Enterprise Strategy Group™ by TechTarget

WHITE PAPER

A Guide to Maximizing the Benefits of Identity Transformation

By Modernizing Identity, Devices, and Access Management with an Open, Cloud-Based Model, Small to Medium-sized Enterprises (SMEs) Can Reduce Costs, Improve Operational Efficiencies, and Strengthen Cybersecurity

By Jack Poller, Senior Analyst
Enterprise Strategy Group

March 2023

Contents

Executive Summary

By modernizing and transforming identity management with an open, cloud-based platform, business leaders and IT teams have a golden opportunity to bring significant benefits to their organizations, including:

- Leveraging modern technology innovations to drive efficiencies, lower costs, improve productivity, and reduce pressure on IT admins and security personnel.
- Facilitating major improvements in cybersecurity, with easier compliance, an accelerated path to Zero Trust, and a model for easier/faster deployment of future technology innovations.
- Embracing freedom of choice to use the most appropriate solutions for the current and ongoing needs of their businesses and workforces.

While these potential benefits are relevant to organizations of all sizes, they are particularly within reach of small and medium-sized enterprises (SMEs). SMEs typically have more flexibility to move faster and with greater agility because they have less invested in legacy solutions that are no longer efficient in today's era of cloud computing and extensive digital and workplace transformation.

What's more, the open, cloud-based technology platform to achieve this type of identity transformation is readily available, simple to deploy, and well proven across nearly 200,000 organizations and 2,000 MSPs around the globe. By embracing identity transformation, SMEs can consolidate identity management in one place and unify control of access, identity, and rights for all users at all locations, whether on-premises, in the cloud, mobile, or all of the above.

The goal of identity transformation is to enable IT admins to centralize management of all ways users must authenticate and verify themselves through integrated device management as well as identification tools such as passwords, biometrics, SSH keys, push-based multifactor authentication, and more for accessing various IT services. With a cloud platform, organizations can easily adopt new techniques and technologies as they are developed. The pathway to a single source of the truth in identity management is possible, and for many SMEs, it is the new reality.

In this white paper, we discuss the key factors that are driving the need for identity transformation, including the more challenging cybersecurity environment, the need to simplify IT management and control costs, and the increased complexities that are endemic to today's era of cloud computing, hybrid work, and ubiquitous digital transformation. We also discuss which features and functions to look for in a modern, open, cloud-based platform and provide practical guidance to SME business leaders and IT admins on best practices for deploying, managing, and maximizing a next-generation identity and access management (IAM) platform.

The Changing IT Landscape

There was a time when identity management was relatively simple and straightforward, at least for organizations that were entrenched in the Microsoft world and where employees worked exclusively on-premises in offices. Microsoft Active Directory was the on-premises hub that managed identity, access, and privileges. For environments that were on-premises and Windows-only, that was all you needed.

But, like many things in IT, the world is no longer that simple. Users, applications, devices, and data are all over the place. In many cases, particularly for SMEs, the cloud has either displaced or supplemented on-premises data centers as the main mechanism for delivering computing resources. Security threats are more sophisticated, and the growth of hybrid work creates challenges that legacy identity solutions can't address.

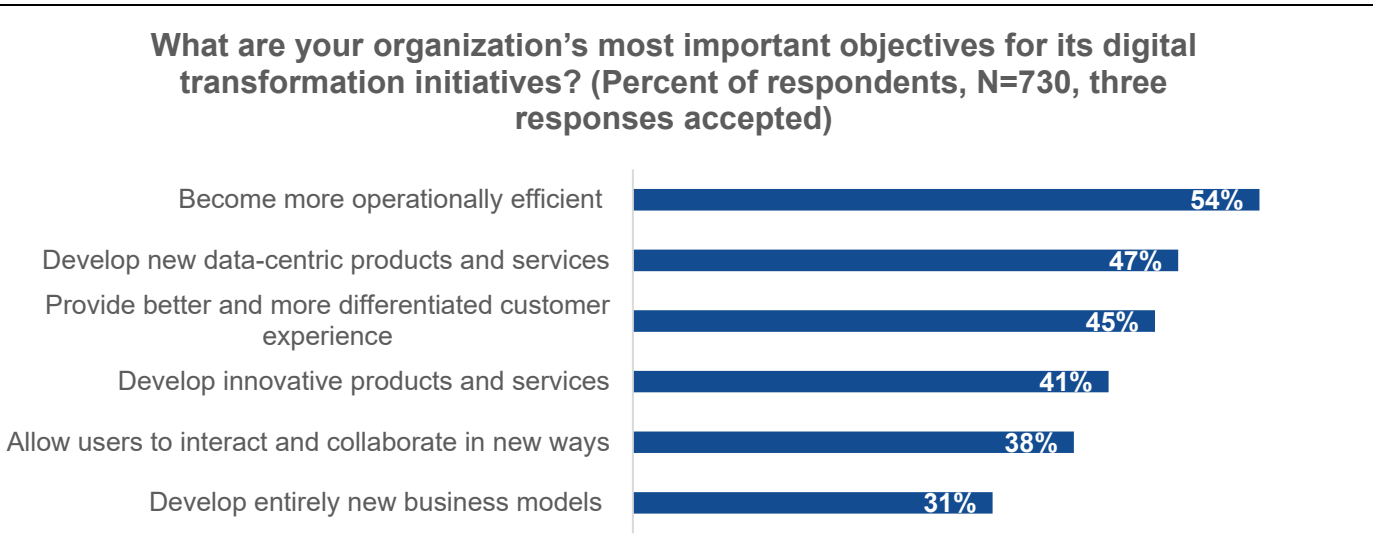
In this world, the perimeter is no longer defined by endpoints, networks, and firewalls. In fact, for many SMEs, identity is the new perimeter. And if it isn't the new perimeter now, it will likely be in the very near future. That's because identity transformation is inextricably linked to digital/cloud transformation and driven by several key factors, including:

- The continuing maturation of digital transformation and the need for operational efficiency and organizational agility in addressing the changing needs of both customers and employees.
- The diversity of devices and operating systems—laptops, tablets, mobile phones, and others that users use as gateways to access work-related resources— and the challenges of making sure these devices are secure in a work-anywhere-with-any-device reality.
- The ability to assign the right level of access to employees to do their jobs in a world where traditional network or group-based access policies are no longer sufficient.
- The need to adopt better, more responsive, more automated cybersecurity tools and approaches, including innovations such as Zero Trust.
- The need to modernize IT at a time when many organizations, especially SMEs, suffer from a chronic lack of cybersecurity and IT skills.
- The growing complexity of IT in the cloud era, including support for hybrid work to empower users anytime, anywhere, and on any device so they can leverage the apps that allow them to be productive, collaborative, and secure.

The challenges of modernizing IT, improving security, and supporting digital transformation in this much more complex environment are manifested in a number of ways, all of which put enormous pressure on business leaders, IT admins, and cybersecurity teams, as illustrated in research by TechTarget's Enterprise Strategy Group.

According to the 2023 Technologies Spending Intentions Survey, 77% of organizations have implemented or are in the process of implementing digital transformation initiatives. Becoming more operationally efficient, developing new data-centric products and services, providing a better and more differentiated customer experience, and developing innovative products and services are among the top factors driving digital transformation expansion (see Figure 1).[1]

Figure 1. Most Important Digital Transformation Initiatives

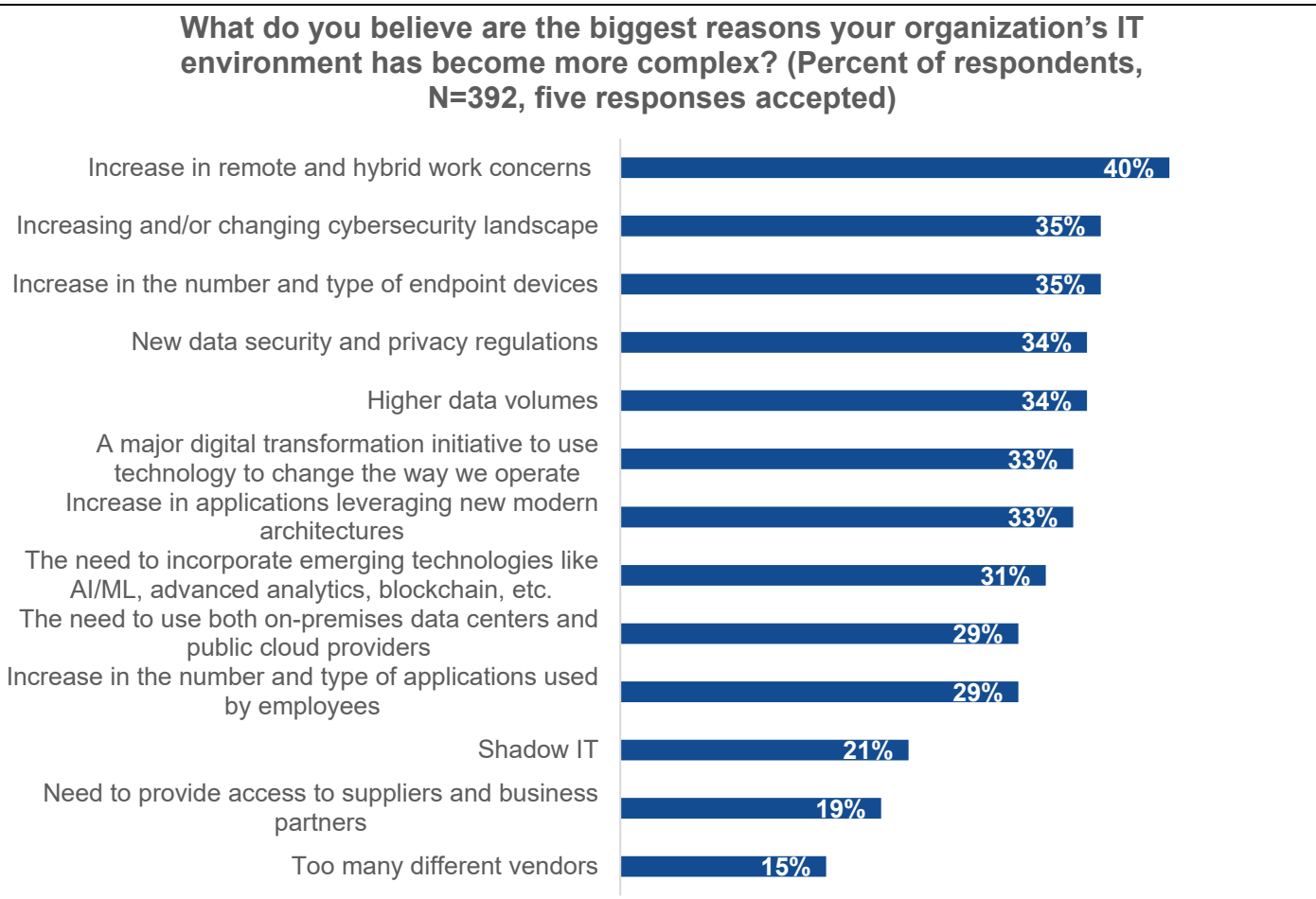


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[1] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

At the same time, organizations are dealing with an IT environment that is growing increasingly complex. Thirty-five percent of IT decision makers said their environments are more complex than they were two years ago. An additional 18% said their environments are significantly more complex. Key driving factors, as seen in Figure 2, include an increase in remote and hybrid work, the changing cybersecurity landscape, and an increase in the number and type of endpoint devices.[2]

Figure 2. Top Ten Most Important Digital Transformation Initiatives



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The 2023 Technology Spending Intentions research survey revealed additional factors that have contributed to the growing complexity of IT, including:[3]

- **The new reality of hybrid work:** Hybrid work is here to stay, but companies are struggling to manage infrastructure due to increased complexity, security concerns, and other issues. The increase in remote and hybrid work concerns is the number one factor in making IT more complex, cited by 40% of respondents.
- **Growing reliance on multi-cloud strategies:** 91% of organizations reported using at least two public cloud infrastructure service providers, and 42% reported using four or more.

[2] Ibid.
[3] Ibid.

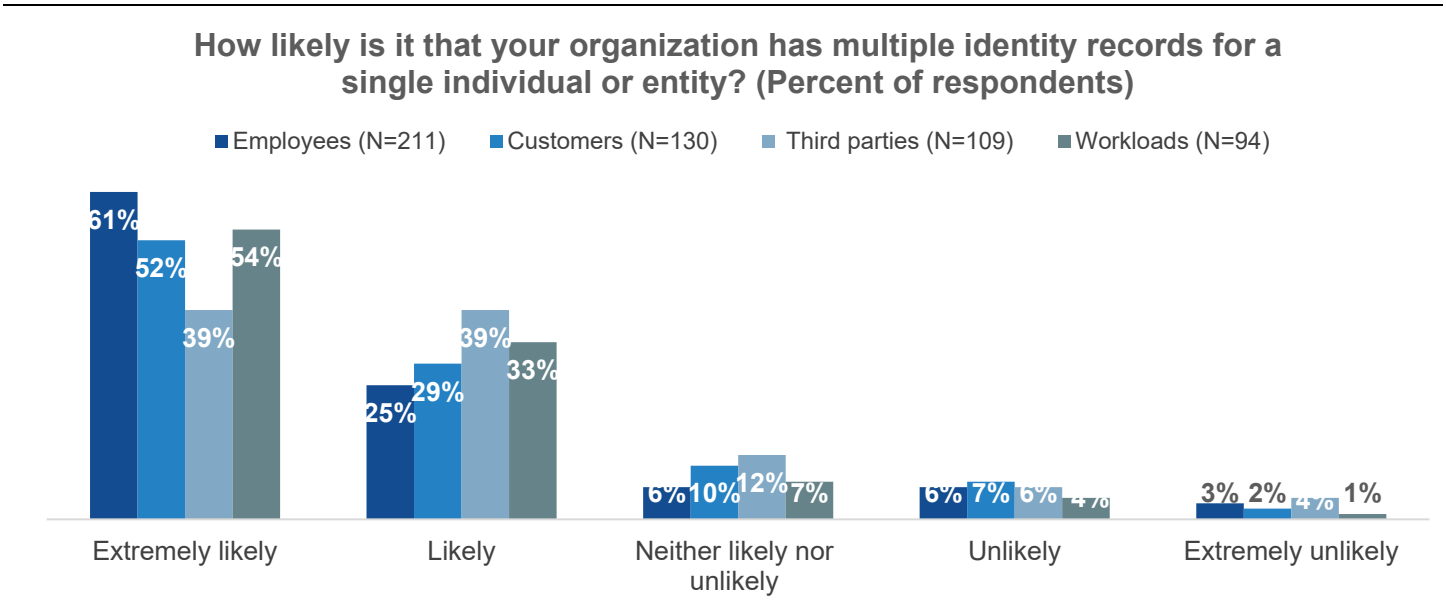
- **Unbridled growth of applications:** 53% of organizations said they use at least 500 applications, and many of these are software-as-a-service apps delivered in the cloud, making security more complex and IAM more essential.
- **Managing exponential growth in the volume and variety of devices**: Integrated device management, with full visibility into each device, is a critical aspect of identity transformation. More than a third of decision-makers (35%) cited the increase in the number and type of endpoint devices as a major factor contributing to IT complexity. In this world of hybrid and remote work, organizations need to securely support all users on all devices at all locations, which means erasing any boundaries that exist between identity and device management.
- **Challenges in hiring qualified personnel:** 45% of IT organizations said they have a problematic shortage of cybersecurity skills. Other key areas of skills shortages are IT architecture/planning (40%), IT orchestration and automation (38%), and cloud architecture/planning (37%). The skills shortage lengthens deployment time, hampers integrations, and puts the organization in a reactive mode, shifting resources from architecting for simplicity to providing basic functionality.

Why Identity Transformation

The challenges of this more diverse IT environment are exacerbated by a more complex IAM and device management environment. Most SMEs can no longer simply rely on Active Directory or Microsoft alone as their solution, and thus must bolt on additional tools that can be costly, difficult to manage, and poorly integrated. Approaches, such as single sign-on (SSO), reduce friction and deliver an improved user experience. But SSO alone is not sufficient in today's environment, where the volume and variety of applications—in the cloud, on-premises, and SaaS—lead to multiple identity siloes and multiple records for a single individual.

Finding a single source of truth without modernization and transformation is more than a challenge; it's a near impossibility. According to the Enterprise Strategy Group research, the overwhelming majority of organizations believe they have multiple identity records for a single individual or entity, as illustrated in Figure 3.[4]

Figure 3. Likelihood of Having Multiple Identity Records for a Single Individual or Entity

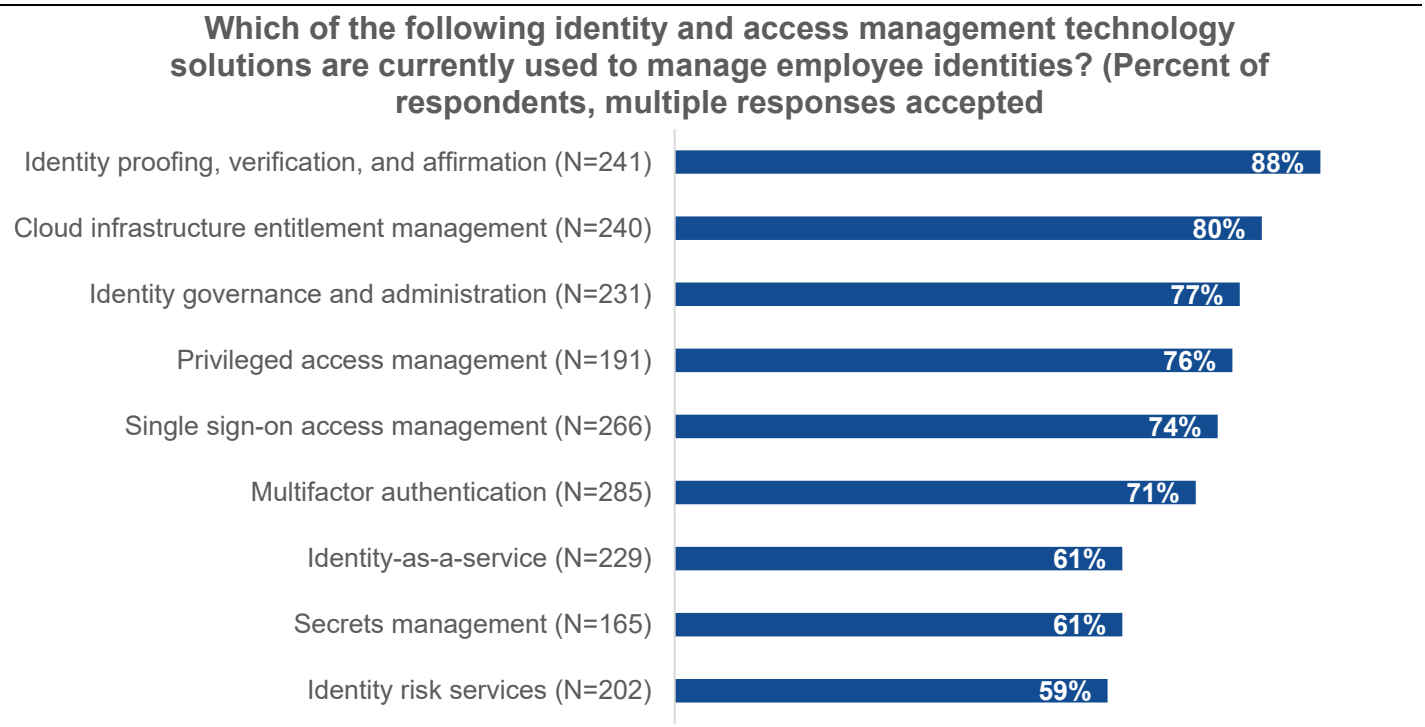


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[4] Source: Enterprise Strategy Group Research Report, *Securing the Identity Perimeter with Defense in Depth*, May 2022.

The research shows that organizations are typically using a multitude of approaches to IAM in response to the changes in the market, particularly in dealing with the growth of hybrid and remote workers and the challenges the hybrid environment brings to cybersecurity, as seen in Figure 4.[5]

Figure 4. IAM Solutions Used to Manage Employee Identities



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The path forward calls for a consolidated solution that eliminates siloes, centralizes IAM management, and supports privileged access management, identified as a top priority by more than 30% of decision makers. In addition, 28% of decision makers said they want to consolidate solutions, and 25% said they intend to migrate to a SaaS IAM solution.[6]

Bolting additional tools on top of Active Directory is not going to give businesses and IT admins the answers they need to address these challenges. That's why a new approach to identity management is imperative for SMEs. But what is the best model for this new approach?

The Benefits of an Open, Cloud-based Platform

For too long, IAM has taken a background role in IT and security. At times, IAM has been treated more as a problem than a solution. Device management is another important issue. In many cases, device management solutions have been deployed separately from IAM. But with identity transformation, IT and security professionals at SMEs have a chance to use IAM integrated with device management as a foundational element of their IT strategy and leverage it as a pathway to more efficient operations, better security, lower costs, and faster access to innovation.

[5] Ibid.
[6] Ibid.

Achieving these benefits is simpler than most business and IT leaders realize. That's because of the availability of solutions that leverage open technologies in a cloud-based platform. SMEs can still use Active Directory, but they can significantly expand their deployment options and centralize all identity management in a single, secure tool that provides full visibility, policy management, logging, consolidation, and friction-free access to whatever technologies are right for their organizations and users. Even organizations that are fully tied into Microsoft can benefit from an open platform model because it gives them flexibility to support all types of devices and operating systems, while taking advantage of multiple clouds, not just Microsoft Azure.

Why choose an open, cloud-based platform with consolidated management? Here are some of the key characteristics:

- **Open platform**
  - **Enable freedom of choice**: SMEs can support whatever devices, applications, clouds, and other services/technologies that make their people, ecosystems, and workplaces more productive. They can use devices with any OS and support bring-your-own device to give remote and hybrid users more flexibility. They can use any cloud platform with no limitations, so within a single environment, there can be a mix of Microsoft Azure, AWS, Google Cloud, and others, along with SaaS applications, such as Salesforce, Box, Workday, Marketo, etc.
  - **Reduce costs and risks**: The flexibility of an open platform enables SMEs to reduce costs through improved operational efficiencies, consolidated management, and the ability to use best-in class solutions that fit into the organization's business goals. With an open platform, SMEs can use the most appropriate technologies while avoiding the risks of being locked into a single-vendor model.
  - **Accelerate access to innovation**: With an open platform, it's not just about technology that is available today; it's also about what may be developed down the road. SMEs are not limited to whatever Microsoft does; they can leverage any new technology that will make their users more productive and their IT and security teams more efficient.
- **Cloud-based**
  - **Empower digital transformation**: As SMEs began embracing the cloud to increase efficiencies and agility, IAM was one of the technologies that didn't make the transition right away. Instead of shifting to the cloud, most organizations took a patchwork approach to IAM and built on top of what they had. But most SMEs have been through that phase of transformation and are now cloud-native. So, it is not only logical to modernize identity in the cloud, it is necessary to empower digital transformation, reduce complexity, and support the hybrid workplace.
  - **Improve efficiencies**: With a centralized, consolidated, cloud-based approach to identity, SMEs can make users and IT teams a lot more productive. IT doesn't have to manage a patchwork of systems and can centralize identity in one place. This makes it much simpler to layer on new features, policies, and security protections. In addition to reducing costs, a cloud model reduces pressure and improves productivity for IT admins and security personnel, which is particularly important for SMEs in today's competitive job market.
  - **Strengthen cybersecurity**: Identity is the foundation for a Zero Trust framework. Before an organization applies any concept of trust—whether it's Zero Trust or implicit trust—it needs to understand who the actors who need access are and which assets they need to access. Everything else is secondary. This is why CISA's Zero Trust Maturity Model places identity as the first pillar of Zero Trust. Additionally, a Zero Trust strategy applies the principle of least privilege access, where users are able to access only the data and systems to do their jobs—nothing more, nothing less.
- **Consolidated management/enhanced user experience**
  - **Enable secure frictionless access**: SMEs can centralize management and control for IT with a unified, centralized database of identities combined with management of devices to unify management of access to resources. This means IT teams can centrally manage all apps, including SaaS, cloud apps, and on-

premises apps. In addition, they can leverage all forms of identity and device management—not only those that are available now, but also innovations that will become available in the future.

- **Maximize automation:** Automation is essential to improving IT productivity, strengthening security, and reducing costs. When considering which platform to use for identity transformation, decision makers should be hypervigilant in making sure that their solution maximizes automation to reduce costs and complexity, while improving IT productivity, security, and an enhanced user experience.
- **A single source of truth (finally!)**: In the cloud era, accessing a single source of the truth for IAM has been elusive. There have simply been too many identity systems. But that no longer needs to be the case. With the right platform, SMEs can consolidate into a single directory. Not only that, but if the directory is open, there is no longer a reliance on strictly AD or Azure AD.

What to Look for in a Next-generation IAM Solution

We've already laid out the basic framework that SME business leaders and IT teams should be looking for in a next-generation IAM solution. This includes:

- An **open platform** for freedom of choice.
- **Cloud-based** to drive digital transformation and globalization.
- **Centralized management** to reduce pressure on IT, lower costs, and deliver a modern user experience.
- Maximum use of **automation**.
- Identity consolidation to **strengthen cybersecurity** and build the right foundation for **Zero Trust**.
- Visibility and **management of user devices** used as gateways to access IT resources.
- **Secure frictionless access** to get to a **single source of truth**.

That's the basic foundation for a next-generation cloud IAM platform. As IT admins dig deeper into the specific requirements for a successful deployment, they will find additional important criteria. For SMEs, additional requirements will typically include capabilities such as:

- Single sign-on to all IT assets.
- Environment-wide multifactor authentication and/or passwordless authentication.
- Agility to manage identities and access control on any device.
- Integration with HR and other sources.
- Simplified deployment, reduced TCO, and investment protection for existing resources.
- Ability to meet rising compliance requirements, including patching and device posture.
- Ability to manage supply chain risks and unify IT with IAM as a pathway to reduced complexity and improved cybersecurity.
- Supports device management, policy execution, and conditional access policies.

The JumpCloud Platform

When it comes to meeting all of the key criteria of a next-generation platform to empower identity transformation, JumpCloud is both a leader and pioneer in setting a new standard with an integrated, consolidated, open cloud platform that delivers maximum benefits to SMEs.

For the business side, JumpCloud delivers greater agility, lower costs, better security, and a simpler path to future innovations. There is no vendor lock-in, so each customer has the freedom to use the best available technology to

meet the needs of the business, supply chain, and workforce. For IT admins and security teams, JumpCloud is simple to deploy and manage, offering high levels of automation, centralized control, and the opportunity to leverage IAM management to improve overall IT operations and efficiencies.

Following are some of the key factors that set JumpCloud apart from the competition when it comes to a cloud-based, next-generation IAM platform:

- **Single sign-on to everything** as part of the core functionality. SAML, OIDC, and RESTful integrations are included in JumpCloud's platform. RADIUS and LDAP are integrated, and identities and assets are protected because the JumpCloud platform also manages the device.
- **Advanced lifecycle management** that integrates with HR systems and other sources, automates group memberships, and schedules user onboarding and offboarding events. As an open directory platform, JumpCloud enables attributes to be imported from other sources of truth, including AD, Azure AD, Google, Okta, and more.
- **Integrated device management** that extends user identity to the Windows, Mac, and Linux endpoints or the iOS or Android mobile devices used to access applications, networks, or other IT resources. JumpCloud's integrated identity, access, and device management adds another layer of IAM security based on device posture and risk, and without the time, effort, and complexity of having to integrate multiple disparate solutions.
- **Compliance and security**, facilitating a Zero Trust approach through environment-wide multifactor authentication, optional conditional access rules, and device trust. For IT admins and security teams, best security practices are easy to achieve, and the cloud-based infrastructure reduces the attack surface area.
- **Total cost of ownership**. Because JumpCloud is cloud-based, most infrastructure costs are eliminated. Advanced lifecycle management and IAM are integrated, along with key IT management apps. As an open directory, there is no penalty for bringing other directories. Key services, such as RADIUS and LDAP, are cloud-based and immediately available. Licensing is workflow-based as opposed to feature-based.

In addition, the JumpCloud platform has a proven track record of success across nearly 200,000 organizations and 2,000 MSPs around the globe.

Conclusion

The world has changed dramatically, and there is no going back to the way things were in the past. Digital transformation, cloud computing, hybrid work, customer experience, and other important trends are making IT management and security more complex and putting pressure on SMEs to modernize their approaches and technology solutions.

In this environment, identity, access, and device management has become more important than ever in enabling SMEs to reduce costs, improve operational efficiencies, strengthen cybersecurity, support workplace and digital transformation, and reduce the pressure on IT admins and security teams. By embracing identity transformation and modernization, SMEs have an opportunity to position their organizations for the future, while also addressing the complexity, security, costs, and efficiency challenges of digital transformation.

The key to identity transformation is embracing an open, cloud-based model that consolidates, unifies, and centralizes IAM, device management, and resources to improve security in many ways, including as the foundation for a Zero Trust framework. JumpCloud is a pioneer in both articulating the advantages of identity transformation and in delivering an open, integrated cloud-based solution that provides business leaders and IT admins in SMEs with a clear, simple, secure, and future-proofed path to their next-generation IAM and device management platform.

About Enterprise Strategy Group
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

contact@esg-global.com
www.esg-global.com