Workforce

Gartner notes that advancements in smartphone technology will drive increased emphasis on serving the needs of the mobile user.[3] Most IT groups are already experiencing this, as employees are using their personal mobile devices at work to improve productivity. And today's workforce is also on the move. 43% of employed Americans are already working from home at least part of the time, according to Gallup.

[2] *Market Pulse Survey*, SailPoint

[3] *Top 10 Strategic IT Trends for 2015*, Gartner



As a result, workers leverage personal devices now more than ever as part of their day-to-day routine. They take devices everywhere, leveraging a range of cellular and Wi-Fi networks to gain access to a wide variety of personal and professional applications. Unfortunately, legacy password management solutions can't keep pace with the need to update/reset passwords anytime, anywhere and on any device. For example, a road warrior working late from a hotel accidentally locks herself out of the corporate network. It's too late to call the IT helpdesk to assist with a password reset. How can a legacy password management solution help this mobile user? It can't. Legacy password management solutions are designed to facilitate password changes only when users have access to the corporate network.

In today's dynamic business environment, a password management solution must support both your workforce across corporate and mobile settings. It must provide users with the option to manage passwords from any device, on any network. In addition, it should support flexible, built-in strong authentication methods (e.g. OTP, SMS, Email, Voice, Q&A) to verify a user's identity before allowing a password change to be confirmed.

Things to consider: Can our employees reset their passwords when they aren't on our network, or do they have to call the helpdesk? Can our employees reset their passwords with their mobile device?

Next-Generation Password Management Offers a New Approach

Organizations that are currently using a legacy password management solution are caught between the proverbial rock and a hard place. On one hand, the solution is already in place and may be providing password management services to the business across existing enterprise applications. However, the adoption of cloud applications and mobile devices are quickly rendering those solutions obsolete. At the same time, replacing a legacy solution represents a hidden opportunity to reduce costs and streamline IT operations.

[2] *Market Pulse Survey*, SailPoint

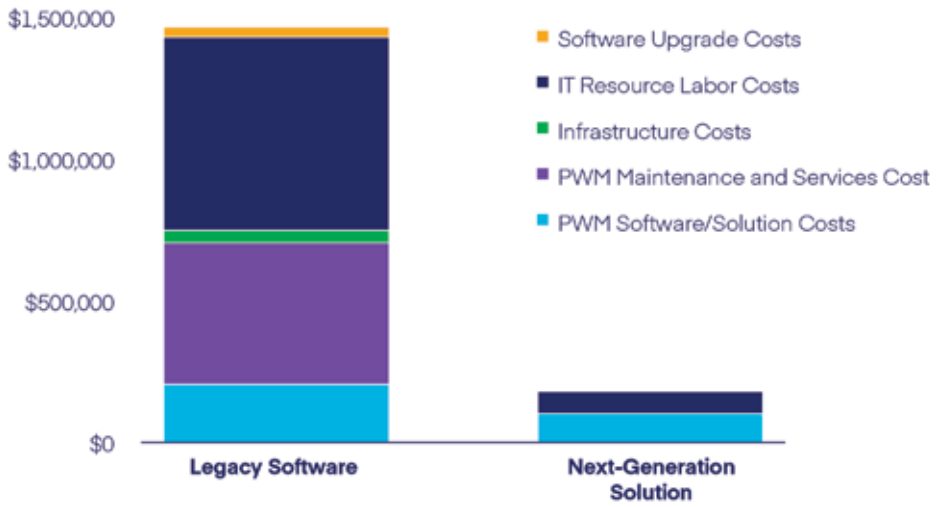
Next-generation password management solutions support all your applications and allow end users to manage password from any device, and from any network. Based on a centralized governance framework, they improve overall corporate security by consistently enforcing strong policies, and deliver a far superior ROI over legacy password management approaches by providing password management as a service delivered from the cloud.

The annual subscription costs of next-generation password management solutions are typically lower than the annual support and maintenance costs of a legacy password management products.

Lower TCO vs. Legacy Solutions

Next-generation password management services eliminate the significant infrastructure requirements, direct costs (for hardware, software, support and maintenance) and administrative overhead typical of legacy solutions. Customers benefit from cloud vendors' economies of scale to realize lower costs, which are typically included in password management service subscription contracts. As a result, cloud-based password management services are significantly less expense to run and maintain as directly compared to a legacy password management solutions, giving enterprises a far lower total cost of ownership (TCO) over time.

Consider a typical 3-year total cost of ownership comparison for a legacy vs. a next-generation password management solution:



As you can see, a next-generation password management service eliminates on-going maintenance and service costs, including the need to regularly upgrade the software with new versions or patches. Ongoing infrastructure upgrade costs are also eliminated, since delivery of the solution is provided by the vendor as part of the service subscription cost. IT resource labor costs are also reduced, as there is no longer a need to provide runtime support for a password management application running on your corporate network. Finally, next-generation solutions cover more use cases, including support for enterprise SaaS applications and off-network password resets from mobile devices, which further reduces calls to the help desk and significantly adds to the overall cost savings.

These differences add up quickly. For an enterprise customer with 10,000 employees, the typical next-generation password management service costs are $50,000 per year or $150,000 over a three-year period. The typical operating costs of a legacy password management solution are between $250,000 - $310,000 per year or up to $930,000 over a three-year period. So a legacy software product can cost a customer 520% more over a three year period compared to a next-generation solution. Put another way, an enterprise customer can decrease operating costs 83% by implementing a next-generation password management service.

Fast Time-to-Value

Unlike legacy password management products, cloud-based services let enterprises quickly and easily leverage a complete, turnkey delivery platform. Production and sandbox environments are available immediately, not in weeks or months. With a cloud-delivered platform, enterprises do not have to buy, deploy and maintain new hardware or middleware. Since no changes are required from the network and infrastructure teams, and configuration is simple, no coding or customization is required. So, enterprises can quickly roll out their password management service without depending on third-party professional services.

Legacy password management solutions are heavy, cumbersome and require an enormous amount of third-party professional services to implement and maintain over time. On the other hand, next-generation password management services are architected to deliver enterprise-grade capabilities at a fraction of the cost to deploy. In addition, as a cloud-based service, all updates to the software, including upgrades, patches and security fixes are automatically applied every two weeks. As a result, internal IT staff or third-party professional services are not required to maintain and upgrade the password management service.

Cloud-based Application Support

While legacy password management solutions were designed to address the burden of changing and resetting password for on-premises applications, a next-generation password management service is designed to span both internal and external applications. Migrating to a next-generation solution delivers immediate value by extending password management services to cloud applications such as Office 365, Google Apps and Salesforce.com. As a result, IT can provide a password solution to the business that simplifies password-related requests for end users, while leveraging a centralized governance framework to consistently enforce password policies across all applications for improved security.

The IT operations and help desk teams also benefit when an organization transitions to a next-generation solution through an immediate reduction in the growing number of help desk calls related to assisting users with log in challenges for cloud applications. The reduction in calls to support end user password reset requests is a direct result of extending existing password management processes such as self-service reset and automated password change synchronization to cloud applications. In addition, next-generation password management solutions which integrate single sign-on (SSO) capabilities can eliminate passwords altogether for cloud applications by leveraging federation technologies such as SAML. The password management and SSO combination is a powerful way to improve security while greatly simplifying how users access applications in the enterprise.

Designed for the Mobile Workforce

In order to maximize the return on investment for a password management solution, next-generation password management is natively designed to support the mobile workforce. It provides a consumer-simple, mobile-first UI experience for password changes and resets from any device on any network across all enterprise applications (on-premises, cloud and mobile).

Unlike legacy password management solutions which only work with a user is physically connected to the corporate network, a next-generation password management service is hosted in the cloud outside the corporate network and DMZ. This allows users to connect from anywhere in the world using any device – desktop, tablet or smartphone. In doing so, users can quickly and easily access the password management service without having to be logged into the corporate enterprise network or on the corporate virtual private network (VPN). Incorporation of additional functionality like Interactive Voice Response (IVR) also enables your workforce to reset passwords from outside the office.

Conclusion

Legacy password management approaches are unable to keep up with today's growing demand for anytime, anywhere access from any device. With a rapidly growing mobile workforce and an unprecedented rate of technology innovation, the high maintenance costs and existing gaps within these solutions will only continue to widen. Next-generation password management services based on a unified governance platform are the future, enabling organizations to empower users with easy-to-use capabilities and on-demand access to manage passwords across both internal and externally hosted applications. Offering a far more scalable and sustainable approach to password management, the benefits of a cloud-based approach to both the user and the enterprise are enormous, including a significantly lower total cost of ownership, increased workforce productivity, a reduced burden on IT, and the flexibility to support a rapidly changing IT environment.

SailPoint IdentityNow: Next Generation is Now

As the leader in ienterprise identity management, SailPoint delivers a next-generation password management solution through its cloud-based IdentityNow service. IdentityNow enables customers to quickly migrate from legacy password management solutions and take advantage of support for cloud applications, mobile end user capabilities and lower operational costs. In addition, for customer looking for a single, comprehensive identity governance solution, IdentityNow also offers access certifications, access requests and provisioning services. As a critical component of the enterprise IT infrastructure, IdentityNow is designed to meet the most stringent security, scalability, performance and availability requirements, including a firewall-friendly approach for managing on-premises resources from the cloud.

For more information go to: **sailpoint.com**

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 in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

WP1010-1709