WHITESWAN
IDENTITY SECURITY

Standing Privileges Never Sleep (But Hackers Do)

Eliminating 24/7 Administrative Rights That Create Persistent Attack Pathways

The Problem

STANDING PRIVILEGES CREATE PERSISTENT ATTACK PATHWAYS

Independent research reveals the scope

68% of professionals retained access to former employers' systems after leaving, while 83% admit to bypassing security processes when current access is too restrictive.[1] Only 29% of organizations use identity-based access as their primary model, leaving the majority vulnerable to persistent privilege abuse.

Current Reality

42% of organizations say their current security and access model will be outdated within two years, while 32% cite balancing security with productivity as their top challenge.[3] Traditional PAM secures credentials but maintains the underlying vulnerability—persistent elevated privileges that exist 24/7 whether needed or not.

Business Impact

6.2M **Average privileged breach cost**

8-month recovery times.[4] Move budget from "credential security" to Zero Standing Privileges that eliminate persistent attack pathways.

WHY WHITESWAN?

Whiteswan eliminates persistent administrative rights with Just-in-Time access controls that provide privileges only when needed for specific business functions

1 Zero Standing Privileges

Eliminate persistent administrative rights through Just-in-Time access provisioning

2 Risk-Based Access Control

Automated approval workflows based on user context, business justification, and threat intelligence

3 Time-Bounded Sessions

Automatic privilege expiration based on business context and operational requirements

4 Legacy System Integration

JIT access for Windows Server 2003-2022 systems that cannot support modern authentication

5 Comprehensive Audit Trails

Complete documentation of access requests, approvals, activities, and session termination

Core Capabilities

Privileged Access Control

- Just-in-Time privilege elevation with automated approval workflows
- Risk-based access decisions using behavioral analytics and business context
- Zero Standing Privileges architecture eliminating persistent administrative rights
- Service account governance with time-bounded access and automated rotation
- Emergency access procedures providing break-glass capabilities with comprehensive audit trails
- Legacy system integration for Windows Server 2003-2022 environments

Secure Remote Access Control

- Session recording and analysis for all administrative activities across RDP/SSH/console access
- Secure Identity-first infrastructure access without reliance on VPN's
- Software-Defined Perimeter creating encrypted micro-tunnels per administrative session
- Behavioral analytics integration detecting account compromise during active sessions
- Automated threat response for immediate session termination and privilege revocation
- Cross-platform coverage including legacy Windows administrative interfaces

Industry Statistics

Sector	Standing Privilege Risk	Implementation Priority
Healthcare	78% use persistent admin rights for medical devices[5]	Emergency access procedures, HIPAA compliance
Financial	84% grant standing privileges to trading systems[6]	SOX segregation of duties, real-time operations
Manufacturing	91% maintain persistent OT administrative access[7]	IT/OT bridge security, safety system protection
Government	69% lack time-bounded clearance-based access[8]	Classified system controls, audit requirements

Technical Implementation Details

JIT Access Workflow Mechanics

Risk-Based Decision Engine

Real-time evaluation using machine learning algorithms analyzing user behavior, device trust, location context, and business justification against baseline patterns.

Approval Automation

Policy-driven workflows with configurable approval chains, automatic approvals for low-risk requests, escalation procedures for high-risk scenarios, and emergency break-glass procedures.

Financial Services

Technical Implementation Details

JIT Access Workflow Mechanics

Privilege Provisioning

Sub-second privilege elevation using native OS capabilities, LDAP group membership modification, application-specific role assignment, and cloud platform IAM integration.

Session Monitoring

Real-time activity logging, behavioral analytics during active sessions, automated anomaly detection, and immediate response capabilities including session termination and privilege revocation.

Technical Implementation Details

Enterprise Integration Capabilities

SIEM/SOC Integration

Native integrations for Splunk, QRadar, ArcSight, and Sentinel, correlation rules, and automated alerting for privileged access anomalies.

Technical Implementation Details

Enterprise Integration Capabilities

API Framework

RESTful APIs for custom integrations, webhook support for real-time notifications, GraphQL queries for complex data retrieval, and SCIM provisioning for automated user lifecycle management.

Business Process Integration

ServiceNow integration for ticketing workflows, Active Directory synchronization for organizational structure alignment, and business calendar integration for time-based access controls.

Technical Implementation Details

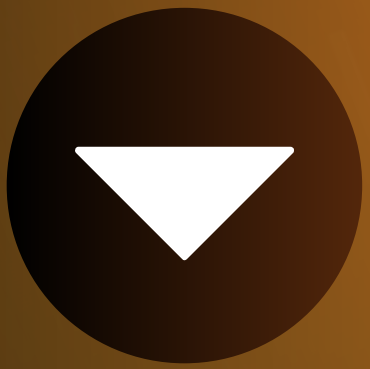
Legacy System Coverage and Limitations

Windows Server 2003-2012 Support

Protocol translation services providing modern JIT access controls while maintaining compatibility with legacy Group Policy and NTLM authentication requirements.

Technical Implementation Details

Legacy System Coverage and Limitations



Windows Server 2003-2012 Support

Protocol translation services providing modern JIT access controls while maintaining compatibility with legacy Group Policy and NTLM authentication requirements.

Coverage Scope

Full support for Windows administrative interfaces (RDP, PowerShell, MMC), partial support for legacy applications requiring custom integration, and documented limitations for systems lacking network connectivity.

Migration Path

Gradual modernization approach allowing legacy systems to benefit from JIT access controls while planning systematic infrastructure upgrades.

Financial Services

Business Outcomes

Metric	Before Whiteswan	After Implementation
Privilege Escalation	Daily standing admin rights	Zero persistent privileges
Attack Containment	Manual incident response	Automated session termination
Administrative Efficiency	VPN bottlenecks, manual approvals	Self-service JIT access
Audit Preparation	8-12 weeks manual review	2-3 days automated reporting
Compliance	Spreadsheet-based access tracking	Real-time compliance documentation

Organizations report substantial productivity improvements following JIT access deployment, with measurable reductions in privilege-related security incidents.

Industry Implementation Priorities

Manufacturing

IT/OT bridge security, SCADA system administrative access management

Healthcare

Emergency access procedures for clinical systems, HIPAA minimum necessary enforcement

Financial Services

SOX segregation of duties, PCI-DSS administrative access controls

Government

Clearance-based access controls, classified system administrative procedures

Technical Requirements

Supported Environments
Windows 7-11, Server 2003-2022 | Linux (RHEL, Ubuntu, CentOS) | macOS | Active Directory, Entra ID, Okta | AWS, Azure, GCP, hybrid, kubernetes.

Deployment Model
Lightweight agent deployment | Agentless Gateway deployment | Sub-second access provisioning | 99.9% SLA | Linear scaling 1K-100K+ identities

30-Day Implementation

Week 1	Privileged access inventory and standing privilege risk assessment
Week 2	JIT access pilot deployment with automated approval workflows
Week 3	Zero Standing Privileges conversion for critical administrative roles
Week 4	Behavioral analytics activation with automated session monitoring

Outcome

Eliminated standing privileges, faster incident containment, improved administrative efficiency, comprehensive compliance documentation.

WHITESWAN
IDENTITY SECURITY

Whiteswan delivers comprehensive Zero Standing Privileges architecture for hybrid enterprise environments.

Ready to Eliminate Standing Privileges?

Whiteswan eliminates persistent administrative rights — stopping attackers where they escalate privileges, not just where they initially authenticate.

- **Free Privileged Access Assessment:** Identify standing privilege risks and administrative access gaps
- **30-Day JIT Access Pilot:** Deploy core capabilities in your most critical administrative environment
- **ROI Analysis:** Calculate savings from eliminated privilege escalation risk and improved compliance

---

Learn More: www.whiteswansecurity.com
Contact: vmamidi@whiteswansecurity.com

Whiteswan Identity Security - Comprehensive Zero Standing Privileges implementation for hybrid enterprise environments