

# Privileged Access Management

in the context of Zero Trust



# Reducing risk exposure by including privileged access management in the Zero Trust toolbox

## Executive summary

The Zero Trust security model is becoming the mantra for CISOs in these times of rampant exploits, breaches, and ransomware attacks. Today's information asset sprawl, along with the advent of the cloud-based services, poses a rich attack surface for cybercriminals. Protecting privileged access to these assets becomes a very important part of a Zero Trust security strategy.

Author

**Sesh Ramasharma**

Global Head, Identity Security  
Digital Foundation Consulting, HCLTech

## Never trust, always verify

With the current popularity of hybrid cloud adoption, information assets often reside outside of organizational network perimeters, so reliance on standard perimeter security is no longer sufficient. And with the advent of significant breaches and ransomware attacks,

Zero Trust network architecture (ZTNA) has gained more visibility and attention as a serious cybersecurity strategy.

Zero Trust security frameworks create localized micro-perimeter defenses around each asset in an organization's extended

network. Correctly designed, the frameworks protect assets regardless of where they reside—on premise, IaaS, PaaS, SaaS or any combination thereof.

Simply put, the key tenet of Zero Trust is

**"Never trust, always verify!"**

# Vulnerability, thy name is Privileged Access

---

For a long time now, many organizations, fearful of reducing productivity, have granted administrative access to corporate assets—disregarding the principle of least privilege. Users and programs should have only the privileges necessary to complete their tasks. In other words, many users with administrative credentials have unfettered access to the assets' underlying services and data. Granting more access than necessary has put organizations in a very risky position.

In the hierarchy of access control, privileged access designates special access beyond that of standard users, and presents the highest risk exposure. A signature of many recent breaches has been purloined privileged credentials that are misused to gain access to sensitive corporate data or even shut systems down. In fact, analysts estimate that 80% of security breaches involve

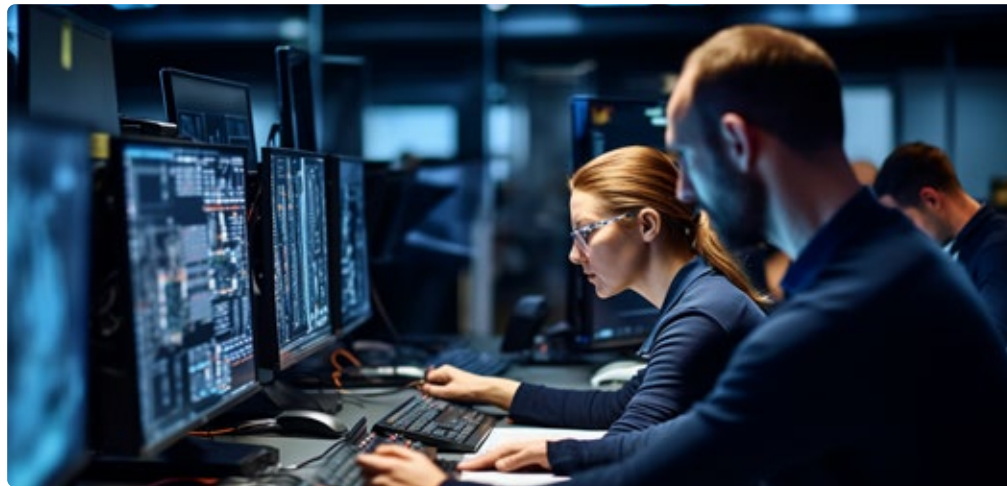
misuse of privileged credentials.

That is why both administrative and privileged accounts need to be protected. The time has come when the risks of data loss and breaches far outweigh the justification to leave these accounts unfettered. Today's privileged access management technology can enforce control over access with minimal friction.

In today's multi-tiered, service-based architectures, organizations often create several service and shared accounts and credentials,

embed them in systems, and forget them. This poses a rich attack surface for eager cyber-predators. Securing these service and shared accounts and credentials is another paramount front in defending organizational assets and resources.

When we consider that many of today's businesses across sectors such as telecommunications, oil pipelines, electricity, healthcare and manufacturing are run on the Internet of Things (IoT), the relevance of Zero Trust and privileged access control becomes obvious.



## A dark cloud inside a silver lining

---

The advent of IaaS, PaaS, and SaaS has increased the number of ephemeral servers and databases instantiated on dynamic demand as well as accounts with access to them. While cloud-based services save significant operations costs, and add flexibility and agility

to an organization's information management assets, they also present issues of account and credential governance. Accounts and credentials, many of which are ephemeral, are rarely connected to identity management and

governance infrastructures, and have their own lifecycle and management tools.

The dynamic nature of accounts, their associated privileges, and the ability to spin up new servers and database instances to support demand and

capacity bring new vulnerabilities. Securing ephemeral credentials, access privileges and servers while they are extant poses a new challenge which requires solutions such as just-in-time provisioning, de-provisioning, and dynamic access control policies.

The adoption of continuous integration and continuous development in the DevOps realm brings additional challenges when organizations create new

assets requiring proper credential security. While some organizations understand the potential benefits of appropriate security controls, many have not yet applied them.

Organizations like to multi-purpose assets to derive the most value. Given that, simple coarse-grained access control provided by proxy-based systems does not suffice. Systems with the capability to execute elevated command privileges at run time through delegation still have

loopholes. Fine-grained access control allows data with varying access requirements to coexist in the same asset, thereby increasing the asset's value while retaining control.

When an organization monitors user behavior, it's important not to rely only on reviews and audits. The keys to access control policy management success are leveraging the connected data and applying analytics and heuristics.

## Privileged Access Management gets Zero Trust

The NIST SP 800-207 and Forrester Zero Trust models both call for key tenets for organizations to leverage in providing strong micro-perimeters that

control and protect computing resources in this ever-expanding universe. The following table provides a perspective on how privileged access

management solutions play a critical role in providing control in a Zero Trust framework.

## Visibility and Analytics

### Zero Trust

Visibility is the foundation of Zero Trust.

It's important to have visibility into all assets and all activities performed on an asset.

Continuous analytics is paramount for dynamic policy management.

### Privileged Access Management Considerations

A privileged access management system with proper hooks into the DevOps and CI/CD pipeline and clear visibility of all assets as well as shared, service, and ephemeral credentials creates sound control.

Session recording and logging that includes observability aspects of privileged access management aid effective implementation of Zero Trust.

In combination with dynamic analytics, dynamic visibility is brought into user behavior analysis and monitoring.

## Automation and Orchestration

---

### Zero Trust

Expanding sprawl creates a challenge to control. Automation is critical to controlling assets.

Using analytics to orchestrate policies dynamically eradicates error prone manual controls.

### Privileged Access Management considerations

Tools for account and asset discovery and automated policy application must be integrated with a privileged access management system to attain an efficient and effective Zero Trust control mechanism.

Integration with user behavior analytics for dynamic policy management and orchestration is also a powerful automation component.

## Segmentation

---

### Zero Trust

Each network-based asset must be secured and segmented appropriately using the principle of least privilege.

### Privileged Access Management considerations

Building a virtual moat around each network-based asset is best accomplished via privileged access management systems that control credentials and access for every use by vaulting credentials and proxying access. Implementation of fine-grain access controls further fortifies critical assets.

This provides the control that has been missing in distributed environments, now further exacerbated by the removal of organizational perimeters, and is a significant step toward establishing a Zero Trust environment.

## Compliance

---

### Zero Trust

All organizations have one or more compliance aspects such as PCIDSS, GDPR and other security and privacy controls.

Compliance is of course mandatory, and is achieved through properly applying controls on organizational assets and demonstrating the control applicable to specific lines of business.

### Privileged Access Management considerations

Privileged access management systems help achieve and demonstrate control via logging and reporting.

## Conclusion

---

In the ever-expanding universe of information assets with disappearing perimeters, an efficient way to reduce risk is to control access to privileged and shared accounts. Adopting the principle of least

privilege is a critical first step toward Zero Trust. Local accounts, administrative accounts and ephemeral accounts for on-premise or cloud devices should be locked down, and applications or tasks that

require elevated permissions should be granted access only via monitored approval.

That's why privileged access management is such an important tool in your Zero Trust toolbox.

To learn more visit <https://www.hcltech.com/digital-foundation/consulting>

**HCLTech** | Supercharging  
Progress™

HCLTech is a global technology company, home to more than 221,000 people across 60 countries, delivering industry-leading capabilities centered around digital, engineering, cloud and AI, powered by a broad portfolio of technology services and products. We work with clients across all major verticals, providing industry solutions for Financial Services, Manufacturing, Life Sciences and Healthcare, Technology and Services, Telecom and Media, Retail and CPG, and Public Services. Consolidated revenues as of 12 months ending September 2023 totaled \$12.9 billion. To learn how we can supercharge progress for you, visit [hcltech.com](https://www.hcltech.com).

[hcltech.com](https://www.hcltech.com)

