BeyondTrust

Understanding the Access Management functions within the Maturity Model & how BeyondTrust PAM can help.

Access Management: Core to CISA's Zero Trust Maturity Model 2.0

TABLE OF CONTENTS

Introduction:

The **Cybersecurity and Infrastructure Security Agency's (CISA)** **Zero Trust Maturity Model Version 2.0** identifies access management as a core function within the **Identity Pillar**, bringing the need for **Privileged Access Management (PAM)** into clear focus.

BeyondTrust's commitment to the PAM market places us in a unique position to fulfill and strengthen an organization's implementation of the Access Management guidelines defined in CISA's Identity Pillar of Zero Trust. The addition of four maturity categories in the access management module of implementation allows for a more in-depth analysis of an organization's current access management posture, which we will examine.

These posture categories are outlined under the Identity Pillar within the newest version of the model as **Traditional, Initial, Advanced, and Optimal**.

Traditional Function:

- Early access management maturity stages. Categorized by manually run identity lifecycles, static security policies, siloed or selective policy enforcement, and limited data or log correlation between systems.
  - **For Access Management:** Permanent access is authorized with periodic reviews for both privileged and unprivileged accounts.

Initial Function:

- Early automation of lifecycle activities (provisioning, decommissioning, etc.) and policy enforcement, increased external system integrations and visibility, and the beginning steps of least privilege enforcement.

  - **For Access Management:** Access is authorized, including for privileged access requests, and expires with automated review.

Advanced Function:

- Automated controls for access configuration and policies wherever possible, centralized visibility into identity activities, integrated policy enforcement, and dynamic least privilege enforcement across internal systems.
  - **For Access Management:** Need-based and session-based access are enabled, including for privileged access request, and are tailored to actions and resources.

Optimal Function:

- Completely automated, just-in-time lifecycle policies, dynamic least privilege access for all assets, and centralized and continuously monitored activity logging that provides complete situational awareness.
  - **For Access Management:** Automation used to authorize just-in-time and just-enough access, each tailored to individual actions and individual resource needs.

Using these categories as an evaluative tool, an organization can pinpoint the maturity stage of their current Zero Trust Architecture and understand what steps to take to progress. While CISA merely adds the language for Access Management as a new function in Version 2.0 of their maturity model, exploring what that means for the identity pillar of zero trust is an important endeavor for any organization serious about adherence to security best practices.

Inside this whitepaper, we explore access management best practices, analyses of the new zero trust Access Management maturity category, and the substantial impact that Privileged Access Management capabilities can have for organizations on their journey towards a mature Zero Trust Architecture.

Identity Pillar Maturity: Traditional Function

In today's digital landscape, organizations face an ever-growing threat of cyberattacks and data breaches – often the result of misconfigured privileges or compromised privileged accounts. Regarding access management, CISA makes it clear that one of the most critical aspects to maintaining robust cybersecurity measures and combatting cyberattacks is controlling and managing privileged access across all assets.

> **"Agency authorizes permanent access with periodic review for both privileged and unprivileged accounts."**
>
> – Cybersecurity & Infrastructure Security Agency (CISA), Zero Trust Maturity Model Version 2.0, April 2023

Privileged access generally refers to elevated user accounts or roles that have extensive permissions to access sensitive systems, data, and resources. These privileged accounts are highly sought after by cybercriminals as they provide a gateway to valuable information and assets. To ensure the security of privileged access, periodic review for authorization becomes crucial. While CISA doesn't elaborate on more than the supplied matrix, we can extrapolate industry best practices on what a "traditional" stance is.

Periodic review for authorization is a basic requirement for a "traditional" level Zero Trust implementation.

Benefits include:

1. **Risk Mitigation:** Regularly reviewing and authorizing privileged access helps mitigate potential risks and vulnerabilities. As employees change roles, leave the organization, or experience other changes in their job responsibilities, their access requirements may change. By conducting periodic reviews, organizations can ensure that only authorized individuals have privileged access, reducing the risk of unauthorized or malicious activities.

2. **Compliance with Basic Government Mandates:** The basic concept of ICAM and CDM — and just about any additional zero trust initiative — requires the implementation of at least a baseline function of PAM to fulfill compliance obligations around identity and access security.

3. **Least Privilege Adherence:** The principle of least privilege states that users should only have the minimum level of access required to effectively perform their job functions. Periodic reviews of privileged access needs help organizations enforce the principle of least privilege (PoLP) by evaluating users' access rights and removing unnecessary privileges. This practice minimizes the potential attack surface and limits the damage caused by compromised accounts.

4. **Detection of Unauthorized Access:** Periodic reviews allow organizations to detect and address any unauthorized or suspicious privileged access activities. By monitoring access logs and comparing them against authorized users, organizations can promptly identify and investigate any anomalies or potential security breaches. This proactive approach enhances the organization's ability to respond effectively to security incidents, and cab severely limit their impact on critical systems and data.

5. **Insider Threat** Prevention: Insiders, including employees, contractors, or third-party vendors, pose a significant threat to an organization's cybersecurity. Periodic reviews for authorization provide an opportunity to identify and mitigate insider threats. By regularly evaluating privileged access rights, organizations can quickly identify any potential misuse or abuse of privileges by insiders, thereby reducing the risk of data leaks, sabotage, or other malicious activities.

6. **Accountability & Transparency:** Periodic reviews for authorization promote accountability and transparency within the organization. By ensuring access rights are properly authorized and regularly reviewed, organizations establish a clear chain of responsibility. This helps develop a culture of cybersecurity awareness and encourages employees to take ownership of their actions — a major step when fostering a secure working environment.

7. **Adaptability to Changing Security Landscapes:** The cybersecurity landscape is constantly evolving with new threats and vulnerabilities emerging regularly. Periodic reviews for authorization allow organizations to effectively adapt and respond to these changes. By staying up to date with the latest access control practices and their current access risk levels, organizations can proactively address emerging threats and always maintain a robust security posture.

Identity Pillar Maturity: Initial Function

In the Version 2 maturity model, the **Initial** stage of access management uses traditional management concepts and adds more advanced capabilities like automated reviews and privilege expiration.

BeyondTrust's ability to add expirations and automated review to privilege access management significantly enhances the security posture of an organization. For organizations currently operating at a **Traditional** stage of access management maturity, BeyondTrust PAM immediately pushes them to the subsequent **Initial** function category defined by CISA.

> **"Agency authorizes access, including for privileged access requests, that expires with automated review."**
>
> – Cybersecurity & Infrastructure Security Agency (CISA), Zero Trust Maturity Model Version 2.0, April 2023

From thousands of implementations and best-practice industry guidelines, here's how initial-stage access management contributes to improved cybersecurity:

1. **Access Expiration:** By setting expirations on privileged access accounts or roles, organizations ensure access is time-limited and regularly reassessed. This practice reduces the risk of dormant or forgotten accounts retaining excessive privileges. When privileged access has a predefined expiration date, it prompts periodic reviews to determine if continued access is necessary. This enforces the principle of least privilege by automatically revoking access when it is no longer required, minimizing the attack surface and the potential for unauthorized access.

2. **Automated Review Cycles:** Automating the review processes for privileged access eliminates manual errors and ensures consistent and timely evaluations. Using PAM tools, organizations can implement automated workflows that trigger periodic reviews based on predetermined schedules. These reviews evaluate access rights, permissions, and user activity logs to validate the appropriateness of privileged access.

Automated systems can also generate alerts or notifications when anomalies or policy violations are detected, enabling quick action to address potential security incidents.

This combination of expirations and automated reviews ultimately leads to the realization of additional security benefits, including:

- **Timely Removal of Access:** Expirations and automated reviews ensure privileged access is promptly revoked when no longer required, minimizing the window of opportunity for unauthorized or malicious activities.

- **Reduced Insider Threats:** By regularly reviewing privileged access, organizations can identify and address any unauthorized access by insiders. Automated alerts can detect unusual or suspicious behavior, aiding in the prevention of nsider threats.

- **Compliance & Audit Readiness:** Automated review processes facilitate compliance with regulatory standards by providing a documented and auditable trail of access reviews. This streamlines the audit process and demonstrates adherence to security best practices.

- **Proactive Security Measures:** Regular, automated reviews allow organizations to proactively address security risks. By promptly identifying and rectifying issues, such as excessive access privileges or policy violations, organizations can enhance their security posture and prevent potential breaches.

Incorporating expirations and automated reviews into privileged access management practices ensures access rights remain aligned with business needs, reduces the risk of unauthorized access, and strengthens the overall resiliency and security posture of an organization's systems and data.

Identity Pillar Maturity: Advanced Function

The **Advanced** level of CISA's Zero Trust Identity Pillar takes protectionary measures several steps further, adding need-based and session-based access tailored to actions and resources.

> **"Agency authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources."**
>
> – Cybersecurity & Infrastructure Security Agency (CISA), Zero Trust Maturity Model Version 2.0, April 2023

This approach ensures that privileged access is granted only when necessary and limited to specific actions or resources. Benefits of this increased access management function level include:

1. **Need-Based Access:** Granting privileged access based on the principle of need ensures individuals have access only to the resources required to perform their specific job functions. By implementing granular access control models, organizations can assign privileges at the most appropriate level, reducing the risk of misuse or accidental exposure of sensitive information. Need-based access limits the attack surface by providing users with the minimum privilege necessary to effectively fulfill their tasks.

2. **Session-Based Access:** Session-based access restricts privileged access to specific sessions or time periods. It ensures access is granted only when needed and is automatically revoked when sessions end. This approach helps prevent unauthorized access, as users must authenticate for each session and are granted access only for a limited duration. This also greatly minimizes the risk of dormant or unattended sessions being exploited by malicious actors.

3. **Tailored Actions & Resources:** By tailoring privileged access to specific actions and resources, organizations can further enhance security. Access rights may be granted on a per-action basis, ensuring that users have access only to the specific actions required to perform their tasks. Similarly, resource-based access control restricts access to specific resources, such as databases or sensitive files, based on the user's role and authorization level. This fine-grained approach prevents unauthorized access to critical assets, reducing the impact of potential breaches.

4. **Privilege Escalation Prevention:** Need-based and session-based access minimize the likelihood of privilege escalation attacks. By carefully defining access levels and session durations, organizations can limit the potential for unauthorized elevation of privileges by attackers. This enhances the overall security posture and prevents attackers from gaining persistent access to sensitive systems or data.

5. **Compliance & Audit Trails:** Tailoring access based on actions and resources provides a clear audit trail and facilitates compliance with regulatory requirements. By associating access permissions with specific actions and resources, organizations can demonstrate accountability and adherence to industry standards during audits or compliance assessments.

By combining need-based and session-based access controls with tailored actions and resources, organizations can significantly increase the hardiness of their identity and access security posture. These measures are designed to ensure privileged access is granted on a "need-to-have" basis, session durations are limited and monitored, and privileged access is restricted to specific actions and resources. This drastically reduces your organization's attack surface, mitigates the risks of privilege abuse, and improves your overall cybersecurity stance, safeguarding critical systems and sensitive data from potential threats.

Identity Pillar Maturity: Optimal Function

The final maturity category as defined by the new CISA guidelines, **Optimal**, includes all previously mentioned functions — **Traditional, Initial, and Advanced** — but with greatly increased automation capabilities.

> **"Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs."**
>
> – Cybersecurity & Infrastructure Security Agency (CISA), Zero Trust Maturity Model Version 2.0, April 2023

Adding automation to authorize just-in-time (JIT) access significantly increases the security stance of any organization. JIT access is when privileged access is granted only when it is needed for a specific task or period – nothing more and nothing less. By automating the authorization process to operate within this razor-thin window, organizations greatly decrease the opportunities for access abuse or breach.

Benefits of an Optimal level of access management include:

1. **Significantly Reduced Exposure:** Automation allows for the quick and efficient granting of privileged access when required, minimizing the overall exposure window. Instead of granting continuous or long-term access, just-in-time access ensures that access is provisioned precisely when it is needed, reducing the opportunity for unauthorized access or misuse.

2. **Greatly Minimized Privilege Creep:** Privilege creep occurs when users accumulate unnecessary or excessive access privileges over time. With automation, JIT access can be used to precisely define and limit the specific actions or resources necessary for tasks at-hand. This approach prevents users from accumulating unnecessary privileges, reducing the potential for abuse and limiting the impact of compromised accounts.

3. **Streamlined Workflows:** Automation streamlines the authorization process by eliminating manual intervention. When users request privileged access, an automated system can evaluate, validate the need, and grant temporary access based on predefined policies and criteria. This accelerates the workflow, ensuring that users have the necessary access in a timely manner—without compromising security.

4. **Auditing & Compliance:** Automating the authorization of JIT access provides a robust audit trail and aids in compliance with regulatory requirements. Automated systems can log and track access requests, approvals, and durations, creating a comprehensive record of privileged activities. This audit trail helps organizations demonstrate compliance during audits, investigations, or compliance assessments.

5. **Quick Revocation:** Just-in-time access automation enables prompt revocation of privileged access when the task is completed, or the authorized time-period expires. This proactive approach ensures access rights are automatically revoked, reducing the risk of lingering privileges and unauthorized access after the task is finished.

By incorporating automation into the authorization process for JIT access, organizations can improve security by reducing exposure, minimizing privilege creep, streamlining workflows, facilitating auditing and compliance, and enabling quick revocation. These measures help establish a dynamic and secure access control framework that aligns privileged access with business needs, mitigates risks, and protects critical systems and data from potential threats.

Level-Up Access Management Maturity with BeyondTrust

BeyondTrust's industry-leading Privileged Access Management solutions are designed to guide organizations as they "level-up" through CISA's Zero Trust maturity model and are enterprise-ready to quickly implement and assist on the journey towards actualized zero trust architecture. Our solutions allow organizations to enforce robust access management while still focusing on delivering mission-critical priorities.

Mapping BeyondTrust to the Identity Pillar of CISA's Zero Trust Maturity Model V2			
Identity Function	**Maturity Level**	**Product Mapping**	**How BeyondTrust Helps**
Identity Stores	Optimal	Password Safe Privilege Management for Windows/Mac Privilege Management for Unix/Linux	**BeyondTrust solutions** ensure identities are mapped appropriately to roles and entitlements using standard connectors to identity stores.
Risk Assessment	Advanced	Identity Security Insights	**Identity Security Insights** identifies privilege creep and provides automated recommendations for reducing risk.
Access Management	Initial	Password Safe	**Password Safe** integrates with other identity providers to deliver automated privilege reviews. Includes automated expiration for roles not reviewed in an appropriate measure of time.
Access Management	Advanced	Password Safe Privilege Management for Windows/Mac Privilege Management for Unix/Linux	**BeyondTrust solutions** use attribute and role-based access to tailor access rights to individual users or roles, enabling access to sessions or applications within designated job functions.
Access Management	Optimal	Password Safe Privilege Management for Windows/Mac Privilege Management for Unix/Linux	**BeyondTrust solutions** can easily integrate with automated identity platforms to implement Just-in-Time (JIT) access based on previously defined policies and can be custom-tailored to individual access and resource demands.

Figure 1: Illustrating how BeyondTrust's solutions map to the Identity Pillar of CISA's Zero Trust Maturity Model 2.0I, Version 2.0

Privileged Management for Windows & Mac: Remove local admin rights, enforce least privilege dynamically across Windows and macOS, prevent malware and phishing attacks, and control applications.

Privilege Management for Unix & Linux: Achieve compliance, establish least privilege and zero trust, and prevent and minimize security breaches—without hurting productivity.

Password Safe: Manage privileged passwords, accounts, credentials, secrets, and sessions for people and machines, ensuring complete control and security.

Identity Security Insights: Gain a centralized view of identities, accounts, and privileged access across your IT estate, and leverage threat intelligence recommendations to improve your identity security posture.

The BeyondTrust Difference: From Access Management to Zero Trust

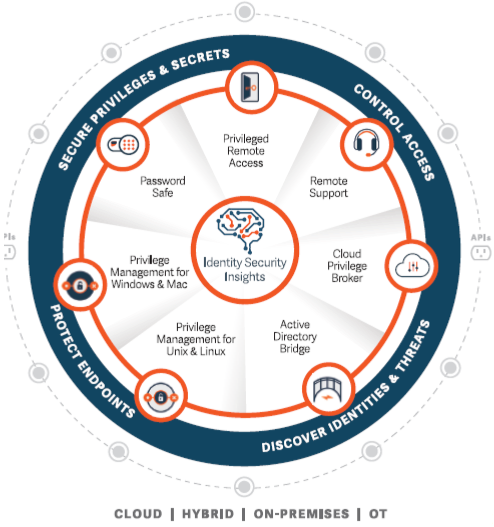
SECURE PRIVILEGES & SECRETS
CONTROL ACCESS
DISCOVER IDENTITIES & THREATS
PROTECT ENDPOINTS
Privileged Remote Access
Password Safe
Remote Support
Identity Security Insights
Cloud Privilege Broker
Privilege Management for Windows & Mac
Privilege Management for Unix & Linux
Active Directory Bridge
PIs
APIs
CLOUD | HYBRID | ON-PREMISES | OT

Figure 1: The BeyondTrust Platform

BeyondTrust delivers what industry experts consider to be the most complete spectrum of privileged access management (PAM) solutions available on the market. Analysts continually recognize BeyondTrust for the unsurpassed depth and breadth of PAM use cases we cover, the completeness of our solutions, our consistent technological innovation and vision, and our centralized management platform.

Our solutions provide coverage over all privileged identities across your organization's endpoints—including Windows, macOS, Unix, Linux, cloud, on-premises, hybrid, human (employee and vendor), and machines.

BeyondTrust uniquely blends three disciplines together—PAM, CIEM, & ITDR—to help organizations holistically strengthen their Identity Security and account for every plane of privilege. These disciplines represent today's top cybersecurity best practices and are must-haves for organizations seeking to adhere to CISA's Zero Trust Model – for access management purposes and beyond.

To learn more about how BeyondTrust can help advance your Access Management maturity, align with Zero Trust fundamentals, and help you meet other security or compliance goals, **contact us today.**

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network. Learn more at **beyondtrust.com**