Whitepaper

Extending Zero Trust to the Network Layer Closing the Identity Gap with Kron Network PAM

networkPAM.com

Executive Summary

Zero Trust is no longer a buzzword it's a foundational security model. While IT environments have adopted identity-based access, multi-factor authentication, and just-in-time privilege models, by not extending these same controls to the network layer, it's become a blind spot and increasingly vulnerable.

Routers, switches, firewalls, load balancers, these core devices still use shared accounts, static credentials, and have minimal if any auditing leaving blind spots.

Those gaps are filled by Kron Network PAM. It brings visibility, identity, and real-time control to your most critical infrastructure without disruption of operations or agents and enables Zero Trust policies to reach all the way across your environment.

The Network Layer: A Blind Spot in Most Zero Trust Strategies

Zero Trust in the typical organization is employed everywhere however network infrastructure seems to have been forgotten.

Network infrastructure is most often the least to be modernized with identity controls if implemented at all. However, routers, switches, and firewalls are among the most critical points of access and most frequently exploited points of attack during breaches. Attackers employ these devices to escalate privilege, slip by detection, and laterally move throughout environments.

High-profile breaches like the Colonial Pipeline and Salt Typhoon highlight the extent to which vulnerable or absent identity controls on network devices create blind spots in security posture. In each of these attacks, attackers bypassed typical perimeter defense and Network Access Controls (NAC) by exploiting shared credentials, static SSH keys, default admin accounts, and absence of session monitoring or strong authentication on network devices.

Salt Typhoon: Insecurely stored and static SSH keys across telecom routers and signaling gateways enabled the attackers to pivot and retrieve subscriber data without triggering NAC or centralized identity controls.

Colonial Pipeline: VPN access to critical systems was protected by a reused password alone and lacked MFA.

These breaches reinforce a critical gap: without identity-aware access controls on network infrastructure, Zero Trust architectures remain incomplete.

Why This Matters

Compromised devices on your network are not only a threat, they're the vehicle they will exploit to move through the environment yet:

- ✓ Identity is rarely enforced at the CLI
- ✓ Shared accounts are still used across critical systems
- ✓ Lack of auditing of who accessed what, when, or why

It's not restricted to those external threats. Insider threat is heightened in Zero Trust designs where infrastructure lacks identity binding and session controls.

Zero Trust maturity is not possible by using the network infrastructure of implicit trust, shared credentials, or invisible privilege escalation.

Kron Network PAM: Enabling Zero Trust for the Network Layer
Impact: Risk, Compliance, and Operational Benefits

Risk Reduction

- ✓ Eliminates lateral movement via shared credentials or out-of-band device access
- ✓ Stops internal misuse and enforces Zero Trust controls at every device session
- ✓ Provides real-time anomaly detection and session termination

Compliance Readiness

- Reports scheduled and mapped to NIST 800-53, ISO 27001, CIS Controls, TSA SDs, and PCI DSS, etc.
- Demonstrable control over privileged access for audit and regulatory response

Operational Efficiency

- No device agents or reconfiguration required
- Reduces staff overhead with automated policy enforcement and centralized auditing
- Accelerates investigations and response time through recorded session data

Kron Network PAM reduces incident response time, audit scope, and operational complexity allowing teams to manage more infrastructure with fewer resources and lower risk.

Benefits/Key Performance Indicators (KPIs) of Extending PAM to Network:

- Reduction in average time to investigate privileged access incidents
- Percentage of network infrastructure with identity-bound access
- Number of shared or static credentials eliminated
- Percentage of privileged sessions with full session recording
- Compliance audit success rate on infrastructure access controls

Bridging the Gap: IT Has It Now Networks Can Too

We have invested heavily in protecting servers, endpoints, and cloud with IAM, PAM, and EDR. Yet infrastructure teams are still managing critical devices with:

- Hardcoded credentials
- TACACS+ logs that lack session visibility
- Manual review processes with no real-time alerting

Kron Network PAM eliminates those blind spots:

- ✓ Vendor-agnostic: Supports Cisco, Fortinet, Juniper, Huawei, Arista, and more
- ✓ Works without change: No impact to routing, switching, or control plane behavior
- ✓ Built for audit: Session logs, access metadata, and behavior alerts go straight to your SIEM

Customer Testimonial

A global cloud and colocation provider with 14+ data centers recognized their NAC logs offered no accountability for CLI access on routers, firewalls, or edge transport.

With Kron Network PAM:

- ✓ SAML + AD required for all CLI and web-based access
- ✓ All sessions were recorded and streamed to the SOC
- ✓ Maintenance access windows were automatically enforced and revoked

The CIO now includes network infrastructure in the company's Zero Trust maturity model, and audit prep time dropped by 60%.

Looking Ahead: Future-Proofing Zero Trust for Infrastructure

As more enterprises shift toward SDN, network automation, and Zero Trust Network Access (ZTNA), Kron Network PAM positions organizations to:

- ✓ Apply identity and policy enforcement even in orchestrated network environments
- ✓ Support compliance as automation replaces human access
- ✓ Integrate with SIEM/SOAR platforms to provide continuous access intelligence

Kron Network PAM isn't just a tactical fix it's a strategic foundation for Zero Trust in the infrastructure era.

Zero Trust doesn't stop at servers. And it can't ignore the network.

Kron Network PAM empowers security leaders to extend identity and access enforcement into the infrastructure layer, reducing risk, simplifying compliance, and ensuring a true Zero Trust architecture from cloud to CLI.

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