SOLUTION BRIEF

Extending Zero Trust to the Kernel

CHALLENGE

Traditional PAM solutions often overlook direct server access and assume network-based controls are enough, leaving the kernel vulnerable to privilege abuse and insider threats.

OPPORTUNITY

Enforcing Zero Trust at the kernel level with host-based Server Control Agents can help organizations close critical security gaps and extend least privilege controls directly to operating systems.

BENEFITS

Symantec PAM Server Control Agents provide always-on protection with granular command-level control, even on isolated systems. This ensures consistent policy enforcement, improved compliance, and reduced risk from credential or network compromise.

Zero Trust in a Post-Pandemic World

As traditional IT defenses strained under the weight of the pandemic, Zero Trust architecture emerged as a vital framework for modern cybersecurity. But what does Zero Trust mean for your organization?

Software vendors have quickly embraced the trend, offering solutions that target identity verification, secure access, and privileged access control—all core components of a Zero Trust strategy. From modern authentication to Secure Access Service Edge (SASE) and Zero Trust Network Access (ZTNA), these tools aim to protect identities and secure network perimeters.

One critical but often overlooked aspect of Zero Trust is the kernel. As the operating system's foundation, the kernel processes the most privileged commands, typically without policy enforcement. In an accurate Zero Trust model, no stack layer—including the kernel—should be implicitly trusted.

This brief explores how extending Zero Trust principles to the kernel is essential, and how Symantec® Privileged Access Management (PAM) makes it achievable.

Two Approaches to Privileged Access Management

Symantec PAM brings together two key architectural frameworks that address privileged access:

- **Password Account and Session Management (PASM)**
  - Vaults credentials to protect privileged accounts
  - Requires users to authenticate to access sensitive systems
  - Simplifies deployment and covers a broad range of use cases
- **Privileged Elevation and Delegation Management (PEDM)**
  - Uses agents installed on host systems to enforce granular access controls
  - Offers deeper protection by controlling user activity at the operating system level

Historically seen as mutually exclusive, these frameworks can—and should—be complementary. While PASM provides robust credential management and session recording, PEDM is uniquely positioned to enforce Zero Trust at the kernel level.

Mitigating Risk with the Assumed Breach Mindset

One of the pillars of Zero Trust is the assumption that breaches will occur. Let's examine how PASM and PEDM work together to mitigate potential breach points.

Addressing Assumed Breach with a PASM Technology

A legitimate user's account could be compromised, granting unauthorized access via the PASM interface. Symantec PAM addresses this:

- User Behavior Analytics continuously monitors user activity and flags deviations
- Automated Mitigation takes corrective action against abnormal behaviors

PASM AND PEDM WORK TOGETHER TO MITIGATE POTENTIAL BREACH POINTS

Compromised Credential Vault

While secure, some PASM systems store credentials in external databases that may have backdoor accounts. If attackers bypass vault policies, Server Control Agents serve as a secondary defense:

- Enforces policies locally
- Controls privileged actions even with valid credentials

Protecting Against Direct Server Access

A central blind spot in proxy-based PASM solutions is direct server access, where attackers bypass the network entirely. When an attacker gains physical or direct network access to a server, PAM controls can be circumvented. The solution to this challenge are host-based agents. Installed directly on the host, Symantec PAM agents ensure the following:

- Enforces security policies at the kernel level
- Operates independently of the network
- Protects even isolated or disconnected systems

Enforcing Least Privileged Access

While PASM limits commands within controlled sessions, agent-based enforcement goes further:

- Kernel Integration intercepts system calls and applies policy before execution.
- Cross-Platform Control enforces least privilege policies on Windows, UNIX, and Linux systems.
- Broad Application works, regardless of how the system is accessed.

SYMANTEC PAM IS BUILT TO PREVENT SECURITY BREACHES ACROSS ON-PREMISES, CLOUD, AND HYBRID ENVIRONMENTS

Introducing Symantec PAM: A Unified Platform

Symantec PAM is built to prevent security breaches across on-premises, cloud, and hybrid environments. It delivers six core capabilities:

- Privileged credential vaulting
- Session management and recording
- User and entity behavior analytics
- Secrets management
- Programmatic access control
- Fine-grained host-based command control

This integrated solution combines a secure PASM appliance with host-based PEDM agents, offering unmatched control and visibility.

Server Control Agents: Enforcing Zero Trust at the Kernel

Symantec Server Control Agents, installed directely on host servers, extend Zero Trust to the operating system and kernel:

- Supported across Windows, UNIX, and Linux
- Centrally managed via a unified console
- Enforce policies even when offline or disconnected

Key Capabilities of the Agents

SYMANTEC PAM CLOSES THE ZERO TRUST GAP OTHERS IGNORE

Feature	Benefit
Access Controls	• *Login restrictions by IP, time, and terminal* • *Concurrent session limits*
User Accountability	• *Impersonation and surrogate user controls* • *Substitution tracking ensures the original ID is logged*
Root and Superuser Containment	• *Blocks even root/admin users from unauthorized actions* • *Enforces least privilege for shared accounts*
File and Process Protection	• *Controls file access beyond OS limits* • *Blocks unauthorized process manipulation* • *Enforces change controls on critical files*
Trusted Program Execution	• *Prevents execution of modified or malicious binaries* • *Flags tampered trusted applications.*
Network and Registry Controls	• *Regulates inbound/outbound network connections* • *Protects Windows registry with rule-based enforcement*

Conclusion: Why Zero Trust Must Extend to the Kernel

Zero Trust isn't just a network concept, it's a principle that must be enforced at every level of your IT stack, including the kernel. With Symantec PAM, organizations can unify PASM and PEDM to achieve true Zero Trust.

The addition of host-based Server Control Agents provides the following advantages:

- Granular enforcement of least privileged access
- Protection from insider and external threats
- Continuous defense—even when systems are isolated

Symantec PAM closes the Zero Trust gap others ignore. Protect your most sensitive systems from the inside out.

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

BROADCOM®
connecting everything®

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

EXT-ZTK-SB101 May 5, 2025