SailPoint

WHITE PAPER

SailPoint + VMware Workspace ONE™

Securing and Governing Access for the Modern Workforce

The rapid transition to a digital world has cut across all industries and required changes in both how organizations manage their workforce and the method they use to deliver access to end users. The workforce has changed, and in addition to full-time employees, it is now far more likely to include contractors, vendors and partners, each of whom have their own set of needs. Meanwhile, data and applications are suddenly spread across both cloud and on-premises infrastructures alike and are being accessed by a myriad of organizational and personal devices including tablets, smartphones and laptops.

While these changes can be difficult to manage, they have also given enterprises a generational opportunity to digitize the way they interact with their workers and spur their next wave of productivity and growth. It's the enterprises who securely enable their workers to be productive – from anywhere, on any device and on any platform – who will gain the business and competitive advantage modernization brings.

VMware and SailPoint have partnered to deliver a holistic identity solution specifically designed to address the challenges modern enterprises face when managing access for a mobile and global workforce. It not only includes the market-leading value provided by each vendor, but also the mutual benefits that result from each technology working in unison. This collaborative solution enables enterprises to centrally manage and govern all users, endpoints and access to network resources in a simple and secure way, while also providing complete control of the access lifecycle.

The consumer simple, enterprise secure VMware Workspace ONE™ digital workspace platform combined with the breadth of governance of the SailPoint identity governance platform lets enterprises weave identity throughout the IT and security fabric of their organization. This results in a mobile workforce able to request and easily access the necessary applications and systems they need to be productive, while also ensuring access is only granted according to defined corporate policies. Enterprises can have confidence VMware and SailPoint can address their most complex mobile workforce management and identity governance needs.

VMware Workspace ONE Digital Workspace

Workspace ONE simply and securely delivers and manages any app on any device by integrating extensive access control along with multi-platform endpoint management. It is available as a cloud service or for on-premises deployment.

Using Workspace ONE, organizations can remove the silos of management that have been created between desktop, mobile and lines of business applications. Workspace ONE combines identity and context into a single platform that gives consumer simplicity for end users and enterprise security for the organization.

Key benefits of VMware Workspace ONE include:

- **Unified Endpoint Management:** A single platform provides management for all devices, from bring your own (BYO) to those fully managed by the organization.
- **Single Sign-On (SSO):** A single set of credentials is available for end users to manage, reset and self-serve across all devices and applications.
- **Rapid Onboarding:** New employees can be onboarded in minutes with all applications in place.
- **Easy Application Access:** Users can gain and manage all application access from one console.
- **Create, Edit and Monitor Policies:** Set and enforce access and data policies across all apps, devices and locations.

SailPoint Identity Governance

Identity governance provides complete visibility into who is accessing what, how are they getting that access, and what kind of risk that access represents so enterprises can respond accordingly. Put simply, SailPoint enables the right individuals to access the right resources at the right times and for the right reasons. SailPoint identity governance solutions are available as a cloud service (IdentityNow) and on-premises deployment (IdentityIQ).

SailPoint identity solutions provide a governance-based approach built upon the foundation of an open identity platform capable of delivering effective and scalable identity governance for mid- and large- enterprises across all industries.

Its extensibility enables access, to all resources across the organization, to be governed. This is fully realized when leveraging the many integration and connectivity capabilities available, including out-of-the box resource connectors, APIs, SDK and a plug-in framework.

The platform allows organizations to build a single preventive and detective control model that supports all identity business processes, across all applications.

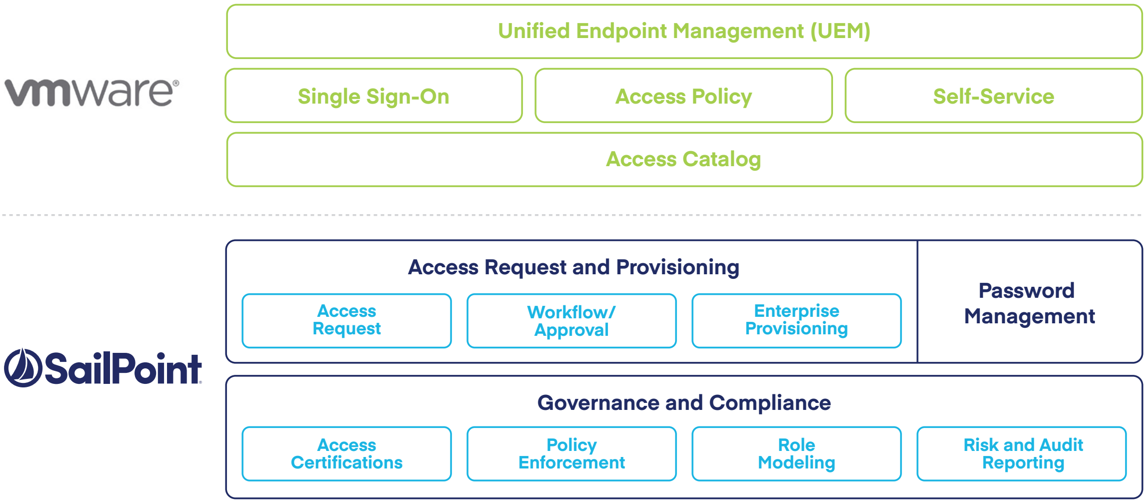
Key benefits of SailPoint identity governance include:

- **Visibility:** Gain a full 360-degree view of everyone's access, including that of privileged accounts where lack of visibility and compromise is most impactful.
- **Automation:** Automation of key processes frees IT staff from manual tasks, empowers users to help themselves, and helps organizations maintain consistent end-to-end access policy adherence.
- **Workforce Empowerment:** Ensure employees, partners and contractors have the right access at the right time, from any device.
- **Separation of Duty:** Scan identity data for separation of duty policy violations, alert business and IT managers, immediately revoke access, or run a pre-defined business process.
- **Line of Business:** Context-specific approval workflows ensure correct access according to line of business.
- **Compliance Management:** Automate access certifications, policy management and audit reporting through the unified governance framework, enabling you to streamline compliance processes and improve the effectiveness of identity governance-all while lowering costs.

Transforming Your Business with VMware and SailPoint

While each vendor's core technology supports proven, standalone, rich identity access management and governance capabilities, the unified solution leverages dynamic workflow functionality that results from this combination. VMware and SailPoint work in tandem to synchronize and streamline the user experience so a single set of credentials enables them to access everything they need across all their devices and platforms.

Conceptual Architecture Components



- Workspace ONE authenticates a user into their app through an access catalog, with SSO making authentication both easy and secure.
- SailPoint then enforces a “least privilege” approach, ensuring each user is only able to access those systems and data that applies to their particular role.
- Users make application access requests via a SailPoint tile included in the Workspace ONE application catalog.
- The request process initiates a business-process workflow to begin the provisioning steps. The process performs a policy evaluation before it begins the approval process to ensure access and compliance policies are adhered to.

Joining the capabilities and depth of VMware Workspace ONE digital workspace and SailPoint identity governance provides organizations three key areas of benefit:

Complete Access Lifecycle Management
Together, VMware and SailPoint give enterprises the means to provision devices with the applications users require from Day One and manage changes to entitlements and access through user-friendly, self-service requests, password management interfaces and automated lifecycle events for their entire workforce.

What’s key is the ability to adjust access according to end-to-end governance policies. As users change jobs and project assignments throughout their employee lifecycle, policy-driven workflows provision what employees need while removing unnecessary access they don’t need, including terminating all access for users who depart.

With VMware and SailPoint, enterprises can:

- Ensure provisioning of all applications and devices adhere to corporate policies.
- Implement full lifecycle management of access with automated processes so access is appropriate when users join an organization, change roles or leave.

Joiner

On Day One, a new user’s account is pre-populated with all applications based on job/role and all permissions provisioned ineach application.

Mover

Internal transfers have their accounts automatically adjusted to reflect new job/roles, and shoe new permissions provisioned and old permissions removed.

Leaver

Upon leaving the organization, a user’s account is automatically terminated and each application’s permissions de-provisioned or suspended.

- Provide context-specific approval workflows for access requests that adhere to an organization's established access policies.
- Automate key processes so mobile devices are either updated with new and applicable resources or completely wiped if an employee leaves the company.

Lowered Costs and Increased Productivity

The realities of modern business require organizations to do more with less, and do it faster. Productivity now relies on being responsive and enabling users to access data from anywhere, and on any device. By extending identity governance to all endpoints, enterprises can both enable their employees and ensure proper, timely and secure access.

By combining Workspace ONE and identity governance, enterprises can significantly reduce their operational and IT costs and increase their productivity by:

- Onboarding a new employee with all applications and devices in under an hour without tickets or help desk calls via automated provisioning and policy driven workflows
- Enabling each user with the specific resources their role requires to successfully accomplish their job
- Supporting self-service functionality for common problems and requests, such as password reset issues and requesting access to applications
- Giving employees the means to securely work from anywhere, on any device

Improved Security and Compliance

Enterprises can reduce risk while also maintaining a secure user experience and help ensure compliance requirements are met. Identity governance is what enables enterprises to maintain comprehensive control of who has access to what, from identities -> accounts -> entitlements. By leveraging the identity context that is generated, organizations can extend and share that information with key security components such as SIEM solutions to enrich and gain clearer insight into security events.

Workspace ONE and identity governance can help enterprises meet and maintain proper security and compliance standards while also enabling users via:

- Managing and governing secure access to any application across any device from a single user-centric platform
- Automated access certifications, policy management and audit reporting that demonstrates proof-of-compliance across a hybrid and mobile infrastructure
- Reducing the risk of over permissioned users
- Defined policies in areas such as entitlements and segregation of duty paired with automatic scans for violations across on-premises and cloud-based resources
- Audit trails to underscore internal and external reviews

Conclusion

We have all transitioned to a world where work is something we do, not a place we go. Employees want to be able to access corporate data, applications and online resources across more devices and locations. Their productivity depends on it. But as organizations gain the business returns enabling this behavior provides, they must be careful not to undermine their existing security posture.

Supporting workplace mobility, minimizing security risks and maintaining compliance is a challenge for IT teams. For these reasons and more, IT and security departments are adopting proven and trusted solutions that can manage a fluid and mobile workforce while also ensuring each user or identity is closely managed and governed.

Workspace ONE and identity goveranance lets enterprises put identity at the center of their IT and security infrastructure and break free from siloed management stacks and user experiences. As VMware brings secure access and authentication to the enterprise, SailPoint delivers the breadth of visibility into who has access to what and the identity context needed to make informed security decisions. It's a solution that ensures the right people have the right access to the right data, and that the wrong people don't.

This collaboration helps mid- and large-enterprises work more efficiently and effectively, and in turn gain a competitive advantage from digitizing how they interact with their workforce. VMware Workspace ONE and SailPoint identity governance can help enterprises both manage access and govern across the entire access lifecycle of users, applications and data, and significantly reduce their operational and IT costs while doing so.