SOLUTION BRIEF

CHALLENGE

The increasing value of data, progressively more stringent regulations, and the number of privileged users that have elevated access all make it increasingly difficult to protect sensitive information and intellectual property. PAM technologies have been deployed to address these challenges, but many organizations are finding new use cases that require a different approach.

OPPORTUNITY

Symantec PAM is the only privileged access management solution that delivers a comprehensive set of features that can be delivered using both proxy-based and agent-based architectures, and managed from a unified management console. This unique offering enables organizations to provide broad-based PAM coverage for their entire environment.

BENEFITS

Organizations can realize significant financial and reputational benefits by effectively managing risk, preventing improper use of privileged accounts, and safeguarding high-value assets. The multiple layers of defense provided by Symantec PAM enables organizations to deploy the appropriate level of security without the need to implement multiple point solutions.

Symantec by Broadcom

Extending Zero Trust to the Kernel

Introduction

As traditional IT defenses were strained during the pandemic, one potential architecture framework emerged as a potential savior to address these business challenges, Zero Trust. But what does that mean to you? Software vendors have seized upon this trend, and it seems that every solution is designed to help you achieve Zero Trust. For some, this assistance is with identities, providing modern authentication services that positively identify legitimate users from fraudulent ones. This user identification is a foundational building block for Zero Trust, because how can you grant access if you do not know who is asking. Others are pushing Zero Trust Network Access and Secure Access Service Edge as a means to secure the deteriorating perimeter, and establish a software-defined perimeter to protect access to network and corporate resources. These security frameworks are an equally important step in your Zero Trust journey. Another aspect of security that is also being pushed is least privileged access, which can be addressed by both Identity Governance and Administration solutions and Privileged Access Management (PAM) solutions. Both of these security solutions are also core aspects of a Zero Trust architecture, but they are not often positioned to address all aspects of achieving Zero Trust. One use case that is not discussed is pushing privileged access controls down to the kernel. Why is this? The kernel is a resource and it processes some of the most elevated and privileged commands, often without any policy controls. The purpose of this brief is to explain why you would want to extend Zero Trust access down to the kernel, and how it can be easily accomplished with Symantec® PAM.

Two Frameworks for PAM

PAM technologies allow organizations to create and enforce controls over users, accounts, and systems that have elevated or privileged entitlements. Traditionally, this control was accomplished by deploying one of the following architecture frameworks:

- **Password Account and Session Management (PASM):** These technologies protect privileged accounts by vaulting their credentials, and forcing privileged users to authenticate themselves to the tool before being granted access.
- **Privileged Elevation and Delegation Management (PEDM):** These technologies leveraged agents to protect privileged accounts by enforcing fine-grained access controls over the users who access the protected devices.

For many years, the two frameworks were considered to be mutually exclusive. An organization would adopt one or the other to address their requirements; however, the majority of deployments were usually PASM solutions. PASM solutions were easier to implement and provided a wide range of coverage for various PAM use cases, but not all. There are a few use cases and protections that can only be achieved through the use of an agent.

Addressing Assumed Breach with a PASM Technology

The third tenet of Zero Trust is to assume breach. This means that you should examine your security technologies, and evaluate how they could be compromised and what could be done to prevent or minimize the damages of that breach. Within a PASM solution, there are two likely breach points:

- Compromised user account
- Compromised vault

In the first scenario, you must assume that a legitimate user, who has access to privileged accounts and credentials, has their account compromised. This scenario would allow an unauthorized and potentially malicious user to authenticate to the PASM solution and gain access to everything the legitimate user would have been authorized to access and use. The solution to address this attack is behavioral analytics. This solution monitors all privileged user activities and then compares current actions to historical ones. The goal is to detect abnormal usage patterns that can trigger automated mitigation actions. This solution also addresses insider threats, because user behaviors typically change dramatically when a trusted insider goes rogue.

In the second scenario, you must evaluate if the encrypted vault can be compromised. For some solutions, the likelihood of this occurring is minimal; however, some solutions leverage an external database to store privileged credentials. This external database can be attacked, especially since many of these solutions provide a backdoor administrative account. This backdoor account can bypass all of the PASM policies and controls to directly retrieve and access the privileged credentials stored within the database. You could argue that this event is unlikely, but within a Zero Trust framework we must assume that it can happen. If so, how do you protect your resources once a malicious user has gained access to the privileged credentials for your privileged accounts? In this case, agents can serve as the secondary line of defense. They can enforce policies with fine-grained control over operating system-level access and privileged user actions, even if the user logs in directly with a legitimate credential.

Addressing Direct Access to Servers

The second issue with PASM solutions is one of route of attack. Most attacks are performed online. The proxy-based approach of the PASM technologies can ensure that hackers must be authenticated and authorized before gaining access to a privileged account or credential. But what happens if the attacker gains direct access to the hardware? They can access the privileged accounts on that server and completely bypass the PASM security controls. Again, this may seem like an unlikely chance, but under the assume breach tenet, you must assume that it could occur. Agents can serve as the secondary line of defense because they are installed on the servers, and they can operate and protect the resources on those servers even if they are isolated from the network.

Addressing Least Privileged Access

PASM technologies have the ability to limit which commands a user can run while using a privileged account; however, these filters typically only work in certain scenarios while accessing a system through the PASM solution. An agent-based approach can enforce extensively higher controls across multiple operating systems, because they are integrated with the kernel, can intercept system calls, and can enforce policies on whether or not to allow those commands to proceed to the kernel for processing.

Introducing Symantec PAM

Symantec PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies, and monitoring and recording privileged user activity across virtual, cloud and physical environments. The solution delivers six core policy enforcement capabilities from a single platform, including: *privileged credential vault, session management and recording, user and entity behavioral analytics, secrets management, programmatic access management, and fine-grained host-based command control.* The solution architecture includes an appliance that delivers the PASM capabilities, and server control agents that deliver the PEDM (such as, the fine-grained, host-based command control capabilities.

PAM Server Control Agents

The PAM Server Control Agents (herein referred to as agents) help to mitigate both internal and external risk by controlling how business or privileged users access and use enterprise data. The architecture is host-based, which is an advantage because it places the security mechanism (the agents) as close to the data as possible, and minimizes the performance penalty incurred for network traffic. The agents are installed on the host servers and operating systems to be secured and are supported on leading platforms including Windows, UNIX, and Linux across on-premise, virtualized and cloud environments. The solution enables organizations to centrally administer all aspects of host server security. They can create, modify, and delete userids and groupids, as well as passwords and file permissions, and access rules that govern access to all protected resources, such as files, userids, network connections, and processes. These policies are created and managed through the unified PAM management console, and then distributed to the agents where they are enforced. Additionally, because the agents maintain their policies locally, they can protect the resources that reside on their host, even when the host is accidentally or intentionally isolated from the network.

Understanding the Power of the Server Control Agents

There are two basic ways to protect against unauthorized use of system resources: block unauthorized users from accessing the system, and block authorized users from accessing items to which they should not have access.

The agents protect your systems in both ways, by enforcing the following controls:

- **Login control:** The agents can enhance login security by limiting user login by originating IP address, terminal ID, type of login program, or time of the day. They can also limit the concurrent login sessions of a user to enforce stringent user access to a server.
- **Impersonation control:** The agents control surrogate user delegation capabilities to reduce the exposure of unauthorized users running applications with enhanced privileges and achieve accountability of shared account activity. This control provides assurance that the original login ID is never lost, and that every log record is tied to the user.
- **Substitution tracking:** Because the agents can always track the user back to their login ID, regardless of account the use, their permissions are always governed by those granted to their original login ID and not the account they are using.
- **Superuser (administrator and root) containment:** The agents inspect all relevant incoming requests at the system level, and enforces authorization based on the defined rules and policies. Not even the privileged root or superuser account can bypass this level of control.
- **Fine-grained enforcement:** The agent provides the ability to enforce granular access privileges to superuser and root accounts. This granularity enables you to support least privileged access and enforce separation of duties for different users or groups, even when using the same shared account.
- **Network connections:** The agents can regulate incoming and outgoing network connecting, helping to control access to network services and ports.
- **Files and folders:** The agents provide enhanced file access restrictions, which protect files beyond native OS limitations. They can control how users may access files or folders, and which programs or applications may be used. They can also enforce change control on critical file and directory systems, which increases data integrity and confidentiality. File level protection is available for all types of files including text files, directories, program files, device files, symbolic links, NFS mounted files, and Windows shares.
- **Processes:** The agents prevent the interruption or stopping of critical processes by highly privileged users. Critical system daemons and application processes, such as database servers, can be accessed only by authorized users according to their defined job functions.
- **Trusted program execution:** Trojan horses and modified programs are a primary source of backdoor and unauthorized access to system resources. The agents provide first-line trusted program protection. Sensitive resources can be marked as trusted and these files and programs will then be monitored, and the agents will block execution from them should they be modified.

- **Windows protection:** The agents provide registry protection through the support of rules that can block administrators from changing or tampering with the registry settings (such as, the agents can protect registry keys from deletion and their corresponding values from modification). The agents also provide enhanced protection to limit the authorized administrators that can start, modify, or stop critical Windows services. This capability protects against denial of service of production applications like database, web, file and print, which are all controlled as services on Windows.
- **Application jailing:** The agents allow accepted actions to be defined for high-risk applications. Any behavior that exceeds these bounds will be restricted by an application jailing function.

Symantec PAM allows administrators to define policies to protect all of these resources, enforce these controls centrally within the management console, and then leverages an automated policy distribution process to propagate policies to multiple disparate servers across multiple domains, ensuring that these access policies are consistently enforced across platforms. In addition, endpoints are grouped into logical host groups and then assigned policies based on this host group membership, regardless of how the endpoints are physically organized. Hosts can be members of a number of logical host groups depending on their properties and policy demands.

Agents – Are They More Expensive to Manage?

One the chief concerns with an agent-based architecture is the cost to support and manage these agents after they have been deployed. The truth is, agents do require more support and maintenance than a proxy-based architecture, which is why we recommend a hybrid approach. Leverage the PAM PASM features to protect privileged credentials and accounts across the larger enterprise. Strategically deploy agents on servers that require a higher level of security, either because they are storing regulated data or running applications that are critical to the business. The strength of the Symantec PAM solution is that both of these architectures can co-exist, so you do not have to choose one or the other. Additionally, to ease the typical management overhead of agents, Symantec PAM features an easy to use REST interface, as well as repository support, to enable the automation of agent deployment and policy management.

Summary

Symantec PAM provides holistic privileged access security for the entire enterprise, covering a wide range of use cases. With regards to the server control agents, they offer in-depth protection of the most critical business servers with powerful, fine-grained protections over operating system-level access and privileged user actions. The agents also monitor and audit privileged user activity to improve security, reduce administrative costs and simplify audit and compliance processes across physical, virtual, and cloud environments.

For more information, please visit broadcom.com/symantec-pam

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

EXT-ZTK-SB100 March 1, 2023