Security
Thought Leadership White Paper

September 2015

Take back control of access management

Discover how an integrated approach to access management can reduce complexity and thwart security breaches

Watch the KuppingerCole webinar on "One IT, One Identity"

Introduction

Many organizations face access management chaos. They have multiple sets of users—employees, contractors, partners and consumers—trying to access critical IT resources through multiple devices, including smartphones, tablets and notebooks. Meanwhile, with the adoption of public and private clouds, these resources are often no longer residing within traditional network boundaries. So IT teams have deployed multiple tools to help manage all the possible access points in the modern, heterogeneous environment.

However, security leaders are increasingly concerned about the threat of cybercriminals turning this access management chaos into their own malicious gain. In a recent IBM survey, nearly 60 percent of security leaders said that the sophistication of attackers was outstripping the sophistication of their organization's defenses. More than 80 percent said that they have seen the external threat increase in the past three years, and now view it as their top challenge.[1]

As businesses grow and adopt new technologies, the need for centralized access management is also growing greater than ever. Disparate tools result in a loss of productivity, a lack of visibility into end-user behavior and increased complexity in facilitating compliance. Without exception, fragmented access management tools are expensive to maintain and challenging to secure.

This white paper examines the need for today's organizations to combat the expanding sophistication of malicious attacks in increasingly heterogeneous environments. It looks at ways to both reduce management complexity and help improve security through a single, integrated access management solution.

Managing access in the cloud era

Despite their many benefits, hybrid cloud environments come with many technical, business and management challenges. Private cloud workloads must access and interact with public cloud workloads, so hybrid clouds require application programming interface (API) compatibility and solid network connectivity. An integrated access management solution that enables single sign-on and identity federation to applications running inside and outside of the enterprise can help address the challenges of hybrid clouds.

An all-in-one access management solution empowers security teams to:

- Quickly establish single sign-on connections to popular software-as-a-service (SaaS) applications
- More easily create custom application connectors with do-it-yourself federations based on the Security Assertion Markup Language (SAML) 2.0 standard
- Deliver single sign-on access to enterprise applications and support user identity propagation in hybrid cloud application interactions
- Simplify deployment and management with appliance-based packaging suitable for small-to-midsized businesses and scalable for large enterprises

Learn more about managing access to the cloud—view the IBM infographic *now.*

Removing barriers to mobile productivity

Bring-your-own-device (BYOD) programs are enabling organizations of all sizes to go mobile without requiring significant hardware or service investments. However, security remains a major concern for mobile devices and applications. In fact, mobile malware has been found to infect more than 11.6 million mobile devices at any given time, and more than 90 percent of the top mobile applications have already been hacked.[2]

As BYOD becomes the norm, access management solutions must have a capacity to integrate with other mobile security measures, stopping malware infections as well as preventing high-risk devices from accessing secure systems. At the same time, users expect seamless access to enterprise applications regardless of device. A richly integrated access management solution can:

- Allow users to easily access enterprise resources with minimal authentication friction
- Utilize existing access management infrastructure to prevent the need for application changes while enabling access from mobile devices
- Enhance productivity and user experience with device-level single sign-on to enterprise resources

Learn more in the IBM Mobile Security webinar.

Securing resources with risk-aware access

Using intelligent security technologies, organizations can now protect user access based on dynamic risk assessments and the confidence level of transactions. The latest tools go beyond authorizing access based on user names and passwords—they also look at IP addresses, geolocation details, device fingerprints and past user behavior. The tools can then transparently register mobile devices and enforce user-centric authentication polices across mobile, cloud and web applications. The robust security can also be supported within APIs.

Integrated access management solutions:

- Dynamically assess risk associated with mobile application access using contextual information about the device, user, environment, resource, malware, device management status and past user behavior
- Provide strong and multi-factor authentication capabilities to protect critical sensitive assets depending on the risk context
- Audit or block fraudulent and high-risk transactions from infected devices without modifying back-end applications

Explore the advantages of risk-aware access management—watch the IBM video *now.*

Providing rich security for large customer bases

Companies that have large customer bases need an access management solution that can scale to millions of users. By providing user-centric identity and access management capabilities for consumer-facing applications, businesses can enable customers to sign in to external applications using common social identity providers. This ability to manage access within and outside the enterprise from one access management solution provides truly integrated access management.

The right all-in-one access management solution should provide:

- A massively scalable directory and multi-tenant access management capable of supporting hundreds of millions of end users
- Self-service tools for end-user registration, password and profile management, and social identity logins
- Federated access to multiple consumer-facing applications to help improve the end-user experience
- Enhanced access controls and unified silos of identity to deliver comprehensive views of every user

To find out more about federated access for consumer-facing applications, watch the IBM webinar *now.*

Conclusion

Cybercriminals are increasingly sophisticated, devising new ways to turn an organization's weakest security links into new avenues for attack. Fragmented access management tools and inconsistent access policies have left organizations more vulnerable than ever. For security teams to successfully thwart these attacks, they will need an integrated approach to access management.

With a single platform that enables businesses to manage access in the hybrid cloud, create seamless access for enterprise mobile users, secure disparate applications with risk-based access policies, and scale access management to large customer bases, integrated access management can provide significant resource efficiencies that enhance both security and competitiveness for the future in a sustainable way.

For more information

To learn about IBM solutions for all-in-one access management, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/identity-access-management

[1] Marc van Zadelhoff, Kristin Lovejoy and David Jarvis, "Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment," *IBM Center for Applied Insights*, December 2014. http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home

[2] Satyakam Jyotiprakash, "Secure, Convenient Mobile Access: The Impossible Dream?" *IBM Security Intelligence*, June 19, 2014. http://securityintelligence.com/secure-convenient-mobile-access-the-impossible-dream/#.VVUDVZN3DPs

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
September 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

♻ Please Recycle