Securing privileged access

learn.microsoft.com/en-us/security/privileged-access-workstations/overview

- Article
- 06/20/2024

In this article

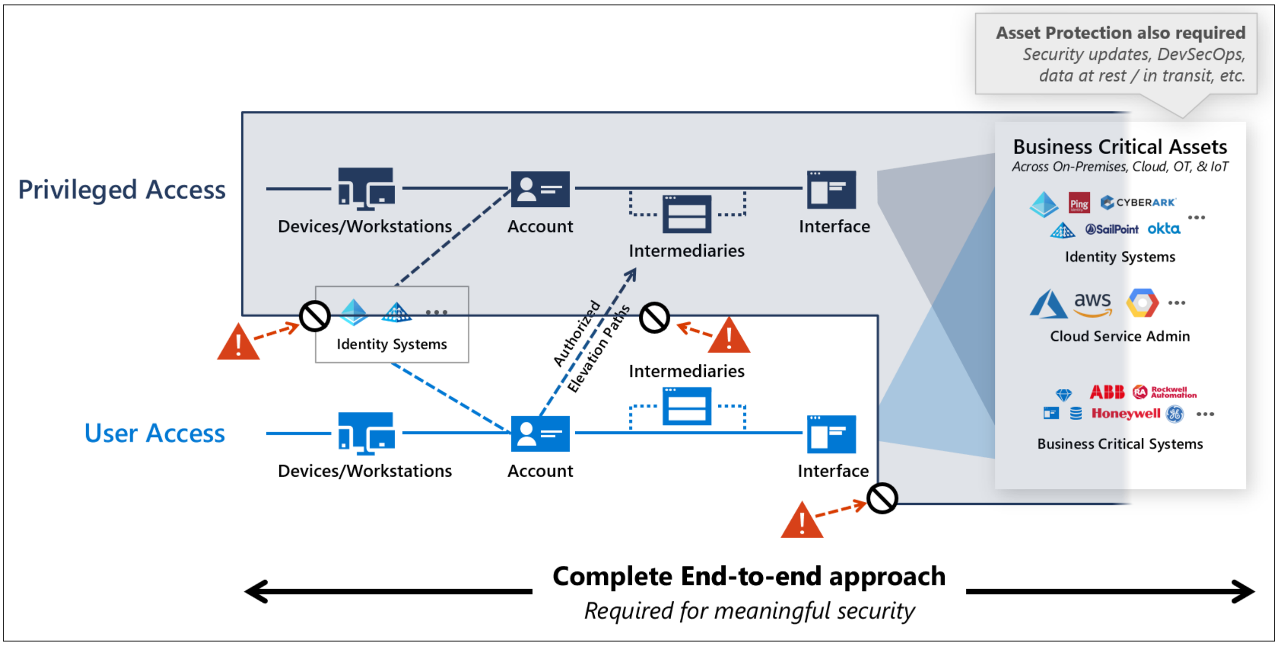
1. Get started and measure progress
2. Industry references
3. Next steps

Organizations should make securing privileged access the top security priority because of the significant potential business impact, and high likelihood, of attackers compromising this level of access.

Privileged access includes IT administrators with control of large portions of the enterprise estate and other users with access to business-critical assets.

Attackers frequently exploit weaknesses in privileged access security during human-operated ransomware attacks and targeted data theft. Privileged access accounts and workstations are so attractive to attackers because these targets allow them to rapidly gain broad access to the business assets in the enterprise, often resulting in rapid and significant business impact.

The following diagram summarizes the recommended privileged access strategy to create an isolated virtual zone that these sensitive accounts can operate in with low risk.



Asset Protection also required
Security updates, DevSecOps, data at rest / in transit, etc.

Complete End-to-end approach
Required for meaningful security

Securing privileged access effectively seals off unauthorized pathways completely and leaves a select few authorized access pathways that are protected and closely monitored. This diagram is discussed in more detail in the article, Privileged Access Strategy.

Building this strategy requires a holistic approach combining multiple technologies to protect and monitor those authorized escalation paths using Zero Trust principles including explicit validation, least privilege, and assume breach. This strategy requires multiple complementary initiatives that establish a holistic technology approach, clear processes, and rigorous operational execution to build and sustain assurances over time.

Get started and measure progress

Image	Description	Image	Description
	Rapid Modernization Plan (RaMP) - Plan and implement the most impactful quick wins		Best practices Videos and Slides

Industry references

Securing privileged access is also addressed by these industry standards and best practices.

UK National Cyber Security Center (NCSC)	**Australian Cyber Security Center (ACSC)**	**MITRE ATT&CK**

Next steps

Strategy, design, and implementation resources to help you rapidly secure privileged access for your environment.

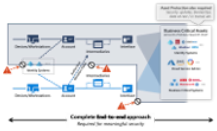
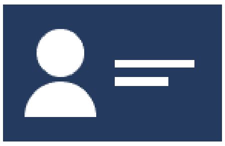
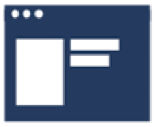
Image	Article	Description
	Strategy	Overview of privileged access strategy

Image	Article	Description
Defender's cost $$$ $$ $ Attacker's cost $$$ $$ $	Success criteria	Strategic success criteria
	Security levels	Overview of security levels for accounts, devices, intermediaries, and interfaces
	Accounts	Guidance on security levels and controls for accounts
	Intermediaries	Guidance on security levels and controls for intermediaries
	Interfaces	Guidance on security levels and controls for interfaces
	Devices	Guidance on security levels and controls for devices and workstations
	Enterprise access model	Overview of Enterprise Access Model (successor to legacy tier model)
	ESAE Retirement	Information on retirement of legacy administrative forest