ManageEngine
PAM360

# Privileged access management in a Zero Trust world

*- Melanie Karunaratne*

www.manageengine.com/pam360

## Introduction

In the early months of the COVID-19 pandemic, with the large-scale shift to working from home, connectivity was the primary focus of organizations. IT administrators rapidly put virtual meetings, live streaming, virtual education, cloud applications, and resources in place to support their remote end users. With many organizations signaling their intent to extend work from home (WFH), it's become clear that remote working and hybrid working dynamics are here to stay. This document outlines the security implications of the new work environment, explains the shift by organizations to a Zero Trust mindset, and the importance of privileged access management to support a Zero Trust security model.

## Access to all areas

The upheaval caused by WFH mandates and the need to keep workers productive at all costs gave rise to rapid access to technology. This access often bypassed regular checks and balances around access requests. Some of the findings that stemmed from the increasing adoption of WFH policies are:

- Businesses, healthcare, education, and governments accelerated the adoption of cloud technology, rapidly migrating some services from on-premises to Software as a Service (SaaS) applications that use public-facing internet addresses entry points.

- Employees were granted access to resources outside of the corporate network.

- New IT vendor contracts were adopted quickly, adding more third-party access to corporate infrastructures and applications.

- VPNs expanded, increasing license costs and the number of IT incidents logged.

- Laptops were procured, provisioned, and pushed out the door with elevated access rights to ensure the workforce could get up and running quickly.

- Workers set up home offices, accessing systems from personal phones, laptops, and tablets, and in some cases, shared family devices. These personal devices often have weaker security configurations. These same devices connect to consumer shopping sites, social media, and home entertainment sites using the same credentials. This increases the likelihood that compromised devices are accessing applications storing corporate data.

- Companies not built for remote working are now dealing with an explosion of known and unknown endpoints accessing their networks on insecure Wi-Fi networks.

Corporate data previously housed in software monitored and maintained by IT teams now resides in unchecked SaaS applications with shared passwords that may be used on personal devices, increasing the security risk of exposure by broadening attack surface areas. As remote working became the new normal, we have witnessed a surge and persistence in cyberattacks over the same period. Threat actors have seized on the shift to home-working, persistently penetrating network perimeters. Sophisticated attacks are disrupting businesses, supply chains, and healthcare at an enormous cost.

## Zero Trust—Trust no one

With users working across multiple devices, on and off the corporate network, it's become a game of cat and mouse to secure the network perimeter against bad actors' efforts.The castle-and-moat approach governs access from a static network perimeter. But the disjointed combination of VPNs, email security, firewalls, etc., is obsolete in our new work-life environment. Complex multi-cloud cloud environments, using platforms like Amazon AWS and Microsoft Azure, hybrid environments, and cloud applications' rapid adoption, mean a perimeter-based approach is no longer defensible. Adversaries are using the perimeter-based security approach against organizations. Some of the worst attacks were successful because cybercriminals penetrated firewalls. They moved around undetected from device to device using trusted credentials exploiting privileges or escalated privileges from the inside.

Trusting everyone inside the perimeter is no longer effective. This is why leading organizations are shifting to Zero Trust models to bolster their security posture and ward off the worst effects of attacks and breaches. A Zero Trust security model acknowledges that potential threats exist inside and outside the traditional perimeter. The assumption is that you are never safe. An attack is inevitable or already underway. Devices may already be compromised, and access requests are untrusted until verified. It's a shift in mindset eliminating implicit trust. Organizations operate by trusting no one inside or outside the network perimeters. Instead, they treat every user and device as a possible threat.

In a Zero Trust environment, all users, devices, and applications are verified before they can connect to corporate networks. They are continually assessed during a session for unusual activity until they leave the network offering real-time protection. The assessment uses granular details and

enforcement of policies. It considers context and location, endpoint and application posture, data access controls, and automation limiting access to only what is needed.

## Privileged access

A Zero Trust security model permeates across networks harnessing multiple layers of security tools and methods to minimize risks. Here we will dive into one layer—privileged access management (PAM).

PAM tools and policies are one of your last lines of defense to thwart the adversaries once they infiltrate. In the new Zero Trust world, PAM tools treat everyone inside as well as outside the organization as a potential threat to reduce the risk of threat attackers obtaining your critical data if systems are compromised. Even without a Zero Trust approach, privileged access management was a recognized foundational element of cybersecurity that many organizations put in place.

But when was the last time your organization reviewed privilege access management tool settings and policies? There is no room for complacency. There may be hundreds or thousands of servers in your environment and many super user administrators whose actions on resources aren't currently identifiable. PAM software cannot be treated as a "set it and forget it" activity. The IT changes over time in operations and devices accommodate work from home orders very well. Security and risk management leaders should view privilege management as a continual process. Identify, verify, protect and constantly monitor any privileged accounts. These include domain administration accounts, external services administration accounts, local administration accounts, and other accounts for installing and managing software.

## Set granular controls

Reviewing and auditing access is a principal component of Zero Trust, addressing head-on a cybercriminal's intent on lateral movement. And, your privilege access management software is a foundational tool.

Now is the time to recalibrate your PAM policies and technologies. Enforce fine-grained access policies based not only on the user role but also on location, device compliance status, health, and accessible data. A user accessing an application in the office environment is probably less risky than accessing the application over a public Wi-Fi, so context is key.

## Define privilege levels

Acknowledge that different account types are in use across the organization. These include personal or shared privilege accounts, service accounts, local administrator and root accounts, application-to-application credentials, and individual privilege levels. These different accounts should all be set up and deployed based on privileged policies. Identifying access levels such as standard users, service users, and super users will simplify the process of limiting access to higher tiers of privilege reducing exposure.

## Identify privileged accounts

In the early days of the pandemic, IT teams granted users more access rights due to a rush to maintain productivity. For example, to install new programs to get operations running quickly. But, those elevated permissions often remained in place months after the user needed them. Yet, we've seen an increase in sophisticated social engineering through the pandemic.

Coronavirus-themed phishing emails delivered Emotet Trojan malware allowing hackers to gain a foothold in accounts. Once inside, the attackers used privileged user accounts to move around the network. So it's vital to review administrative accounts granted for one specific task and revert these to standard user accounts.

Long-forgotten, orphaned, and unmanaged privileged accounts and service accounts offer accessible backdoors putting your organization at unnecessary risk. The existence of unaccounted privileged access carries significant risk, widening the attack surface area for cybercriminals.

Here is where your PAM tools should be finding privileged accounts. Start by scanning and discovering every privileged account and use case. Pinpoint who has administrator account access and who has elevated privileges. Rank the access based on risk and exposure to critical assets and data. Investigate all scenarios. For example, can a user with privileged access to work on a task in one asset inadvertently gain access to other controls or applications?

It's essential to understand what privileged accounts are accessing—record who owns resources and handles granting access. Also, it's important to put in place processes to discover any servers or applications that offer privileged access rights. Compare who was previously granted access to accounts, applications, and databases with who has access.

We highlighted earlier that context is key, and it's just as important to consider and record where access takes place and when. Once those with administrator or elevated access are identified, determine whether the additional privileges are still necessary based on the granular policies and remove excessive access. To keep abreast of constant changes in personnel, devices, systems, and infrastructure, comprehensive discovery and identification of privileged access must be a continuous activity.

## Use the principle of least privilege

Zero Trust exercises the least privilege principle over your users, applications, and devices. Issue just enough privileges for users, system administrators, and database administrators, and authorize elevated privileges only when needed. To follow this premise, grant users privileged access rights based on who requests permissions. Find out why an individual needs access. Ensure the minimal level of access required to perform a role and the least amount of time necessary. It's equally important to apply the least privileged lens across non-human entities. Review anything that uses credentials like robotic process automation tools, PowerShell scripts, or hard-coded credentials in DevOps tools like Chef and Puppet. Take advantage of your PAM solution to employ API calls for password retrieval and eradicate hard-coded passwords.

The rise in outsourcing back-office and core functions has led to increased vendor access to critical systems such as healthcare systems. Enforce the same least privilege principle concept to every access decision for third-party vendors and contractors. Make sure to monitor and log their access activity as part of your processes. When workers need higher privileges, use just-in-time controls to limit exposure. The best way to achieve this is to put in place just-in-time access requests and approval processes. Have users submit requests to elevate privileges for a set amount of time. A defined request and approval process ensures productivity is not affected, but Zero Trust security is still at the forefront of access decisions. Using your privilege access management tools to manage how and why privilege accounts are set up will prevent future sprawl.

## Lock down devices and applications

Following the Zero Trust approach, take steps to review end-user laptops and workstations. Lock each one down by removing local administrative

rights. Even an action as simple as a user's ability to change their machine's date and time can cause complications, affecting auditing efforts. Then, get more granular. For example, update settings and select the processes and applications a user can terminate from their machines. Regulating settings will ensure users avoid inadvertently disabling security protection software. Reduce the risk of introducing malware by restricting application downloads. Allow only trusted applications to run and block the rest. Trusted applications should still run with standard privileges to mitigate security risks. When an application is no longer in use, deprovision it. Deprovisioning not only helps to secure systems, but potentially saves money through license reclamation and reuse.

## Separate credentials

For the sake of speed, many administrators today are not separating their administrator accounts from their end-user work accounts. These same credentials are also used across servers. Why is this a concern? Threat actors target accounts with administrative privileges to access corporate resources and execute payloads. The SolarWinds Sunburst attack in December 2020 is a prime example as other security companies became a pathway for further attacks. The blast range affected hundreds of America's largest corporations and government agencies. Super users must not perform end-user tasks such as accessing emails while logged in using Windows administrator accounts or Linux root account privileges. Enforce the separation of privileges. Establish separate monitored accounts for administrative tasks. Segregate these from their end-user standard accounts and auditing accounts.

## Manage privileged accounts

Under the rule of trust no one, it's important to manage even legitimate privileged accounts. Begin with basic cyber hygiene checks. For example, ensure these accounts don't use default passwords. Remember that attackers hijack privileged accounts to launch attacks from the inside and remain undetected. So privileged accounts must be verified when connecting to the network. While the session is in progress, use your PAM tools to continue to monitor the account activity. Investigate any deviation in user behavior to ensure that an account has not been compromised. Identified risky activities should automatically trigger session termination to guard against privilege misuse. Exercise the same management and supervision levels over third-party vendors and contractors with privileged access to your systems. Closely monitor third-party vendors and contractor privileged sessions or even shadow sessions. End any session that seems suspicious or violates privileged access policies.

## Automate and integrate

To establish full visibility and control in your Zero Trust model, automate and integrate tools as much as possible. Smooth the experience of privileged access requests. Integrate PAM tools with your IT service management tools. Create workflows to manage just-in-time elevation requests from your service management tools. Also, make use of automated workflows to revoke temporary access efficiently. Avoid a "set it and forget it" scenario from occurring. Prevent hackers from finding orphaned or abandoned accounts and elevating privileges. Add automated workflows to identify and remove these accounts and save discovery time in the future. Sometimes, trusted administrators access accounts and make changes outside of the protective PAM tools. Eradicate these blindspots. Sharing data and correlating events with other tools like security information and event management (SIEM) tools supports your Zero Trust approach.

It's easier to detect access or anomalies in privileged access operations within and outside your PAM environment with more insights.

## Be audit-ready

Compliance standards and industry regulations like SOX, HIPAA, and PCI DSS require organizations to track and monitor critical systems' access and prove to auditors that the necessary security controls are in place. Use PAM tools to ease the audit burden.Your PAM tools should record, monitor, and audit any privileged access and privileged session activity. Make sure to record data about access approvals as well. Granular reports and tamper-proof session recordings facilitate better governance and accountability of privileged access.

## How ManageEngine can help with your Zero Trust journey

As organizations adopt remote or hybrid work environments and turn to Zero Trust models for protection, it's critical to ensure no privileged access to critical systems, data, or other assets is left unmanaged, unknown, or unmonitored. ManageEngine provides solutions to manage privileged user accounts, administrative access to critical IT assets, and compliance mandates. PAM360 from ManageEngine is a comprehensive privilege access management solution easily incorporated into an organization's Zero Trust model. It defends organizations against privilege misuse by regulating access to sensitive company information. PAM360 helps manage access for the IT infrastructure as a whole, including databases, switches, routers, firewalls, load balancers. The solution incorporates powerful, privileged access governance, workflow automation, and advanced analytics.

PAM360 also includes contextual integrations with various IT services for deeper correlation of privileged access data and overall network data. These integrations enable stricter control and governance over your administrative permissions and access across your entire IT infrastructure—users, systems, and applications.

## Supporting account governance

The first step to Zero Trust is to understand your security environment. PAM360 automatically discovers all privileged accounts across the IT infrastructure, including cloud applications. The solution can remotely reset account passwords for Windows local administrator accounts and Linux route accounts. It's simple to capture all events associated with privilege accounts as context-rich audit logs and reports. Granular reports and session recordings ease governance and provide better insights into privileged sessions. PAM360 provides a central point of management for audit and compliance. Avoid scrambling to pull together data for compliance audits at the last minute; readily demonstrate compliance to auditors and forensic investigators with PAM360's out-of-the-box reports on various compliance regulations such as PCI-DSS, NERC-CIP, ISO/IEC 27001, and GDPR.

## Elevating privileges

PAM360 is a powerful tool for regulating privileges. It enables the authorization, assignment, and tracking of controls for domain accounts and local accounts. The software can elevate privileges for a limited timeframe which reduces the risk of ongoing exposure. For just-in-time access requests, PAM360 provides a request-approve workflow mechanism for users to submit a request. With iPhone, Android, and Windows apps, administrators can authorize requests from anywhere.

Where multiple teams own a single device, dual approvals are also achievable with PAM360.

## Monitoring privileges

Once privileges are granted, in the trust no one approach, it's vital to monitor privileged users' activities closely. PAM360 provides the ability to shadow privileged sessions in real time, for example, to check third-party contractors or vendor activities. The solution allows for immediate session termination in the event of the detection of the misuse of privileges. PAM360 can also record, save, and playback a session as video files for tracking and auditing purposes.

## Managing sessions

To prevent unauthorized access and ensure systems are safe, IT admins must disable SSH access permissions and remote desktop services on corporate devices. PAM360 acts as a gateway to start a remote session, launch remote connections, and log into target machines via RDP, SSH, SQL, VNC, or web connections. Harness PAM360's functional for granular control and to restrict user activities. The solution can control which applications a user has access to through whitelisting capabilities.

## Automating and integrating workflows

PAM360's support of a Zero Trust model is wide-ranging. Contextual integration of PAM360 with applications and appliances across the IT infrastructure allows the automation of tasks and enhanced visibility. Organizations can eliminate hard-coded credentials within automation scripts with PAM360. The solution integrates with DevOps tools to fetch credentials in real time. Use the RESTful API and SSH CLI API to replace

usernames and passwords in PowerShell scripts, config files, or anywhere there are hardcoded credentials. Integrate PAM360 with robotic process automation tools to securely fetch credentials and deliver these to bots to perform operations.

PAM360 also integrates with your IT service management tools. This integration enables requests and approvals for credentials to take place within the ITSM environment. Without the necessary context, it's easy to be misled by blind spots in security incidents. PAM360 marries privileged data with endpoint event logs for context-aware event correlation. Integrating with SIEM tools enables forwarding all the raw audit data from PAM360 to SIEM solutions, such as Splunk, for deeper insights. Integrations ensure complete access, increasing awareness and visibility to enable more informed decisions.

## Managing SSH keys and SSL certificates

Manage SSH keys and SSL certificates with ease. PAM360 provides a centralized repository to store SSH keys for lifecycle administration and policy enforcement. The solution discovers keys, removes unused keys, as well as generates and deploys new keys to target systems. Also, PAM360 discovers, consolidates, and manages SSL certificates. The solution can send expiry alerts and check certifications for vulnerabilities. It can also automate workflows for certificate generation.

## Detecting anomalies

The faster you can root out harmful threats, the faster you can limit the damage. Integrating with ManageEngine's Analytics Plus, PAM360 enables comprehensive analysis of privileged account activities. Artificial intelligence and machine learning capabilities continuously

detect suspicious and harmful activities. Using data from PAM360, a risk assessment and risk score are designated for each operation. If a risk score is breached, a threshold notification is sent. The solution can trigger mitigating controls, such as session termination. It continually learns user behavior and patterns to detect anomalies.

## A wake-up call

Remote working, cloud platforms, and cloud applications have redefined an organization's security perimeter. Security and risk management leaders must re-evaluate the security perimeter and harden defenses with Zero Trust. The model embraces our pandemic and post-pandemic working environment, protecting users no matter their location or device. Rather than securing the network perimeter, a Zero Trust approach relocates security measures close to the application, system, or resource that needs protection.

To put you in a strong position and build a Zero Trust foundation, leverage the full extent of PAM practices and processes enforced by effective tool capabilities. Use PAM tools to take advantage of auditing functionality to identify a baseline and continue reporting. Enforce more granular policies. Introduce workflows for requesting and revoke access. Verify privileged and administrative access to your systems. Record and monitor access sessions on an ongoing basis. Mitigate attacks and use PAM as the cornerstone of a Zero Trust model. COVID-19 is our wake-up call in more ways than one.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360