Whitepaper

Modern Network Access Without the NAC Tax Kron Network PAM as a Cost-Effective Alternative

networkPAM.com

Executive Summary

Network Access Control (NAC) platforms such as Cisco ISE, FortiNAC, and Aruba ClearPass continue to play an critical role in enterprise network security. However for some customer needs the full breadth of NAC features may go underutilized, due to the complexity while the cost still remains high.

With these kinds of deployments, Kron Network PAM delivers a more focused, identity-oriented approach to securing privileged access to mission-critical infrastructure like routers, switches, and firewalls. Kron Network PAM, where the typical usage case is more about enforcing access control rather than full-spectrum network posture control can be a less expensive and simplified alternative that also improves your security posture through additional auditing, enforcement, and operational efficiency.

NAC Complexity vs. PAM Simplicity

Functionality	Traditional NAC	Kron Network PAM
Access Control Enforcement	MAC-based, VLAN/ACL-based control	Secure admin interfaces, enforce MFA, audit use
Authentication	802.1X, RADIUS/TACACS+	SAML 2.0, LDAP, Active Directory, Entra ID
Posture Assessment	Agent-based, endpoint health checks	N/A
Session Visibility	Device-level traffic monitoring	Full session recording, metadata tagging, real-time SIEM export
Identity Binding	Limited or indirect (MAC/IP binding)	Strong identity assurance via AD/SAML + ephemeral credentials
Enforcement Actions	VLAN changes, quarantine, ACL push	Command filtering, JIT access revocation, session kill

How Kron Network PAM Technically Replaces NAC for Privileged Access

Identity-Aware Session Brokering: Authentication via SAML/LDAP/AD; ephemeral access credentials.

Session Logging & Command Attribution: Real-time SIEM streaming, command logging with session metadata.

Policy-Based Command Enforcement: Allow/block specific commands; detect anomalies.

Multi-Vendor Infrastructure Control: Supports SSH, Telnet, HTTPS, SNMP; agentless; vendor-agnostic.

Framework	Relevant Controls	Kron Network PAM Coverage
NIST 800-53	AC-2, AC-6, AU-2, AU-12	Identity enforcement, least privilege, session audit, log integrity
ISO 27001	A.9.4.1, A.12.4, A.5.15	User accountability, access logging, credential lifecycle control
CIS Controls	5.3, 6.2, 6.6	Secure admin interfaces, enforce MFA/ identity, log session usage
TSA SD 01/02	Access Management, Audit Trail	Validated access only, full traceability, break-glass coverage
PCI DSS 4.0	7.2.5, 10.2.1, 10.2.7	Restrict admin access, log CLI activity, detect unauthorized commands

What Kron Network PAM Doesn’t Do (and Why That’s OK)

While Kron Network PAM secures the identity layer and privileged session control, it does not replicate layer-2 NAC posture assessment or automatic segmentation enforcement. However, in many large-scale infrastructure environments, these features are unnecessary or impractical due to:

- Vendor incompatibility with 802.1X
- Lack of agent support across network gear
- Highly deterministic access policies (e.g., routed backbone environments)
- Instead, Kron Network PAM enforces real-world controls at the exact point of risk — the administrative interface.

FAQs

Q: Is Kron Network PAM a full NAC replacement?

A: No. Kron Network PAM does not handle Layer 2 posture or VLAN segmentation. But for privileged access enforcement, it completely replaces the need for NAC in environments where the primary concern is infrastructure control — not endpoint hygiene.

Q: Can I enforce different levels of access based on job role or region?

A: Yes. Access can be restricted by AD group, authentication method, time-of-day, source IP, and device group with command-level granularity.

Q: How is Kron Network PAM deployed?

A: It's agentless sessions are proxied through PAM nodes with policy enforcement applied before access is granted.

Q: Does Kron Network PAM scale across global networks?

A: Yes. Each node supports thousands of concurrent sessions. It's built for telco-scale with native load balancing and SIEM integrations.

Conclusion

For organizations where privileged access to infrastructure is the real risk not guest WiFi or device posture Kron Network PAM delivers what NAC can't: session-level visibility, real-time enforcement, and auditable identity control at scale.

And it does it for a fraction of the cost.

Schedule a demo or download our integration guide at **networkpam.com**

Kron
TECHNOLOGIES

Security for infrastructure must extend beyond NAC. KronPAM provides the visibility, control, and compliance coverage organizations require.

Schedule a demo or download our deployment blueprint from krontech.com