

Eliminating Identity Sprawl:

# Palo Alto Networks' Guide to Modernizing Linux IAM



## Why Linux Identity Integration is Needed

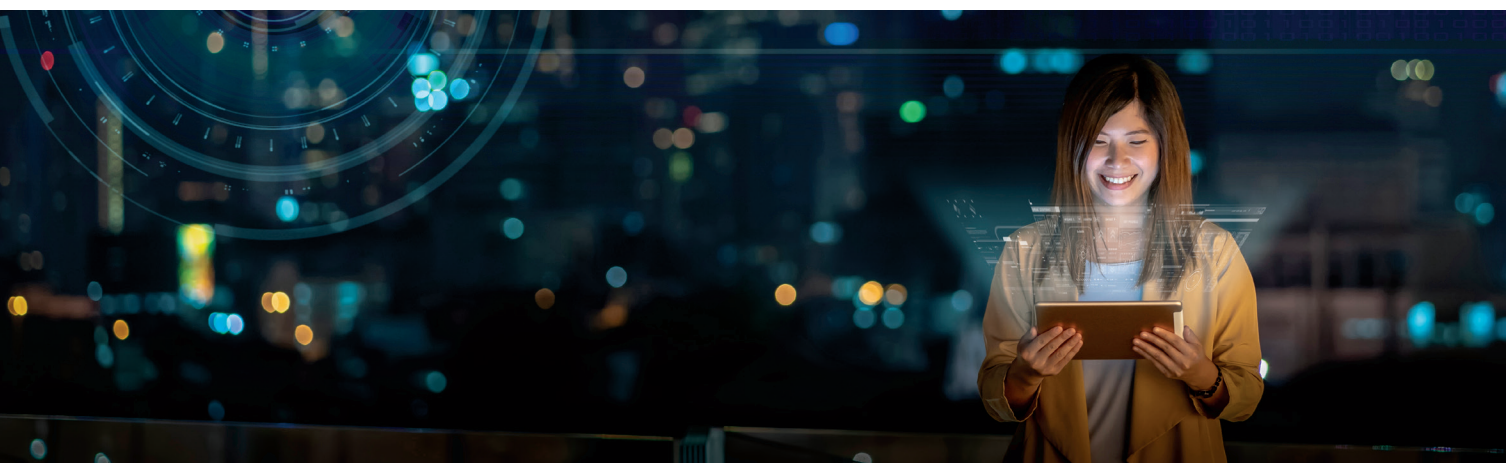
Linux systems are essential to modern IT infrastructures, running critical workloads across on-premises and cloud environments. Today, Linux powers more than 90% of virtual machines in cloud platforms like AWS, Google Cloud and Microsoft Azure, serving as a backbone of hybrid environments.

Yet, unlike other operating systems, which can be natively, centrally managed through modern cloud directories or on-prem directory services, Linux machines often require local and manual management for user accounts.

Since each Linux server, virtual machine or cloud instance cannot natively integrate with the directory, IT teams are forced to either manually manage user accounts — creating, updating and de-provisioning them locally — or automate what remains a decentralized process. Such an approach increases administrative burdens, but more importantly, it breeds new identities and generates complexity and security risks. These challenges grow exponentially as organizations scale, resulting in fragmented identities, orphaned accounts and inconsistent policies across hundreds or thousands of servers.

Without a centralized way to integrate Linux systems into Identity and Access Management (IAM) frameworks, IT teams face challenges such as:

- **Identity and privilege sprawl on Linux machines** — due to the lack of native capabilities for central management of user identities, authentication, and authorization. Every Linux machine would have a separate local account for the user, creating identity sprawl.
- **Stalled strategic IAM modernization programs** — such as Unified Identity Governance and Administration, Federated Identity Management (decentralization of identities), Security-First Identity, Identity Fabric, Zero Trust and others.
- **Weak, legacy authentication methods in corporate Linux environments significantly lower an organization's security posture** — such outdated methods often lack robust encryption and multi-factor authentication, which are essential for protecting sensitive data. As a result, they create numerous entry points for attackers, increasing the risk of data breaches.





## Addressing Identity and Privilege Sprawl on Linux

Key contributors to identity and privilege sprawl include:

- **Local account multiplication.** Each Linux machine operates as a silo, requiring separate local accounts. As users gain access to multiple machines, their identities multiply across the environment, creating management inefficiencies and inconsistencies.
- **Orphaned accounts.** When employees leave or change roles, their local accounts are often overlooked during de-provisioning, leaving behind active credentials that attackers can exploit.
- **Privilege sprawl.** Admins are often assigned blanket elevated privileges to avoid managing individual access policies. This, together with the sprawl of identities, expands the attack surface and exposes critical systems to breach risks.
- **Operational bottlenecks.** IT teams are forced to manually provision, update and remove accounts on each Linux machine. Even with automation, the process is time-consuming and error-prone and diverts resources away from strategic initiatives.
- **Compliance complexity.** Audit and compliance requirements demand clear visibility into who accessed which systems and when. Without centralized logs and consistent access controls, proving compliance with frameworks like NIST CSF, ISO 27001, E.O. 14028 and regulations becomes a significant challenge.

**Lack of native Linux capabilities for centralized management of user identities, authentication and authorization leads to identity and privilege sprawl on Linux machines, opening doors for potential breaches. Linux is exceptional, but it shouldn't be an exception.**

— Brandon Traffanstedt, Sr. Director, Field Technology Office, Palo Alto Networks

## Keys to Simplifying Identity Management

To address fragmented Linux account management in many organizations today, CISOs need to adopt solutions that unify access control across on-premises, cloud-native and hybrid environments. Key components of this approach include:

- 1. Identity federation and directory-agnostic integration** — to seamlessly connect Linux servers, VMs and cloud workloads with Active Directory (AD) as well as modern, cloud-based directories and Identity Providers (IdPs). This enables organizations to integrate Linux systems even with most complex Identity and Access Management (IAM) setups.
- 2. Centralized policy enforcement** — to enforce consistent access policies across all systems. With role-based access control (RBAC) and enforcement of least privilege, organizations can define access policies once and apply them universally to on-premises, cloud and hybrid Linux environments. This reduces administrative complexity and minimizes the risk of over-provisioned access.
- 3. Modern authentication support** — to enhance security with features like phishing-resistant multi-factor authentication (MFA) for server sign-ins and step-up authentication to help ensure only verified users gain access. These capabilities mitigate risks associated with stolen

credentials, complicating unauthorized initial access to critical systems and lateral movement.

**4. Auditability across Linux systems** — a centralized audit trail provides a single, unified view of user authentication, with each user represented by the same centralized account across the entire Linux estate. This simplifies log analysis and correlation across systems, boost visibility and improves detection and response times.

**5. Streamlined compliance readiness** — using centralized accounts across all Linux servers, VMs and cloud workloads simplifies compliance with frameworks such as NIST CSF, ISO 27001, E.O. 14028 and others. Automated reporting capabilities eliminate the manual effort of preparing compliance evidence, ensuring organizations can respond to audits and regulatory requirements more efficiently.

## Overcoming Identity and Privilege Sprawl

Within Idera Endpoint Privilege Manager, Identity Bridge was designed to help resolve challenges by integrating Linux machines with centralized, modern — or any — directories and IdPs for authentication, access and authorization management. With Idera EPM, IT teams gain the ability to:

- Simplify account management by eliminating the need for separate local accounts on each Linux machine by enabling users to log in with a single, centralized account stored in a directory or IdP.
- Reduce administrative complexity by automating and centralizing identity management processes, freeing IT teams from manual account provisioning and de-provisioning tasks across multiple machines.
- Enhance security oversight by enforcing consistent privileged access policies and least privilege principles through centralized integration, reducing risk and strengthening compliance without directly managing Linux accounts.

By integrating Linux machines into existing IAM systems, Identity Bridge reduces identity sprawl, simplifies access control and strengthens overall security without directly managing Linux or cloud accounts.



## Real-World Benefits of Centralized Linux Identity Management

Unlike alternatives that require machines to be domain-joined, Identity Bridge offers a truly directory-agnostic approach that includes:

- **Simplified integration** — ensures compatibility with both modern and legacy directories and IdPs without the operational overhead often associated with traditional directory-based solutions.
- **Rapid deployment** — enabling immediate integration by helping teams to centralize access within hours, not weeks. This contrasts with other solutions that require extensive prerequisites and slower deployment processes, ensuring IT teams can deliver value quickly.
- **By integrating with Idira Secure Infrastructure Access capabilities, Identity Bridge also enhances Privileged Access Management (PAM) integration for Linux** — by enabling Just-in-Time (JIT) access, Zero Standing Privileges (ZSP) and simplified session management. For Idira PAM customers, this integration further streamlines privileged access workflows by extending centralized access to Linux systems.

## How Idira Endpoint Privilege Manager Stands Out

Palo Alto Networks differentiates itself with a modern AD Bridging solution supporting cloud directories, called Identity Bridge, to help simplify access and least privilege management for critical IT infrastructure assets. With innovative capabilities, Palo Alto Networks addresses the evolving needs of hybrid and multi-cloud environments, including:

- **Unified Identity Integration across Linux systems** — Identity Bridge integrates Linux machines directly with centralized IAM frameworks, removing the need for local accounts. This approach enables organizations to enforce consistent access controls, reduce identity sprawl and simplify identity management at scale.
- **Zero Trust alignment** — By centralizing access controls and boosting visibility, Identity Bridge supports Zero Trust principles. Organizations can enforce least privilege policies, monitor user activity and reduce attack surfaces across hybrid IT infrastructures.
- **Scalable flexibility** — Identity Bridge is directory-agnostic, integrating seamlessly with cloud-based IdPs and on-premises systems. This flexibility ensures compatibility with existing IAM solutions while supporting long-term digital transformation goals.
- **Streamlined Security and Auditability** — By ensuring consistency of user access and action attribution through centralized accounts, IT teams can quickly identify anomalies, track access patterns and generate compliance reports. These streamlined processes reduce the manual workload on IT teams and improve overall security readiness.





- **Enhancing Idira PAM deployments** — For existing Idira PAM customers, Identity Bridge enhances privileged access workflows by extending centralized access to Linux systems. This integration simplifies Just-in-Time (JIT) access, Zero Standing Privileges (ZSP) and session recording, ensuring Linux systems benefit from the full range of Idira’s PAM capabilities.

As part of Idira Endpoint Privilege Manager, Identity Bridge empowers organizations to centralize visibility into identity activities, access logs and compliance reporting — all from a single platform.

This contributes to Zero Trust goals by:

- Enforcing strict access controls across Linux environments;
- Tying access to verified identities stored in directories or IdPs, eliminating the need for local accounts;
- Providing real-time insights into who accessed which system, when, and how.

By integrating Linux systems directly into IAM frameworks, Identity Bridge enables consistent policy enforcement and reduces the attack surface. Its support for phishing-resistant MFA ensures that even if credentials are compromised, unauthorized access is prevented.



**We simplify administration. Alternatives often require extensive prerequisites and domain joins. But more importantly, scaling what works on one Linux machine to cover the entire Linux estate in a complex enterprise IT infrastructure can be very challenging. Idira EPM makes it simple — it’s just a few clicks to get things started and it’s the same management console that helps manage least privilege policies. Easy.**

— Andrey Pozhogin, Director of Product Marketing, Palo Alto Networks



## Next Steps to Simplify Linux Identity Management

Controlling access in an environment filled with identity sprawl is a difficult challenge. Attackers know every orphaned account and over-privileged user offers a clear path to breach critical systems. Ensuring all users are accounted for and that only the right people have access at the right time, is essential to securing modern enterprises and achieving Zero Trust implementation goals.

By reducing identity sprawl and integrating Linux systems into a unified identity framework, Identity Bridge enables organizations to maintain robust Zero Trust security postures across hybrid IT environments.

CISOs face mounting pressure to simplify identity management across complex Linux and hybrid environments. Using fewer, smarter tools that centralize access and simplify identity management delivers a clear step forward. Palo Alto Networks' Identity Bridge unites Linux, cloud and hybrid identity systems under one roof. By enabling directory-agnostic integration, enforcing centralized access controls and supporting modern authentication methods, Palo Alto Networks empowers organizations to make strategic progress in their Zero Trust journey.

Ready to modernize your identity strategy? Take the next step toward unified identity management. Discover how Idira EPM empowers your organization to streamline Linux access and strengthen Zero Trust security. [Request a personalized demo today.](#)

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

























