WHITE PAPER–JUNE 2020

Moving to Identity-Based Access

Foundational digital workspace journey milestones

vmware®

Table of Contents

Executive Summary . . . 3
Recommendations . . . 3
Why Federated Identity and Access Matters . . . 4
Benefits of Federated Identity and Access Investments . . . 5
Build a Coalition to Drive Adoption and Rollout . . . 7
Consider Zero Trust . . . 8
Navigating the Zero Trust Maturity Curve: Lessons Learned . . . 8
Stage 0: Fragmented access . . . 9
Stage 1: Unified Access Management . . . 9
Stage 2: Contextual access . . . 10
Stage 3: Adaptive access . . . 11
Taking the Next Steps to Identity-Based Access . . . 11

Executive Summary

Users IDs and passwords can no longer be the only way to secure access to the digital workspace. Passwords are vulnerable, burdensome to users, and expensive for IT to manage.

Increasingly, user identities reside in multiple "realms," both internally and externally, with each realm requiring its own credentials. The most effective solution to this growing problem is federated identity, which facilitates secure interconnections between identity realms that do not inherently trust each other. With a federated single sign-on (SSO) solution, you can streamline secure access by integrating on-premises, virtual, cloud, and mobile applications. The integration of identity stores and providers and federated access solutions delivers efficiencies and cost savings around controlling user entitlements, password management, as well as minimizes security breaches involving stolen credentials.

Credential sprawl is a known security concern, yet many organizations, especially large ones, have been reluctant to address the issue in fear of creating disruption for users and the business. However, federated identity and access is not only a prerequisite for other steps in the digital workspace journey, it enhances user productivity and satisfaction. Federation is the baseline for delivering risk-based, adaptive access to the digital workspace, presenting users all the resources they need—and only what they need—in a tightly managed business context. Users can be automatically granted or denied access from any location according to their entitlements and other relevant context parameters. Moreover, context can be reassessed as needed to ensure security and compliance of new and emerging work styles.

Do not let fear of change be a roadblock in your digital workspace journey and limit user productivity and satisfaction. Learn how you can navigate the roadmap to achieve simplified and more secure access and bypass resistance by addressing change management concerns.

Recommendations

Federated identity and access strengthens security, ensures workplace compliance, and streamlines the employee experience. To move your organization to identity-based access:

- Determine the tactical and strategic value that federated identity and access can offer to your organization by evaluating hard and soft benefits, the risks of inadequately securing workspace access, and the potential impact of delaying your digital workspace journey.
- Fight organizational inertia by building a coalition across functional roles that have a vested interest in simplifying access to company resources. Engage with this coalition to document the business need and to strategize around rollout and policy definitions.
- Replace your existing architecture for accessing corporate resources with one that aligns with your employees' work style.
- Address fear of change by creating a roadmap that integrates legacy technologies and also sets a path for the evolution of identity and access over time.
- Plan for continual review of architecture, policies, and processes to drive and optimize federated identity and access.

Why Federated Identity and Access Matters

Most organizations have a variety of on-premises applications and one or more user stores or directories, often based on Microsoft Active Directory (AD). Organizations also often have different sets of applications, for instance, productivity applications, each with its own dedicated single sign-on (SSO) method. And with the growing adoption of software-as-a-service (SaaS) applications and other externally hosted applications, the number of identity realms (or circles of trust) has also grown.

An identity realm contains a user directory, an authentication and authorization system, and one or more applications. Within each realm, all components are considered trusted. The identity provider (IdP) issues an authenticated user a token to access the systems and applications inside the realm. Midsize and larger organizations typically have multiple identity realms.

For example, an organization has an AD directory for defining access rights to internal resources—call this Realm A. The organization partially embraces a cloud office suite, so it also needs a directory in the cloud to define access to those applications—Realm B. However, users defined in Realm A cannot use their credentials to access the applications in Realm B. Instead, they must use different credentials to authenticate to Realm B. But with federation, you can establish trust between different identity realms, so a user's authentication to one realm is trusted by other realms.

Federated SSO solutions are built on standards and can integrate on-premises, virtual, and cloud applications, even mobile applications. You can set different levels of assurance (LOA) when validating a user's identity and use the LOA as proof of identity in downstream systems, such as with multifactor authentication (MFA). You can even deny a user access or demand remediation actions. Federation strengthens access security, ensures workplace compliance, and streamlines the employee experience.

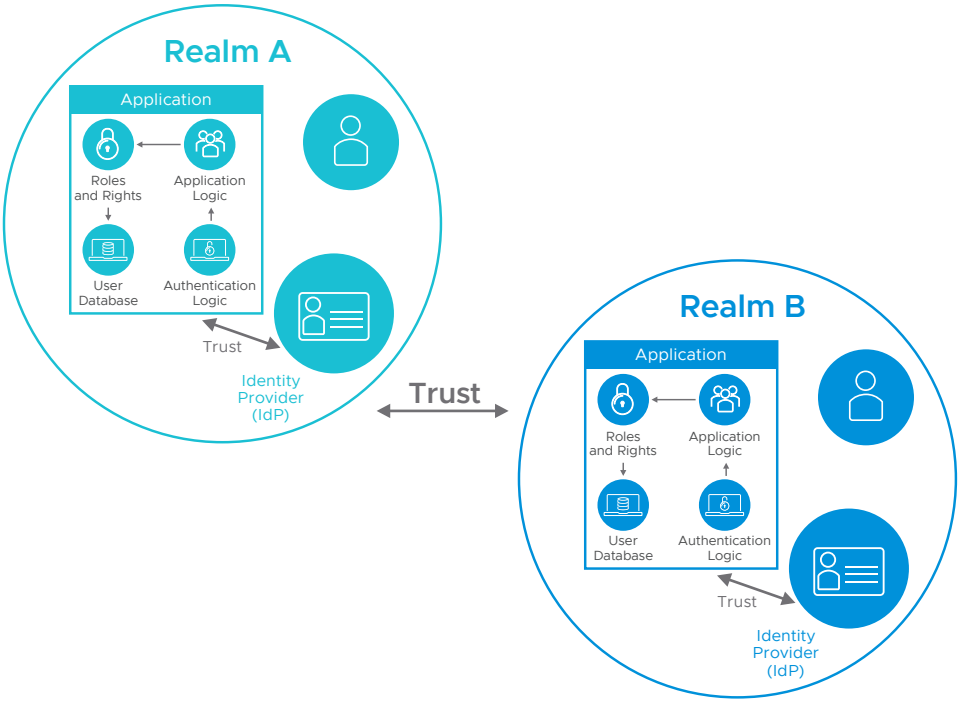

Figure 1: Using Federation to Establish Trust Between Identity Realms

Benefits of Federated Identity and Access Investments

Many organizations still view federation projects as tactical, something to employ in response to an immediate, short-term requirement, such as increasing security following an attack. But organizations often overlook federation's long-term benefits in their business justifications, like enabling secure access to the evolving digital workspace or the positive impact on employee satisfaction and workspace compliance.

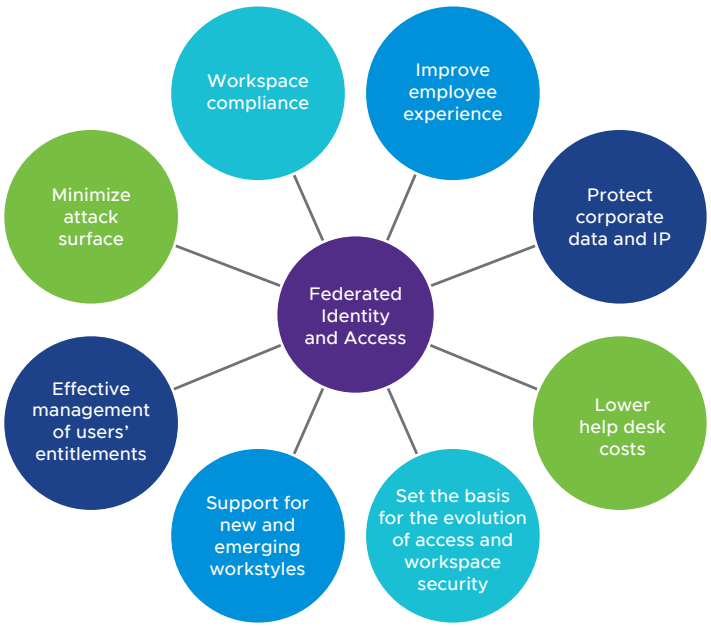

Figure 2: Benefits of Federated Identity and Access

When advocating for the adoption of a federation solution, consider these points to support your business case.

Workspace compliance and attack surface reduction – As the number of applications provisioned to employees increases, so does the number of passwords, credentials, and points of access that they need to remember and manage. Passwords are vulnerable to phishing and hacking, and they are frequently reused for different applications. To keep track of them, users often store passwords in insecure places. Federated identity and access brings convenience by letting a user authenticate once to access multiple, if not all, applications. SSO provides the dual benefit of enhancing the user experience and reinforcing secure access to the workspace. With federation, you can extend the range of authentication methods, such as using MFA, as well as step up authentication demands at need or to impose remediation measures.

Lower help desk costs – For many organizations, the key benefit of federated identities revolves around lowering the cost and time devoted to password management. Integrating multiple realms of trust and identity stores through SSO significantly reduces the number of passwords that users have to remember. The ability to use MFA, such as biometrics, instead of entering a password, lowers password reset costs—the business case for moving to federation is often built on this benefit alone. Password resets are consistently ranked among the most frequent calls handled by help desks. Organizations without a federation solution typically deal with 4 to 12 credential management support issues per user, per year. Managing a help desk ticket usually costs around $15, so the potential savings is easily demonstrated.

Improved employee experience – Employees welcome the idea of easier access and reducing the time devoted to password management and resolving issues. With federated identity and access, employees can securely access their corporate resources anywhere from any device, including their personal ones, facilitating remote working and working from home.

Accurate management of user entitlements – Federated identity and access solutions are easier to integrate with HR management systems, providing more accurate control of a user's entitlements throughout employment. Some of the benefits are quicker access to corporate applications and systems at onboarding, the ability to rapidly modify entitlements when an employee's role changes, and easy revocation of all entitlements when the employee leaves the organization. You can also give job applicants and former employees partial access to corporate systems. Accurate entitlement management lets employees achieve full productivity faster, improves their working experience, and helps protect corporate data and intellectual property.

Next-generation workspace security for new and emerging work styles – Work as we know it is changing. It is now essential to have all the resources we need to stay informed and to get work done from anywhere and on any device, enabling the best combination of office and remote work. Employees increasingly use multiple and differing devices, not all of which are company owned, running a variety of applications from different locations. In response, a growing number of organizations are implementing zero trust frameworks, where access to corporate resources is granted only after verifying multiple factors that are defined by corporate policy. To be effective, the verification process must be frictionless for the user yet allow the organization to alter the verification factors in real time as risks change. Federated identity and access supports zero trust by enabling flexibility in the way users work without compromising the security of corporate applications and data. This approach becomes even more critical as new device types enter the enterprise and work processes are redesigned.

Build a Coalition to Drive Adoption and Rollout

Inertia toward embracing federated access is often connected to difficulties in gathering clear requirements and strong sponsorship for the initiative. To assess and encourage adoption, form a coalition of all stakeholders—IT and non-IT—who will benefit from federation. A cross-functional coalition reinforces the business case and ensures support for organizational rollout and adoption. Consider the following leaders to help co-design the policies and security posture.

- **End-user computing leaders**, the main sponsors and owners of the digital workspace journey roadmap.
- **Identity team representatives** wanting to reconcile the sprawl of user identities and identity providers.
- **Security operations and incident response representatives** looking to reduce the time and effort spent on credential and password issues.
- **Security engineers** concerned with reducing the corporate attack surface and protecting credentials and access to corporate data and IP.
- **Application owners** who need to prioritize the use of business-critical applications and ensure access to other applications, including legacy ones. Applications owners, along with end-user computing leaders, might also want to offer employees a unified catalog of enterprise applications, which requires a federation access solution.
- **IT operations**, the likely promoters, along with security engineers, of an automated approach for managing access to applications and other resources.
- **HR** seeking a more effective integration of IT with HR management systems to better manage employee entitlements across the full term of employment.
- **Employee experience owners** interested in promoting frictionless access to corporate resources and eliminating the overhead for workers of credential and password management.
- **Line-of-business representatives** looking to promote more flexible work styles for employees.

Consider Zero Trust

An access architecture that assumes a firmly identified workspace perimeter is inadequate for a workforce that accesses corporate data from multiple locations and networks with a variety of devices. The concept of zero trust is rapidly emerging as a more effective method to managing access, particularly for new and evolving work styles. Zero trust is not a single technology or product but an IT approach that considers every user and every device to be untrusted until a number of factors have been verified. Only after verification has been completed is access to corporate applications and data granted. Moreover, the requirement of verification is ongoing rather than occurring once. A digital workspace strategy benefits from embracing at least some elements of the zero trust model. Federated identity and access is a foundational component of a zero trust architecture.

Many technologies that contribute to a zero trust vision are already mainstream. Others are still maturing and so can be more complex to implement. You can combine different levels of trust to build out a true zero trust model, depending on the use case. Most organizations add security capabilities as they get more comfortable or as the technology improves.

Modifying how employees and partners can access corporate information is a major change and will likely encounter resistance. To push through such resistance, it is essential to break down the architectural changes into smaller steps to minimize the potential disruption for users and business.

Navigating the Zero Trust Maturity Curve: Lessons Learned

The zero trust maturity curve for end-user computing comprises four stages, with most enterprises positioning themselves between stage 0 (fragmented access) and stage 1 (unified access management). Stage 3 (adaptive access) is an aspirational goal for most organizations today. VMware customers who are further along this maturity curve have shared the following observations and best practices.

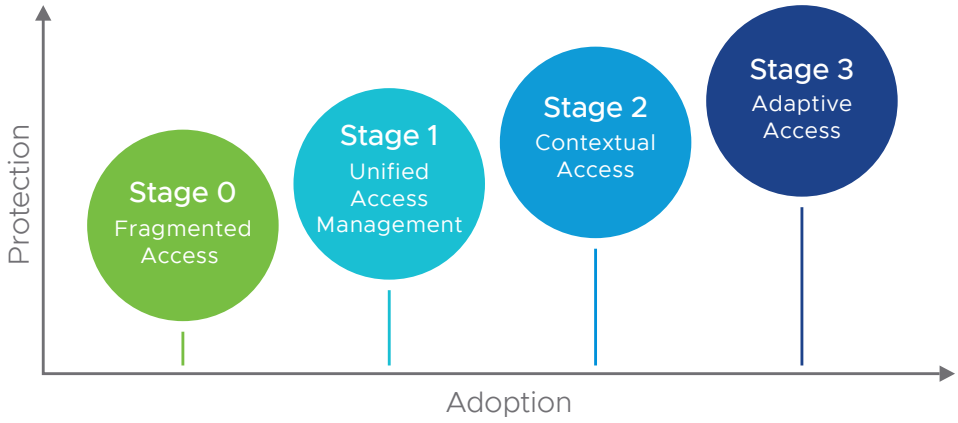

Figure 3: Stages of the Zero Trust Maturity Curve

Stage 0: Fragmented access

You do not want to be at stage 0. At this stage, an organization has multiple identity realms with multiple IdPs and both on-premises and cloud-based user directories. No integration across realms exists, and users are required to supply different insecure credentials and passwords everywhere. Some services might even be in use without IT's knowledge. To enhance security, reduce support costs, and improve user satisfaction, an organization must exit this stage as rapidly as possible.

Stage 1: Unified Access Management

Moving to stage 1 requires consolidating access management policies across systems and implementing SSO where possible. A common obstacle to advancing to unified access management is the complex stratification of the existing point-solution tools. Instead of replacing current tools and processes, the best way to overcome this issue—and minimize cost and disruption—is to select technologies that you can reuse and federate.

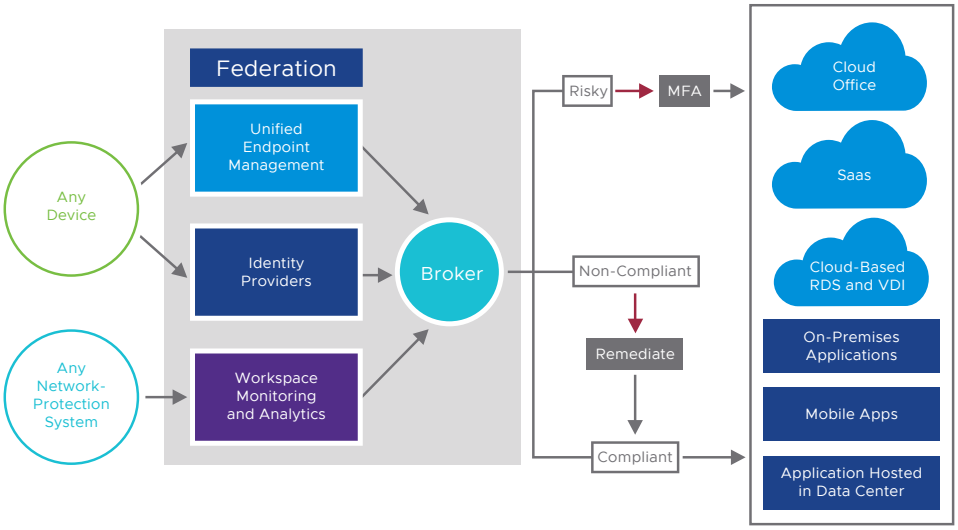

Figure 4: Federating Existing Realms and Tools for Unified Access Management

Moving to stage 1 typically involves:

- Federating the existing IdPs, user directories, and point solutions. Integrating these preexisting elements is key, because full replacement is usually too disruptive for users and the organization.
- Adopting a comprehensive SSO solution, ideally one that can broker access from all devices to all applications: on-premises, web-based, SaaS, and mobile.
- Prioritizing the selection of tools that integrate with the third-party MFA tools already in place. These tools must integrate with all existing unified endpoint management (UEM) instrumentation to be able to define policies across devices, applications, and servers and support existing IT service management solutions.

Stage 2: Contextual access

After you have achieved unified access, the next step is to add context-based policies to control who can access what and how. To create effective policies involves gathering data with UEM tools about a variety of factors: each user's context—who are they, which applications do they need to access, and are they in a more or less risky group?—devices in use, locations, and available networks.

Examples of policies for contextual access include:

- Enabling access to corporate resources only for registered or recognized devices
- Ensuring the ability to remotely wipe company information from lost or stolen devices
- Allowing only fully managed corporate devices to be used, such as in highly regulated environments where the comingling of personal and business assets is not permitted
- Requiring a higher level of authentication, such as MFA, whenever a user needs to access sensitive or confidential data
- Increasing authentication requirements based on the access context

Best practices for moving to contextual access include:

- Form a cross-functional team to define and review access policies. The team typically includes end-user computing, the identity team, IT and security operations, and HR.
- Establish a framework to analyze user workflows and identify where access controls need to be optimized. For example, when a user changes roles, the policies enable automated provisioning to access the necessary work tools. In the case of a departure, the policies facilitate automatic revocation of access to services and applications and mitigate the risk of orphaned accounts.
- Apply access controls to all technologies used by the workforce, including securing access to APIs. APIs are the building blocks of modern applications and can expose sensitive data.
- Prepare to address employee concerns about data privacy. Be transparent about which information you can access and which information remains confidential, such as photos, message trails, browsing history, and personal contacts. Consider launching a communication campaign with adequate assets and the support of champions.

Stage 3: Adaptive access

In this final stage, authentication no longer occurs just at the "front gate"—the time or point of initial access—but continuously, using adaptive, risk-based assessments of potential threats. If a device goes out of compliance during a session, action is taken, such as disconnecting the session or requiring the user to perform a remediation workflow. Reaching this stage requires:

- Rich workspace analytics
- Ongoing security monitoring capabilities
- A decision engine that correlates all relevant data and provides rapid, automated mitigation responses

Examined risk factors could include user characteristics, device security settings, the volume and nature of applications downloaded, and device compliance in terms of patches and updates. An assessment score determines the amount of authentication required.

Moving to this stage involves:

- Understanding the level of integration needed between the intelligent decision engine and tools already in use to implement risk-based access, such as user experience management processes to gather device-level data, endpoint monitoring and analytics tools, and HR management systems. Ideally, the engine will also benefit from integrating with endpoint detection and response tools.
- A cross-functional effort to establish the main access decision factors, with participation from the endpoint, application, and identity teams.
- Creating a decision map to determine the access mechanisms required—such as MFA, certificates, remediation, denial—for each risk level as defined by the application being accessed, the network and device in use, and the user's profile.

Taking the Next Steps to Identity-Based Access

The digital workspace journey unlocks next-generation levels of employee engagement and productivity by enabling new work styles and processes. But it also demands a new approach that ensures secure access to corporate resources and a frictionless experience for users. This change can be complex and met with resistance and fear of disruption. The lessons learned and best practices shared here by organizations who have successfully tackled such inertia can help you unlock the next steps in your digital workspace journey.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: FY21-5847-VMW-MOVING-TO-IDENTITY-BASED-ACCESS-WP-USLET-20200601 6/20