WHITE PAPER – **AUGUST 2018**

EUC TRANSFORMATION BEST PRACTICE GUIDE: FEDERATING IDENTITY AND ACCESS

vmware®

Table of Contents

Executive Summary

The ways an organization's users access applications today are far more complex than they were for prior generations of workers. Enterprise and productivity applications can be accessed through mobile devices, desktops, laptops, or thin clients. These applications may reside on the devices themselves—in the data center, on web servers, or in the cloud—or perhaps even in multiple locations. Not all these applications will be managed by IT; an increasing number of applications are accessed by the user without organizational involvement. These new dynamics that now exist around users, devices, and applications serve to make end-user computing significantly more complex to manage.

To support these requirements, most organizations have embraced a multi-modal style of end-user computing that enables any user to potentially work with any application, any devices, and any infrastructure. Although beneficial in terms of productivity and user engagement, this approach also introduces new risks and issues. Threats associated with malware, viruses, ransomware, digital highjacks, information theft, identity theft, data integrity, and compromised information have increased significantly due to this "any-to-any," multi-modal style of end-user computing.

Identity and Access Management (IAM) technology is a key means of supporting this "any-to-any" approach. IAM enables users to access the applications they need in a way that is easy to use, secure, and reliable. IAM systems typically integrate with specific sets of applications residing on internal servers, devices, and web servers. IAM can also integrate with cloud-provisioned applications and assist in how users access applications that do not reside with their organization.

Most organizations have deployed IAM solutions in a piecemeal fashion, with different products and technologies managing access from different types of devices or to different types of applications. Integration between these solutions can require significant additional effort in application packaging and delivery, so many organizations either integrate partially or not at all. The result tends to be different access approaches for different types of devices, with many applications still residing outside of any IAM system. For the user, this means multiple sets of credentials are required to access the applications they need. Complexity, extra support issues, and loss of productivity are the natural outcomes.

To overcome these concerns and extend the benefits of IAM, we must apply the concept of *Federated Access Management:* a single sign-on approach that provides access to all applications by leveraging the systems already in place. Not only does this approach help organizations overcome the functional and user-satisfaction concerns of the piecemeal approach, it also delivers the lowest-cost path to improvement by maximizing the re-use of existing resources.

In this paper we discuss typical IAM deployment scenarios, how existing solutions provide value, and how Federated Access Management can deliver the desired user experience that organizations are striving for. We also describe some of the steps and considerations that organizations should be mindful of when pursuing successful deployments.

What's Different?

The challenge of working across multiple types of applications is not new to IT. There has always been great diversity among application types, the platforms they run on, and the devices used to gain access. Terminals were used for mainframe access, PCs to run Win32 and Win64 source code, web apps require a browser, and mobile devices (tablets and smartphones) run applications provisioned (usually self-provisioned) through app stores.

Recent trends around unification of access have prompted use-case scenarios in which users desire access to all application types regardless of where they are, the devices they use, the network they are on, or the underlying platform from which the application is delivered. Application access has evolved significantly, and users now often expect and demand access to most of the applications they need through a variety of devices.

Providing unified application access has given rise to Identity and Access Management (IAM) solutions, which are designed to provide organizations the ability to simplify user access, increase application security, monitor usage, and apply administrative policies that are in the best interest of both the organization and the user.

IAM provides the following functions:

- **Identity** – The creation, management, and deletion of identities associated with users
- **Login** – ID and password or credential access to applications, devices, and services
- **Policy** – An intelligence engine that applies role-based and personalized, rule-based access to applications and data for each user and their devices
- **Unified access** – A system that allows a user to authenticate once to a range of applications and services without necessarily knowing their login credentials for each application or service

IAM systems are directory-based and govern access to the device, applications, and associated data, and the context for use. IAM has become valuable to organizations by providing features that deliver both simplicity for users and additional control for IT, such as single sign-on, multifactor authentication, compliance verification, and context-aware policies.

Unfortunately, IAM solutions do not typically provide full access to all the desired or required applications. Some applications require proprietary IAM solutions to service only a subset of application types (such as web or cloud apps). In larger, more complex organizations it has become standard practice to deploy multiple IAM solutions or omit certain applications from IAM inclusion.

One of the most frequent scenarios is a lack of integration between IAM systems and enterprise mobility management (EMM) approaches. Most EMM products require dedicated packaging of mobile applications (using specific tools or software development kits) before they can expose mobile applications to IAM systems. Because of the resulting increased integration efforts and delayed deployment time, many organizations choose not to integrate their IAM and EMM systems, leading to a fragmentation of user credentials, an increase in related support incidents, and a loss of control for IT.

What Changes?

The key components of IAM are not new: Many organizations have successfully deployed Identity Management (IDM) systems for many years. The need for IDM was initially driven by security teams, to both manage access and simplify credential management through single sign-on functionality. As end-user computing evolved from Windows and PCs to the "any-to-any" scenario we see today, the focus of IDM shifted from a mainly security-led posture to one of providing better end-user access (IAM).

The Past

Currently, the use of IAM is essential for any organization embracing a digital workspace strategy. IAM has become a key component of EUC strategy and is complementary to other EUC technologies such as VDI, application publishing, unified endpoint management (UEM), PCLM, and EMM.

IAM systems are designed such that

- Access to applications can occur natively on virtually any device.
- Password reset is user initiated.
- Identities are automatically synchronized across different systems.
- Nearly every type of application can be accessed.
- Enhanced security features such as single sign-on (SSO), multifactor authentication (MFA), and conditional access are supported.

The Future

Moving forward, most organizations will leverage Federated Access Management (FAM) as means to enhance IAM and provide additional digital workspace functionality. As mentioned earlier, there is a strong likelihood that multiple IAM solutions are in use for most complex environments. The use of FAM means that a single access approach can be implemented across the organization, allowing users simple and easy access to nearly every application they require and desire. FAM does not displace existing IAM systems; rather it works with them by providing users with a single point of entry that provides access to all applications and systems. Having the ability to federate multiple IAM solutions enables customers to leverage their existing IAM sunk investments while simultaneously increasing ease of use, security, and adoption.

FAM systems offer added value in the areas of

- IAM integration
- Conditional access
- Ease of use
- Enhanced policy management
- Management and intelligence (such as auditing and reporting)

The use of FAM is key to *IAM integration* and is analogous to grease on the gears of an engine: It makes parts that touch each other work together more smoothly. IAM systems are typically targeted at certain types of workloads, infrastructures, or applications, so these systems are optimized to manage access within a specific context (for example, certain applications, infrastructures, and devices), but incomplete in terms of their ability to work with other applications. FAM systems broker to multiple unique IAM systems, so that all applications, infrastructures, and devices can be equally serviced.

Delivering applications securely and reliably to users also requires access to additional devices. This is usually achieved using *conditional access* to apply policy rules, as illustrated in Figure 1. Conditional access protects content by requiring that certain criteria be met before granting access to the content. Content can be data or applications that reside on the device or in the data center, or are delivered as a cloud-based service. The key to conditional access is the ability to determine the posture of the device (typically a PC or smartphone) so that IT administrators can either apply policy based on context to the device, or block access to the resources that are being accessed. For example, a user, using their iPhone, might be permitted to access certain applications when on the company Wi-Fi, but not when attempting to access them from a public Wi-Fi.

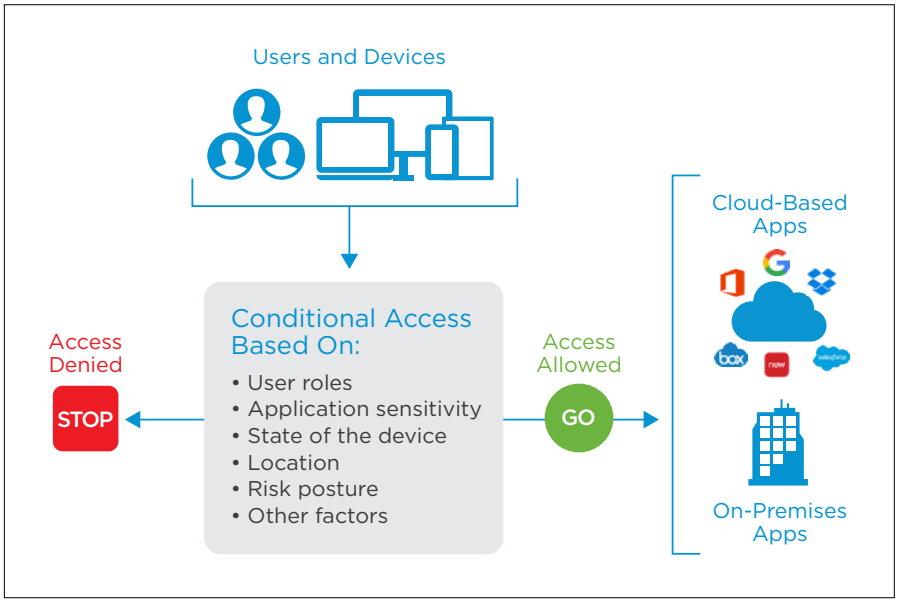

Figure 1: Conditional Access

Successful conditional access requires integration with device management. Knowledge of whether a device is jailbroken, in a state of compromise, or in an unsecure location are some aspects of posture that must be read to ensure applications and content can be accessed securely. This means that FAM systems must seamlessly integrate with EMM so that end-to-end management, based on policy and context, can be achieved. If the integration is not seamless, and requires additional packaging effort, it is highly unlikely that the FAM system will be able to support access to all applications.

Enabling users with a *simple, secure, and reliable way to access applications* is a critical success factor for any FAM or IAM system. Most users are burdened with multiple methods of application access, login IDs, and password requirements. This overload gives rise to "sticky note" access, where users rely on pen and paper to record current credentials and simplify their access experience. Such antiquated password-management approaches present growing risks: Recent surveys indicate that nearly one in three users have been hacked or compromised. FAM helps consolidate access by streamlining where and how applications are managed so that the ID and password memorization burden is, at worst, greatly simplified for the user and, at best, eliminated completely.

FAM also introduces new functionality in the area of *policy.* Policy enhancements include the ability to apply policy-based rules to specific scenarios. For example, IT administrators may disable access to some applications and data (for instance, sales data) at specific times, such as at the end of a financial quarter. Another common scenario is to apply policy so that access is only granted to "known" or "good" networks and devices, while all other networks and devices are prohibited. Some organizations find that having the ability to apply management policy based on scenarios and context offers more granular control, better reliability, and increased protection of IT applications and data.

Finally, FAM provides better back-end *management and intelligence* capabilities for IT administrators, including key features such as reporting and audit capabilities. Expanded device and application diversity dramatically increases the complexity of traditional management approaches, making it extremely difficult for administrators to assess real threats, exposure, and attacks. Consolidated and complete, real-time information on users, their devices, applications in use, frequency of changes and updates, methods of connection, and location are critical for IT forensics, threat detection, trend analysis, and automated, holistic management.

Implications of Transforming Identity and Access Management

Customers beginning their adoption of FAM will find that their users, administrators, help desk, and application development teams change how applications are accessed, supported, and developed. For some, the changes are minimal and will have little impact. Others find that FAM changes are more complex and require new skills and processes.

Impact on IT Operations and Users

IT administrators will likely be huge beneficiaries of the move to a Federated Access Management approach. With application access, policy, and verification all consolidated, administrators will be able to create policies, perform management, and gather intelligence on deployment and use from a single source. The result is simplification, a significant reduction in overhead, and a consummate improvement in time to deploy.

Users also benefit from the better administration provided by FAM. The biggest advantage for users involves access via ID and passwords: It is not uncommon for nearly 40 percent of all calls to an organization's help or service desk to involve password resets. In fact, many VMware customers claim to deal with between 4 and 12 credential-management support issues per user, per year. Consolidating access approaches with FAM enables automation of all credential management through dedicated tools, which most users prefer. Done correctly, FAM will lead to fewer calls for password resets, in turn resulting in better customer service levels, lower cost, and more user productivity. Users also report significant improvements in their ability to seamlessly and efficiently access the apps and data they require.

Once FAM is implemented, users will need some training (most likely informal). The way users access and authenticate to applications will likely change. The good news, however, is that the new access methods are significantly simpler and easier to understand. And because FAM consolidates access in one location, users find the changes very welcome.

Behind-the-scenes application provisioners will have new work as well. Applications must be configured in such a way that access is part of a unified method, that is, a common portal. This means that applications are made available in only one way: through the FAM. Over time, the use of FAM for access makes application configuration easier and FAM becomes the de-facto method of application access.

Impact of Transforming Identity and Access Management on End-User Support

The mindset regarding the value of providing outstanding end-user support is changing. Most organizations have historically considered end-user support and operations as a necessary cost of technology adoption. Executive management is coming to realize that providing a better user experience is not only good for users but for the organization as well. With a renewed emphasis on outstanding service, help desk and support teams have broadened the types of problems and issues they help with. As such, technologies (such as FAM) are a great investment that aids in providing world-class support.

FAM makes end-user support easier to deliver, more reliable, and less costly. Support teams will find that application access can be automatically governed by policies set by IT. Instead of dealing with frequent ID and password support issues, help desk teams can focus on helping with more complex issues that users face.

One of the real benefits associated with FAM is that user convenience no longer comes at the expense of security. With FAM, making security easier for end users also makes those users more secure. To achieve this, users are no longer required to be exclusively dependent upon complex password requirements that change every 30, 60, or 90 days. Dependence upon a single set of credentials, along with a second factor of authentication (for example, biometrics), offers a more reliable method of access that is more secure and less costly to manage.

IT managers must adjust as well. Deploying FAM means embracing new forms of authentication, focusing on policy management, and vetting third-party application providers for methods of access. Changes associated with help desks, second-level support, and self-support are needed as well. Embracing FAM typically means changes for the support teams in how they service users. Instead of different answers for different applications, commonality of access to all applications now makes support more uniform as well.

Cost Changes for Identity and Access Management

Direct costs affected include the following:

- Staff – Help desk, IT admin, and security teams now perform more work in less time, which may reduce the number of support staff needed for employees.
- Infrastructure needed for IAM.
- The noteworthy reduction or elimination of help-desk tickets related to credential management will deliver significant savings. Industry analysts estimate that each help-desk ticket costs around $15 to process.

Indirect costs affected include the following:

- More user uptime and productivity, through fewer credential-management issues and more consistent access to applications.
- Accelerated deployment schedules for new applications and devices.
- Better knowledge and insight gleaned from application access provide for better operational planning at lower costs.
- Flexible application access improves user SLAs with fewer incidents and outages.
- Rapid deployment and configuration of application access improves availability and allows users to commence or resume job functions following workforce adds, moves, and changes.
- Multi-device use makes users more productive.
- Reduction in the number of applications deployed outside of IT access management.

Preparing for the Adoption of Identity and Access Management

To prepare to adopt IAM, organizations should take the following steps:

- *Understand* that IAM and IDM have morphed into FAM.
- *Further, understand* that as customers embrace a digital workspace strategy, FAM becomes essential.
- *Recognize* that the value associated with FAM goes beyond security, as users, support teams, and administrators will all benefit.
- *Establish* a holistic deployment strategy that allows for the delivery of applications that can be front-ended with FAM.
- *Leverage* IAM benefits to help drive other application acquisition and development efforts.
- *Consider* the organizational and operational challenges and changes implied for the security, support, and administrative teams.
- *Build* consensus with key stakeholders so that a unified application-access strategy can be created and embraced across the organization.
- *Learn* about the new, unique, and strategic features of FAM that offer a holistic model for dealing with devices, users, applications, policy, and context.
- *Test* a variety of application scenarios, use cases, and user types (for example, knowledge worker, kiosk, road warrior) with FAM.
- *Create* a detailed analysis of existing applications, their users, and requirements.
- *Eliminate* applications that are no longer needed or relevant to the user or organization.
- *Review* all assumptions, configurations, processes, and other aspects of alternative application-access methods.
- *Justify* further expansion of your IAM strategy by measuring SLAs, costs (direct and indirect), and value (with ROI, if possible).
- *Understand* that different operational processes will likely coexist for some time.
- *Communicate, communicate, communicate!*

Conclusions

IAM is the task of controlling information about users on computers and devices. Deploying IAM offers users a better and easier experience that dramatically increases productivity. IAM also offers IT administration a consolidated approach to application access at lower cost, with better reliability and additional insight into actual user activity. Customers considering IAM should devise a FAM strategy that is inclusive to all relevant components (device, user, OS, application, network, and context) needed for a complete solution.

About the Author

Mark Margevicius, Director of EUC Strategy and Chief Customer Advocate, VMware, wrote this paper. Mark's primary function is to assist customers in understanding the trends and directions of the end-user-computing landscape. In this advisory role, he provides tactical guidance on EUC initiatives and assists in EUC strategy development in the areas of desktop transformation, mobile computing, DaaS, VDI, and desktop virtualization.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com