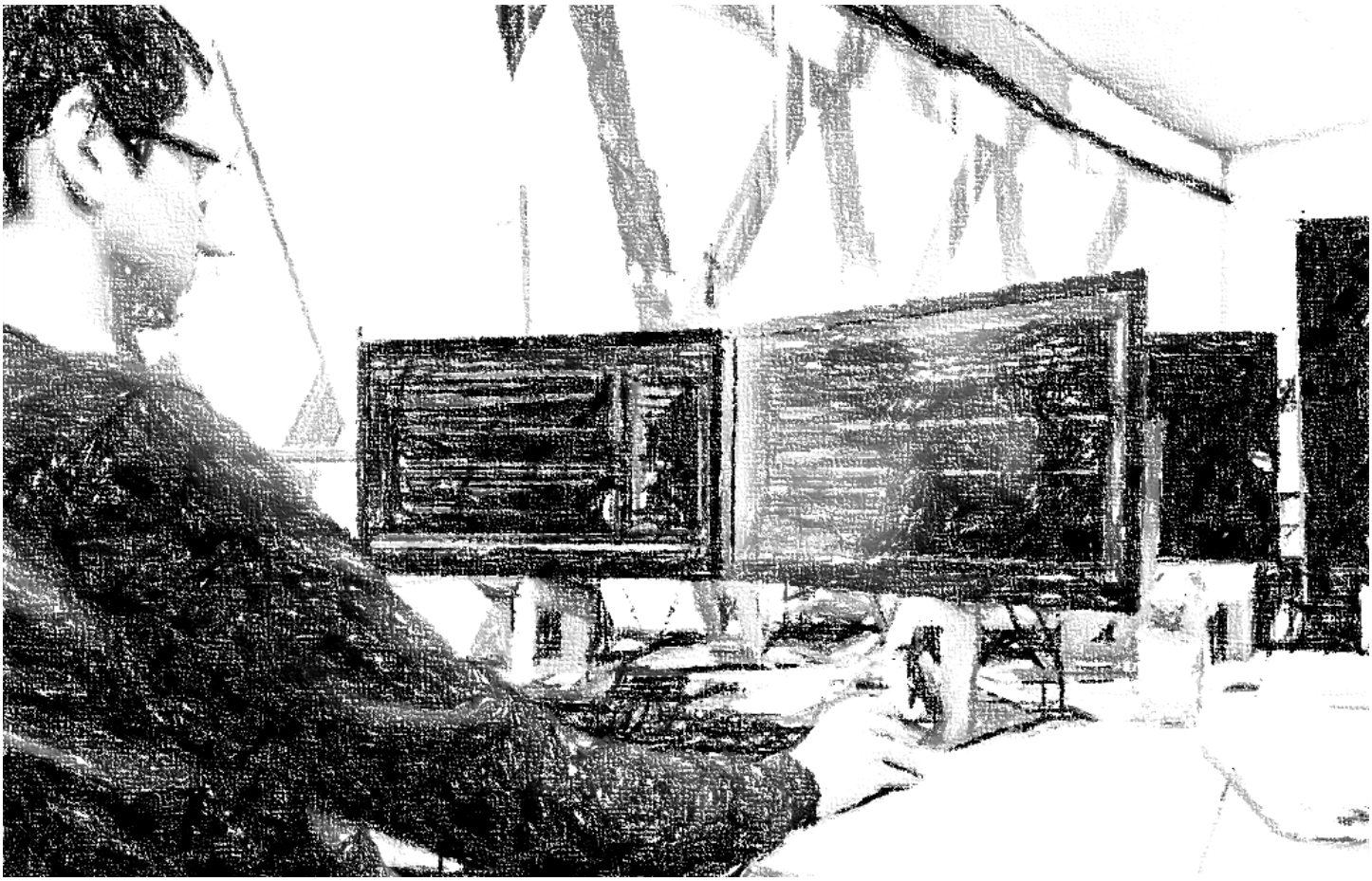
Enforcing Zero Standing Access

A different approach to Privileged Access Management



Abhishek Kumar
Principal Program Manager at Microsoft

Caroline Shin
Sr. Product Marketing Manager at Microsoft

Last updated September 24, 2018

Executive Summary

- Organizations are twice as likely to get breached through compromised credentials than any other threat vector.
- Perpetual or standing privileged access to an application is all that is needed to execute commands to expose data and inflict damage.
- Managing privileged access is challenging for many organizations as their business evolves.
- Zero Standing Access changes the paradigm to how traditional PAM solutions approach privileged access.
- Microsoft applies the principle of Zero Standing Access for service provider access with Customer Lockbox.
- Privileged access management in Office 365 enables organizations to enforce Zero Standing Access for any user (admin) within the customers' tenant.

Introduction

Organizations are twice as likely to get breached through compromised credentials than any other threat vector. Having perpetual or standing privileged access to an application is all that is needed to execute commands to expose data and inflict damage, such as create fake accounts, exfiltrate sensitive data, cause damage to infrastructure, and delete or hold data for ransom – all of which can impact a company's reputation and bottom line.

Oftentimes, these risks are amplified due to users having more privileges than required or due to general negligence in monitoring and managing privileged accounts. For instance, a user who needs to perform a single privileged task – such as Reset Password or putting Legal Holds – should not get privileges of a 'super' or global admin, which have significantly broader access than is required. Or an admin that left their role but continues to have broad access despite no longer needing them.

Therefore, it's not surprising that managing accounts with privileged access, and the extent of such access, is one of the top priorities for any organization. For example, Gartner lists Privileged Account Management as the #1 in their list of top 10 security projects for an organization.

However, managing privileged accounts is challenging for many organizations. As businesses evolve (mergers, acquisitions, divestitures, growth in new markets), their data, and the people, processes and systems also evolve, therefore, making it more difficult to manage privileged access at scale.

One way to address this is by adopting the principle of Zero Standing Access.

At Microsoft, when it comes to securing its data center, we mitigate risks associated with accounts with privileged access – from malicious actors both inside and outside an organization – through the principle of Zero Standing Access. This enables Microsoft to operate without any privileges available to any user by default. Combined with the principles of Just-In-Time and Just-Enough-Access, it provides a robust framework for organizations to be secure and compliant by default. More importantly, Microsoft is extending the same level of security rigor to customers to manage access privileges more granularly for any user.

This whitepaper looks to share the benefits of enforcing zero standing access, and how this concept can be used by customers to gain more control over privileged access to their sensitive data. Additionally, since administrators tend to have the greatest privileges with broad access to applications and the system, this document will focus primarily on administrators.

Traditional PAM solutions

Today, if customers are managing privileged access they may have a PAM solution in place. Gartner defines PAM as "*a set of technologies to provide secured privileged access to critical assets and meet compliance requirements by securing, managing and monitoring privileged accounts and access*."[1]

Traditional PAM solutions are built around managing privileged accounts with access to sensitive tasks, resources and data, and they enable sharing of such accounts among administrators who need to perform privileged tasks. These systems allow checking out accounts just-in-time and provide automated password and session management, with secure access control, auditing and alerting.

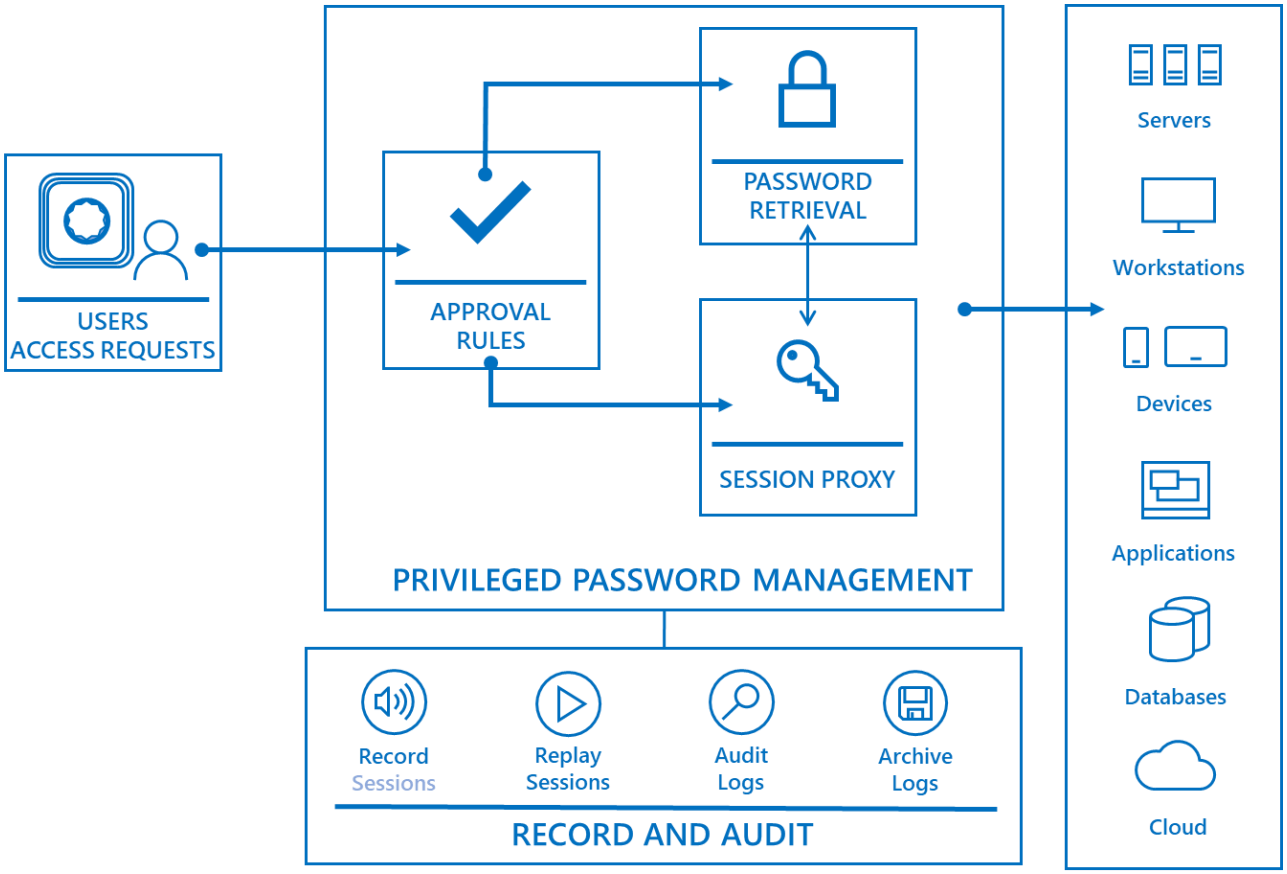


Figure 1: Traditional PAM systems with Account, Credential and Session management[2]

However, the approach of credential management that traditional PAM systems take, has a set of limitations.

Standing Privileged Access – Managed privileged accounts have perpetual rights to perform highly sensitive tasks. This creates a vulnerability wherein if such an account is ever compromised or misused, it will grant significant privileges to malicious actors.

Lack of clear Auditing – Using shared account for privileged access makes it harder to track and audit subsequent access. Establishing *who-did-what* depends on collecting and cross-referencing multiple log streams. This also prevents makes it harder to implement real-time alerting for misuse of privileges.

Password and session management Overhead – The fact that these managed accounts are shared across an organization's administrators requires that significant controls are built to manage the password and sessions.

This is important to prevent credential leaks and ensure secure usage, however it results in significant cost and affects admin experience.

Lack of granular access controls – These managed accounts typically use Role Based Access Control that grants a broad range of privilege. Reliance on RBAC limits the amount of control PAM systems can assert at a very granular level and create a system where privileges are granted in terms of all or nothing.

A New Approach to Privileged Access Management: Zero Standing Access

A new approach to Privileged Access Management systems, is to work with the principle of Zero Standing Privileged Access. With zero standing privileged access, there are no operational administrative accounts in an organization that will have privileged access by default. This voids the need for a system that manages credentials, and sessions – thereby reducing overheads, and simplifying administrator experience.

Furthermore, such a system should allow administrators to use their own accounts and get privileged access just in time –eliminating the need for managing shared accounts, and further simplifying admin experience.

Such a system will most noticeably have these features:

Zero standing access – No operational account has privileged access by default. All access is requested and granted only when needed, with time-bound access that expires after the approved duration has passed. This is extremely significant to mitigate the risks of compromises that result in malicious actors gaining unfretted privileged access within an organization.

Clear Auditing and Accountability – Such systems would replace shared account management with elevation management, wherein administrators are able to elevate and de-elevate to gain privileged access. Such a system allows for clear auditing of *who-did-what* and allows creating real-time monitoring on detecting and preventing misuse.

Resource level Access enforcement – Using individual accounts allows applications and resources to evaluate the access restrictions on specific users, which ensures that only accounts with right eligibilities are allowed, and any compromises are isolated.

Just Enough Access – Going beyond role-based access control, such systems should allow managing access at a more granular level, where organizations can have configurable controls at multiple levels, to manage access to privileged tasks and resources.

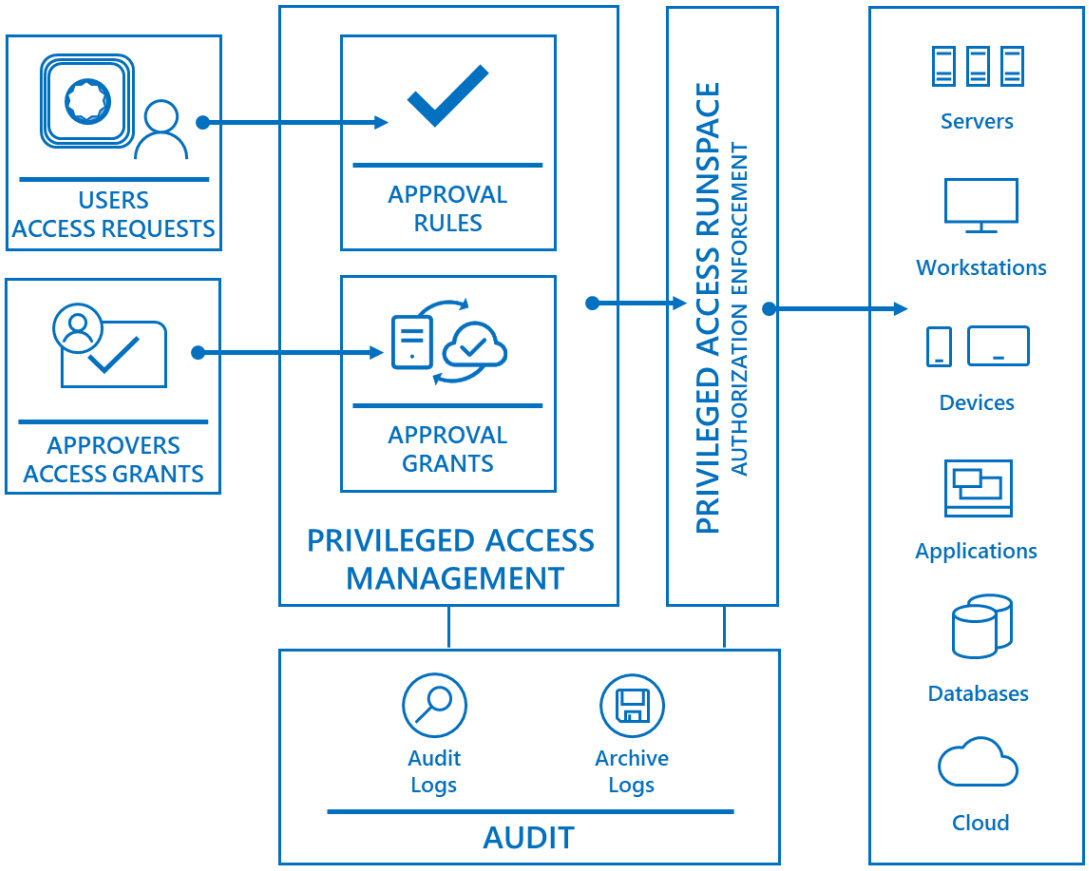


Figure 2: PAM systems with Zero Standing Access, JIT, JEA & Approvals

Microsoft's approach to enforcing Zero Standing Access to your data

Microsoft runs their organization and datacenters on the principle of Zero Standing Admin Access – that means users do not have permissions by default to perform privileged tasks, or access sensitive data on their own. When required, all access requests go through a privileged access workflow, allowing users just-in-time and just-enough access for the task they need to perform. All such requests require approvals and have significant oversight. The said access events are logged and are available for audit.

Beyond datacenter management, Microsoft applies even stricter controls on who can access customer content stored in our datacenters during service operations. One additional control over access to customer content – Customer Lockbox – requires the customer, such as the tenant admin or a custom role like the compliance manager, to approve the request before access is granted to Microsoft engineers. The transparency, control and security rigor provided through this Customer Lockbox workflow is above and beyond what other major SaaS vendors offer today.

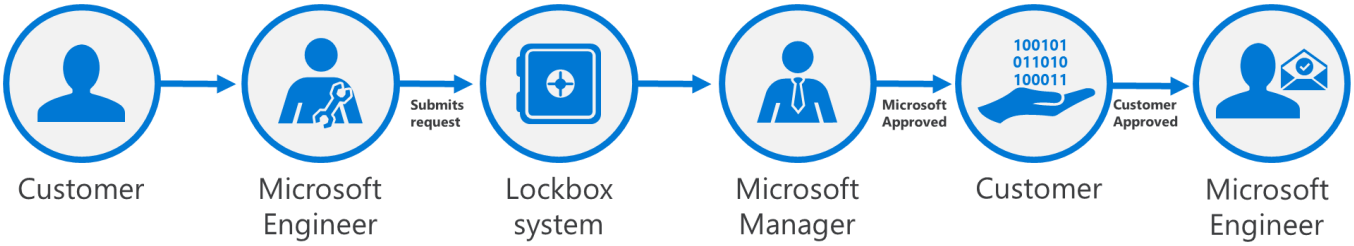


Figure 3: Access request flow for Customer Lockbox – Customer as the final approver.

Together, these controls enable Microsoft engineers and customers, to enforce Zero Standing Access by default for service provider access, which is a significant leap in keeping our datacenters and our customers' data secure and compliant.

Enforcing Zero Standing Access to your users (admins)

Taking all the learnings from how Microsoft manages its own datacenter, Office 365 has built a similar Privileged Access Management system to help customers manage privileged admin access to their users who typically are the tenant admins. This system is built on the principles of Zero Standing Access and requires users to request just-in-time and just-enough access to perform their tasks at hand.

With privileged access management in Office 365, access requests must be approved by an authorized set of approvers. Requests for access can be automatically or manually approved. Either way, all the activity is logged and auditable, so that both privileged access requests and approvals can be reviewed and seamlessly provided for internal reviews and auditor requests.

Privileged access management in Office 365 goes beyond traditional access control capabilities by enabling access governance more granularly for specific tasks.

For example, privileged access management in Office 365 enables customers to:

- **Enforce Zero Standing Access**
  Privileged Access Management in Office 365 enables organizations to enforce users to elevate their own account with just-in-time with just-enough-access. This removes the dependency on having a set of privileged accounts with standing access.
- **Manage Compliance and Access Governance**
  A good access governance strategy requires not just policy implementation but reviewing and monitoring privileged access to remediate and implement additional policies.

  With Privileged access management in Office 365, all access within an organization is governed. All instances generate logs and security events, that are extremely useful to monitor and build alerting on. This allows an organization to always have a finger on the pulse.

  Event logs – with information about requests, duration, approvals, and actions performed – are audit ready, and can be aggregated and presented as evidence to meet growing compliance requirements.
- **Control Access in One Management Plane**
  Privileged access management in Office 365 also brings together several capabilities across Microsoft 365 to manage access governance across different scopes – including service provider access,
    - Customer Lockbox in Office 365
    - Privileged Access Management in Office 365

These are just a few investments that enable organizations to protect their sensitive data through the principle of zero standing access that can also be managed in one management plane.

Get Started!

Whether you are new to PAM or an expert, privileged access management in Office 365 is flexible so that you can start by creating policies that automatically approves requests, then review the requests to enforce manual approval for certain tasks.

Review the resources below to help you get started!

Privileged access management in Office 365

- Privileged access management in Office 365 - 2 min Video
- Blog: Announcing GA of privileged access management in Office 365
- Technical Documentation

Customer Lockbox in Office 365

- Customer Lockbox 2 Min Video
- Customer Story: Exelon selects Customer Lockbox for Office 365 to power up data security and privacy
- Office 365 - Customer Lockbox SOC 1 SSAE 16 Type I Report
- Customer Lockbox Webinar: Own your data with next generation access control technology in Office 365

[1] What is privileged access management (PAM) software? https://www.gartner.com/reviews/market/privileged-access-management-solutions

[2] Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations

Terms & Conditions

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, this document should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This is for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue or problem. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.